2018-01-19

Computing Isogeny Volcanoes of Rank Two Drinfeld Modules

Caranay, Perlas

UNIVERSITY OF CALGARY

Computing Isogeny Volcanoes of Rank Two Drinfeld Modules

by

Perlas Caranay

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF DOCTOR OF PHILOSOPHY

GRADUATE PROGRAM IN MATHEMATICS AND STATISTICS

CALGARY, ALBERTA

January, 2018

Abstract

Elliptic curves have long been widely studied mathematical objects. They do not only feature prominently in established areas of mathematics such as number theory, algebraic geometry, and topology, but have recently gained practical importance due to applications in coding theory and cryptography. More recently, Drinfeld modules have received increased attention due to their surprising similarity to elliptic curves - objects to which they bear little superficial resemblance. However, little is yet known about real-world applications of Drinfeld modules.

Elliptic curves come in two kinds – ordinary and supersingular. Endomorphism rings of ordinary and supersingular elliptic curves, made up of isogenies, are very different. An analogous dichotomy holds for Drinfeld modules. Recently, major progress has been achieved by researchers in explicitly computing endomorphism rings of elliptic curves using isogeny volcanoes, but very little if anything of this kind has yet been done for Drinfeld modules.

Our aim here is to study the theoretical and computational aspects of isogeny volcanoes of rank two Drinfeld modules defined over finite fields and determine how to explicitly compute these mathematical structures. We establish theoretical properties of isogeny volcanoes in the Drinfeld module case. Then we design, analyze, and implement algorithms for computing (1) j-invariants and Drinfeld modular polynomials, (2) isogeny volcanoes, and (3) endomorphism rings and explicit isogenies of rank two Drinfeld modules.

Acknowledgements

I would like to express my deepest gratitude to the people who played a great part in the completion of this thesis. I am greatly indebted to my supervisors, Dr. Matthew Greenberg and Dr. Renate Scheidler. Thank you for guiding me through this endeavor. Without your guidance and expertise, I would not be able to complete this difficult task. Thank you for being patient with me during our meetings and for answering all my questions. I greatly appreciate the moral and financial support you extended to me. Thank you for introducing me to Drinfeld modules.

Thank you to Dr. Hugh Williams for giving me financial support. This support helped me in my studies. Thanks for all your help and guidance during my early years here in the university.

I would like to thank Dr. Imin Chen, Dr. Vassil Dimitrov, Dr. Kristine Bauer, and Dr. Mark Bauer who agreed to serve on my examination committee. Thank you for giving me your comments and insightful ideas for the improvement of this thesis.

I would also like to thank Dr. Sarah Chisholm for helping me when I was starting my graduate studies here at the Univerity of Calgary. I am also indebted to Dr. Dustin Moody for giving me some guidance and resources related elliptic curve computations, especially some SAGE material.

Thanks to my friends and family for understanding my shortcomings and for encouraging me through difficult times. I would like to thank Erwin for all the sacrifices he made so that I can focus on my thesis. Thank you for your support and understanding. Finally, thanks to my wonderful sons, David and Daniel, for providing me joy and necessary diversion during the preparation of this thesis. Thank you for being my inspiration.

Table of Contents

List of Tables

List of Figures and Illustrations

List of Symbols, Abbreviations and Nomenclature

Symbol	Definition/Description
$\mathbb{N}, \mathbb{Z}$	Set of natural numbers, ring of integers
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$	Fields of rational numbers, real numbers, and complex numbers
p	A prime in $\mathbb{Z}$
q	A power of p
$\mathbb{F}_q$	Finite field with q elements
$\#S$	number of elements of a set S
$[G : H]$	Index of H in G; degree of an extension G/H
$\ker m$	Kernel of a function/map m
$\mathrm{Gal}(K/F)$	Galois group of some field extension K/F
$\overline{K}$	Algebraic closure of a field K
$\mathfrak{a}, \mathfrak{b}, \mathfrak{f}$	Ideals in a ring
$\mathfrak{a}^{-1}, \overline{\mathfrak{a}}$	Inverse of $\mathfrak{a}$, conjugate ideal of $\mathfrak{a}$
$\mathfrak{l}, \mathfrak{p}, \mathfrak{q}, \mathfrak{P}$	Prime ideals in a ring
$\gcd(a, b)$	Greatest common divisor of a and b
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$a^n \parallel b$	a^n exactly divides $b; a^n \mid b$, but $a^{n+1} \nmid b$, for an integer $n \geq 1$
FFT	Fast Fourier Transform algorithm
$\square$	End of proof

Elliptic Curves

Symbol	Definition/Description
K	An arbitrary field

$E, E/K$	Elliptic curve, elliptic curve E defined over the field K
O	A point at infinity
$E(K)$	Set of K-rational points on the elliptic curve E/K
$K(E)$	Function field of E/K
Δ	Discriminant of the Weierstrass equation of E/K
$j, j(E)$	j-invariant of E/K
ϕ, ψ, λ	Isogenies of elliptic curves
$\widehat{\phi}$	Dual isogeny of ϕ
$[m]$	Multiplication-by-m map
$E[m]$	m-torsion subgroup of E/K
π	Frobenius isogeny of $E/\mathbb{F}_q$
ℓ	A prime in $\mathbb{Z}$
$T_\ell(E)$	(ℓ-adic) Tate module associated to E/K
$\mathrm{End}(E)$	Endomorphism ring of E
t	Trace of Frobenius
Λ	Lattice in $\mathbb{C}$
$\mathbb{C}/\Lambda$	Complex torus
$\wp(z)$	Weierstrass $\wp$-function
$j(\Lambda), j(\mathfrak{a})$	j-invariant of a lattice Λ, j-invariant of an $\mathcal{O}$-ideal $\mathfrak{a}$
$\mathcal{O}$	Order in an imaginary quadratic field
Γ	Modular group $SL_2(\mathbb{Z})$
$\mathcal{H}$	Complex upper half plane
$G_{2k}(\Lambda)$	Eisenstein series for Λ of weight $2k$ with $k \in \mathbb{N}$
$\zeta(s)$	Riemann zeta function
$\sigma_k(n)$	Sum of divisors function for $n \in \mathbb{Z}$
$\Phi_n(X, Y)$	Modular polynomial of order n for $n \in \mathbb{Z}$

$\mathcal{O}_K$	Maximal order of an imaginary quadratic field K
$\mathcal{O}_E$	Endomorphism order; endomorphism ring of E
$\mathbb{Z}[\pi]$	Frobenius order
D_K, D_E, D_π	Discriminants of $\mathcal{O}_K$ (or K), $\mathcal{O}_E$, and $\mathbb{Z}[\pi]$, respectively
f_π, f_E	Conductors of the orders $\mathbb{Z}[\pi]$ and $\mathcal{O}_E$, respectively
$\left(\frac{\cdot}{\cdot}\right)$	Kronecker symbol; quadratic residue symbol
$G_\ell(\mathbb{F}_q)$	ℓ-isogeny graph of elliptic curves over $\mathbb{F}_q$
(G, C)	An isogeny volcano G with crater C
$\mathcal{N}_\ell(E)$	Number of roots of $\Phi_\ell(j(E), Y)$ over $\mathbb{F}_q$

Function Fields and Drinfeld Modules

Symbol	**Definition/Description**
$\mathbf{A}$	$\mathbb{F}_q[T]$; ring of polynomials in one indeterminate T over $\mathbb{F}_q$
$\operatorname{sgn}(a)$	Leading coefficient of $a \in \mathbf{A}$
$\deg_T(a)$	Degree of a as a polynomial in T, with $a \in \mathbf{A}$
$\lvert a \rvert$	$q^{\deg_T(a)}$; absolute value of $a \in \mathbf{A}$
$\mathbf{A}^*$	$\mathbb{F}_q^*$; group of units of $\mathbf{A}$
$\mathbf{A}/a\mathbf{A}$	Residue class ring of $\mathbf{A}$ modulo a, for $a \in \mathbf{A}$
$\left(\frac{\cdot}{\cdot}\right)_d, \left(\frac{\cdot}{\cdot}\right)$	d-th power residue symbol and quadratic residue symbol in $\mathbf{A}$
$\mathbf{K}$	$\mathbb{F}_q(T)$; field of fractions of $\mathbf{A}$; function field of one variable
ℓ, P, Q	Monic irreducible polynomials in $\mathbf{A}$
$\mathbf{A}_P$	Localization of $\mathbf{A}$ at P
∞	$1/T$; prime at infinity
$\mathcal{K}$	A quadratic function field extension of $\mathbf{K}$
$N(\alpha)$	Norm of $\alpha \in \mathcal{K}$
$\mathcal{O}_\mathcal{K}$	Integral closure of $\mathbf{A}$ in $\mathcal{K}$; maximal order in $\mathcal{K}$

$\mathcal{O}$	An order in $\mathcal{K}$
$\mathcal{O}_{\mathcal{K}}^*, \mathcal{O}^*$	Set of units of $\mathcal{O}_{\mathcal{K}}$, set of units in $\mathcal{O}$
$\mathcal{I}(\mathcal{O})$	Multiplicative group of proper $\mathcal{O}$-ideals
$\mathcal{P}(\mathcal{O})$	Subgroup of principal $\mathcal{O}$-ideals in $\mathcal{I}(\mathcal{O})$
$\mathcal{C}l(\mathcal{O})$	Class group of $\mathcal{O}$
f	Conductor of an order $\mathcal{O}$
$\mathcal{I}(\mathcal{O}, f)$	Set of proper $\mathcal{O}$-ideals prime to f
$\mathcal{P}(\mathcal{O}, f)$	Set of principal $\mathcal{O}$-ideals prime to f
$h(\mathcal{O}), \mathbf{H}(\mathcal{O})$	Class number of $\mathcal{O}$, Hurwitz class number of $\mathcal{O}$
$\chi_{\mathcal{K}}(*)$	Kronecker symbol associated with $\mathcal{K}$
$h(\mathcal{K})$	Number of divisor classes of degree zero of $\mathcal{K}$
$\mathbb{L}, \mathbb{L}^*$	A field containing $\mathbb{F}_q$, set of units in $\mathbb{L}$
$\mathbb{L}[x]$	Ring of polynomials with coefficients in $\mathbb{L}$
$\mathcal{A}(\mathbb{L})$	Set of additive polynomials with coefficients in $\mathbb{L}$
τ	q-th power map, with $q = p^s$ for an integer $s \geq 1$
$\mathbb{L}\{\tau\}$	Ring of polynomials in τ with commutation rule $\tau\alpha = \alpha^q\tau$, $\alpha \in \mathbb{L}$
$\deg_\tau(m)$	Degree of m as a polynomial in τ, with $m(\tau) \in \mathbb{L}\{\tau\}$
$\mathrm{rgcd}(f(\tau), g(\tau))$	Right greatest common divisor of $f(\tau), g(\tau) \in \mathbb{L}\{\tau\}$
$\mathrm{rlcm}(f(\tau), g(\tau))$	Right least common multiple of $f(\tau), g(\tau) \in \mathbb{L}\{\tau\}$
ν_∞	Valuation associated to $\infty = 1/T$
$\mathbf{K}_\infty$	$\mathbb{F}_q((1/T))$; the completion of $\mathbf{K}$ with respect to ν_∞
$\overline{\mathbf{K}}_\infty$	A fixed algebraic closure of $\mathbf{K}_\infty$
$\mathbf{C}$	Completion of $\overline{\mathbf{K}}_\infty$ from the canonical extension of ν_∞ to $\overline{\mathbf{K}}_\infty$
γ	A structure map from $\mathbf{A}$ to $\mathbb{L}$
$\mathfrak{p}$	$\mathrm{char}_{\mathbf{A}}(\mathbb{L})$; $\mathbf{A}$-characteristic of $\mathbb{L}$
φ, ψ	Drinfeld $\mathbf{A}$-modules mapping $\mathbf{A}$ to $\mathbb{L}\{\tau\}$

φ_a	Image of $a \in \mathbf{A}$ under φ
$\gamma(a)$	Constant term of φ_a; image of a under γ
ρ	Carlitz module determined by $\rho_T = T + \tau$
$\varphi[a]$	Set of a-torsion points of φ; set of roots of $\varphi_a(x)$ in $\overline{\mathbb{L}}$
r	Rank of a Drinfeld module over $\mathbb{L}$
$\nu_{\mathfrak{p}}$	Normalized valuation associated to $\mathfrak{p}$
$\mathrm{Hom}_{\mathbb{L}}(\varphi, \psi)$	Set of all morphisms from φ to ψ over $\mathbb{L}$
$\mathrm{End}_{\mathbb{L}}(\varphi)$	Endomorphism ring of φ over $\mathbb{L}$
u	An isogeny from φ to ψ
$\widehat{u}$	Dual isogeny to u from ψ to φ
$\mathbf{A}^+$	Set of monic polynomials in $\mathbf{A}$
Λ	An $\mathbf{A}$-lattice in $\mathbf{C}$
$\mathrm{Hom}(\Lambda_1, \Lambda_2)$	Set of all morphisms from Λ_1 to Λ_2
$\mathrm{End}(\Lambda)$	Endomorphism ring of Λ
$e_\Lambda(z)$	Exponential function on $\mathbf{C}$ associated to Λ
φ^Λ	Drinfeld module over $\mathbf{C}$ associated to the $\mathbf{A}$-lattice Λ
φ_a^Λ	Image of $a \in \mathbf{A}$, $a \neq 0$, under φ^Λ
$\mathbf{C}\{\{\tau\}\}$	Ring of (left) twisted power series generated by τ over $\mathbf{C}$
$L_{\mathbf{A}}(\mathbf{C}), D_{\mathbf{A}}(\mathbf{C})$	Set of $\mathbf{A}$-lattices in $\mathbf{C}$, set of Drinfeld $\mathbf{A}$-modules over $\mathbf{C}$
$\log_\Lambda(z)$	Composition inverse for $e_\Lambda(z)$
$E_k(\Lambda)$	Eisenstein series of weight k for Λ
$[k]$	$T^{q^k} - T \in \mathbf{A}$; the product of monic primes in $\mathbf{A}$ of degree dividing k
F_k	Product of all monic polynomials in $\mathbf{A}$ of degree k
ρ_a	Image of $a \in \mathbf{A}$ under the Carlitz module ρ
β_i	Coefficients of ρ_a for $i = 0, 2, \ldots, \deg_T(a)$
$\gamma(T), g, \Delta$	Coefficients of a rank two Drinfeld module φ

$j, j(\varphi)$	j-invariant of a Drinfeld module φ
Ω	Drinfeld upper half plane
Γ	General linear group $\mathrm{GL}_2(\mathbf{A})$
$t, t(z)$	Uniformizer for Laurent series expansions of Drinfeld modular forms
t_a	$t(az)$ for nonzero $a \in \mathbf{A}$
$f_a(X)$	a-th inverse cyclotomic polynomial
s	t^{q-1}
$g(z), \Delta(z)$	Modular forms for $\mathrm{GL}_2(\mathbf{A})$
$j(z)$	Modular function for the j-invariant
n	A monic polynomial in $\mathbf{A}$
S_{n}	Γ-coset representatives of primitive $\alpha \in M_2(\mathbf{A})$, $\det(\alpha) = \mu\mathsf{n}$, $\mu \in \mathbb{F}_q^*$
$\Phi_{\mathsf{n}}(X, Y)$	Drinfeld modular polynomial for j
$\mathbf{A}((t))$	Ring of formal Laurent series in t with coefficients in $\mathbf{A}$
$\mathbf{A}[t]$	Ring of power series in t with coefficients in $\mathbf{A}$
(g, Δ)	A rank two Drinfeld module determined by $\varphi_T = \gamma(T) + g\tau + \Delta\tau^2$
$\deg_{isog}(u)$	Degree of an isogeny u of Drinfeld modules
e_a	A pairing for rank two Drinfeld modules
F	Frobenius endomorphism associated to a rank two Drinfeld module φ
$\varphi[\mathfrak{a}]$	$\mathfrak{a}$-torsion points of an ideal $\mathfrak{a} \subset \mathbf{A}$
$T_{\mathfrak{l}}(\varphi)$	$\mathfrak{l}$-adic Tate module of φ for a prime ideal $\mathfrak{l} \subset \mathbf{A}$, $(0) \neq \mathfrak{l}$
$P_\varphi(X), P_{a,b}$	Characteristic polynomial of the Frobenius endomorphism F of φ
$M_\varphi(X)$	Minimal polynomial of the Frobenius endomorphism F of φ
$a(\varphi), b(\varphi)$	Trace and norm of the Frobenius endomorphism F of φ
$\mathbb{F}_{\mathfrak{p}}$	$\mathbf{A}/\mathfrak{p}$; a residue field
$H(\varphi)$	Hasse invariant of φ
π	A Weil number of rank two

$\mathrm{Aut}_{\mathbb{L}}(\varphi)$	Automorphism group of φ over $\mathbb{L}$
$\mathcal{L}, \mathcal{O}_{\mathcal{L}}$	A finite extension of $\mathbf{K}$, maximal order of $\mathcal{L}$
$\overline{\varphi}$	Reduction of φ at some nonzero prime $\mathcal{O}_{\mathcal{L}}$-ideal
$\mathcal{O}_{\varphi}$	Endomorphism order of φ in $\mathcal{K}$
$\mathcal{DM}(\mathcal{O}_{\varphi})$	Isomorphism class of Drinfeld modules ψ over $\mathbf{C}$ with $\mathrm{End}(\psi) \simeq \mathcal{O}_{\varphi}$
$\mathfrak{a} * \varphi^{\Lambda}$	Action of $\mathcal{C}l(\mathcal{O}_{\varphi})$ on $\mathcal{DM}(\mathcal{O}_{\varphi})$
$\varphi/\mathbb{F}_{\mathfrak{p}}, \psi/\mathbb{F}_{\mathfrak{p}}$	Rank two Drinfeld modules defined over $\mathbb{F}_{\mathfrak{p}}$
$\mathbf{A}[F]$	Frobenius order in $\mathcal{K}$
$D_{\mathcal{K}}, D_F, D_{\varphi}$	Discriminants of $\mathcal{O}_{\mathcal{K}}$, $\mathbf{A}[F]$ and $\mathcal{O}_{\varphi}$, respectively
f_F, f_{φ}	Conductors of $\mathbf{A}[F]$ and $\mathcal{O}_{\varphi}$, respectively
$G_{\ell}(\mathbb{F}_{\mathfrak{p}})$	An ℓ-isogeny graph of rank two Drinfeld modules
$j_{a,b}(\mathbb{F}_{\mathfrak{p}})$	Set of $\overline{\mathbb{F}}_{\mathfrak{p}}$-isomorphism classes of Drinfeld modules $\varphi/\mathbb{F}_{\mathfrak{p}}$ with characteristic polynomial $P_{a,b}$
ν_{ℓ}	ℓ-adic valuation on $\mathbf{A}$
G	An ℓ-isogeny volcano
$\mathcal{N}_{\ell}(\varphi)$	Number of roots of $\Phi_{\ell}(j(\varphi), Y)$
$\mathbf{A}[[s]]$	Ring of formal power series in s with coefficients in $\mathbf{A}$
$\mathbf{A}_m^+$	Set of monic polynomials in $\mathbf{A}$ of degree m
$\mathbf{A}_{\leq m}^+$	Set of monic polynomials in $\mathbf{A}$ of degree at most m
$\mathcal{R}$	A generic coefficient ring
$M(n)$	Number of $\mathcal{R}$-operations to multiply two degree n polynomials over $\mathcal{R}$
$R(n)$	Number of operations to find all roots in $\mathcal{R}$ of a polynomial of degree n over $\mathcal{R}$
$O(*)$	Asymptotic complexity
N_g, N_{Δ}, N	Precisions for the s-expansions of g, Δ, and j, respectively
$w_{\mu,\nu}$	Coefficients of $\Phi_{\ell}(X, Y)$ with $0 \leq \mu \leq \lvert\ell\rvert$ and $0 \leq \nu \leq \mu$

Chapter 1

Introduction

1.1 Historical Background

A prominent area of research in number theory is the study of analogies between number fields and function fields. *Elliptic curves* and *Drinfeld modules* play a fundamental role in making these analogies possible.

Elliptic curves are objects that constitute a beautiful and deep area of research in mathematics. They have been and still are being studied for their theoretical and algorithmic properties as well as their applications in the real world. These objects come up prominently in different established areas of mathematics such as number theory, algebraic geometry, and topology, and in more applied areas like coding theory and cryptography. In recent years, they have gained importance in security and authenticity infrastructures for mobile computing, wireless communications, and the Internet.

Elliptic curves come in two classes – *ordinary* and *supersingular*. This distinction manifests in an algebraic structure called the *endomorphism ring* (see Section 2.2) associated to an elliptic curve. Structurally, endomorphism rings of ordinary and supersingular elliptic curves are very different. Endomorphism rings are comprised of *isogenies* of elliptic curves, morphisms of algebraic curves that preserve a distinguished rational point. The study of the computational aspects of these structures has received considerable attention in the last two decades or so, and it is still a very active area of research. Major progress pertaining to these mathematical objects has already been achieved by researchers.

In his PhD thesis [Koh96] in 1996, D. Kohel introduced a result that paved the way to the classification of *n-isogenies* (see Definition 2.1.6) of ordinary elliptic curves. Through this result, he was able to develop an algorithm that computes endomorphism rings of el-

liptic curves over finite fields. Using Kohel's classification method, one can determine the relationship between the endomorphism rings of two n-isogenous elliptic curves. The set of elliptic curves belonging to the same *n-isogeny class* (see Definition 2.1.5) can be represented using an *isogeny graph*. Kohel's theorem shows that each component of an isogeny graph has a particular shape. M. Fouquet, who further studied isogeny graphs in [Fou01], aptly called this shape a *volcano*. Fouquet used *isogeny volcanoes* (see Definition 2.4.11) for point counting on elliptic curves. See also [FM02]. Isogeny volcanoes can also be used to identify supersingular elliptic curves or to compute Hilbert class polynomials and modular polynomials, see [Sut13] for an exposition.

One important tool in studying isogenies of elliptic curves is the *classical modular polynomial* $\Phi_n \in \mathbb{Z}[X, Y]$ (see Section 2.3.3). It parametrizes pairs of elliptic curves over $\mathbb{C}$ related by a cyclic n-isogeny. If n is prime, then an n-isogeny is always cyclic and for two elliptic curves E_1 and E_2 over $\mathbb{C}$ with j-invariants (see Definition 2.1.2)) $j(E_1)$ and $j(E_2)$, respectively,

$$\Phi_n(j(E_1), j(E_2)) = 0$$

if and only if E_1 and E_2 are n-isogenous. Classical modular polynomials are hard to compute since their coefficients tend to get large as n increases. However, substantial progress is being made toward efficient computation of such polynomials. See, for example, [BCRS99], [BLS12], and [CL04] for some developments on computing modular polynomials in the elliptic curve case.

In the function field case, there is an object that has features analogous to those of an elliptic curve in the number field case. In the late 1970s, V. Drinfeld introduced the concept of elliptic modules in his proof of the Langlands conjecture for the general linear group GL(2) over function fields, see [Dri74]. Elliptic modules are now known as Drinfeld modules (see Section 4.2). These mathematical objects became an important tool in exploring arithmetic properties of function fields. This is evident, for example, in the works of D. Goss [Gos78,

Gos80a, Gos80b], E.-U. Gekeler [Gek83, Gek85, Gek86, Gek88, Gek91, Gek08], and D. Hayes [Hay79], to name a few.

One particular reason why Drinfeld modules received much attention is due to their surprising theoretical similarity to elliptic curves. Drinfeld modules take on every *rank* r, where r is a positive integer. Their similarities to elliptic curves are much more striking in the rank two case. Drinfeld modules have j-invariants, just like elliptic curves, which can be used to classify them up to isomorphism. They have isogenies, and they can be grouped into isogeny classes. See Section 6.1. Drinfeld modules also have endomorphism rings (see Section 6.2). Based on the structure of their endomorphism rings, they can also be classified as ordinary or supersingular, see Definition 6.3.13. As in the case of elliptic curves, pairs of *ℓ-isogenous* Drinfeld modules are parametrized by modular polynomials which we refer to as *Drinfeld modular polynomials* to distinguish them from the elliptic modular polynomials (see Section 5.5). Algorithms for computing these polynomials are given in [BL97] and [Sch95] for rank two Drinfeld modules. A treatment of Drinfeld modular polynomials for higher ranks is given in [BR09]. More analogies between Drinfeld modules and elliptic curves will be presented in the succeeding chapters.

1.2 A Brief Description of the Thesis

This thesis is geared toward the algorithmic aspects of Drinfeld modules and is motivated by computational developments in the study of elliptic curves over finite fields, especially those results pertaining to the computation of their isogeny volcanoes and endomorphism rings. Due to the established similarities between elliptic curves and Drinfeld modules, at least from the theoretical point of view, it is of interest to develop algorithms for computing isogeny volcanoes and endomorphism rings of Drinfeld modules defined over finite fields. We focus on the rank two case since this is where the similarity to elliptic curves is most evident. It is our hope that the algorithmic results we present here will lead to new constructions,

a better understanding of not only these objects but possibly elliptic curves as well, and potential applications in related areas of mathematics.

We have four main goals in this research. Our first goal is to establish properties of isogeny volcanoes for rank two Drinfeld modules. In order to achieve this goal, we use the parametrization of orders in quadratic function fields by their conductors to establish a result analogous to Kohel's theorem which allows the classification of isogenies of Drinfeld modules. We use this parametrization theorem, together with properties of isogeny classes of Drinfeld modules and roots of Drinfeld modular polynomials, to fully describe the structure of isogeny volcanoes in the Drinfeld module case. Our second goal is to design an algorithm to compute isogeny volcanoes of rank two Drinfeld modules using roots of Drinfeld modular polynomials. Our third goal is to compute Drinfeld modular polynomials. These polynomials play a major part in our subsequent computation of isogeny volcanoes. Here, we transform the method of computing these polynomials given [BL97] into an algorithmic form. Note that Drinfeld modular polynomials are obtained from the Laurent series of j-invariants, so we also give an algorithm for computing Laurent series (up to a certain precision) of j-invariants of rank two Drinfeld modules. The computation of the Laurent series for the j-invariant is quite difficult due to the coefficients of the modular forms involved. As far as the author knows, there are no published results regarding algorithms along these lines in the Drinfeld module case. Finally, our fourth goal is to compute endomorphism rings and explicit isogenies of rank two Drinfeld modules over finite fields. We give an algorithm for computing endomorphism rings of Drinfeld modules using properties of isogeny volcanoes and the structure of imaginary quadratic function fields. As for computing explicit isogenies of Drinfeld modules, we design an algorithm based on basic properties of isogenies of Drinfeld modules. We include a complexity analysis for each of the algorithms presented here. We implemented all these algorithms using SAGE ([S$^+$17]). A summary of our major results in the thesis is given in Table 1.1.

Chapter	**Results**
Chapter 6	Proposition 6.1.6
Chapter 7	Theorem 7.1.5, rest of Section 7.2
Chapter 8	Algorithms 8.2.11, 8.3.2, 8.4.1, 8.5.1,8.5.4,8.5.7; Theorems 8.2.12, 8.3.3, 8.4.3, 8.5.2, 8.5.8

Table 1.1: Major results in the thesis

To the best of our knowledge, this research regarding algorithms for computing isogeny volcanoes and endomorphism rings of rank two Drinfeld modules over finite fields is the first foray into computational aspects of Drinfeld modules and explicit computation of their associated isogeny graphs. Although the theoretical aspects of Drinfeld modules already received much attention in previous years, their algorithmic aspects had yet to be tapped prior to the work herein.

There are very few examples of Drinfeld modular polynomials $\Phi_\ell(X, Y)$ in the literature, and these are all for irreducible polynomials ℓ of degree 1. Our method provably generalizes to any degree of ℓ, and in further support, we computed higher degree examples. These are the first higher degree examples of Drinfeld modular polynomials in the literature. The computation of Drinfeld modular polynomials proved to be the most challenging part of this thesis, particularly in terms of code implementation and complexity analysis.

Organization of the Thesis

In Chapter 2 we revisit some important properties of elliptic curves over finite fields and over the field of complex numbers. These properties include those of isogenies and endomorphism rings of elliptic curves. Furthermore, we consider j-invariants and modular polynomials associated to elliptic curves which are the main ingredients in the computation of isogeny volcanoes of elliptic curves. Here we revisit Kohel's theorem for elliptic curves. This is the most important tool in studying structural properties of isogeny graphs arising from isogenous elliptic curves. Then we present some attributes of isogeny volcanoes of elliptic

curves. This chapter serves as our guide in meeting the objectives of this thesis.

In Chapter 3 we discuss some number theoretic properties of polynomial rings over finite fields and some basics regarding quadratic extensions of rational function fields. This chapter includes a review of orders of imaginary quadratic function fields and their corresponding class groups and class numbers. The concepts presented here are used in Chapters 7 and 8.

Chapter 4 provides an introduction to Drinfeld modules. This includes a discussion of additive polynomials and the ring they form under *twisted multiplication*. Here we discuss basics such as ranks, heights, torsion points, and morphisms of Drinfeld modules.

Chapter 5 covers the analytic aspects of Drinfel modules. We review properties of Drinfeld modules defined over $\mathbf{C}$, where $\mathbf{C}$ is the characteristic p, nonarchimedean analogue of the field $\mathbb{C}$ of complex numbers. We discuss lattices and the exponential function on $\mathbf{C}$ and the construction of Drinfeld modules over $\mathbf{C}$. This chapter includes a treatment of isogenies and endomorphism rings of Drinfeld modules over $\mathbf{C}$. We also describe coefficients of Drinfeld modules over $\mathbf{C}$ giving particular attention to the rank one and two cases. Moreover, we consider modular forms, series expansions of j-invariants, and modular polynomials for Drinfeld modules over $\mathbf{C}$. This work is used heavily in Chapters 7 and 8. Most of the results presented in this chapter are analogues of well known results for elliptic curves.

In Chapter 6 we give a more detailed description of morphisms of rank two Drinfeld modules defined over some field $\mathbb{L}$ of characteristic p. Here we define the *degree* of an isogeny and present a method of constructing or computing *linear* isogenies of Drinfeld modules. Then we discuss dual isogenies of Drinfeld modules. Another important object related to a Drinfeld module is the characteristic polynomial of its Frobenius. We present a result that gives this polynomial in terms of residue symbols and an analogue of the Hasse invariant in the Drinfeld module case. We also discuss additional properties of endomorphism rings of Drinfeld modules and how they are used to classify Drinfeld modules as ordinary or supersingular. Then we discuss reduction and lifting of Drinfeld modules, the latter using

an analogue of Deuring's Lifting Theorem in the Drinfeld module case. We end this chapter by including a short treatment of the action of the ideal class group of the endomorphism ring of a Drinfeld module φ on the set of isomorphism classes of Drinfeld modules with endomorphism rings isomorphic to that of φ. The concepts presented here are used in Chapter 7.

In Chapter 7 we present our results pertaining to ℓ-isogeny volcanoes of ordinary rank two Drinfeld modules over finite fields. The endomorphism rings of these Drinfeld modules are orders $\mathcal{O}$ in an imaginary quadratic function field extension $\mathcal{K}$ of $\mathbb{F}_q(T)$. We discuss properties of such orders. These are parametrized by their conductor ideals $\mathfrak{c}$. The j-invariants $j(\varphi)$ and $j(\psi)$ of two ℓ-isogenous Drinfeld modules φ and ψ, respectively, over $\mathbf{C}$ satisfy $\Phi_\ell(j(\varphi), j(\psi)) = 0$, where $\Phi_\ell(X, Y)$ is the Drinfeld modular polynomial for ℓ. We use this result, the relation among orders in $\mathcal{K}$, and the Deuring Lifting Theorem to establish an analogue of Kohel's theorem for Drinfeld modules which then allows us to classify isogenies of ordinary Drinfeld modules. In this chapter we give a detailed treatment of the structural properties of isogeny volcanoes using our classification theorem, isogeny classes of Drinfeld modules, and roots of Drinfeld modular polynomials. The results presented in this chapter are new in the Drinfeld module case. These results comprise the necessary theoretical aspects of isogeny volcanoes for Chapter 8.

Chapter 8 is entirely devoted to the computational aspects of Drinfeld modules. We present a total of six algorithms in this chapter. The first algorithm is for computing series expansions of j-invariants up to a certain precision. The second one is for computing Drinfeld modular polynomials. We mention that this second algorithm follows the method given in [BL97], but here we present it in algorithmic form and implement it. The main tool in this algorithm is the j-invariant. The third algorithm computes isogeny volcanoes of rank two Drinfeld modules defined over some finite extension $\mathbb{F}_\mathfrak{p}$ of $\mathbb{F}_q$ using the roots of Drinfeld modular equations. The fourth algorithm is created for computing endomorphism

rings of ordinary Drinfeld modules. Here we use the location of a Drinfeld module in its isogeny volcano to determine its endomorphism ring. Finally, the fifth and sixth algorithms are designed to compute isogenies and dual isogenies, respectively, of ℓ-isogenous rank two Drinfeld modules over $\mathbb{F}_{\mathfrak{p}}$. Our main tools in constructing these last two algorithms are the properties of isogenies of Drinfeld modules. This chapter also includes a proof of validity and a detailed complexity analysis for each of the algorithms presented. Computational examples are also given in this chapter. All the algorithms presented here were implemented using SAGE [S$^+$17]. We point out that the results in Chapter 8, with the exception of a few lemmas, are new in the Drinfeld module case.

Chapter 9 contains a summary of the new results in this thesis and some possible research directions related to our findings in this research.

Finally, we conclude this dissertation with two appendices containing several more examples of Drinfeld modular polynomials, isogeny volcanoes, some additional algorithms, and proofs.

Chapter 2

Elliptic Curves

The core of this chapter is elliptic curves. We give a review and summary of the basic properties of these curves over finite fields. Particular attention is given to maps between such curves and the endomorphism ring of a given curve. Then we revisit the analytic aspects of elliptic curves. We go over the features of some analytic functions and modular polynomials for these curves over the field of complex numbers. Finally, we review basic properties of isogeny volcanoes for elliptic curves. In particular, we revisit Kohel's theorem, which is fundamental to the study of isogeny volcanoes.

2.1 Basics of Elliptic Curves

We give a summary of some features of elliptic curves over finite fields from [Sil09] and [CF06]. These features will then be used to build analogous results for Drinfeld modules. Throughout this section, let K be a field, $\mathbb{F}_q$ a finite field of $q = p^s$ elements with $p \in \mathbb{Z}$ a prime, and $\overline{K}$ an algebraic closure of K.

Definition 2.1.1. An *elliptic curve E over a field K*, denoted E/K, is an algebraic curve defined by the *Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

with $a_1, a_2, a_3, a_4, a_6 \in K$ such that for each point (x, y) with coordinates in $\overline{K}$ satisfying (2.1), at least one of the partial derivatives $\partial y = 2y + a_1x + a_3$ and $\partial x = 3x^2 + 2a_2x + a_4 - a_1y$ is nonzero. The set of *K-rational points* on the elliptic curve E/K is

$$E(K) = \{(x, y) \in K^2 \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\},$$

where O is the point at infinity.

The condition on partial derivatives in this definition guarantees that E is nonsingular. It is well known that $E(K)$ forms a group under addition with identity O. For $K = \mathbb{F}_q$, $E(\mathbb{F}_q)$ is either cyclic or is isomorphic to a product of two cyclic groups $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ where $d_1 \mid d_2$ and $d_1 \mid q-1$ ([CF06], p. 272).

We now look into some properties of (2.1). Two Weierstrass equations for E as in (2.1) are *equivalent* if and only if they are related by a linear change of variables of the form

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t,$$

where $u \in K^*$ and $r, s, t \in K$ ([Sil09, Proposition III.3.1(b)]). One can also simplify (2.1) by using an appropriate change of variables. If $\mathrm{char}(\overline{K}) \neq 2$, then we can use the substitution $y \longmapsto y - (a_1x + a_3)/2$ to simplify (2.1) to the equation

$$E : y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}, \tag{2.2}$$

where $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$ and $b_6 = a_3^2 + 4a_6$. In addition, let

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j &= (b_2^2 - 24b_4)^3/\Delta. \end{aligned}$$

Definition 2.1.2. The quantity Δ above is the *discriminant* of the Weierstrass equation and the number j is the *j-invariant* of E, also denoted $j(E)$.

If further $\mathrm{char}(\overline{K}) \neq 2, 3$, then by applying the transformation $x \longmapsto x - b_2/12$ to (2.2) we can express (2.1) as

$$E : y^2 = x^3 + Ax + B, \tag{2.3}$$

where

$$A = \frac{b_4}{2} - \frac{b_2^2}{48} \quad \text{and} \quad B = b_6 - \frac{b_2b_4}{24} + \frac{b_2^3}{864}.$$

Corresponding to this equation are the quantities

$$\Delta = -16(4A^3 + 27B^2) \quad \text{and} \quad j(E) = -1728\frac{(4A)^3}{\Delta} = 1728\ \frac{4A^3}{4A^3 + 27B^2}.$$

Function Fields of Elliptic Curves

Let E be an elliptic curve over a field K given by the Weierstrass equation (2.1). Let

$$F(x, y) := y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6.$$

We define the *function field* of E/K, denoted $K(E)$, as the quotient field of the ring

$$K[E] = \frac{K[x, y]}{\langle F(x, y)\rangle}$$

of regular functions on E, where $\langle F(x, y)\rangle$ is the principal $K[x, y]$-ideal generated by $F(x, y)$.

Isomorphisms of Elliptic Curves

Suppose $\mathrm{char}(K) \neq 2, 3$. Let $E_1 : y^2 = x^3 + A_1x + B_1$ and $E_2 : y^2 = x^3 + A_2x + B_2$ be elliptic curves defined over K. Denote the j-invariant of E_i by $j(E_i)$ for $i = 1, 2$.

Proposition 2.1.3. *E_1 and E_2 are isomorphic over $\overline{K}$ if and only if $j(E_1) = j(E_2)$.*

Proof. See [Sil09, Proposition III.1.4(b)]. □

Note that two equivalent Weierstrass equations in the form (2.3) are related by a change of variable as described previously and yield the same j-invariant. Thus, the isomorphism in this proposition must be of the form $(x, y) \longmapsto (u^2x, u^3y)$, where $u \in \overline{K}^*$ satisfies

$$\begin{aligned} u &= (B_1/B_2)^{1/6}, && \text{if } A_1 = 0 \ (j = 0); \\ u &= (A_1/A_2)^{1/4}, && \text{if } B_1 = 0 \ (j = 1728); \\ u &= (A_1/A_2)^{1/4} = (B_1/B_2)^{1/6}, && \text{if } A_1B_1 \neq 0 \ (j \neq 0, 1728). \end{aligned} \tag{2.4}$$

Isogenies of Elliptic Curves

As above, let E_1 and E_2 be elliptic curves over K. We consider maps between elliptic curves that preserve the group identity O.

Definition 2.1.4. Let E_1 and E_2 be elliptic curves over K. An *isogeny* over K from E_1 to E_2 is a morphism $\phi : E_1 \longrightarrow E_2$ over K that satisfies $\phi(O) = O$. Moreover, E_1 and

E_2 are said to be *isogenous* if there is an isogeny $\phi : E_1 \longrightarrow E_2$ defined over K such that $\phi(E_1) \neq \{O\}$. The *kernel* of ϕ is the set $\ker \phi = \{P \in E_1(\overline{K}) \mid \phi(P) = O\}$. Denote the set of isogenies from E_1 to E_2 defined over K by $\mathrm{Hom}_K(E_1, E_2)$, and if $E_1 = E_2$, denote this by $\mathrm{End}_K(E_1)$. The set of isogenies from E_1 to E_2 defined over $\overline{K}$ is denoted by $\mathrm{Hom}(E_1, E_2)$, and by $\mathrm{End}(E_1)$ if $E_1 = E_2$.

Note that the isogeny ϕ in the previous definition is a group homomorphism (see [Sil09, Theorem III.4.8]).

Definition 2.1.5. The set of all elliptic curves over K that are isogenous to an elliptic curve E/K is called an *isogeny class*.

Define the zero isogeny by $[0](P) = O$ for all $P \in E_1$. Since every morphism between curves is either constant or surjective, it follows that an isogeny satisfies either $\phi(E_1) = \{O\}$ or $\phi(E_1) = E_2$. So every nonzero isogeny is a finite surjective map of curves, and hence we obtain an injection of function fields

$$\phi^* : \overline{K}(E_2) \longrightarrow \overline{K}(E_1).$$

The degree of ϕ, denoted $\deg \phi$, is equal to $[\overline{K}(E_1) : \phi^*(\overline{K}(E_2))]$. Similarly, we can also define the *separable* and *inseparable degrees* of ϕ, denoted by $\deg_s \phi$ and $\deg_i \phi$, respectively. The isogeny ϕ is categorized as *separable*, *inseparable*, or *purely inseparable* depending on the property of the field extension. We will discuss this in more detail further on. By convention, we set $\deg[0] = 0$ to ensure that

$$\deg(\psi \circ \phi) = \deg(\psi) \deg(\phi)$$

for all chains of isogenies $E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3$.

Definition 2.1.6. An isogeny $\phi : E \longrightarrow E'$ of degree n is called an *n-isogeny*.

Example 2.1.7. We consider two important isogenies of elliptic curves over K.

1. Let $m \in \mathbb{N}$. The *multiplication-by-m* map is defined by

$$\begin{aligned} [m] : E &\longrightarrow E \\ P &\longmapsto [m]P = \underbrace{P + P + \cdots + P}_{m \text{ terms}}. \end{aligned}$$

This definition can be extended to all $m \in \mathbb{Z}$ by setting $[m]P = [-m](-P)$ for $m < 0$ and, as defined above, $[0]P = O$ for $m = 0$. The set

$$E[m] = \{P \in E \mid [m]P = O\}$$

is the set of points of E of order dividing m, and is called the *m-torsion subgroup of* E.

2. Let $K = \mathbb{F}_q$. The *Frobenius isogeny* is given by

$$\pi : E \longrightarrow E, \quad (x, y) \longmapsto (x^q, y^q).$$

Note that π fixes the finite group $E(\mathbb{F}_q)$, so

$$E(\mathbb{F}_q) = \ker\left(\pi - 1 : E(\overline{\mathbb{F}}_q) \longrightarrow E(\overline{\mathbb{F}}_q)\right).$$

It is distinct from the map $[m]$ for all $m \in \mathbb{Z}$. Moreover, this map is an important tool in determining the number of points in $E(\mathbb{F}_q)$.

We now look into some properties related to $[m]$.

Proposition 2.1.8. *Let E be an elliptic curve over K and $m \in \mathbb{Z}$ with $m \neq 0$. Then the map $[m] : E \longrightarrow E$ is nonconstant.*

Proof. See [Sil09, Proposition III.4.2(a)]. □

For a nonconstant isogeny $\phi : E_1 \longrightarrow E_2$ of degree m, there exists a unique isogeny $\widehat{\phi} : E_2 \longrightarrow E_1$ which satisfies the relation

$$\widehat{\phi} \circ \phi = \phi \circ \widehat{\phi} = [m].$$

This isogeny is called the *dual isogeny of* ϕ. If $\phi = [0]$, then we set $\widehat{\phi} = [0]$. The basic properties of the dual isogeny are given in the following theorem.

Theorem 2.1.9. *Let $\phi : E_1 \longrightarrow E_2$, $\psi : E_1 \longrightarrow E_2$, and $\lambda : E_2 \longrightarrow E_3$ be isogenies of elliptic curves.*

(a) If $\deg \phi = m$, then $\widehat{\phi} \circ \phi = [m]$ on E_1 and $\phi \circ \widehat{\phi} = [m]$ on E_2.

(b) $\widehat{\lambda \circ \phi} = \widehat{\phi} \circ \widehat{\lambda}$.

(c) $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$.

(d) For all $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ and $\deg[m] = m^2$.

(e) $\deg \widehat{\phi} = \deg \phi$.

(f) $\widehat{\widehat{\phi}} = \phi$.

Proof. See [Sil09, Theorem III.6.2]. □

Corollary 2.1.10. *Let E be an elliptic curve over K and $m \in \mathbb{Z}$ with $m \neq 0$.*

(a) If char(K) is either zero or prime to m, then

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

(b) If char$(K) = p$, then either

$$E[p^e] = \{O\}, \text{ for all } e \geq 1 \quad \text{or} \quad E[p^e] = \frac{\mathbb{Z}}{p^e\mathbb{Z}}, \text{ for all } e \geq 1.$$

Proof. See [Sil09, Corollary III.6.4]. □

If the first case in Corollary 2.1.10(b) holds, then E is called *supersingular*. Otherwise the curve is called *ordinary*.

Another notion related to the multiplication-by-m isogeny is the *Tate module* associated to an elliptic curve E. Let $\ell \in \mathbb{Z}$ be prime. The (ℓ-adic) Tate module of E is the group

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

where the inverse limit is taken with respect to the natural maps $E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n]$. Each $E[\ell^n]$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module, so the Tate module is a $\mathbb{Z}_\ell$-module, where $\mathbb{Z}_\ell$ denotes the ℓ-adic integers.

Now recall the following definition.

Definition 2.1.11. A field K is *perfect* if either (a) K has characteristic 0, or (b) K has characteristic $p > 0$ and every element of K is a p-th power in K, i.e., $K = K^p$.

Example 2.1.12. Examples of perfect fields include finite fields and algebraically closed fields.

The next results describe some properties of the Frobenius map, where K is assumed to be a perfect field. Again, we let $\mathrm{char}(K) = p$ and $q = p^s$, for some positive integer s. Let $E^{(q)}/K$ be the curve defined by raising each coefficient of the equation for E to the q-th power.

Proposition 2.1.13. *Let $\mathrm{char}(K) = p > 0$, E an elliptic curve over K, and $\pi : E \longrightarrow E^{(q)}$ the q-th power Frobenius morphism.*

(a) $\pi^* K(E^{(q)}) = K(E)^q = \{f^q \mid f \in K(E)\}$.

(b) π *is purely inseparable.*

(c) $\deg \pi = q$.

Proof. See [Sil09, Proposition II.2.11]. □

Corollary 2.1.14. *Every isogeny $\psi : E_1 \longrightarrow E_2$ over a field of characteristic $p > 0$ factors as*

$$E_1 \xrightarrow{\pi} E_1^{(q)} \xrightarrow{\sigma} E_2,$$

where q is the inseparable degree of ψ, the map π is the q-th power Frobenius, and the isogeny σ is separable.

Proof. See [Sil09, Corollary II.2.12]. □

We now summarize some additional properties of isogenies of elliptic curves (for example, see [Sil09, Propositions III.4.10 and III.4.12]). In what follows, the symbol $\#S$ stands for the cardinality of a set S.

Proposition 2.1.15. *Let E, E_1, and E_2 be elliptic curves over an algebraically closed field K.*

1. *Let $\phi : E_1 \longrightarrow E_2$ be a nonzero isogeny. If ϕ is separable, then $\#\ker\phi = \deg\phi$.*
2. *Given a finite subgroup G of E, there is a unique elliptic curve E' and a unique separable isogeny $\psi : E \longrightarrow E'$ satisfying $\ker\psi = G$.*

2.2 Endomorphism Rings of Elliptic Curves

The set of all isogenies $E_1 \longrightarrow E_2$ defined over $\overline{K}$, $\mathrm{Hom}(E_1, E_2)$, forms a group under addition. The sum of two isogenies is given by

$$(\phi + \psi)(P) = \phi(P) + \psi(P), \qquad P \in E(K).$$

If $E_1 = E_2$, then composition of isogenies is also possible. So if E is an elliptic curve, we let the set

$$\mathrm{End}(E) = \mathrm{Hom}(E, E),$$

as introduced in Definition 2.1.4, be the ring where addition is as given above and multiplication is composition of isogenies

$$(\phi\psi)(P) = \phi(\psi(P)), \qquad P \in E(K).$$

We call this ring the (full) *endomorphism ring* of E. The isogenies given in Example 2.1.7 are actually endomorphisms of E. The invertible elements of $\mathrm{End}(E)$ form a group called the *automorphism group* of E, and we denote this group by $\mathrm{Aut}(E)$. $\mathrm{End}(E)$ can be characterized as follows.

Proposition 2.2.1. *Let E be an elliptic curve.*

1. $\mathrm{End}(E)$ *is a ring of characteristic 0 with no zero divisors.*
2. $\mathrm{End}(E)$ *is a free $\mathbb{Z}$-module of rank at most 4.*
3. $\mathrm{End}(E)$ *possesses an anti-involution $\phi \longrightarrow \widehat{\phi}$ (i.e., $\widehat{\phi\psi} = \widehat{\psi}\widehat{\phi}$).*
4. *For $\phi \in \mathrm{End}(E)$, the product $\phi\widehat{\phi}$ is a nonnegative integer. Furthermore, $\phi\widehat{\phi} = 0$ if and only if $\phi = 0$.*

Proof. See [Sil09, Proposition III.4.2(c), Corollary III.7.5, Theorem III.6.2, and Corollary III.6.3]. □

Any ring R that satisfies the preceding proposition is one of the following rings (see [Sil09, Theorem III.9.3]): (a) $R \cong \mathbb{Z}$. (b) R is an order in an imaginary quadratic field extension K of $\mathbb{Q}$. (c) R is an order in a quaternion algebra K over $\mathbb{Q}$. By an order here, we mean a subring of K that is finitely generated as a $\mathbb{Z}$-module and satisfies $R \otimes \mathbb{Q} = K$.

Next, consider the relationship between the endomorphism ring and the Tate module associated to E. Let $K = \mathbb{F}_q$. Suppose $\ell \in \mathbb{Z}$ is prime and distinct from $p = \mathrm{char}(\mathbb{F}_q)$. Let $\phi \in \mathrm{End}(E)$. So ϕ induces a map

$$\phi : E[\ell^n] \longrightarrow E[\ell^n].$$

Thus, it induces a $\mathbb{Z}_\ell$-linear map

$$\phi_\ell : T_\ell(E) \longrightarrow T_\ell(E),$$

and hence the map

$$\mathrm{End}(E) \longrightarrow \mathrm{End}(T_\ell(E)), \qquad \phi \longmapsto \phi_\ell$$

is a ring homomorphism. By choosing a $\mathbb{Z}_\ell$-basis for $T_\ell(E)$, one can write ϕ_ℓ as a 2×2 matrix and calculate its determinant and trace, $\det(\phi_\ell), \mathrm{tr}(\phi_\ell) \in \mathbb{Z}_\ell$.

Proposition 2.2.2. *Let $\phi \in \mathrm{End}(E)$ and $\phi_\ell : T_\ell(E) \longrightarrow T_\ell(E)$ be the map induced by ϕ on $T_\ell(E)$. Then*

$$\det(\phi_\ell) = \deg \phi \quad \text{and} \quad \mathrm{tr}(\phi_\ell) = 1 + \deg \phi - \deg(1 - \phi).$$

In particular, $\det(\phi_\ell), \mathrm{tr}(\phi_\ell) \in \mathbb{Z}$ *and both are independent of* ℓ.

Proof. See Propositions III.8.6 or V.2.3 in [Sil09]. □

We now consider additional important properties of the endomorphism ring of E. Because of the existence of the $[m]$ map, it is known that $\mathbb{Z} \subseteq \mathrm{End}(E)$. When $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, we say that E has *complex multiplication (CM)*, and in this case $\mathrm{End}(E)$ is an order in an imaginary quadratic field or in a definite quaternion algebra. In the finite field case $\mathrm{End}(E)$ is always strictly larger than $\mathbb{Z}$ because the Frobenius map is an element of $\mathrm{End}(E) - \mathbb{Z}$, so in this case E always has CM. One fundamental result in the characteristic p case is given next ([Sil09, Theorem V.3.1]).

Theorem 2.2.3. *Let K be a field with $\mathrm{char}(K) = p$, and let E/K be an elliptic curve. For each integer $r \geq 1$, let*

$$\pi_r : E \longrightarrow E^{(p^r)} \quad \text{and} \quad \widehat{\pi}_r : E^{(p^r)} \longrightarrow E$$

be the p^r-power Frobenius map and its dual.

(1) The following conditions are equivalent.

- *(a) $E[p^r] = \{O\}$ for all $r \geq 1$, i.e., E is supersingular.*
- *(b) $\widehat{\pi}_r$ is (purely) inseparable for all $r \geq 1$.*
- *(c) The map $[p] : E \longrightarrow E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.*
- *(d) $\mathrm{End}(E)$ is an order in a quaternion algebra.*

(2) If the equivalent conditions in part (1) do not hold, i.e., E is ordinary, then

$$E[p^r] = \frac{\mathbb{Z}}{p^r\mathbb{Z}}$$

for all $r \geq 1$. *Moreover, if* $j(E) \in \overline{\mathbb{F}}_p$, *then* $\mathrm{End}(E)$ *is an order of an imaginary quadratic field.*

This result gives another way of classifying elliptic curves as ordinary or supersingular. E is supersingular if the equivalent conditions in Theorem 2.2.3(1) hold. In this case, we also say that E has *Hasse invariant* 0. Otherwise we say that E is ordinary, or that E has *Hasse invariant* 1.

The Trace of Frobenius

By using Proposition 2.2.2, we can compute the number of points on $E(\mathbb{F}_q)$. This result also leads to an important property of the Frobenius endomorphism.

Theorem 2.2.4. *Let* E *be an elliptic curve over* $\mathbb{F}_q$ *and* $\pi \in \mathrm{End}(E)$ *the* q*-th power Frobenius endomorphism. Also, let*

$$t = q + 1 - \#E(\mathbb{F}_q).$$

(a) If $\alpha, \beta \in \mathbb{C}$ *are the roots of the polynomial* $f(x) = x^2 - tx + q$, *then* α *and* β *are complex conjugates satisfying* $|\alpha| = |\beta| = \sqrt{q}$, *and for every integer* $n \geq 1$

$$\#E(\mathbb{F}_q) = q^n + 1 - \alpha^n - \beta^n.$$

(b) In $\mathrm{End}(E)$, *the Frobenius endomorphism* π *satisfies the relation*

$$\pi^2 - t\pi + q = 0.$$

Proof. See Theorem V.2.3.1 in [Sil09]. □

The unique number t (same as the trace of π acting on the Tate module $T_\ell(E)$) in Theorem 2.2.4 is called the *trace of Frobenius* and the polynomial $f(x) = x^2 - tx + q$ is called the *characteristic polynomial* of the Frobenius endomorphism. This terminology comes from the fact that t is equal to the trace of the q-th power Frobenius map taken as a linear

transformation of $T_\ell(E)$. For the Frobenius endomorphism π, we obtain from Proposition 2.2.2 the relation

$$\mathrm{tr}(\pi_\ell) = 1 + \deg \pi - \deg(1 - \pi) = 1 + q - \#E(\mathbb{F}_q) = t.$$

The following result, known as the Hasse bound on t, is very useful in determining the number of rational points in $E(\mathbb{F}_q)$.

Theorem 2.2.5 (Hasse)**.** *Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then*

$$|1 + q - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Proof. See [Sil09, Theorem V.1.1]. □

2.3 Digression to Complex Analysis

In this section we revisit some results from complex analysis pertaining to elliptic and modular functions, the j-invariant, and modular polynomials. For a deeper treatment of the material presented here, see for example [Cox89], [Lan87], [Sil94] and [Sil09].

2.3.1 Elliptic Functions

Let Λ be a *lattice* in $\mathbb{C}$, i.e., Λ is an additive subgroup of $\mathbb{C}$ generated by two complex numbers ω_1 and ω_2 which are linearly independent over $\mathbb{R}$. We write such a lattice as $\Lambda = [\omega_1, \omega_2]$. By an *elliptic function* for Λ we mean a meromorphic function on the the complex plane which is invariant under translation by Λ. So if f is an elliptic function on $\mathbb{C}$, it must satisfy the condition

$$f(z + \omega) = f(z) \qquad \text{for all } z \in \mathbb{C},\ \omega \in \Lambda.$$

Note that an elliptic function can be viewed as a meromorphic function on the complex torus $\mathbb{C}/\Lambda$. This gives us a way to parametrize elliptic curves over $\mathbb{C}$.

Weierstrass $\wp$-Function

A classical example of an elliptic function is the *Weierstrass $\wp$-function*. For a fixed lattice Λ in $\mathbb{C}$, this function is defined as follows

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right].$$

Some basic properties of this function are given in the next result.

Theorem 2.3.1. *Let $\wp(z)$ be the Weierstrass $\wp$-function for the lattice Λ. Then*

1. *$\wp(z)$ is an elliptic function for Λ having double poles at $\omega \in \Lambda$ as its only singularities.*
2. *$\wp(z)$ satisfies the differential equation*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda), \tag{2.5}$$

   where the coefficients $g_2(\Lambda)$ and $g_3(\Lambda)$ are defined, respectively, by

$$g_2(\Lambda) = 60 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^4}, \quad \text{and} \quad g_3(\Lambda) = 140 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^6}.$$

3. *$\wp(z)$ satisfies the addition law*

$$\wp(z+w) = -\wp(z) - \wp(w) + \frac{1}{4} \left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} \right)^2,$$

   where $w, z, z+w \notin \Lambda$.

Proof. See [Cox89, Theorem 10.1]. □

Let $g_2 = g_2(\Lambda)$ and $g_3 = g_3(\Lambda)$. The preceding theorem shows that the point $(\wp(z), \wp'(z))$ satisfies the equation

$$y^2 = 4x^3 - g_2 x - g_3, \tag{2.6}$$

where the cubic polynomial on the right-hand side has discriminant

$$\Delta = g_2^3 - 27 g_3^2. \tag{2.7}$$

The polynomial $4x^3 - g_2x - g_3$ has three distinct roots given by

$$\wp\left(\frac{\omega_1}{2}\right), \quad \wp\left(\frac{\omega_2}{2}\right) \quad \text{and} \quad \wp\left(\frac{\omega_3}{2}\right),$$

where ω_1 and ω_2 are the generators of Λ and $\omega_3 = \omega_1 + \omega_2$. This implies that the discriminant Δ does not vanish. Moreover, the elliptic curve E defined by the Weierstrass equation (2.5) over $\mathbb{C}$ is parametrized by the functions $\wp(z)$ and $\wp'(z)$. So the map given by

$$\mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}), \quad z \longmapsto (\wp(z), \wp'(z)) \tag{2.8}$$

is an isomorphism of groups and of Riemann surfaces (see for example, [Sil09], Proposition VI. 3.6). The lattice Λ in this isomorphism is unique up to homothety (see [Sil09, Corollary VI.5.1.1]).

2.3.2 The j-Invariant of a Lattice

Recall that an elliptic function is dependent on the lattice that is being used. However, it is also possible that different lattices can have essentially the same elliptic functions. This happens when two lattices Λ and Λ' are *homothetic*; that is, there exists a nonzero complex number γ such that $\Lambda' = \gamma\Lambda$, where $\gamma\Lambda := \{\gamma\lambda \mid \lambda \in \Lambda\}$. Homothety is an equivalence relation on the set of lattices on $\mathbb{C}$, so lattices can be classified up to homothety. In this case, one can verify that if $f(z)$ is an elliptic function for Λ, then $f(\gamma z)$ is an elliptic function for Λ'.

Using the coefficients g_2 and g_3 of (2.5), the discriminant corresponding to Λ is given by (2.7). The j-invariant $j(\Lambda)$ of the lattice Λ is the complex number given by

$$j(\Lambda) = 1728\ \frac{g_2^3}{g_2^3 - 27g_3^2} = 1728\ \frac{g_2^3}{\Delta}, \tag{2.9}$$

which is always defined since Δ is nonzero. One useful result regarding $j(\Lambda)$ is that this number characterizes the lattice Λ up to homothety.

Theorem 2.3.2. *Let Λ and Λ' be lattices in $\mathbb{C}$. Then $j(\Lambda) = j(\Lambda')$ if and only if Λ and Λ' are homothetic.*

Proof. See [Cox89, Theorem 10.9]. □

Corollary 2.3.3. *Let $E/\mathbb{C}$ and $E'/\mathbb{C}$ be elliptic curves corresponding to the lattices Λ and Λ', respectively. Then E and E' are isomorphic over $\mathbb{C}$ if and only if Λ and Λ' are homothetic.*

Remark 2.3.4. Note that we can also define j-invariants for ideals of an order $\mathcal{O}$ in an imaginary quadratic field K. Let $\mathfrak{a}$ be a proper fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is a $\mathbb{Z}$-module of rank two, so $\mathfrak{a} = [\alpha, \beta]$ for some $\alpha, \beta \in K$ (see [Cox89, Exercise 7.8]). The elements α and β are linearly independent over $\mathbb{R}$ (see [Cox89, Exercise 10.11]). We can consider K as a subset of $\mathbb{C}$, so $\mathfrak{a}$ is an additive subgroup of $\mathbb{C}$ generated by the complex numbers α and β which are linearly independent over $\mathbb{R}$. So $\mathfrak{a}$ is a lattice in $\mathbb{C}$, and hence, the j-invariant $j(\mathfrak{a})$ is defined. Note that $j(\mathfrak{a})$ is an algebraic integer, see [Cox89, Theorem 11.1].

2.3.3 Modular Functions and Modular Forms

Let Γ be the *modular group* $SL_2(\mathbb{Z})$ and let $\mathcal{H}$ be the *upper half plane* $\{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$. Recall that Γ is generated by the matrices

$$\mathrm{T} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathrm{S} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Moreover, Γ acts on $\mathcal{H}$ via fractional linear transformations

$$\alpha\tau = \frac{a\tau + b}{c\tau + d}, \quad \text{for } \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,\ \tau \in \mathcal{H}.$$

Note that $\alpha\tau \in \mathcal{H}$, so Γ maps $\mathcal{H}$ to itself. Observe that

$$\mathrm{Im}(\alpha\tau) = \mathrm{Im}(\tau)\frac{\det \alpha}{|c\tau + d|^2} > 0 \quad \text{if } \det \alpha > 0.$$

Definition 2.3.5. Let $k \in \mathbb{Z}$. A meromorphic function f on $\mathcal{H}$ is called a *weakly modular function of weight* $2k$ for Γ if it satisfies

$$f(\alpha\tau) = (c\tau + d)^{2k} f(\tau) \quad \text{for all } \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, \tau \in \mathcal{H}.$$

Note that all nontrivial weakly modular functions for Γ are of even weights only. To see this, suppose $\alpha = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and k is an odd integer. If f satisfies $f(\alpha\tau) = (c\tau + d)^k f(\tau)$, then

$$f(\tau) = (-1)^k f(\tau) = -f(\tau).$$

So f is identically zero. This explains the restriction to even weights in Definition 2.3.5.

By using the matrix generators T and S of Γ, we see that a meromorphic function f on $\mathcal{H}$ is weakly modular of weight $2k$ if it satisfies

$$f(\mathrm{T}\tau) = f(\tau + 1) = f(\tau) \quad \text{and} \quad f(\mathrm{S}\tau) = f\left(\frac{-1}{\tau}\right) = \tau^{2k} f(\tau).$$

It follows from the first identity that f can be expressed as a function of

$$\mathrm{q} := \mathrm{e}^{2\pi \mathrm{i} \tau},$$

and that f is meromorphic in the punctured unit disc $D = \{\mathrm{q} \in \mathbb{C} \mid 0 < |\mathrm{q}| < 1\}$ (recall, from complex analysis, that the $\mathbb{Z}$-periodic map $\tau \longmapsto \mathrm{q}$ takes $\mathcal{H}$ to D). So f has a Fourier expansion

$$f^*(\mathrm{q}) = \sum_{n=-\infty}^{\infty} c_n \mathrm{q}^n. \tag{2.10}$$

We also call $f^*(q)$ the q-*expansion* of f. We say that

(a) f is *meromorphic at* ∞ if $f^*(\mathrm{q}) = \sum_{n=-N}^{\infty} c_n \mathrm{q}^n$ for some integer N.

(b) f is *holomorphic at* ∞ if $f^*(\mathrm{q}) = \sum_{n=0}^{\infty} c_n \mathrm{q}^n$.

Definition 2.3.6. A weakly modular function for Γ that is meromorphic at ∞ is called a *modular function for* Γ. A modular function for Γ that is holomorphic on $\mathcal{H}$ and at ∞ is called a *modular form*.

Remark 2.3.7. Note that we can also define modular functions and modular forms for any subgroup of Γ. See, for instance, [DS05, Section 1.2].

Let $\Lambda = [\omega_1, \omega_2] \subset \mathbb{C}$ be a lattice. Then Λ is homothetic to $\Lambda_\tau := [1, \tau]$, for some $\tau \in \mathcal{H}$. To see this, note that

$$[\omega_1, \omega_2] = \omega_1 \left[1, \frac{\omega_2}{\omega_1}\right] = \omega_2 \left[1, \frac{\omega_1}{\omega_2}\right],$$

where ω_1/ω_2 or ω_2/ω_1 is in $\mathcal{H}$. The *Eisenstein series* for Λ is the series

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^{2k}},$$

which is absolutely convergent for all integers $k \geq 2$ (see [Sil09, Theorem VI.3.1]). Notice that the coefficients g_2 and g_3 in (2.5) are special cases of this series. For $\tau \in \mathcal{H}$, write

$$G_{2k}(\tau) = G_{2k}(\Lambda_\tau) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m + n\tau)^{2k}}.$$

G_{2k} is a modular form of weight $2k$ for an integer $k \geq 2$, see [Sil94, Proposition I.3.4.2]. Its q-expansion is

$$G_{2k}(\tau) = 2\zeta(2k) + 2\frac{(2\pi \mathrm{i})^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) \mathrm{q}^n, \tag{2.11}$$

where

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} \quad \text{and} \quad \sigma_k(n) = \sum_{d|n} d^k$$

are the Riemann zeta function and sum of divisors function, respectively. See, for example, [Sil94, Proposition I.7.1] for the derivation of (2.11). Of particular interest are the special cases g_2 and g_3 with q-expansions

$$g_2(\tau) = 60G_4(\tau) = (2\pi)^4 \frac{1}{2^2 3} (1 + 240A) \tag{2.12}$$

and

$$g_3(\tau) = 140G_6(\tau) = (2\pi)^6 \frac{1}{2^3 3^3} (1 - 540B) \tag{2.13}$$

respectively, where

$$A = \sum_{n=1}^{\infty} \sigma_3(n) \mathrm{q}^n \quad \text{and} \quad B = \sum_{n=1}^{\infty} \sigma_5(n) \mathrm{q}^n.$$

See [Lan87], p. 44.

Recall that Δ can be expressed in terms of g_2 and g_3, see (2.7). By using (2.12) and (2.13), we obtain

$$\Delta = (2\pi)^{12}\frac{1}{2^6 3^3}\left((1+240A)^3-(1-540B)^2\right),$$

where the coefficients of $(1+240A)^3-(1-540B)^2$ are all divisible by 12^3 (see [Sil94], p. 59). The following result gives the q-expansion of Δ.

Proposition 2.3.8. *The* q*-expansion of* Δ *is*

$$\Delta(\tau) = (2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)\mathrm{q}^n,$$

where $\tau(1)=1$ *and* $\tau(n)\in\mathbb{Z}$.

Proof. See [Sil94, Proposition I.7.4]. □

The j-Function

Consider the *j-function* $j(\tau)$, which is defined by

$$j(\tau) = j([1,\tau]), \qquad \tau\in\mathcal{H}.$$

Its properties depend on the action of the group Γ on the upper half plane $\mathcal{H}$. We summarize these properties as follows:

Theorem 2.3.9. *Let* $\tau\in\mathcal{H}$.

1. $j(\tau)$ *is a holomorphic function on* $\mathcal{H}$.
2. *If* $\tau'\in\mathcal{H}$, *then* $j(\tau)=j(\tau')$ *if and only if* $\tau'=\alpha\tau$ *for some* $\alpha\in\Gamma$. *In particular,* $j(\tau)$ *is invariant under the action of* Γ *on* $\mathcal{H}$.
3. $j:\mathcal{H}\longrightarrow\mathbb{C}$ *is surjective.*

Proof. See [Cox89, Theorem 11.2]. □

As $j(\tau)$ is Γ-invariant, it follows that $j(\tau+1)=j(\tau)$. So $j(\tau)$ has a q-expansion. This expansion can be obtained by using (2.12), (2.13), and Proposition 2.3.8.

Theorem 2.3.10. *The* q*-expansion of* $j(\tau)$ *is given by*

$$j(\tau) = \frac{1}{\mathrm{q}} + 744 + 196884\mathrm{q} + \cdots = \frac{1}{\mathrm{q}} + \sum_{n=0}^{\infty} c_n \mathrm{q}^n, \tag{2.14}$$

where the coefficients c_n *are integers for all* $n \geq 0$*.*

Proof. See [Lan87, Ch. 4 §1] or [Sil94, Proposition I.7.4]. □

One remarkable result for modular functions for Γ is that they can be described by means of $j(\tau)$.

Theorem 2.3.11. *The* j*-function* $j(\tau)$ *is a modular function for* Γ*, and every modular function for* Γ *is a rational function in* $j(\tau)$*.*

Proof. See, for example, [Cox89, Theorem 11.9]. □

Theorem 2.3.12. *Let* $f(\tau)$ *be a modular function for* Γ *with* q*-expansion* (2.10)*. If* $f(\tau)$ *is holomorphic on* $\mathcal{H}$*, then it is a polynomial in* $j(\tau)$ *with coefficients in the* $\mathbb{Z}$*-module generated by the coefficients* c_n*.*

Proof. See [Lan87, Theorem 2, Ch. 5 §2]. □

Modular Polynomials for Elliptic Curves

Our next concern is to study the j-invariants of isogenous elliptic curves. To do this, we need to investigate $j \circ \alpha$ where α is a rational matrix. After this, we will study a special kind of polynomial, known as a *modular polynomial*, whose roots are the j-invariants of isogenous elliptic curves. This polynomial will then be used to construct *isogeny graphs* for elliptic curves in the next section.

Let $M_2^+(\mathbb{Q})$ and $M_2^+(\mathbb{Z})$ be the sets of 2×2 matrices with entries from $\mathbb{Q}$ and $\mathbb{Z}$, respectively, and whose determinants are positive. As before, let $\Gamma = SL_2(\mathbb{Z})$ and $\mathcal{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$. For a positive integer n, we consider the following subsets of $M_2^+(\mathbb{Z})$:

$$W_n = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2^+(\mathbb{Z}) \mid ad - bc = n \right\}$$

and

$$W_n^* = \left\{ \begin{pmatrix} a & b \\ & \\ c & d \end{pmatrix} \in W_n \mid \gcd(a,b,c,d) = 1 \right\}.$$

Note that Γ acts on W_n via multiplication. Indeed, for every $\gamma \in \Gamma$ and $\alpha \in W_n$, $\det(\gamma\alpha) = n$, so $\gamma\alpha \in W_n$. So it is immediate that Γ also acts on W_n^* via multiplication. We now characterize the cosets $\Gamma\alpha$ for $\alpha \in W_n^*$.

Theorem 2.3.13. *Γ acts left transitively on the right Γ-cosets, and also right transitively on the left Γ-cosets of W_n^*.*

Proof. See [Lan87, Theorem 1, Ch. 5 §1]. □

A set of representatives for the left Γ-cosets of W_n^* can be obtained as follows. Let $\alpha = \begin{pmatrix} a & b \\ & \\ c & d \end{pmatrix} \in W_n^*$. One can always find $\gamma \in \Gamma$ such that $\gamma\alpha = \begin{pmatrix} a_1 & b_1 \\ & \\ 0 & d_1 \end{pmatrix}$. An example of such a matrix is given by $\gamma = \begin{pmatrix} x & y \\ & \\ z & w \end{pmatrix} \in \Gamma$, where $\gcd(w,z) = 1$ such that $az + cw = 0$, and $x, y \in \mathbb{Z}$ such that $xw - yz = 1$. So we can now assume that α is an upper triangular matrix $\alpha = \begin{pmatrix} a & b \\ & \\ 0 & d \end{pmatrix}$. Observe that

$$\begin{pmatrix} 1 & k \\ & \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ & \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b+kd \\ & \\ 0 & d \end{pmatrix}.$$

So a left coset contains a representative with $0 \leq b < d$. One can verify that the set

$$C_n = \left\{ \begin{pmatrix} a & b \\ & \\ 0 & d \end{pmatrix} \mid ad = n,\ 0 < a,\ 0 \leq b < d,\ \gcd(a,b,d) = 1 \right\}$$

is the complete set of distinct left coset representatives of W_n^*. If $n = p$ is a prime number, then the left coset representatives are given by

$$\begin{pmatrix} p & 0 \\ & \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & m \\ & \\ 0 & p \end{pmatrix} \quad \text{for} \quad 0 \leq m < p.$$

So $\#C_p = p + 1$. In general, the number of distinct left cosets of W_n^* is

$$\#C_n = n \prod_{p|n} \left(1 + \frac{1}{p}\right),$$

see [Lan87], p. 53.

Let $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2^+(\mathbb{Q})$. We now consider the function $j \circ \alpha$ defined by

$$j \circ \alpha(\tau) = j\left(\frac{a\tau + b}{c\tau + d}\right) \quad \text{for} \quad \tau \in \mathcal{H}.$$

If m is a positive integer such that $m\alpha$ is an integral matrix, then by homogeneity,

$$j \circ m\alpha = j \circ \alpha.$$

So we can reduce our investigation of $j \circ \alpha$ to the case where α is an integral matrix. Obviously, if $\alpha \in \Gamma$, then $j \circ \alpha = j$ since the j-function is Γ-invariant. Note also that for any integral matrix α, we can always factor out the greatest common divisor of its components. So we can consider an integral α whose components are relatively prime, i.e., $\alpha \in W_n^*$.

Let $k = \#C_n$ and $\alpha_1, \alpha_2, \ldots, \alpha_k$ the representatives of the right cosets of W_n^* for Γ. It follows that the functions $j \circ \alpha_i$ are permuted transitively by the action of Γ. Here the action of Γ on a function f is given by $f \longmapsto f \circ \gamma$, for $\gamma \in \Gamma$.

We consider the polynomial

$$\Phi_n(X) = \prod_{i=1}^{k} (X - j \circ \alpha_i) = \sum_m s_m X^m,$$

whose coefficients $s_m = s_m(\tau)$ are the m-th elementary symmetric functions of the $j \circ \alpha_i$, $i = 1, 2, \ldots, k$.

Remark 2.3.14. The coefficients of $\Phi_n(X)$ are holomorphic on $\mathcal{H}$, and they satisfy the following properties (see [Sil94], pp. 144-146):

1. $s_m(\alpha\tau) = s_m(\tau)$ for all $\alpha \in \Gamma$ and $\tau \in \mathcal{H}$.

2. $s_m \in \mathbb{C}[j]$.

3. s_m has a Fourier expansion with coefficients in $\mathbb{Z}$.

4. $s_m(\tau) \in \mathbb{Z}[j]$.

It follows from Theorem 2.3.12 and the preceding remark that the coefficients of $\Phi_n(X)$ are polynomials in j with integer coefficients. So $\Phi_n(X)$ can be viewed as a polynomial in the variables X and j, and we write this as

$$\Phi_n(X) = \Phi_n(X, j) \in \mathbb{Z}[X, j].$$

This polynomial is called the *modular polynomial of order* n. Its properties are summarized as follows:

Theorem 2.3.15. *Let n be a positive integer.*

(i) The polynomial $\Phi_n(X, j)$ is irreducible over $\mathbb{C}(j)$, and has degree $\#C_n$.

(ii) $\Phi_n(X, j) = \Phi_n(j, X)$.

(iii) If n is not a square, then $\Phi_n(j, j)$ is a polynomial of degree > 1 and with leading coefficient ± 1.

(iv) If $n = p$ is a prime number, then the Kronecker congruence

$$\Phi_p(X, j) \equiv (X - j^p)(X^p - j) \pmod{p}$$

holds.

Proof. See [Lan87], Theorem 3 in Ch. 5 §2 for parts (i) – (iii) and pp. 57–58 for part (iv). □

Corollary 2.3.16. *Let $\alpha \in M_2^+(\mathbb{Z})$. Then the function $j \circ \alpha$ is integral over $\mathbb{Z}[j]$.*

Proof. See [Sil94, Theorem II.6.3(b)]. □

The next result establishes that the j-invariant is integral over $\mathbb{Z}$. See [Sil94, Corollary II.6.3.1] or [Lan87, Theorem 4, Ch. 5 §2] for a detailed proof.

Corollary 2.3.17. *If $E/\mathbb{C}$ is an elliptic curve with complex multiplication, then $j(E)$ is an algebraic integer.*

We now determine the relationship between modular polynomials and isogenies of elliptic curves. Let E and E' be elliptic curves over $\mathbb{C}$. Suppose Λ is a lattice in $\mathbb{C}$ with sublattice $\Lambda' \subset \Lambda$ such that $E \cong \mathbb{C}/\Lambda$ and $E' \cong \mathbb{C}/\Lambda'$. Then there exists an isogeny $\phi : E' \longrightarrow E$ and a commutative diagram

$$\begin{array}{ccc} \mathbb{C}/\Lambda' & \longrightarrow & \mathbb{C}/\Lambda \\ \downarrow & & \downarrow \\ E' & \xrightarrow{\phi} & E \end{array}$$

where the top map is the canonical homomorphism. It has the finite group Λ/Λ' as its kernel. Let $\Lambda = [1, \tau]$, so that $\Lambda' = [a\tau + b, c\tau + d]$ for some $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2^+(\mathbb{Z})$. Then $j(E) = j(\tau) = j(\Lambda)$ and $j(E') = j(\alpha\tau)$. In particular, $j(\alpha\tau)$ is a root of $\Phi_n(X, j(\tau)) \in \mathbb{Z}[X, j(\tau)]$. So evaluating functions at τ shows that for any particular value of $\tau \in \mathcal{H}$, the roots of the modular polynomial of order n are exactly the numbers

$$j(\alpha_i \tau), \qquad i = 1, 2, \ldots, \#C_n.$$

Now suppose we write the $\mathbb{Z}$-basis of a sublattice $\Lambda' \subset \Lambda$ in terms of the $\mathbb{Z}$-basis of Λ by using a matrix $\alpha \in M_2(\mathbb{Z})$. Using the elementary divisor theorem, it can be shown that the quotient Λ/Λ' is a cyclic group if and only if the entries of α are relatively prime. Hence sublattices of Λ with this property correspond to the isogenies with a cyclic kernel, whose index is given by $[\Lambda : \Lambda'] = \det(\alpha)$. Thus for any given $\tau \in \mathcal{H}$, the roots of the modular polynomial $\Phi_n(X, j(\tau))$ are precisely the j-invariants of all elliptic curves E' having a cyclic isogeny $\phi : E' \longrightarrow E$ of degree n. We now have the following result.

Theorem 2.3.18. *Let E and E' be elliptic curves over $\mathbb{C}$. Then there exists an isogeny $\phi : E' \longrightarrow E$ whose kernel is cyclic of degree n if and only if $j(E')$ is a root of the equation $\Phi_n(X, j(E)) = 0$.*

This result holds in any field of characteristic 0 by embedding such field into $\mathbb{C}$. As for characteristic p, this result also holds as long as p does not divide n (see [Igu59]).

2.3.4 Endomorphism Rings of Elliptic Curves over $\mathbb{C}$

Suppose Λ_1 and Λ_2 are lattices in $\mathbb{C}$ such that $\alpha\Lambda_1 \subset \Lambda_2$ for some $\alpha \in \mathbb{C}$. The multiplication-by-α map induces a well-defined holomorphic homomorphism

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2, \quad z \longmapsto \phi_\alpha(z) = \alpha z \pmod{\Lambda_2}.$$

The following result shows that the maps ϕ_α are the only holomorphic maps from $\mathbb{C}/\Lambda_1$ to $\mathbb{C}/\Lambda_2$. Let $M = \{\text{holomorphic maps } \phi : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2 \text{ with } \phi(0) = 0\}$.

Theorem 2.3.19.

(a) The association

$$\{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subset \Lambda_2\} \longrightarrow M, \quad \alpha \longmapsto \phi_\alpha$$

is a bijection.

(b) Let E_1 and E_2 be the elliptic curves corresponding to Λ_1 and Λ_2, respectively, as given in (2.8)*. Then the natural inclusion*

$$\{\textit{isogenies } \phi : E_1 \longrightarrow E_2\} \longrightarrow M$$

is a bijection.

Proof. See [Sil09, Theorem VI.4.1]. □

Now suppose E is an elliptic curve over $\mathbb{C}$. By using the preceding theorem, we can identify $\mathrm{End}(E)$ with a certain subring of $\mathbb{C}$. So if $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ as in (2.8), then

$$\mathrm{End}(E) \cong \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\}.$$

Recall that Λ is unique up to homothety, so this ring is independent of the choice of Λ. Via this description of $\mathrm{End}(E)$, the endomorphism rings that may occur for elliptic curves over $\mathbb{C}$ can be completely characterized. The following result gives such characterization of endomorphism rings.

Theorem 2.3.20. *Let $E/\mathbb{C}$ be an elliptic curve, and let $\Lambda = [\omega_1, \omega_2]$ be the lattice associated to E by* (2.8)*. Then one of the following holds.*

(a) $\mathrm{End}(E) \cong \mathbb{Z}$.

(b) Let $\tau = \omega_2/\omega_1$. The field $\mathbb{Q}(\tau)$ is an imaginary quadratic extension of $\mathbb{Q}$ and $\mathrm{End}(E)$ *is isomorphic to an order in $\mathbb{Q}(\tau)$.*

Proof. See [Sil09, VI.5.5]. □

Recall that $\Lambda = [\omega_1, \omega_2]$ is homothetic to $[1, \tau]$. If Theorem 2.3.20(b) holds, then τ is an algebraic number. So it is a root of some quadratic polynomial $ax^2 + bx + c$. We may choose $a, b, c \in \mathbb{Z}$ such that $a > 0$ and $\gcd(a, b, c) = 1$. Then $\mathbb{Q}(\tau) = \mathbb{Q}\left(\sqrt{b^2 - 4ac}\right)$. We have the following result (see [Gal99, Lemma A.5.3] or [Lan87, Theorem 1, Ch. 8 §1]).

Lemma 2.3.21. *Let $E/\mathbb{C}$ be isomorphic to $\mathbb{C}/[1, \tau]$ via* (2.8)*, where τ is a root of the quadratic polynomial $ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$, $a > 0$, and* $\gcd(a, b, c) = 1$. *Then* $\mathrm{End}(E)$ *is isomorphic to an order in $\mathbb{Q}(\tau)$ with discriminant $b^2 - 4ac$.*

Proof. See [Lan87, Theorem 1, Ch. 8 §1]. □

2.3.5 Reduction and Lifting of Elliptic Curves

We consider a connection between elliptic curves over $\mathbb{C}$ and those defined over some finite field $\mathbb{F}_p$. Deuring's theorems show that during reduction or lifting of a curve its endomorphism ring is preserved. Here the basic idea of reduction is as follows. Suppose E is an elliptic curve defined by (2.1) over a number field K. Let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_K$. We

introduce a change of variables (see (2.4)) to obtain a *minimal Weierstrass equation* for E. Note that every elliptic curve E/K has a unique minimal Weierstrass equation ([Sil09, Proposition VII.1.3]). We reduce this minimal Weierstrass equation modulo $\mathfrak{P}$ to obtain an elliptic curve $\overline{E}$ over $\mathcal{O}_K/\mathfrak{P}$ defined by

$$\overline{E} : y^2 + \overline{a}_1 xy + \overline{a}_3 y = x^3 + \overline{a}_2 x^2 + \overline{a}_4 x + \overline{a}_6,$$

with resulting discriminant $\overline{\Delta}$. In this case $\overline{E}$ is called the *reduction* of E modulo $\mathfrak{P}$. If $\overline{\Delta} \neq 0$ in $\mathcal{O}_K/\mathfrak{P}$, then E is said to have *good reduction modulo* $\mathfrak{P}$.

In what follows, we let $\mathcal{O}$ be an order in an imaginary quadratic field K. Let L be the ring class field of $\mathcal{O}$, i.e., $L = K(j(\mathfrak{a}))$, where $\mathfrak{a}$ is a proper fractional $\mathcal{O}$-ideal (see [Cox89, Theorem 11.1]). The following result arises from Deuring's theorems.

Theorem 2.3.22. *Let $\mathcal{O}$, K and L be as above. Let $p \in \mathbb{Z}$ be a prime that splits completely in L and $\mathfrak{P}$ a prime ideal of L lying above p. Let E be an elliptic curve over L with $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$. If E has good reduction modulo $\mathfrak{P}$, then there exists $\pi \in \mathcal{O}$ such that $p = \pi\overline{\pi}$ and*

$$\#E(\mathbb{F}_p) = p + 1 - (\pi + \overline{\pi}).$$

Furthermore, if $\overline{E}$ is the reduction of E modulo $\mathfrak{P}$, then $\mathrm{End}_{\overline{\mathbb{F}}_p}(\overline{E}) = \mathcal{O}$ and every elliptic curve over $\mathbb{F}_p$ with endomorphism ring (over $\overline{\mathbb{F}}_p$) equal to $\mathcal{O}$ arises in this way.

Proof. See [Cox89, Theorem 14.16]. □

2.4 Kohel's Theorem and Isogeny Volcanoes

Isogenies comprise the endomorphism ring of an elliptic curve, see Definition 2.1.4 and Section 2.2. This section is devoted to graphs, known as *isogeny volcanoes*, that arise from isogenies between ordinary elliptic curves. We revisit Kohel's result regarding the classification of ℓ-isogenies of such curves. Then we review some basic properties of isogeny volcanoes

for elliptic curves. We will prove the counterparts of the results presented here in the Drinfeld module case in Chapter 7.

2.4.1 Kohel's Theorem

Let $E/\mathbb{F}_q$ be an ordinary elliptic curve, where $\text{char}(\mathbb{F}_q) = p$. Let $\mathcal{O}_E := \text{End}(E)$. Recall that $\mathcal{O}_E$ is always strictly larger than $\mathbb{Z}$ because the q-th power Frobenius endomorphism π is in $\mathcal{O}_E$. So the orders $\mathbb{Z}[\pi]$ and $\mathcal{O}_E$ satisfy the relation

$$\mathbb{Z} \neq \mathbb{Z}[\pi] \subseteq \mathcal{O}_E.$$

Suppose t is the trace of π. Recall from Theorem 2.2.4 that π satisfies

$$\pi^2 - t\pi + q = 0$$

in $\mathcal{O}_E$. So the discriminant of $\mathbb{Z}[\pi]$ is

$$D_\pi = t^2 - 4q, \tag{2.15}$$

and $\mathbb{Z}[\pi]$ embeds in the imaginary quadratic field $K := \mathbb{Q}\left(\sqrt{t^2 - 4q}\right)$ (see Theorem 2.2.5) which contains the order $\mathcal{O}_E$ since E is an ordinary elliptic curve. Let $\mathcal{O}_K$ be the ring of integers of K. Then the relation of the orders $\mathbb{Z}[\pi]$, $\mathcal{O}_E$, and $\mathcal{O}_K$ in K is given by

$$\mathbb{Z}[\pi] \subseteq \mathcal{O}_E \subseteq \mathcal{O}_K, \tag{2.16}$$

where the last inclusion holds since $\mathcal{O}_E$ is an order in K and $\mathcal{O}_K$ is the maximal order in K. Note that $\mathcal{O}_K$ can be written as $\mathcal{O}_K = [1, \omega_K]$, where

$$\omega_K = \frac{D_K + \sqrt{D_K}}{2}$$

and D_K is the discriminant of K. (See [Cox89], p. 103.) The *conductor* of $\mathcal{O}_E$, denoted f_E, in K is the index of $\mathcal{O}_E$ in $\mathcal{O}_K$; that is, $f_E = [\mathcal{O}_K : \mathcal{O}_E]$. It follows that $\mathcal{O}_E$ can be written as

$$\mathcal{O}_E = \mathbb{Z} + f_E\mathcal{O}_K = [1, f_E\omega_K].$$

See [Cox89, Lemma 7.2]. The discriminant of $\mathcal{O}_E$ is the integer

$$D_E := f_E^2 D_K$$

(see, for example, [Cox89], p. 133). In particular, if $f_\pi := [\mathcal{O}_K : \mathbb{Z}[\pi]]$, then the discriminant D_π of $\mathbb{Z}[\pi]$ can also be written as

$$D_\pi =: f_\pi^2 D_K. \tag{2.17}$$

We use properties of endomorphism rings to classify ℓ-isogenies between ordinary elliptic curves. In particular, since these endomorphism rings are orders in an imaginary quadratic field, we can use their conductors to classify isogenies of elliptic curves of degree ℓ. Consider the diagram given in Figure 2.1 showing the relationship of the conductors f_π, f_E and f_π/f_E. Knowing two of these conductors allows us to find the third one (see [Fou01, Lemma 5.1.1], or [Koh96], pp. 39-40).

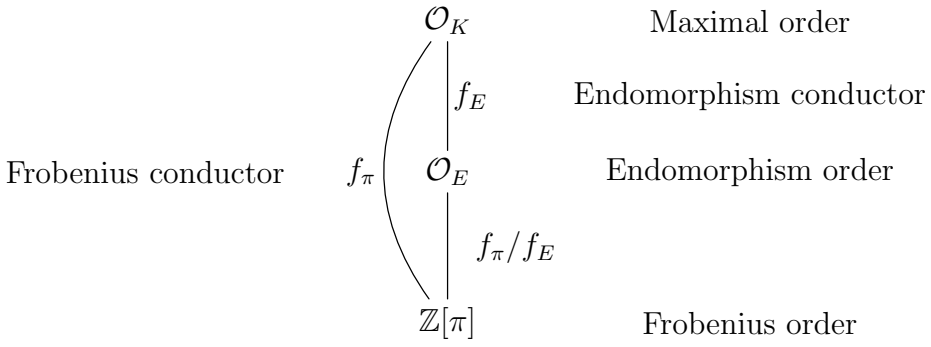


Figure 2.1: Relationship of the conductors f_π, f_E, and f_π/f_E

Consider the conductor of $\mathcal{O}_E$. Note that f_E divides f_π. If $f_\pi = 1$, then (2.16) becomes an equality of sets, and so the endomorphism ring of E must be the full ring of integers of K. Suppose this is not the case, i.e., $f_\pi > 1$. Let $f_\pi = \prod_{i=1}^{s} \ell_i^{e_i}$, where the ℓ_i are distinct primes and the e_i are positive integers for $1 \leq i \leq s$, then f_E must be of the form

$$f_E = \prod_{i=1}^{s} \ell_i^{d_i}$$

with $0 \leq d_i \leq e_i$ for $1 \leq i \leq s$. We can determine f_E by computing its ℓ_i-adic valuations; that is, to determine the value of d_i for all $1 \leq i \leq s$. As this is done independently for

each ℓ_i, we can work on a particular prime ℓ dividing f_π. So supposing ℓ^e exactly divides f_π, we need to find the largest exponent d such that ℓ^d divides f_E. Our main interest here is to determine this power via a method using modular polynomials. We exploit the fact that modular polynomials give a parametrization of pairs of elliptic curves with an ℓ-isogeny between them. The method presented here uses the relationship between two ℓ-isogenous elliptic curves, say E and E', and their corresponding endomorphism rings. Let $\mathcal{O}_E := \mathrm{End}(E)$ and $\mathcal{O}_{E'} := \mathrm{End}(E')$.

Lemma 2.4.1 ([Koh96])**.** *Let $\phi : E \longrightarrow E'$ be an ℓ-isogeny of elliptic curves. Then exactly one of the following holds:*

(a) $[\mathcal{O}_E : \mathcal{O}_{E'}] = \ell$*, in which case* $\mathcal{O}_{E'} \subset \mathcal{O}_E$*,*

(b) $[\mathcal{O}_{E'} : \mathcal{O}_E] = \ell$*, in which case* $\mathcal{O}_E \subset \mathcal{O}_{E'}$*,*

(c) $\mathcal{O}_E = \mathcal{O}_{E'}$*.*

Proof. See [Koh96, Proposition 21]. □

Remark 2.4.2. In this lemma we treat the endomorphism rings as orders in an imaginary quadratic field. So it makes sense to consider containment of one order in the other. In fact, the set of orders $\mathcal{O} \subseteq \mathcal{O}_K$ forms a partially ordered set under the ordering of containment.

Definition 2.4.3. Let $\phi : E \longrightarrow E'$ be an ℓ-isogeny of elliptic curves. We say that ϕ is

1. *ascending* ($\uparrow$) if $[\mathcal{O}_{E'} : \mathcal{O}_E] = \ell$.
2. *horizontal* ($\rightarrow$) if $\mathcal{O}_E = \mathcal{O}_{E'}$.
3. *descending* ($\downarrow$) if $[\mathcal{O}_E : \mathcal{O}_{E'}] = \ell$.

The next theorem we present here is the main result of Kohel (see [Koh96, Proposition 23]) which makes it possible to compute endomorphism rings of ordinary elliptic curves over $\mathbb{F}_q$.

Theorem 2.4.4 (Kohel)**.** *Let E be an ordinary elliptic curve defined over $\mathbb{F}_q$ whose endomorphism ring $\mathcal{O}_E$ is an order of discriminant D_E in an imaginary quadratic field K, let $\ell \in \mathbb{Z}$ be a prime different from $p = char(\mathbb{F}_q)$, and let $\left(\frac{D_E}{\ell}\right)$ be the Kronecker symbol.*

1. *If $\ell \nmid [\mathcal{O}_K : \mathcal{O}_E]$, then E has $1 + \left(\frac{D_E}{\ell}\right)$ horizontal ℓ-isogenies.*
2. *If $\ell \mid [\mathcal{O}_K : \mathcal{O}_E]$, then E has one ascending ℓ-isogeny.*
3. *If $\ell \nmid [\mathcal{O}_E : \mathbb{Z}[\pi]]$, then E has no descending ℓ-isogeny.*
4. *If $\ell \nmid [\mathcal{O}_K : \mathcal{O}_E]$ and $\ell \mid [\mathcal{O}_E : \mathbb{Z}[\pi]]$, then E has $\ell - \left(\frac{D_E}{\ell}\right)$ descending ℓ-isogenies.*
5. *If $\ell \mid [\mathcal{O}_K : \mathcal{O}_E]$ and $\ell \mid [\mathcal{O}_E : \mathbb{Z}[\pi]]$, then E has ℓ descending ℓ-isogenies.*

Proof. See [Koh96, Proposition 23], [Fou01, Theorem 5.3.1], or [Gal99, Theorem A.5.4]. □

Remark 2.4.5. Note that Theorem 2.4.4 contains a converse. In particular, it is obvious that if E has an ascending ℓ-isogeny, then $\ell \mid [\mathcal{O}_K : \mathcal{O}_E]$. It is also clear that if E has a descending ℓ-isogeny, then $\ell \mid [\mathcal{O}_E : \mathbb{Z}[\pi]]$.

The results from Theorem 2.4.4 are summarized in Table 2.1 below. If ℓ does not divide $[\mathcal{O}_K : \mathcal{O}_E] = f_E$, then

$$\left(\frac{D_E}{\ell}\right) = \left(\frac{f_E^2 D_K}{\ell}\right) = \left(\frac{D_K}{\ell}\right).$$

So we use $\left(\frac{D_K}{\ell}\right)$ in Table 2.1.

2.4.2 Isogeny Volcanoes of Elliptic Curves

Let ℓ be a prime distinct from $p = \text{char}(\mathbb{F}_q)$. We consider graphs of ℓ-isogenies of elliptic curves. The *ℓ-isogeny graph* of elliptic curves over $\mathbb{F}_q$, denoted $G_\ell(\mathbb{F}_q)$, is a graph whose vertex set is $\mathbb{F}_q$ and edges (j_1, j_2) are present whenever $\Phi_\ell(j_1, j_2) = 0$ and with multiplicity equal to the multiplicity of j_2 as a root of $\Phi_\ell(j_1, Y)$, where $j_1, j_2 \in \mathbb{F}_q$ (see [Sut13]). So, depending on the multiplicity of j_2 as a root of $\Phi_\ell(j_1, Y)$, an ℓ-isogeny graph may contain loops or multiple edges. Note that for any fixed field $\mathbb{F}_q$, the graphs $G_\ell(\mathbb{F}_q)$ all have vertex

$\left(\frac{D_K}{\ell}\right)$	Case		Number of Isogenies			
			$\rightarrow$	$\uparrow$	$\downarrow$	Total
0	$\ell \nmid [\mathcal{O}_K : \mathcal{O}_E]$	$\ell \nmid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	1	0	0	1
		$\ell \mid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	1	0	ℓ	$\ell+1$
	$\ell \mid [\mathcal{O}_K : \mathcal{O}_E]$	$\ell \nmid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	0	1	0	1
		$\ell \mid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	0	1	ℓ	$\ell+1$
1	$\ell \nmid [\mathcal{O}_K : \mathcal{O}_E]$	$\ell \nmid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	2	0	0	2
		$\ell \mid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	2	0	$\ell-1$	$\ell+1$
	$\ell \mid [\mathcal{O}_K : \mathcal{O}_E]$	$\ell \nmid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	0	1	0	1
		$\ell \mid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	0	1	ℓ	$\ell+1$
-1	$\ell \nmid [\mathcal{O}_K : \mathcal{O}_E]$	$\ell \nmid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	0	0	0	0
		$\ell \mid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	0	0	$\ell+1$	$\ell+1$
	$\ell \mid [\mathcal{O}_K : \mathcal{O}_E]$	$\ell \nmid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	0	1	0	1
		$\ell \mid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	0	1	ℓ	$\ell+1$

Table 2.1: Number and type of ℓ-isogenies based on $\left(\frac{D_K}{\ell}\right)$, $[\mathcal{O}_K : \mathcal{O}_E]$ and $[\mathcal{O}_E : \mathbb{Z}[\pi]]$

set $\mathbb{F}_q$, but their edge sets vary, depending on ℓ. Moreover, due to the existence of dual isogenies, we treat (j_1, j_2) as the same edge (j_2, j_1). So the resulting graphs are undirected graphs.

Let E be an ordinary elliptic curve over $\mathbb{F}_q$ with q-th power Frobenius endomorphism π and j-invariant $j(E) \neq 0, 1728$. We exclude the elliptic curves with j-invariants $j = 0, 1728$ because they have extra automorphisms (see [Sil09, Theorem III.10.1]), which makes it difficult to distinguish the curves that are isogenous to E over $\mathbb{F}_q$ from those that are isogenous to E only over an algebraic closure of $\mathbb{F}_q$.

We know that $\mathcal{O}_E = \mathrm{End}(E)$ is an order in an imaginary quadratic field K. Let t be the trace of π. From (2.16), we see that $[\mathcal{O}_K : \mathcal{O}_E]$ divides $[\mathcal{O}_K : \mathbb{Z}[\pi]]$. This is also the case for any ordinary elliptic curve $E'/\mathbb{F}_q$ with Frobenius trace t, i.e., $[\mathcal{O}_K : \mathcal{O}_{E'}]$ divides $[\mathcal{O}_K : \mathbb{Z}[\pi]]$. We define

$$\mathrm{Ell}_t(\mathbb{F}_q) = \{j(E) \mid E/\mathbb{F}_q \text{ has trace of Frobenius } t\},$$

to be the set of $\overline{\mathbb{F}}_q$-isomorphism classes of elliptic curves E over $\mathbb{F}_q$ with trace of Frobenius t. Note that two elliptic curves over $\mathbb{F}_q$ are $\mathbb{F}_q$-isogenous if and only if they have the same trace of

Frobenius [Hus04, Theorem 13.8.4]. So this set corresponds to an $\mathbb{F}_q$-isogeny class. However, due to the existence of quadratic twists of elliptic curves, the equality $\mathrm{Ell}_t(\mathbb{F}_q) = \mathrm{Ell}_{-t}(\mathbb{F}_q)$ also holds. Here, a quadratic twist of an elliptic curve E of trace t has the same j-invariant as E and trace $-t$.

Let E' be another ordinary elliptic curve over $\mathbb{F}_q$ and $\mathrm{End}(E') = \mathcal{O}_{E'}$ with $j(E') \neq 0, 1728$. As we have seen in Section 2.4.1, if $\phi : E \longrightarrow E'$ is an ℓ-isogeny, then the index of one order in the other divides ℓ. This isogeny can be classified accordingly as ascending, descending, or horizontal. The set of elliptic curves over $\mathbb{F}_q$ with the same trace of Frobenius $\pm t$ can be represented as an undirected graph, whose vertices are the j-invariants (or the isomorphism classes) of elliptic curves and whose edges represent the ℓ-isogenies between curves at two vertices. This resulting graph is a connected component of $G_\ell(\mathbb{F}_q)$ whose shape depends on the number of solutions of the modular polynomial $\Phi_\ell(j(E), Y)$. Our main focus here is to describe the connected components of $G_\ell(\mathbb{F}_q)$ containing j-invariants $j \neq 0, 1728$ of ordinary elliptic curves only, and refer to [Fou01], [Koh96], and [Sut13]. We refer to these components as *ordinary components* of $G_\ell(\mathbb{F}_q)$.

Suppose $\phi : E \longrightarrow E'$ is an ℓ-isogeny of ordinary elliptic curves with dual $\widehat{\phi} : E' \longrightarrow E$. We describe a connected component of $G_\ell(\mathbb{F}_q)$ containing $j(E)$ and $j(E')$ using the relationship of the orders $\mathbb{Z}[\pi]$, $\mathcal{O}_E$, $\mathcal{O}_{E'}$, and $\mathcal{O}_K$ with respect to ℓ. We say that an order $\mathcal{O} \subseteq \mathcal{O}_K$ is *ℓ-maximal* if $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$.

Note that ϕ is horizontal (resp. ascending) if and only if $\widehat{\phi}$ is horizontal (resp. descending), see [Fou01, Lemma 6.1.1]. A horizontal ℓ-isogeny $\phi : E \longrightarrow E'$ results from the action of an invertible $\mathcal{O}_E$-ideal $\mathfrak{l}$ of norm ℓ on j-invariants of elliptic curves. This ideal is the ideal which contains endomorphisms $\alpha \in \mathcal{O}_E$ whose kernels contain the kernel of ϕ. If ℓ divides $[\mathcal{O}_K : \mathcal{O}_E]$, then no such ideals exist. The number of invertible $\mathcal{O}_E$-ideals of norm ℓ that give

rise to horizontal ℓ-isogenies is

$$1 + \left(\frac{D_K}{\ell}\right) = \begin{cases} 0 & \text{if } \ell \text{ is inert in } \mathcal{O}_K \\ 1 & \text{if } \ell \text{ is ramified in } \mathcal{O}_K \\ 2 & \text{if } \ell \text{ splits in } \mathcal{O}_K \end{cases}$$

(see [Sut13], for example). This is also shown in Table 2.1.

Remark 2.4.6. If ℓ splits in K, then $(\ell) = \mathfrak{l} \cdot \bar{\mathfrak{l}}$, and the $\mathfrak{l}$-orbits partition $\mathrm{Ell}_{\mathcal{O}_E}(\mathbb{F}_q)$ into cycles corresponding to the cosets of the ideal $\langle [\mathfrak{l}] \rangle$ in the class group $\mathcal{C}l(\mathcal{O}_E)$. If $\mathfrak{l}$ is principal, then the ideal class $[\mathfrak{l}]$ is trivial, and hence leads to loops in $G_\ell(\mathbb{F}_q)$. It is also possible to have the equality $[\mathfrak{l}] = [\bar{\mathfrak{l}}]$ even if $\mathfrak{l} \neq \bar{\mathfrak{l}}$. This, in turn, leads to double edges in $G_\ell(\mathbb{F}_q)$. (See [Sut13].)

Now consider the order $\mathbb{Z}[\pi]$. From the relationship given in (2.16), we see that $\mathbb{Z}[\pi]$ may or may not be ℓ-maximal. Suppose this order is ℓ-maximal. Then $\mathcal{O}_E$ is also ℓ-maximal. This implies that

$$\ell \nmid [\mathcal{O}_K : \mathcal{O}_E] \quad \text{and} \quad \ell \nmid [\mathcal{O}_E : \mathbb{Z}[\pi]].$$

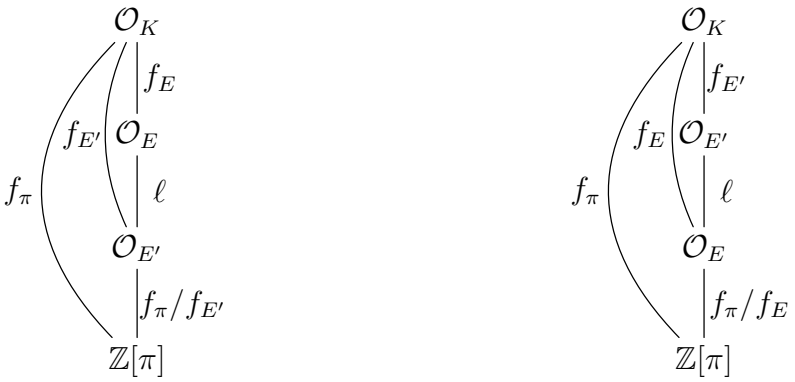
By Table 2.1, we see that if E has an ℓ-isogeny, then it is horizontal. See [Fou01, Lemma 6.1.2].

Now, if $\mathbb{Z}[\pi]$ is not ℓ-maximal and E is ℓ-isogenous to another curve E', then two cases arise from this situation, see Figure 2.2 below. From these diagrams, we obtain information regarding the highest power of ℓ that divides f_E or $f_{E'}$. In the first case, for example, suppose that $\nu_\ell(f_\pi) = n$ and $\nu_\ell(f_E) = r$, then $\nu_\ell(f_{E'}) = r + 1$ and $\nu_\ell(f_\pi / f_{E'}) = n - (r + 1)$.

Definition 2.4.7. The *level* of an elliptic curve E (or a j-invariant $j(E)$) in a connected component of an ℓ-isogeny graph is the ℓ-adic valuation $\nu_\ell(f_E)$ of the conductor f_E of $\mathcal{O}_E$.

Lemma 2.4.8 ([Fou01], Lemma 6.1.3)**.** *If $\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$ and $\ell \nmid [\mathcal{O}_E : \mathbb{Z}[\pi]]$, then the unique ℓ-isogeny $\phi : E \longrightarrow E'$ of E in Table 2.1 is such that $\ell \mid [\mathcal{O}_{E'} : \mathbb{Z}[\pi]]$; that is, $\nu_\ell(f_{E'}) = n - 1$ for $n \geq 1$ such that $\nu_\ell(f_\pi) = n$.*

In the next lemma, let $\mathcal{O}_{E_i} = \mathrm{End}(E_i)$ and $[\mathcal{O}_K : \mathcal{O}_{E_i}] = f_{E_i}$ for $i = 1, 2, 3$.



(a) $[\mathcal{O}_E : \mathcal{O}_{E'}] = \ell$ (b) $[\mathcal{O}_{E'} : \mathcal{O}_E] = \ell$

Figure 2.2: The orders $\mathcal{O}_E$, $\mathcal{O}_{E'}$, and $\mathbb{Z}[\pi]$ and their conductors in K

Lemma 2.4.9 ([Fou01], Lemma 6.1.4)**.** *Let $\alpha : E_1 \longrightarrow E_2$ be a descending ℓ-isogeny. If $\ell \mid [\mathcal{O}_{E_2} : \mathbb{Z}[\pi]]$, then for any ℓ-isogeny $\beta : E_2 \longrightarrow E_3$ such that $\mathcal{O}_{E_3} \ncong \mathcal{O}_{E_1}$, β is a descending ℓ-isogeny. In addition, there are ℓ isogenies β of this type.*

For the next result, we continue to assume that $\mathbb{Z}[\pi]$ is not ℓ-maximal.

Lemma 2.4.10. *[Fou01, Lemma 6.1.5] If there exist two ℓ-isogenies of an elliptic curve E to another curve E', different up to isomorphism, then these are both horizontal ℓ-isogenies. Furthermore, ℓ splits in $\mathcal{O}_E$.*

These lemmas give us an idea of the graph of ℓ-isogenies of elliptic curves sharing the same Frobenius trace $\pm t$. This connected component of $G_\ell(\mathbb{F}_q)$ resembles the structure of a *volcano*. The crater comes from horizontal ℓ-isogenies which can be obtained when $\mathcal{O}_E$ is ℓ-maximal, see Table 2.1. The rest of the structure of a connected component of an ℓ-isogeny graph is obtained when $\mathcal{O}_E$ is not ℓ-maximal, see Lemmas 2.4.8 and 2.4.9. We provide a graph-theoretic definition of a volcano.

Definition 2.4.11. A *volcano* is a pair (G, C), where G is a connected graph with at most one cycle, C is a regular graph of degree at most two, $C \subset G$, and $G - C$ is a forest. The subgraph C of a volcano is called its *crater* and a connected component of a volcano excluding the edges on the crater is called a *side*.

Remark 2.4.12. From the preceding definition, we see that each side of a volcano is a tree in the graph-theoretic sense.

The structure of an ℓ-isogeny volcano can be explored further by relating the results from Theorem 2.4.4 to the number of roots, denoted $\mathcal{N}_\ell(E)$, of the modular polynomial $\Phi_\ell(j(E), Y)$ over $\mathbb{F}_q$. This relationship is summarized in Table 2.2 (see [Fou01], Table 6.2). By using this table we get the other parts of an isogeny volcano.

$\mathcal{N}_\ell(E)$	**Type**	**Case**	$\left(\frac{D_E}{\ell}\right)$	$\left(\frac{D_\pi}{\ell}\right)$
0	none	$\ell \nmid [\mathcal{O}_K : \mathcal{O}_E]$ and $\ell \nmid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	-1	-1
2	$\rightarrow$	$\ell \nmid [\mathcal{O}_K : \mathcal{O}_E]$ and $\ell \nmid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	$+1$	$+1$
1	$\rightarrow$	$\ell \nmid [\mathcal{O}_K : \mathcal{O}_E]$ and $\ell \nmid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	0	0
	$\uparrow$	$\ell \mid [\mathcal{O}_K : \mathcal{O}_E]$ and $\ell \nmid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	0	0
$\ell+1$	$1+\left(\frac{D_E}{\ell}\right)$ $\rightarrow$ $\ell-\left(\frac{D_E}{\ell}\right)$ $\downarrow$	$\ell \nmid [\mathcal{O}_K : \mathcal{O}_E]$ and $\ell \mid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	unknown	0
	1 $\uparrow$ ℓ $\downarrow$	$\ell \mid [\mathcal{O}_K : \mathcal{O}_E]$ and $\ell \mid [\mathcal{O}_E : \mathbb{Z}[\pi]]$	0	0

Table 2.2: Properties of $\mathcal{O}_E$ based on the number and type of ℓ-isogenies of E

Definition 2.4.13. The *height*, n, of a volcano is the ℓ-adic valuation of the conductor of $\mathbb{Z}[\pi]$. All curves at level n comprise the *floor* of the volcano.

In the graph-theoretic sense, the height of a tree is the number of edges of the longest path from a root to a leaf of the tree. Definition 2.4.13 agrees with the graph-theoretic notion of the height of a tree. This definition entails that we have to compare $\mathbb{Z}[\pi]$ with $\mathcal{O}_K$ to determine the crater and the floor of an ℓ-isogeny volcano. We can determine whether or not a vertex j is on the floor of a volcano. This is done by counting the outgoing edges from j, which is the number of roots of $\Phi_\ell(j, Y)$ in $\mathbb{F}_q$ counted with multiplicity. If $n = 0$, then the volcano is a regular graph of degree at most 2. It follows that j also has degree at most 2. If $n > 0$, then $\ell \mid [\mathcal{O}_K : \mathcal{O}_E]$ and we see from Table 2.1 that j is either of degree 1 or $\ell + 1$. If j is on the floor of the volcano, then it can only admit an ascending isogeny. So it must be of degree 1.

Suppose an elliptic curve E is in an isogeny volcano G of height $n \geq 1$. If E is on the crater of G, then this can result into three different cases as depicted in Figure 2.3. As we can see from this figure, every horizontal isogeny in G is at level 0. If E is on the side of the volcano, then we have the case shown in Figure 2.4.

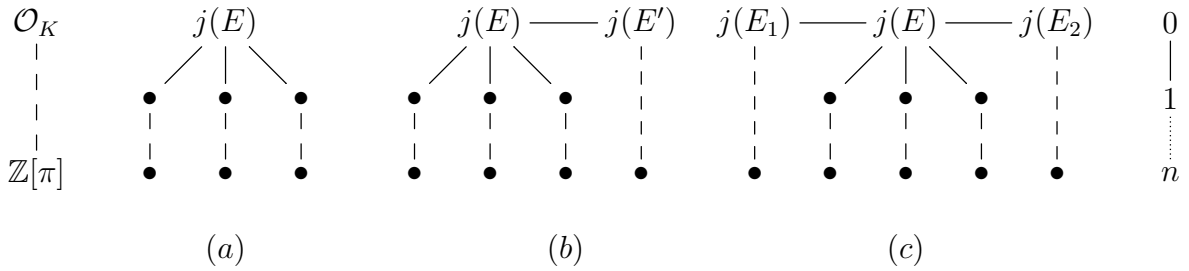


Figure 2.3: Curves such that $\ell \nmid [\mathcal{O}_K : \mathcal{O}_E]$ and $\ell \mid [\mathcal{O}_E : \mathbb{Z}[\pi]]$

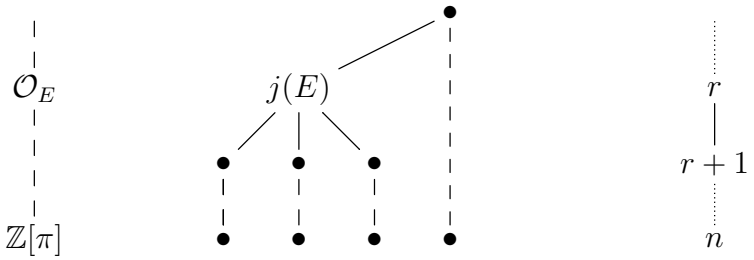


Figure 2.4: Curves such that $\ell \mid [\mathcal{O}_K : \mathcal{O}_E]$ and $\ell \mid [\mathcal{O}_E : \mathbb{Z}[\pi]]$

In the next lemma, we assume that $\mathbb{Z}[\pi]$ is not ℓ-maximal.

Lemma 2.4.14. *If ℓ splits (respectively, ramifies, or is inert) in $\mathcal{O}_K$, then every vertex in the crater of a volcano admits $\ell - 1$ (respectively, ℓ, or $\ell + 1$) descending ℓ-isogenies.*

Lemma 2.4.15. *All descending ℓ-isogenies in a volcano of height $n > 0$ have pairwise distinct targets.*

Remark 2.4.16. The sides of an isogeny volcano are rooted trees. So the level of a vertex in a rooted tree coincides with the level of an elliptic curve in an isogeny volcano.

One of the important properties of an isogeny volcano is given in the next theorem. We give a detailed proof of this result in Chapter 7. Here, we use the following convention for counting degrees of vertices in a volcano:

1. a single edge connecting two vertices counts as 1 toward the degree,

2. a double edge connecting two vertices counts as 2 toward the degree, and

3. any loop counts as 1 toward the degree.

Theorem 2.4.17. *Let $G_\ell(\mathbb{F}_q)$ be the ℓ-isogeny graph of elliptic curves over $\mathbb{F}_q$ and E an ordinary elliptic curve over $\mathbb{F}_q$ with $j(E) \neq 0, 1728$. Then the connected component G of $G_\ell(\mathbb{F}_q)$ containing $j(E)$ with horizontal subgraph H is a volcano (G, H), all of whose sides are complete trees with internal vertices all of degree $\ell + 1$.*

Finally, we can traverse a volcano by creating paths from a vertex. These paths can be used to locate an elliptic curve in an isogeny volcano. For the next results, assume that $j(E)$ is at level r for $r \in \mathbb{N}$ (see Figure 2.4).

Definition 2.4.18. A *descending path* of an elliptic curve E is a series of isogenies

$$j(E) = j(E_0) \longrightarrow j(E_1) \longrightarrow j(E_2) \longrightarrow \cdots \longrightarrow j(E_{m-1}) \longrightarrow j(E_m),$$

where each $j(E_i) \longrightarrow j(E_{i+1})$ for $i \in \{0, 1, \ldots, m-1\}$ is a descending ℓ-isogeny and $\ell \nmid [\mathcal{O}_{E_m} : \mathbb{Z}[\pi]]$. We call this path a *complete descending path* if the endomorphism ring $\mathcal{O}_{E_0}$ of E_0 is ℓ-maximal.

Lemma 2.4.19 ([Fou01], Lemma 6.2.1)**.** *We use the same notations as in Definition 2.4.18. If $j(E)$ is at level r, then $j(E_i)$ is at level $r + i$.*

Lemma 2.4.20 ([Fou01], Lemma 6.2.2)**.** *Let the height of the volcano containing $j(E)$ be equal to n, P a descending path starting from $j(E)$, and $m = length(P)$. Then $j(E)$ is at level $n - m$.*

Definition 2.4.21. An *ascending path* of an elliptic curve E is a path of elliptic curves

$$j(E) = j(E_0) \longrightarrow j(E_{-1}) \longrightarrow j(E_{-2}) \longrightarrow \cdots \longrightarrow j(E_{-(s-1)}) \longrightarrow j(E_{-s}),$$

where each $j(E_{-i}) \longrightarrow j(E_{-(i+1)})$ for $i \in \{0, 1, \ldots, s-1\}$ is an ascending ℓ-isogeny and $\mathcal{O}_{E_{-s}}$ is maximal with respect to ℓ. This path is called a *complete ascending path* if $\mathrm{End}(E) \simeq \mathbb{Z}[\pi]$ with respect to ℓ.

Lemma 2.4.22 ([Fou01], Lemma 6.2.4)**.** *We use the same notations as in Definition 2.4.21. If $j(E)$ is at level r, then $j(E_{-i})$ is at level $r - i$.*

Corollary 2.4.23. *If the length of the ascending path starting from $j(E)$ is $r+1$, then $j(E)$ is at level $r + 1$.*

Chapter 3

Function Field Preliminaries

This chapter deals with the necessary background material regarding function fields. We present an exposition of some preliminary number theoretic properties of polynomials rings over finite fields and quadratic extensions of function fields. Then we give the class number formula for orders in an imaginary quadratic function field.

3.1 Polynomial Rings over Finite Fields

The material presented in this section can be found in [Ros02] (Chapters 1 and 3). In all that follows we use the standard notation $\mathbf{A}$ to denote the polynomial ring $\mathbb{F}_q[T]$ over the finite field $\mathbb{F}_q$, where $q = p^s$ for some prime $p \in \mathbb{Z}$. Any element $a \in \mathbf{A}$ can be written in the form

$$a = a_0 + a_1 T + \cdots + a_{n-1} T^{n-1} + a_n T^n, \qquad a_i \in \mathbb{F}_q.$$

If $a_n \neq 0$, then a is of degree n. We write this as $\deg_T(a) = n$. Let $\operatorname{sgn}(a) := a_n$ with $a_n \in \mathbb{F}_q^*$. For our purposes, we define the sign of the zero polynomial as zero and its degree as $-\infty$. If $a_n = 1$, then a is said to be *monic*. Monic polynomials in $\mathbf{A}$ play the role of positive integers in $\mathbb{Z}$. The polynomial ring $\mathbf{A}$ has properties similar to those of $\mathbb{Z}$.

Proposition 3.1.1. *Let $a, b \in \mathbf{A}$ with $b \neq 0$. Then there exist unique elements $w, r \in \mathbf{A}$ such that $a = bw + r$ with $r = 0$ or $\deg_T(r) < \deg_T(b)$.*

Proof. See [Ros02, Proposition 1.1]. □

This means that there exists a division algorithm in $\mathbf{A}$. As a consequence, we see that $\mathbf{A}$ is a Euclidean domain. Thus it is a principal ideal domain and a unique factorization domain as well.

Proposition 3.1.2. *For a nonzero $a \in \mathbf{A}$, the ring $\mathbf{A}/a\mathbf{A}$ is finite with $q^{\deg_T(a)}$ elements.*

Proof. See [Ros02, Proposition 1.2]. □

Definition 3.1.3. Let $a \in \mathbf{A}$. The *absolute value* of a is given by

$$|a| := \begin{cases} q^{\deg_T(a)}, & \text{if } a \neq 0 \\ 0, & \text{if } a = 0. \end{cases}$$

This absolute value gives a way of measuring elements of $\mathbf{A}$. Note that for $a, b \in \mathbf{A}$, the absolute value satisfies the following properties:

(i) $|ab| = |a||b|$, and

(ii) $|a + b| \leq \max(|a|, |b|)$, where equality holds if $|a| \neq |b|$ or if $|a| = |b|$ and $\text{sgn}(a) \neq -\text{sgn}(b)$.

$\mathbf{A}$ also has a finite number of units, see [Ros02, Proposition 1.3].

Proposition 3.1.4. *The group of units of $\mathbf{A}$, denoted $\mathbf{A}^*$, is $\mathbb{F}_q^*$. In particular, $\mathbf{A}^*$ is cyclic with $q - 1$ elements.*

A polynomial $a \in \mathbf{A}$ is called *irreducible* if it cannot be expressed as a product of two polynomials in $\mathbf{A}$, each of positive degree. Since $\mathbf{A}$ is a principal ideal domain, a polynomial in $\mathbf{A}$ is irreducible if and only if it is prime. Another consequence of $\mathbf{A}$ being a principal ideal domain is the validity of the Chinese Remainder Theorem in $\mathbf{A}$.

Proposition 3.1.5. *Let $m_1, m_2, \ldots, m_t \in \mathbf{A}$, with $\gcd(m_i, m_j) = 1$ for $i \neq j$. Let $m = \prod_{i=1}^{t} m_i$ and π_i be the natural homomorphism from $\mathbf{A}/m\mathbf{A}$ to $\mathbf{A}/m_i\mathbf{A}$. Then the map*

$$\begin{array}{ccc} \pi : \mathbf{A}/m\mathbf{A} & \longrightarrow & \mathbf{A}/m_1\mathbf{A} \oplus \mathbf{A}/m_2\mathbf{A} \oplus \cdots \oplus \mathbf{A}/m_t\mathbf{A} \\ a & \longmapsto & \pi(a) = (\pi_1(a), \pi_2(a), \ldots, \pi_t(a)) \end{array}$$

is a ring isomorphism.

Corollary 3.1.6. *If the map π given in Proposition 3.1.5 is restricted to $\mathbf{A}^*$, then it gives rise to a group isomorphism*

$$(\mathbf{A}/m\mathbf{A})^* \cong (\mathbf{A}/m_1\mathbf{A})^* \times (\mathbf{A}/m_2\mathbf{A})^* \times \cdots \times (\mathbf{A}/m_t\mathbf{A})^*.$$

As $\mathbf{A}$ is a unique factorization domain, every nonzero element $a \in \mathbf{A}$ can be written uniquely as

$$a = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t},$$

where $\alpha \in \mathbb{F}_q^*$, the P_i are distinct monic irreducible polynomials, and the e_i are nonnegative integers. It follows from Corollary 3.1.6 that

$$(\mathbf{A}/a\mathbf{A})^* \cong (\mathbf{A}/P_1^{e_1}\mathbf{A})^* \times (\mathbf{A}/P_2^{e_2}\mathbf{A})^* \times \cdots \times (\mathbf{A}/P_t^{e_t}\mathbf{A})^*.$$

Thus we can focus on the case where $a = P^e$. The following proposition considers the case $e = 1$.

Proposition 3.1.7. *If $P \in \mathbf{A}$ is a monic irreducible polynomial, then the group $(\mathbf{A}/P\mathbf{A})^*$ is cyclic with $|P| - 1$ elements.*

This proposition shows that the structure of $(\mathbf{A}/P\mathbf{A})^*$ is similar to that of $(\mathbb{Z}/p\mathbb{Z})^*$ in $\mathbb{Z}$. The next result considers the case $e > 1$. See [Ros02, Proposition 1.6] for a detailed proof.

Proposition 3.1.8. *Let $a = P^e \in \mathbf{A}$, where P is a monic irreducible polynomial and $e \in \mathbb{Z}$ is positive. The group $(\mathbf{A}/P^e\mathbf{A})^*$ has $|P|^{e-1}(|P| - 1)$ elements. Let N be the kernel of the natural map from $(\mathbf{A}/P^e\mathbf{A})^*$ to $(\mathbf{A}/P\mathbf{A})^*$. Then N is a p-group of order $|P|^{e-1}$, and as e tends to infinity, the minimal number of generators of N also tends to infinity.*

There also exist analogues of the Euler ϕ-function, Fermat's Little Theorem, and Euler's Theorem in $\mathbf{A}$. For a nonzero element $a \in \mathbf{A}$, define

$$\Phi(a) := \#(\mathbf{A}/a\mathbf{A})^*, \tag{3.1}$$

which is equal to the number of nonzero polynomials in $\mathbf{A}$ which are of degree less than $\deg_T(a)$ and relatively prime to a. This is the analogue of Euler's totient function. For the proofs of the next two propositions, see [Ros02, Propositions 1.7 and 1.8].

Proposition 3.1.9. *For a nonzero $a \in \mathbf{A}$,*

$$\Phi(a) = |a| \prod_{P|a} \left(1 - \frac{1}{|P|}\right).$$

Proposition 3.1.10. *Let $a, b \in \mathbf{A}$ be nonzero elements such that $\gcd(a, b) = 1$. Then*

$$a^{\Phi(b)} \equiv 1 \pmod{b}.$$

Corollary 3.1.11. *If $P \in \mathbf{A}$ is irreducible and $a \in \mathbf{A}$ such that P does not divide a, then*

$$a^{|P|-1} \equiv 1 \pmod{P}.$$

Proof. See corollary to Proposition 1.8 in [Ros02]. □

We conclude this section by giving a short description of residue symbols over $\mathbf{A}$. Most of the material presented here can be found in [Ros02, Ch. 3] and [SS07].

Let $a, b \in \mathbf{A}$ be nonzero such that $\gcd(a, b) = 1$. Suppose d is a divisor of $q - 1$. We say that a is a d-th power residue modulo b if the equation

$$x^d \equiv a \pmod{b}$$

has a solution in $\mathbf{A}$. As before, let $P \in \mathbf{A}$ be an irreducible polynomial. Since $|P| = q^{\deg_T(P)}$, we see that d divides $|P| - 1$. If $a \in \mathbf{A}$ is not divisible by P, then it follows from Corollary 3.1.11 that $a^{|P|-1} \equiv 1 \pmod{P}$. Hence $a^{\frac{|P|-1}{d}}$ is a d-th root of unity in $\mathbb{F}_q^*$.

Definition 3.1.12. The d-th *power residue symbol* $(a/P)_d \in (\mathbf{A}/P\mathbf{A})^* \simeq \mu_{|P|-1}$ is defined as

$$\left(\frac{a}{P}\right)_d = \begin{cases} 0, & \text{if } P \mid a \\ a^{\frac{|P|-1}{d}} \pmod{P}, & \text{if } P \nmid a. \end{cases}$$

Note that the value of this residue symbol is always in the finite field $\mathbb{F}_q$. If $d = 2$, we drop the subscript d and just use $\left(\frac{a}{P}\right)$ to represent the quadratic residue symbol. Also, if $d = 2$, then this symbol is the counterpart of the Legendre symbol in elementary number theory. The properties of the d-th power residue symbol can be found in [Ros02, Propositions 3.1 and 3.2].

Theorem 3.1.13 (The d-th power reciprocity law)**.** *If $P, Q \in \mathbf{A}$ are distinct monic irreducible polynomials, then*

$$\left(\frac{Q}{P}\right)_d = (-1)^{\frac{q-1}{d}\deg_T(P)\deg_T(Q)} \left(\frac{P}{Q}\right)_d.$$

Proof. See [Ros02, Theorem 3.3]. □

As in the classical case, Definition 3.1.12 can be extended to the case where P is replaced with a nonzero polynomial $b \in \mathbf{A}$.

Definition 3.1.14. Let $b \in \mathbf{A}$ be nonzero with prime decomposition $b = \beta P_1^{e_1} P_2^{e_2} \cdots P_s^{e_s}$. Let $a \in \mathbf{A}$, the *d-th residue symbol* $\left(\frac{a}{b}\right)_d$ is defined as

$$\left(\frac{a}{b}\right)_d = \prod_{i=1}^{s} \left(\frac{a}{P_i}\right)_d^{e_i}.$$

This definition ignores the unit $\beta = \operatorname{sgn}(b)$. Hence $\left(\frac{a}{b}\right)_d$ only depends on the principal ideal $b\mathbf{A}$. In the quadratic case, this symbol corresponds to the Jacobi symbol. The properties of $\left(\frac{a}{b}\right)_d$ are given in [Ros02, Proposition 3.4]. Theorem 3.1.13 can now be extended to accommodate the general case. See [Ros02, Theorem 3.5].

Theorem 3.1.15 (The general reciprocity law)**.** *If a and b are nonzero polynomials in $\mathbf{A}$ that are relatively prime, then*

$$\left(\frac{a}{b}\right)_d = (-1)^{\frac{q-1}{d}\deg_T(a)\deg_T(b)} \operatorname{sgn}_d(a)^{\deg_T(b)} \operatorname{sgn}_d(b)^{-\deg_T(a)} \left(\frac{b}{a}\right)_d,$$

where $\operatorname{sgn}_d(*) = \operatorname{sgn}(*)^{\frac{q-1}{d}}$.

An algorithm for computing d-th power residue symbols is given in [SS07] for the case where q is even or $(q-1)/d$ is even.

3.2 Quadratic Extensions of Function Fields

This section gives a summary of the properties of function fields and their quadratic extensions. These properties will be utilized in the remaining chapters of this work. The material included here can be found in [Art24], [Gek08], [Ros02], and [Sch01]. Throughout this section we assume that q is a power of an odd prime $p \in \mathbb{Z}$.

Recall the following definition.

Definition 3.2.1. Let $\mathbf{k}$ be an arbitrary field. A *function field* of one variable over $\mathbf{k}$ is a field extension $\mathbf{K}/\mathbf{k}$ such that the following conditions are satisfied:

(i) $\mathbf{k}$ is algebraically closed in $\mathbf{K}$,

(ii) $\mathbf{K}$ is finitely generated over $\mathbf{k}$, and

(iii) $\mathbf{K}$ is of transcendence degree 1 over $\mathbf{k}$.

In this case, $\mathbf{k}$ is called the *constant field* of $\mathbf{K}$.

A simple example of a function field is the *rational function field* $\mathbf{K} = \mathbf{k}(x)$ for some element $x \in \mathbf{K}$ which is transcendental over $\mathbf{k}$.

A *prime element* of $\mathbf{K}$ is a discrete valuation ring R with maximal ideal P such that $\mathbf{k} \subset R$ and R has $\mathbf{K}$ as its field of quotients. Let $\mathrm{ord}_P(*)$ denote the order function associated with R. Define the degree of P, $\deg(P)$, to be the dimension of R/P over $\mathbf{k}$. This value is finite, see [Ros02], p. 46.

We are interested in the case where $\mathbf{K} = \mathbb{F}_q(T)$. This is the field of quotients of $\mathbf{A} = \mathbb{F}_q[T]$. From the previous section, we see that every nonzero prime ideal in $\mathbf{A}$ is generated by a unique monic irreducible polynomial $P \in \mathbf{A}$. The *localization* of $\mathbf{A}$ at P, $\mathbf{A}_P$, is a discrete valuation ring. By abuse of notation, let P denote the maximal ideal of $\mathbf{A}_P$. Then P is clearly a prime element of $\mathbf{K}$ in the above sense. Let $\mathbf{A}' = \mathbb{F}_q[T^{-1}]$ and P' the prime ideal of $\mathbf{A}'$ generated by T^{-1} in $\mathbf{A}'$. The localization of $\mathbf{A}'$ at P' is again a discrete valuation

ring, and hence it defines a prime element of $\mathbf{K}$, which is called the *prime at infinity*. We denote this by ∞. The associated order function, $\mathrm{ord}_\infty(*)$, assigns the value $-\deg_T(a)$ to $a \in \mathbf{A}$ and the value $\deg_T(b) - \deg_T(a)$ to any rational function a/b for $a, b \in \mathbf{A}$ with $b \neq 0$. It can be shown that the only primes of $\mathbf{K}$ are those associated to the monic irreducible polynomials in $\mathbf{A}$, called the *finite primes*, and ∞. The degree of any finite prime is equal to the degree of the irreducible polynomial to which it is associated, and the degree of ∞ is 1.

We now move on to extensions of function fields. In what follows, we assume that $\mathbf{K} = \mathbb{F}_q(T)$ where q is odd.

Definition 3.2.2. A *quadratic function field* extension of $\mathbf{K}$ is a finite algebraic extension $\mathcal{K}/\mathbf{K}$ such that $[\mathcal{K} : \mathbf{K}] = 2$.

Equivalently, $\mathcal{K} = \mathbb{F}_q(T, y)$ with $y^2 = D(T)$. Here $D(T) \in \mathbf{A}$ is a square-free polynomial of degree $2g + 1$ or $2g + 2$ where g is the *genus* of $\mathcal{K}$. $D(T)$ is called the *discriminant* of $\mathcal{K}$.

Now we consider the behaviour of primes in $\mathbf{K}$. Let P be an arbitrary prime in $\mathbf{K}$. Let $\mathcal{O}_P$ be a discrete valuation ring in $\mathbf{K}$ with maximal ideal P and field of quotients $\mathbf{K}$. Also, let $\mathcal{O}_\mathfrak{P}$ be a discrete valuation ring in $\mathcal{K}$ with maximal ideal $\mathfrak{P}$. We say that $\mathfrak{P}$ lies above P if $\mathcal{O}_P = \mathbf{K} \cap \mathcal{O}_\mathfrak{P}$ and $P = \mathfrak{P} \cap \mathcal{O}_P$, and denote this condition by $\mathfrak{P}|P$. We assign to this condition the integers $e = e(\mathfrak{P}|P)$ and $f = f(\mathfrak{P}|P)$ called the *ramification index* and *inertia degree* of P, respectively. The ramification index is the field extension degree that satisfies $\mathrm{ord}_\mathfrak{P}(\alpha) = e\ \mathrm{ord}_P(\alpha)$ for every $\alpha \in \mathbf{K}$, while the inertia degree is the integer $f = [\mathcal{O}_\mathfrak{P}/\mathfrak{P} : \mathcal{O}_P/P]$. For primes $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_m$ in $\mathcal{K}$ lying above P, let $e_i = e(\mathfrak{P}_i|P)$ and $f_i = f(\mathfrak{P}_i|P)$. Then

$$\sum_{i=1}^{m} e_i f_i = [\mathcal{K} : \mathbf{K}],$$

where $[\mathcal{K} : \mathbf{K}] = 2$ in our case. See [Ros02, Proposition 7.2 or Theorem 7.6] for the general case. If $m = 1$ and $e_1 = 2$, then $P = \mathfrak{P}_1^2$, and we say that P is *(totally) ramified*. If $m = 1$ and $e_1 = 1$, then we say that $P = \mathfrak{P}$ is *inert*. Finally, if $m = 2$, then we say that $P = \mathfrak{P}_1\mathfrak{P}_2$

splits (completely).

Quadratic function fields can be classified according to the decomposition of the infinite prime of $\mathbf{K}$ in $\mathcal{K}$. For ease of notation, let $D_{\mathcal{K}} = D(T) \in \mathbf{A}$.

Proposition 3.2.3. *Let $D_{\mathcal{K}}$ be a nonzero square-free element of $\mathbf{A}$ and $\mathcal{K} = \mathbf{K}(\sqrt{D_{\mathcal{K}}})$.*

(i) If $\deg_T(D_{\mathcal{K}})$ is even and $\operatorname{sgn}(D_{\mathcal{K}})$ is a square in $\mathbb{F}_q^*$, then ∞ splits in $\mathcal{K}/\mathbf{K}$.

(ii) If $\deg_T(D_{\mathcal{K}})$ is even and $\operatorname{sgn}(D_{\mathcal{K}})$ is not a square in $\mathbb{F}_q^*$, then ∞ is inert in $\mathcal{K}/\mathbf{K}$.

(iii) If $\deg_T(D_{\mathcal{K}})$ is odd, then ∞ ramifies in $\mathcal{K}/\mathbf{K}$.

Proof. See [Ros02, Proposition 14.6]. □

The quadratic function field $\mathcal{K}$ given in Proposition 3.2.3 is *real* if ∞ splits in $\mathcal{K}$. Otherwise, $\mathcal{K}$ is *imaginary*. A detailed treatment of quadratic function fields is presented in [Art24].

For the rest of this section we assume that $\mathcal{K} = \mathbf{K}(\sqrt{D_{\mathcal{K}}})$ is an imaginary quadratic function field. We introduce some additional terms analogous to those in the quadratic number field setting. An element $\alpha \in \mathcal{K}$ is of the form $\alpha = a + b\sqrt{D_{\mathcal{K}}}$, where $a, b \in \mathbf{K}$. Note that the nontrivial automorphism $\sigma \in \operatorname{Gal}(\mathcal{K}/\mathbf{K})$ takes $\sqrt{D_{\mathcal{K}}}$ to $-\sqrt{D_{\mathcal{K}}}$. From this, we define the *conjugate* of α in $\mathcal{K}$, denoted $\overline{\alpha}$, by $\overline{\alpha} = a - b\sqrt{D_{\mathcal{K}}}$. Define the *norm* of α, $N(\alpha)$, by

$$N(\alpha) = \alpha\overline{\alpha} = a^2 - b^2 D_{\mathcal{K}}.$$

Orders

Let $\mathcal{O}_{\mathcal{K}}$ be the integral closure of $\mathbf{A}$ in $\mathcal{K}$; that is, $\mathcal{O}_{\mathcal{K}}$ is the *ring of functions in $\mathcal{K}$ regular away from infinity*. It is an $\mathbf{A}$-module of rank two with basis $\{1, \sqrt{D_{\mathcal{K}}}\}$, i.e., $\mathcal{O}_{\mathcal{K}} = \mathbf{A} + \mathbf{A}\sqrt{D_{\mathcal{K}}}$. To see this, suppose $\alpha = a + b\sqrt{D_{\mathcal{K}}} \in \mathcal{K}$ is integral over $\mathbf{A}$. Then $\sigma(\alpha) = a - b\sqrt{D_{\mathcal{K}}} = \overline{\alpha}$ is

also integral over $\mathbf{A}$. It follows that

$$\alpha + \overline{\alpha} = 2a \quad \text{and} \quad \alpha\overline{\alpha} = a^2 - b^2 D_{\mathcal{K}}$$

are also integral over $\mathbf{A}$. The ring $\mathbf{A}$ is integrally closed, so $2a$ and $a^2 - b^2 D_{\mathcal{K}}$ are in $\mathbf{A}$. Since we may divide by 2, we see that $a \in \mathbf{A}$. Also $b^2 D_{\mathcal{K}} \in \mathbf{A}$, and note that $D_{\mathcal{K}} \in \mathbf{A}$ is square-free. So it follows that $b \in \mathbf{A}$, too. This establishes the inclusion $\mathcal{O}_{\mathcal{K}} \subseteq \mathbf{A} + \mathbf{A}\sqrt{D_{\mathcal{K}}}$. The other inclusion is clear.

Note that if an element $\alpha \in \mathcal{K}$ belongs to $\mathcal{O}_{\mathcal{K}}$, then $N(\alpha) \in \mathbf{A}$. Otherwise, $N(\alpha) \in \mathbf{K}$. If $N(\alpha) \in \mathbb{F}_q^*$, then α is called a *unit* of $\mathcal{O}_{\mathcal{K}}$. Denote the set of units of $\mathcal{O}_{\mathcal{K}}$ by $\mathcal{O}_{\mathcal{K}}^*$. This forms a group under multiplication.

An $\mathbf{A}$-*order* $\mathcal{O}$ in $\mathcal{O}_{\mathcal{K}}$ is a subring of $\mathcal{O}_{\mathcal{K}}$ which contains $\mathbf{A}$ and is a free module of rank two over $\mathbf{A}$. Thus we can also consider orders as lattices in $\mathcal{K}$. $\mathcal{O}_{\mathcal{K}}$ is the *maximal order* in $\mathcal{K}$. One important invariant of an order is its *discriminant*. If $\{\alpha, \beta\}$ forms a basis for $\mathcal{O}$, then the discriminant of $\mathcal{O}$ is defined as

$$D_{\mathcal{O}} = \det \begin{pmatrix} \alpha & \overline{\alpha} \\ \beta & \overline{\beta} \end{pmatrix}^2,$$

which is a polynomial in $\mathbf{A}$. It is independent of the basis of $\mathcal{O}$ up to a factor that is a square in $\mathbb{F}_q^*$. If we express α and β in terms of the basis $\{1, \sqrt{D_{\mathcal{K}}}\}$ of $\mathcal{O}_{\mathcal{K}}$, then we get

$$D_{\mathcal{O}} = 4f^2 D_{\mathcal{K}} \tag{3.2}$$

for some $f \in \mathbf{A}$. Note $\mathrm{char}(\mathbb{F}_q) \neq 2$, so the factor 4 in this discriminant is just a square of a unit. Hence, unlike in the quadratic number field case, we do not need to introduce a congruence class restriction on $D_{\mathcal{O}}$. The next result shows that f is actually unique.

Proposition 3.2.4. *Let $\mathcal{O}$ be an order in $\mathcal{K}$, and let $\mathcal{O}_{\mathcal{K}} = [1, \sqrt{D_{\mathcal{K}}}]$. There exists a unique monic polynomial $f \in \mathbf{A}$ such that*

$$\mathcal{O} = [1, f\sqrt{D_{\mathcal{K}}}] = \mathbf{A} + f\mathcal{O}_{\mathcal{K}}.$$

Proof. The proof is similar to the quadratic number field case, see [Lan87, Theorem 3, Ch. 8 §1]. □

Definition 3.2.5. The polynomial f in Proposition 3.2.4 is called the *conductor* of $\mathcal{O}$.

Note that the maximal order has conductor 1.

Proposition 3.2.6. *Let $\mathcal{O}$ be an order in $\mathcal{K}$ of conductor f. Then the index of $\mathcal{O}$, as an abelian group, is $[\mathcal{O}_\mathcal{K} : \mathcal{O}] = |f|$.*

Proof. Define a map $\theta : \mathcal{O}_\mathcal{K} \longrightarrow \mathbf{A}$ by sending an element $a + b\sqrt{D_\mathcal{K}} \in \mathcal{O}_\mathcal{K}$ to $b \in \mathbf{A}$. Note that θ is a homomorphism of additive groups since for $a_1 + b_1\sqrt{D_\mathcal{K}}, a_2 + b_2\sqrt{D_\mathcal{K}} \in \mathcal{O}_\mathcal{K}$ we have

$$\begin{aligned} \theta\left((a_1 + b_1\sqrt{D_\mathcal{K}}) + (a_2 + b_2\sqrt{D_\mathcal{K}})\right) &= \theta\left(a_1 + a_2 + (b_1 + b_2)\sqrt{D_\mathcal{K}}\right) \\ &= b_1 + b_2 = \theta(a_1 + b_1\sqrt{D_\mathcal{K}}) + \theta(a_2 + b_2\sqrt{D_\mathcal{K}}). \end{aligned}$$

Also, any $b \in \mathbf{A}$ has pre-image $0 + b\sqrt{D_\mathcal{K}} \in \mathcal{O}_\mathcal{K}$. So θ is surjective.

Let π be the natural projection map from $\mathbf{A}$ onto $\mathbf{A}/f\mathbf{A}$. Then the map $\pi \circ \theta : \mathcal{O}_\mathcal{K} \longrightarrow \mathbf{A}/f\mathbf{A}$ has kernel $\mathcal{O}$. To see this, we show containment of one set in the other. If $a + b\sqrt{D_\mathcal{K}} \in \ker(\pi \circ \theta)$, then

$$f\mathbf{A} = \pi \circ \theta(a + b\sqrt{D_\mathcal{K}}) = \pi(b) = b + f\mathbf{A}.$$

So $f \mid b$, i.e., $b = hf$ for some $h \in \mathbf{A}$. Hence $a + b\sqrt{D_\mathcal{K}} = a + hf\sqrt{D_\mathcal{K}} \in \mathcal{O}$, giving the inclusion $\ker(\pi \circ \theta) \subseteq \mathcal{O}$. Now if $a + bf\sqrt{D_\mathcal{K}} \in \mathcal{O}$, then it is clear that the image of this element under θ is $bf \equiv 0 \pmod{f}$ giving $\ker(\pi \circ \theta) \supseteq \mathcal{O}$. We now obtain the isomorphism

$$\frac{\mathcal{O}_\mathcal{K}}{\mathcal{O}} \cong \frac{\mathbf{A}}{f\mathbf{A}}.$$

By Proposition 3.1.2, $[\mathcal{O}_\mathcal{K} : \mathcal{O}] = |f|$. □

Now consider $\mathbf{A}$-orders $\mathcal{O}$ and $\mathcal{O}'$ with discriminants $D_\mathcal{O} = 4f^2 D_\mathcal{K}$ and $D_{\mathcal{O}'} = 4f'^2 D_\mathcal{K}$, respectively.

Lemma 3.2.7. *Let $\mathcal{O}$ and $\mathcal{O}'$ be $\mathbf{A}$-orders with conductors f and f' respectively. If $\mathcal{O}' \subseteq \mathcal{O}$, then the conductor of $\mathcal{O}'$ in $\mathcal{O}$ is f'/f.*

Proof. Clearly, $\mathcal{O}' \subseteq \mathcal{O}$ if and only if f divides f'. Let $\{\alpha, \beta\}$ be a basis of $\mathcal{O}'$. If we write α and β in terms of the basis $\{1, f\sqrt{D_{\mathcal{K}}}\}$ of $\mathcal{O}$, then

$$D_{\mathcal{O}'} = \left(\frac{f'}{f}\right)^2 D_{\mathcal{O}}.$$

So the conductor of $\mathcal{O}'$ in $\mathcal{O}$ is f'/f. □

3.3 Ideals of the Maximal Order

Now we consider ideals of the maximal order $\mathcal{O}_{\mathcal{K}}$. A subring $\mathfrak{a}$ of $\mathcal{O}_{\mathcal{K}}$ is an *integral* $\mathcal{O}_{\mathcal{K}}$-ideal if $\gamma\alpha \in \mathfrak{a}$ for every $\gamma \in \mathcal{O}_{\mathcal{K}}$. Note that sums and products of ideals are again ideals, and multiplication of ideals is both associative and commutative. We say that $\mathfrak{a}$ *divides* $\mathfrak{b}$ if $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ for some ideal $\mathfrak{c}$ and we denote this condition by $\mathfrak{a}|\mathfrak{b}$. Equivalently, we say that $\mathfrak{a}$ is a *divisor* of $\mathfrak{b}$. Note that $\mathfrak{a}|\mathfrak{b}$ if and only if $\mathfrak{b} \subseteq \mathfrak{a}$. This may not be the case in non-maximal orders. Moreover, if $\mathfrak{a}|\mathfrak{b}$ and $\mathfrak{b}|\mathfrak{a}$, then $\mathfrak{a} = \mathfrak{b}$. Note that $\mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$ and $\mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b}$. So $\mathfrak{a} + \mathfrak{b}|\mathfrak{a}$ and $\mathfrak{a} + \mathfrak{b}|\mathfrak{b}$; that is, $\mathfrak{a} + \mathfrak{b}$ is a common divisor of $\mathfrak{a}$ and $\mathfrak{b}$. Suppose $\mathfrak{d}$ is a common divisor of $\mathfrak{a}$ and $\mathfrak{b}$. Then $\mathfrak{a} \subseteq \mathfrak{d}$ and $\mathfrak{b} \subseteq \mathfrak{d}$. By definition of sum of ideals and since $\mathfrak{d}$ is closed under addition and negation, it follows that $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{d}$. So $\mathfrak{d}$ divides $\mathfrak{a} + \mathfrak{b}$. Hence, $\mathfrak{a} + \mathfrak{b}$ is the *greatest common divisor* of $\mathfrak{a}$ and $\mathfrak{b}$.

A *fractional* $\mathcal{O}_{\mathcal{K}}$-ideal $\mathfrak{f}$ is a finitely generated nonzero $\mathcal{O}_{\mathcal{K}}$-submodule of $\mathcal{K}$. Equivalently, there exists a nonzero $d \in \mathbf{A}$ such that $d\mathfrak{f}$ is an integral $\mathcal{O}_{\mathcal{K}}$-ideal. The unique monic polynomial d of minimal degree such that $d\mathfrak{f}$ is an integral ideal is called the *denominator* of $\mathfrak{f}$. We say that $\mathfrak{f}$ is a *principal fractional ideal* if there exists a nonzero $\alpha \in \mathcal{K}$ such that $\mathfrak{f} = \alpha\mathcal{O}_{\mathcal{K}}$. Two fractional ideals $\mathfrak{f}$ and $\mathfrak{f}'$ are *equivalent* if and only if $\mathfrak{f}' = (\beta) \cdot \mathfrak{f}$ for some nonzero $\beta \in \mathcal{K}$, and we write this as $\mathfrak{f} \sim \mathfrak{f}'$. Equivalence of ideals is an equivalence relation, and each equivalence class is called an *ideal class*.

Recall that $\mathcal{O}_\mathcal{K}$ has $\mathbf{A}$-basis $\{1, \sqrt{D_\mathcal{K}}\}$. Let $\mathfrak{a}$ be an integral ideal in $\mathcal{O}_\mathcal{K}$ with basis $\{\alpha_1, \alpha_2\}$ and $d \in \mathbf{A}$ the denominator of the fractional ideal $\mathfrak{f}$ such that $d\mathfrak{f} = \mathfrak{a}$. Then $\mathfrak{f} = \mathfrak{a}/d$ has $\{\alpha_1/d, \alpha_2/d\}$ as a basis. By expressing α_1 and α_2 in terms of the basis $\{1, \sqrt{D_\mathcal{K}}\}$ of $\mathcal{O}_\mathcal{K}$, we get

$$\frac{\alpha_i}{d} = \frac{a_i + b_i\sqrt{D_\mathcal{K}}}{d}$$

with $a_i, b_i \in \mathbf{A}$ for $i = 1, 2$. The *norm* of a fractional ideal $\mathfrak{f}$ is

$$N\mathfrak{f} = \alpha \frac{1}{d^2} \det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix},$$

where $\alpha \in \mathbb{F}_q^*$ is chosen so that $N\mathfrak{f}$ is monic. Clearly, $N\mathfrak{f} \in \mathbf{K}$ and if $\mathfrak{f}$ is integral, i.e., $d = 1$, then $N\mathfrak{f} \in \mathbf{A}$. In addition, the *absolute norm* of $\mathfrak{f}$ is the value $|N\mathfrak{f}| = q^{\deg(N\mathfrak{f})}$.

For a given ideal $\mathfrak{a}$, define $\overline{\mathfrak{a}} := \{\overline{\alpha} \mid \alpha \in \mathfrak{a}\}$. This set is closed under addition. Moreover, for $\alpha \in \mathfrak{a}$ and $\gamma \in \mathcal{O}$ we have $\gamma\overline{\alpha} = \overline{\overline{\gamma}\alpha}$, with $\overline{\gamma}\alpha \in \mathfrak{a}$. So $\overline{\mathfrak{a}}$ is also an ideal, and we call it the *conjugate ideal* of $\mathfrak{a}$. If $\{\alpha_1, \alpha_2\}$ is a basis of $\mathfrak{a}$, then $\{\overline{\alpha}_1, \overline{\alpha}_2\}$ is a basis of $\overline{\mathfrak{a}}$. For ideals $\mathfrak{a}$ and $\mathfrak{b}$, the conjugate ideal of $\mathfrak{ab}$ is $\overline{\mathfrak{a}}\overline{\mathfrak{b}}$. The product $\mathfrak{a}\overline{\mathfrak{a}}$ is a principal ideal equal to $(N\mathfrak{a})$ (for example, see [Art24], p. 168). Note that for nonzero ideals $\mathfrak{a}$ and $\mathfrak{b}$ we have $N(\mathfrak{ab}) = N\mathfrak{a}N\mathfrak{b}$.

We represent each nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_\mathcal{K}$ using the basis representation $\left\{cs, bs + s\sqrt{D_\mathcal{K}}\right\}$, where $b, c, s \in \mathbf{A}$, $cs \neq 0$, and c divides $b^2 - D_\mathcal{K}$. To make the polynomials c and b unique, we assume that c and s are monic and, upon subtracting an appropriate multiple of c from b, that $\deg_T(b) < \deg_T(c)$. If $s = 1$, we say that $\mathfrak{a}$ is *primitive*.

One of the most important results concerning $\mathcal{O}_\mathcal{K}$ is the existence of unique prime ideal factorization. This follows from the fact that $\mathcal{O}_\mathcal{K}$ is a Dedekind domain.

Theorem 3.3.1. *Every nonzero ideal in $\mathcal{O}_\mathcal{K}$ has a unique (up to order) prime ideal factorization.*

Proof. See [Art24], p.169. □

3.4 Class Group of an Order

Let $\mathcal{O}$ be an order in $\mathcal{K}$. We define fractional, integral, and equivalent $\mathcal{O}$-ideals as in the previous section. Note that a non-maximal order $\mathcal{O}$ does not possess all the properties of the maximal order $\mathcal{O}_\mathcal{K}$. For instance, $\mathcal{O}$ is not a Dedekind domain. So unique factorization of ideals fails in $\mathcal{O}$. However, there is a certain set of ideals in $\mathcal{O}$ for which unique prime ideal factorization holds. We need some additional definitions. An ideal $\mathfrak{a}$ of $\mathcal{O}$ is *proper* if the equality

$$\mathcal{O} = \{\alpha \in \mathcal{K} \mid \alpha\mathfrak{a} \subset \mathfrak{a}\} \tag{3.3}$$

holds. So principal ideals are always proper, and for the case of $\mathcal{O}_\mathcal{K}$, all its ideals are proper. A fractional $\mathcal{O}$-ideal that satisfies (3.3) is called a *proper fractional ideal*. An $\mathcal{O}$-ideal $\mathfrak{a}$ is *invertible* if there exists an $\mathcal{O}$-ideal $\mathfrak{a}'$ such that $\mathfrak{a}\mathfrak{a}' = \mathcal{O}$. The inverse of $\mathfrak{a}$, denoted $\mathfrak{a}^{-1}$, is the fractional ideal

$$\mathfrak{a}^{-1} = \{\alpha \in \mathcal{K} \mid \alpha\mathfrak{a} \subseteq \mathcal{O}\}.$$

Notice that all principal ideals are invertible. It can be shown that the proper fractional ideals of $\mathcal{O}$ are exactly the invertible fractional ideals of $\mathcal{O}$ as in the quadratic number field case (see [Cox89], p. 136). It follows that the set of proper fractional $\mathcal{O}$-ideals is a multiplicative group. We can also define divisibility of $\mathcal{O}$-ideals in the same way as it was defined for $\mathcal{O}_\mathcal{K}$-ideals. An *irreducible* proper $\mathcal{O}$-ideal $\mathfrak{p} \neq \mathcal{O}$ is a proper $\mathcal{O}$-ideal which cannot be factored as $\mathfrak{p} = \mathfrak{a}\mathfrak{b}$ with proper $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ such that both ideals are distinct from $\mathfrak{p}$.

One can determine proper fractional ideals in an order using the following result (see [Cox89, Lemma 7.5]).

Lemma 3.4.1. *Let $\mathcal{K} = \mathbf{K}(\tau)$ be an imaginary quadratic function field, and let $ax^2 + bx + c$ be the minimal polynomial of τ where $a, b, c \in \mathbf{A}$, a monic, and $\gcd(a, b, c) = 1$. Then $[1, \tau]$ is a proper fractional ideal for the order $[1, a\tau]$.*

Proof. Observe that $a\tau$ is algebraic over $\mathcal{K}$, so $[1, a\tau]$ is an order. From the minimal polynomial of τ, we have

$$\tau^2 = \frac{-b\tau - c}{a}.$$

Let $\beta \in \mathcal{K}$. Note that $\beta[1,\tau] \subset [1,\tau]$ if and only if $\beta \cdot 1 \in [1,\tau]$ and $\beta \cdot \tau \in [1,\tau]$. The condition $\beta \cdot 1 \in [1,\tau]$ is equivalent to $\beta = m + n\tau$ for some $m, n \in \mathbf{A}$. For the condition $\beta \cdot \tau \in [1,\tau]$, we have

$$\beta\tau = m\tau + n\tau^2 = m\tau + n\left(\frac{-b\tau - c}{a}\right) = m\tau - \frac{nb}{a}\tau - \frac{nc}{a} = -\frac{nc}{a} + \left(m - \frac{nb}{a}\right)\tau.$$

Since $\gcd(a, b, c) = 1$, it follows that $\beta\tau \in [1,\tau]$ if and only if a divides n. So

$$[1, a\tau] = \{\beta \in \mathcal{K} \mid \beta[1,\tau] \subset [1,\tau]\}.$$

□

Let $\mathcal{I}(\mathcal{O})$ denote the multiplicative group of proper fractional $\mathcal{O}$-ideals. Inside this group is the subgroup $\mathcal{P}(\mathcal{O})$ of principal fractional $\mathcal{O}$-ideals. So we can form the quotient group given in the following definition which is a finite abelian group.

Definition 3.4.2. For an order $\mathcal{O}$ of $\mathcal{K}$, the quotient group

$$\mathcal{C}l(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O})$$

is called the *class group* of $\mathcal{O}$.

We now give a summary of some important properties of this group. The material presented here is based on [Cox89, Ch. 2 §7] and [Lan87, Ch. 8 §1].

Let $\mathcal{O}$ have conductor $f \in \mathbf{A}$ and let $\mathfrak{a}$ be a nonzero $\mathcal{O}$-ideal. We say that $\mathfrak{a}$ is *prime* to the conductor f of $\mathcal{O}$ if $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$ or $\mathfrak{a} + f\mathcal{O}_{\mathcal{K}} = \mathcal{O}$. These two conditions are actually equivalent. See [Lan87], p. 92. It is clear that $\mathfrak{a}$ is prime to f if and only if $\overline{\mathfrak{a}}$ is prime to f.

Lemma 3.4.3. *Let $\mathcal{O}$ have conductor $f \in \mathbf{A}$ and let $\mathfrak{a}$ be a proper $\mathcal{O}$-ideal. Then there exists an element $\alpha \in \mathcal{K}$ such that $\alpha\mathfrak{a} \subset \mathcal{O}$ and $\alpha\mathfrak{a} + f\mathcal{O} = \mathcal{O}$. In other words, the equivalence class of $\mathfrak{a}$ contains an integral ideal prime to f.*

Proof. The proof is similar to the quadratic number field case, see [Lan87, Theorem 5, Ch. 8 §1]. □

Lemma 3.4.4.

1. *An $\mathcal{O}$-ideal $\mathfrak{a}$ is prime to f if and only if* $\gcd(N(\mathfrak{a}), f) = 1$.

2. *An $\mathcal{O}$-ideal $\mathfrak{a}$ prime to f is a proper $\mathcal{O}$-ideal.*

Proof. See [Cox89, Lemma 7.18]. □

Let $\mathcal{I}(\mathcal{O}, f)$ be the set of $\mathcal{O}$-ideals prime to f. As a consequence of this lemma, we see that $\mathcal{I}(\mathcal{O}, f) \subset \mathcal{I}(\mathcal{O})$. Let $\mathcal{P}(\mathcal{O}, f)$ be the set of principal $\mathcal{O}$-ideals prime to f.

Theorem 3.4.5. *The inclusion $\mathcal{I}(\mathcal{O}, f) \subset \mathcal{I}(\mathcal{O})$ induces a group isomorphism*

$$\frac{\mathcal{I}(\mathcal{O}, f)}{\mathcal{P}(\mathcal{O}, f)} \cong \frac{\mathcal{I}(\mathcal{O})}{\mathcal{P}(\mathcal{O})} = \mathcal{C}l(\mathcal{O}).$$

Proof. The proof is similar to the number field case. See, for example, [Cox89, Proposition 7.19]. □

Let $\mathcal{I}(\mathcal{O}_\mathcal{K}, f)$ be the set of $\mathcal{O}_\mathcal{K}$-ideals prime to f. The following result has proof similar to that of Theorem 4 in [Lan87, Ch. 8, §1].

Theorem 3.4.6. *Let $\mathcal{O}$ be an order of conductor f. There exists an isomorphism $\mathcal{I}(\mathcal{O}_\mathcal{K}, f) \cong \mathcal{I}(\mathcal{O}, f)$ given by the inverse mappings*

$$\mathfrak{a} \longmapsto \mathfrak{a} \cap \mathcal{O}, \quad \text{for } \mathfrak{a} \in \mathcal{I}(\mathcal{O}_\mathcal{K}, f)$$
$$\mathfrak{a} \longmapsto \mathfrak{a}\mathcal{O}_\mathcal{K}, \quad \text{for } \mathfrak{a} \in \mathcal{I}(\mathcal{O}, f).$$

This theorem can be used to show that $\mathcal{O}$-ideals prime to f can be factored uniquely into prime $\mathcal{O}$-ideals which are prime to f. See for instance, [Cox89, Exercise 7.26].

Let $\mathcal{P}(\mathcal{O}_\mathcal{K}, f)$ be the subgroup of $\mathcal{I}(\mathcal{O}_\mathcal{K}, f)$ generated by principal ideals of the form

$$\mathfrak{a} = \alpha\mathcal{O}_\mathcal{K},$$

where $\alpha \in \mathcal{O}_{\mathcal{K}}$ satisfies

$$\alpha \equiv a \pmod{f\mathcal{O}_{\mathcal{K}}}$$

for some $a \in \mathbf{A}$, $\gcd(a, f) = 1$.

Lemma 3.4.7. *Let $\mathfrak{a} \in \mathcal{P}(\mathcal{O}_{\mathcal{K}}, f)$. Then $\mathfrak{a} \cap \mathcal{O} = \alpha\mathcal{O}$, where $\alpha \equiv a \pmod{f\mathcal{O}_{\mathcal{K}}}$ for some nonzero $a \in \mathbf{A}$ such that $\gcd(a, f) = 1$.*

Proof. See [Lan87, Lemma 1, Ch. 8 §1]. □

Theorem 3.4.8. *Let $\mathcal{O}$ be an order in an imaginary quadratic function field $\mathcal{K}$. Then there is an isomorphism of quotient groups given by*

$$\frac{\mathcal{I}(\mathcal{O}_{\mathcal{K}}, f)}{\mathcal{P}(\mathcal{O}_{\mathcal{K}}, f)} \cong \frac{\mathcal{I}(\mathcal{O}, f)}{\mathcal{P}(\mathcal{O}, f)}.$$

Proof. Consider the isomorphism $\mathcal{I}(\mathcal{O}_{\mathcal{K}}, f) \cong \mathcal{I}(\mathcal{O}, f)$ from Theorem 3.4.6 via the map $\mathfrak{a} \longmapsto \mathfrak{a} \cap \mathcal{O}$. Under this isomorphism we claim that the inverse image of $\mathcal{P}(\mathcal{O}, f)$ is the subgroup $\mathcal{P}(\mathcal{O}_{\mathcal{K}}, f) \subset \mathcal{I}(\mathcal{O}_{\mathcal{K}}, f)$.

The preceding lemma shows that $\mathcal{P}(\mathcal{O}_{\mathcal{K}}, f)$ is contained in the inverse image of $\mathcal{P}(\mathcal{O}, f)$. For the other direction of inclusion, suppose that $\mathfrak{a} \cap \mathcal{O} = \alpha\mathcal{O}$ with $\alpha \equiv a \pmod{f\mathcal{O}_{\mathcal{K}}}$ and $a \in \mathbf{A}$ with $\gcd(a, f) = 1$. Then $\mathfrak{a} = \alpha\mathcal{O}_{\mathcal{K}}$. Therefore $\mathfrak{a} \in \mathcal{P}(\mathcal{O}_{\mathcal{K}}, f)$. □

As an immediate consequence of Theorems 3.4.5 and 3.4.8 we obtain the isomorphism

$$\mathcal{C}l(\mathcal{O}) \cong \frac{\mathcal{I}(\mathcal{O}_{\mathcal{K}}, f)}{\mathcal{P}(\mathcal{O}_{\mathcal{K}}, f)}, \tag{3.4}$$

which gives a description of the group $\mathcal{C}l(\mathcal{O})$ in terms of the maximal order $\mathcal{O}_{\mathcal{K}}$.

3.5 Class Number of an Order

We present a class number formula for an $\mathbf{A}$-order $\mathcal{O}$ analogous to the formula in the quadratic number field case, see for example [Cox89, Theorem 7.24] or [Lan87, Theorem 7, Ch. 8 §1]. As before, let $\mathbf{A} = \mathbb{F}_q[T]$ with quotient field $\mathbf{K} = \mathbb{F}_q(T)$, where q is odd.

Throughout this section we assume that $\mathcal{K} = \mathbf{K}(\sqrt{D_{\mathcal{K}}})$ is an imaginary quadratic function field where $D_{\mathcal{K}} \in \mathbf{A}$ is square-free.

The order of the group $\mathcal{C}l(\mathcal{O})$, denoted $h(\mathcal{O})$, is called the *class number* of $\mathcal{O}$. If $\mathcal{O}$ is the integral closure of $\mathbf{A}$ in $\mathcal{K}$, then $\mathcal{O}$ is a Dedekind domain. In this case, $\mathcal{O} = \mathcal{O}_{\mathcal{K}}$, so $\mathcal{C}l(\mathcal{O})$ is the class group $\mathcal{C}l(\mathcal{O}_{\mathcal{K}})$ and $h(\mathcal{O})$ is just the usual class number of $\mathcal{K}$.

Suppose $\mathcal{O}$ has conductor $f \in \mathbf{A}$. We aim to write $h(\mathcal{O})$ in terms of f and the class number $h(\mathcal{O}_{\mathcal{K}})$ of the maximal order. We require the following terminology.

Definition 3.5.1. The *Kronecker symbol*, $\chi_{\mathcal{K}}$, associated with $\mathcal{K}$ is

$$\chi_{\mathcal{K}}(P) = \begin{cases} 1, & \text{if } P \text{ splits in } \mathcal{K} \\ 0, & \text{if } P \text{ ramifies in } \mathcal{K} \\ -1, & \text{if } P \text{ is inert in } \mathcal{K}, \end{cases}$$

for a prime $P \in \mathbf{A}$.

Observe that this symbol coincides with the quadratic residue symbol when $\mathbf{K} = \mathbb{F}_q(T)$. In this case we use the symbol $\left(\frac{\cdot}{P}\right)$ instead. In general, for primes $P_i \in \mathbf{A}$

$$\chi_{\mathcal{K}}\left(\prod P_i^{e_i}\right) = \prod \chi_{\mathcal{K}}(P_i)^{e_i},$$

see [Yu95a], p. 324.

The next result holds for any quadratic function field.

Theorem 3.5.2. *If $\mathcal{O}$ is an $\mathbf{A}$-order with conductor $f \in \mathbf{A}$, then*

$$h(\mathcal{O}) = \frac{|f|\ h(\mathcal{O}_{\mathcal{K}})}{[\mathcal{O}_{\mathcal{K}}^* : \mathcal{O}^*]} \prod_{P|f} \left(1 - \frac{\chi_{\mathcal{K}}(P)}{|P|}\right), \tag{3.5}$$

where P runs through the prime divisors of f and $|\cdot|$ is the absolute value given in Definition 3.1.3.

Proof. The proof is similar to the number field case, see [Cox89, Theorem 7.24] or [Lan87, Theorem 7, Ch. 8 §1], for example. □

As a consequence of this theorem, we see that $[\mathcal{O}_{\mathcal{K}}^* : \mathcal{O}^*]$ is finite. Here we exclude the case where $\mathcal{K}$ is a quadratic extension of the constant field of $\mathbf{K}$. For this particular case, $\mathcal{K} = \mathbb{F}_{q^2}$, the maximal order is $\mathcal{O}_{\mathcal{K}} = \mathbb{F}_{q^2}[T]$ and $\chi_{\mathcal{K}}(P) = (-1)^{\deg_T(P)}$ (see [Gek08], p. 1710). With this exclusion, we have $\mathcal{O}_{\mathcal{K}}^* = \mathcal{O}^* = \mathbb{F}_q^*$.

Theorem 3.5.3. *Let $\mathcal{K}$ be an imaginary quadratic function field. Then*

$$h(\mathcal{O}_{\mathcal{K}}) = \eta h(\mathcal{K}),$$

where $\eta = 1$ if ∞ is ramified and $\eta = 2$ if ∞ is inert in $\mathcal{K}$.

Proof. See [Ros02, Proposition 14.7] or [Art24], pp. 212–217. □

We mention a result that gives the class number $h(\mathcal{O}_{\mathcal{K}})$ of the maximal order of $\mathcal{K}$ in terms of $h(\mathcal{K})$, where $h(\mathcal{K})$ denotes the *number of divisor classes of degree zero* of $\mathcal{K}$. This lemma holds for any quadratic function field.

Lemma 3.5.4. *$h(\mathcal{K})$ is finite and bounded as*

$$(\sqrt{q} - 1)^{2g} \leq h(\mathcal{K}) \leq (\sqrt{q} + 1)^{2g},$$

where g is the genus of $\mathcal{K}$.

Proof. See [Ros02, Lemma 5.6and Proposition 5.11]. □

We end this section by defining the *Hurwitz class number* of an $\mathbf{A}$-order $\mathcal{O}$ which we denote by $\mathbf{H}(\mathcal{O})$ (see [Yu95a, Section 6]). Let

$$w(\mathcal{O}) = \frac{\#\mathcal{O}^*}{q-1} \quad \text{and} \quad h'(\mathcal{O}) = w(\mathcal{O})^{-1} h(\mathcal{O}).$$

Then

$$\mathbf{H}(\mathcal{O}) = \sum_{f' | f} h'(\mathcal{O}'), \tag{3.6}$$

where f and f' are the conductors of $\mathcal{O}$ and $\mathcal{O}'$, respectively, and $\mathcal{O}'$ runs through all the $\mathbf{A}$-orders in $\mathcal{O}_{\mathcal{K}}$ containing $\mathcal{O}$. Again, we leave out the case $\mathcal{O}_{\mathcal{K}} = \mathbb{F}_{q^2}[T]$, so $w(\mathcal{O}') = 1$, and hence $h'(\mathcal{O}) = h(\mathcal{O})$ for each $\mathcal{O}'$ in (3.6).

Chapter 4

Introduction to Drinfeld Modules

We introduce the necessary preparations for the study of Drinfeld modules in this chapter. These preparations include additive polynomials and "twisted" rings built from these polynomials. Then we lay out some fundamental properties of Drinfeld modules. Finally, we give basic descriptions of morphisms between Drinfeld modules.

4.1 Additive Polynomials

This section deals with additive polynomials and their basic properties. These polynomials will play a central role in building up the definition of Drinfeld modules in the next section. We also present some properties of the "twisted" ring of polynomials, which is isomorphic to the ring of additive polynomials with coefficients from a given field $\mathbb{L}$. We give a summary of some important material from [Gos98] (Chapter 1), [Ros02] (Chapters 12 and 13), and [Sal06] (Chapters 12 and 13).

Definition 4.1.1. Let $\mathbb{L}$ be a field and $f(x) \in \mathbb{L}[x]$. Then $f(x)$ is *additive* if

$$f(x+y) = f(x) + f(y)$$

holds inside the polynomial ring $\mathbb{L}[x, y]$.

Example 4.1.2. In $\mathrm{char}(\mathbb{L}) = p > 0$, let τ be the p-th power map. It can be shown that monomials of the form $\tau^i(x) := x^{p^i}$, for a nonnegative integer i, are additive via the binomial theorem (this is generally known as "Freshmen's Dream"). Moreover, the polynomials spanned by them are also additive.

The following result characterizes additive polynomials.

Proposition 4.1.3. *Let $\mathbb{L}$ be a field and $f(x) \in \mathbb{L}[x]$, Then $f(x)$ is additive if and only if the following hold.*

(a) If char$(\mathbb{L}) = 0$, then $f(x) = ax$ for some $a \in \mathbb{L}$.

(b) If char$(\mathbb{L}) = p > 0$, then there exist $r \in \mathbb{Z}$ with $r \geq 0$ and $a_i \in \mathbb{L}$, $0 \leq i \leq r$, such that $f(x) = \sum_{i=0}^{r} a_i x^{p^i}$.

Proof. Clearly polynomials of the form given in (a) and (b) are additive. Conversely, let $f(x) = \sum b_i x^i \in \mathbb{L}[x]$ be any additive polynomial. So $f(x+y) = f(x) + f(y)$. We have

$$\left[\frac{d}{dx} f(x+y)\right]_{x=0} = \left[\frac{d}{dx} f(x)\right]_{x=0} = f'(0),$$

so the formal derivative of f must be a constant. Now, $f'(x) = \sum i b_i x^{i-1}$.

(a) If char$(\mathbb{L}) = 0$, $f'(x)$ is constant if and only if $f(x)$ is linear, i.e., $f(x) = b_0 + b_1 x$. Note that $f(x+y) = f(x) + f(y)$ implies that $f(0) = 0$. Hence, $f(x) = b_1 x$.

(b) If char$(\mathbb{L}) = p > 0$, then $f'(x)$ is constant if and only if $b_i = 0$ for each $i > 1$ with $\gcd(i, p) = 1$. Write $f(x)$ as

$$f(x) = b_1 x + \sum_{j \geq 1} b_{pj} x^{pj} = b_1 x + g(x)^p,$$

with $g(x) \in \mathbb{L}_1[x]$, where $\mathbb{L}_1$ is the field obtained by adjoining the p-th roots of the coefficients b_{pj} to $\mathbb{L}$. It can be checked easily that $g(x)$ is additive in $\mathbb{L}_1[x]$. Using induction on the degree of $f(x)$ allows us to assume that $g(x) = \sum_{h \geq 0} c_h x^{p^h}$. So

$$f(x) = b_1 x + \sum_{h \geq 0} c_h^p x^{p^{h+1}}.$$

Since $c_h^p \in \mathbb{L}$ for all h, it follows that $f(x)$ is of the desired form.

□

Assume that char$(\mathbb{L}) = p > 0$. Let $\mathcal{A}(\mathbb{L})$ be the set of additive polynomials with coefficients in $\mathbb{L}$.

Proposition 4.1.4. *Let $f(x), g(x) \in \mathcal{A}(\mathbb{L})$. Then*

(a) $f(x) + g(x) \in \mathcal{A}(\mathbb{L})$;

(b) for $\alpha \in \mathbb{L}$, $\alpha f(x) \in \mathcal{A}(\mathbb{L})$; and

(c) $f(g(x)) \in \mathcal{A}(\mathbb{L})$.

Proof. This proposition follows immediately from Definition 4.1.1. □

If $\mathbb{L} \neq \mathbb{F}_p$, then it is clear from Proposition 4.1.4 that $\mathcal{A}(\mathbb{L})$ forms a noncommutative ring (also an $\mathbb{L}$-module) under ordinary addition and composition of polynomials. Note that x is the identity in $\mathcal{A}(\mathbb{L})$ under the second operation.

Let τ be the p-th power map on $\mathbb{L}$. We next define a ring that is isomorphic to $\mathcal{A}(\mathbb{L})$.

Definition 4.1.5. Denote by $\mathbb{L}\{\tau\}$ the ring of polynomials in τ with "twisted" multiplication; that is for every $\alpha \in \mathbb{L}$,

$$\tau \cdot \alpha = \alpha^p \tau. \tag{4.1}$$

Relation (4.1) results from the calculation

$$(\tau\alpha)(x) = \tau(\alpha x) = (\alpha x)^p = \alpha^p x^p = (\alpha^p \tau)(x).$$

This means that multiplication in $\mathbb{L}\{\tau\}$ is similar to that in a polynomial ring except that when an element of $\mathbb{L}$ is multiplied by a power of τ, relation (4.1) must be employed. $\mathbb{L}\{\tau\}$ forms a ring under composition

$$f(g(\tau)) := f(\tau) \cdot g(\tau), \qquad \text{for } f(\tau), g(\tau) \in \mathbb{L}\{\tau\}$$

with identity τ^0. It is the subspace of $\mathbb{L}[x]$ spanned by τ^i for $i = 0, 1, 2, \ldots$. Note that for $\mathbb{L} \neq \mathbb{F}_p$, $\mathbb{L}\{\tau\}$ is not commutative. This follows immediately from (4.1). We associate to each $f(x) = \sum_{i=0}^{r} a_i x^{p^i} \in \mathcal{A}(\mathbb{L})$ the polynomial in τ given by $g(\tau) = \sum_{i=0}^{r} a_i \tau^i$. Observe that $f(x) = g(\tau(x))$ since $\tau(x) = x^p$, and this association gives a bijection

$$\begin{aligned} \gamma : \mathcal{A}(\mathbb{L}) &\longrightarrow \mathbb{L}\{\tau\} \\ f(x) &\longmapsto g(\tau). \end{aligned}$$

We now modify our definition of τ to accommodate the field $\mathbb{F}_q$ with $q = p^s$ elements. Our goal is to work only with $\mathbb{F}_q$-algebras. Assume that $\mathbb{F}_q \subseteq \mathbb{L}$ and we only look at $\mathbb{F}_q$-linear polynomials, i.e., additive polynomials for which

$$f(\alpha x) = \alpha f(x), \quad \forall\ \alpha \in \mathbb{F}_q. \tag{4.2}$$

So for $f(\tau) = \sum a_i \tau^i$, this requirement is seen to be equivalent to

$$\alpha^{p^i} = \alpha, \quad \forall\ \alpha \in \mathbb{F}_q \tag{4.3}$$

whenever $a_i \neq 0$. We redefine τ to be the q-th power map, so the commutation rule given in (4.1) becomes

$$\tau \cdot \alpha = \alpha^q \tau, \quad \forall\ \alpha \in \mathbb{L}. \tag{4.4}$$

Lemma 4.1.6. *If $\mathbb{F}_q \subseteq \mathbb{L}$ and $f(x) \in \mathbb{L}[x]$, then $f(x)$ is $\mathbb{F}_q$-linear if and only if $f(x)$ is of the form $f(x) = \sum_{i=0}^{r} a_i x^{q^i}$, where $a_i \in \mathbb{L}$.*

Proof. Clearly, every polynomial of the form $\sum_{i=0}^{r} a_i x^{q^i}$ is $\mathbb{F}_q$-linear. Conversely, assume that $f(x) \in \mathbb{L}[x]$ is $\mathbb{F}_q$-linear. So $f(x)$ is additive, and hence $f(x) = \sum_{j=0}^{r} b_j x^{p^j}$ by Proposition 4.1.3(b), where $b_j \in \mathbb{L}$. It also satisfies (4.2) for every $\alpha \in \mathbb{L}$. Thus

$$\sum_{j=0}^{r} b_j \alpha^{p^j} x^{p^j} = \sum_{j=0}^{r} b_j \alpha x^{p^j}.$$

So $\alpha^{p^j} = \alpha$ for every j such that $b_j \neq 0$. The result follows. □

In the above setting, $\mathbb{L}\{\tau\}$ is now made up of $\mathbb{F}_q$-linear polynomials in τ. Let $f(\tau) = \sum_{i=0}^{t} a_i \tau^i$, with $a_t \neq 0$, and set $t = \deg_\tau(f)$. Observe that

$$q^{\deg_\tau(f)} = \deg_x(f(x)).$$

The next result is known as the "Fundamental Theorem of Additive Polynomials". Set $d = \deg_x(f(x))$ and assume that $\mathbb{L} \supseteq \mathbb{F}_q$ is an algebraically closed field.

Theorem 4.1.7. *Let $f(x) \in \mathbb{L}[x]$ be a separable polynomial with set of roots*

$$W = \{w_1, w_2, \ldots, w_d\} \subset \mathbb{L}.$$

Then $f(x)$ is additive if and only if W forms an additive subgroup of $\mathbb{L}$.

Proof. If $f(x)$ is additive, then W can be easily seen to satisfy the subgroup criterion. So W is an additive subgroup of $\mathbb{L}$.

Conversely, suppose W is an additive subgroup of $\mathbb{L}$. We want to show that $f(x+y) = f(x) + f(y)$ in $\mathbb{L}[x, y]$. As $f(x)$ is separable, we can write it as

$$f(x) = \prod_{i=0}^{d} (x - w_i), \qquad w_i \in W.$$

It is easy to check that $f(x + w) = f(x)$ for all $w \in W$. Let $y \in \mathbb{L}$ and set

$$h(x) = f(x + y) - f(x) - f(y).$$

Then $\deg_x(h(x)) < \deg_x(f(x))$. On the other hand,

$$h(w) = f(w + y) - f(w) - f(y) = 0, \quad \forall\ w \in W.$$

Thus $h(x)$ must be identically 0 because $d = \deg_x(f(x)) > \deg_x(h(x))$. Now let y be an arbitrary indeterminate and set

$$h_1(x) = f(x + y) - f(x) - f(y) \in \mathbb{L}[x][y] = \mathbb{L}[x, y].$$

So $h_1(\alpha) = 0$, for $\alpha \in \mathbb{L}$. Since $\mathbb{L}$ is algebraically closed, it must be infinite. Note that over an infinite field, a polynomial evaluates to 0 at every point if and only if it is identically 0. It follows that $h_1(y)$ is identically 0. Therefore, $f(x)$ is additive. □

Corollary 4.1.8. *Let $f(x) \in \mathbb{L}[x]$ be a separable polynomial with set of roots*

$$W = \{w_1, w_2, \ldots, w_d\}.$$

Then $f(x)$ is $\mathbb{F}_q$-linear if and only if W forms an $\mathbb{F}_q$-vector subspace of $\mathbb{L}$.

Proof. Let W be an $\mathbb{F}_q$-vector subspace of $\mathbb{L}$ and $\alpha \in \mathbb{F}_q$. Set

$$h(x) = f(\alpha x) - \alpha f(x).$$

If $\#W = q^j$, then $\deg_x(f(x)) = q^j$. Note that $\alpha^{q^j} = \alpha$, so $\deg_x(h(x)) < q^j$. On the other hand, W is a subspace of $\mathbb{L}$ so $\alpha w \in W$ and $h(w) = 0$ for every $w \in W$. Therefore, $h(x)$ must be identically 0.

The converse is clear by Theorem 4.1.7. □

Divisibility Theory in $\mathbb{L}\{\tau\}$

We continue to discuss some features of the ring $\mathbb{L}\{\tau\}$ pertaining to divisibility. Let $f(x) \in \mathbb{L}[x]$, $\mathbb{F}_q \subseteq \mathbb{L}$, and $\overline{\mathbb{L}}$ a fixed algebraic closure of $\mathbb{L}$.

Theorem 4.1.9. *There exists a nonzero element $g(\tau) \in \mathbb{L}\{\tau\}$ such that $f(x)$ divides $g(x)$.*

Proof. Set $d = \deg_x(f(x))$ and define $f_i(x)$ to be the residue when x^{q^i} is divided by $f(x)$, so

$$x^{q^i} \equiv f_i(x) \pmod{f(x)}.$$

Let v be the smallest integer such that the set $\{f_0(x), \ldots, f_v(x)\}$ is linearly dependent over $\mathbb{L}$. Also let

$$\sum_{j=0}^{v} \beta_j f_j(x) = 0$$

be a nontrivial relation with $\{\beta_j\} \subseteq \mathbb{L}$. It follows that $g(\tau) = \sum \beta_j \tau^j \in \mathbb{L}\{\tau\}$ and $f(x)$ divides $g(x) = \sum \beta_j x^{q^j}$. □

The set of all polynomials $g(\tau) \in \mathbb{L}\{\tau\}$ satisfying the condition of the preceding theorem forms a nontrivial left ideal in $\mathbb{L}\{\tau\}$. We move on to some divisibility properties of polynomials in the ring $\mathbb{L}\{\tau\}$. Let $f(\tau), g(\tau) \in \mathbb{L}\{\tau\}$. Note that if $f(\tau) \cdot g(\tau) = 0$ in $\mathbb{L}\{\tau\}$, then $f(\tau) = 0$ or $g(\tau) = 0$. So multiplication in $\mathbb{L}\{\tau\}$ has both left and right cancellation properties. Next, we define relationships between elements of $\mathbb{L}\{\tau\}$.

Definition 4.1.10.

1. $f(\tau)$ is *right divisible* by $g(\tau)$ if there exists an element $h(\tau) \in \mathbb{L}\{\tau\}$ such that

$$f(\tau) = h(\tau) \cdot g(\tau).$$

2. $f(\tau)$ is *left divisible* by $g(\tau)$ if there exists an element $m(\tau) \in \mathbb{L}\{\tau\}$ such that

$$f(\tau) = g(\tau) \cdot m(\tau).$$

Proposition 4.1.11 (Right Division Algorithm)**.** *Let $f(\tau), g(\tau) \in \mathbb{L}\{\tau\}$ with $g(\tau) \neq 0$. Then there exist unique polynomials $h(\tau), r(\tau) \in \mathbb{L}\{\tau\}$ such that*

$$f(\tau) = h(\tau) \cdot g(\tau) + r(\tau)$$

with $r(\tau) = 0$ or $\deg_\tau(r) < \deg_\tau(g)$.

Proof. Let $f(\tau) = \sum_{i=0}^{m} a_i\tau^i$, $g(\tau) = \sum_{j=0}^{n} b_j\tau^j$ and $h(\tau) = \sum_{t=0}^{m-n} c_t\tau^t$. So for a suitably chosen $c_t \in \mathbb{L}$ we get

$$\sum_{i=0}^{m} a_i\tau^i = \sum_{i=0}^{m} \left(\sum_{j+t=i} c_t b_j^{q^t} \right) \tau^i + \sum_{i=0}^{n-1} d_i\tau^i \quad \text{with } d_i \in \mathbb{L} \text{ for } 0 \leq i \leq n-1.$$

□

From this proposition we note that $r(x)$ is the remainder when the usual division algorithm is applied to $f(x), g(x) \in \mathbb{L}[x]$. The following corollary implies that the twisted polynomial ring $\mathbb{L}\{\tau\}$ is a left principal ideal domain.

Corollary 4.1.12. *Every left ideal in $\mathbb{L}\{\tau\}$ is principal.*

Proof. Suppose I is a nonzero left ideal in $\mathbb{L}\{\tau\}$. Take an element $g(\tau) \in I$ of least degree in τ. If $f(\tau) \in I$, then by the preceding proposition, there exist unique polynomials $h(\tau)$ and $r(\tau)$ such that $f(\tau) = h(\tau) \cdot g(\tau) + r(\tau)$ with $r(\tau) = 0$ or $\deg_\tau(r) < \deg_\tau(g)$. By definition of $g(\tau)$ and the fact that $r(\tau) \in I$, we conclude that $r(\tau) = 0$. Thus, every element $f(\tau) \in I$ is right divisible by $g(\tau)$. The result follows. □

One can also obtain the left analogue of Proposition 4.1.11 in perfect fields (See Definition 2.1.11). The perfectness is needed to ensure that the coefficients of $h(\tau)$ and $r(\tau)$ are in $\mathbb{L}$.

Theorem 4.1.13 (Left Division Algorithm)**.** *Let $\mathbb{L}$ be a perfect field and $f(\tau), g(\tau) \in \mathbb{L}\{\tau\}$, with $g(\tau) \neq 0$. Then there exist unique polynomials $h(\tau), r(\tau) \in \mathbb{L}\{\tau\}$ such that*

$$f(\tau) = g(\tau) \cdot h(\tau) + r(\tau)$$

with $r(\tau) = 0$ or $\deg_\tau(r) < \deg_\tau(g)$.

□

Corollary 4.1.14. *If $\mathbb{L}$ is a perfect field, then every right ideal of $\mathbb{L}\{\tau\}$ is principal.*

□

Example 4.1.15. Let $\mathbb{L} = \mathbb{F}_q(T)$ and $f(\tau), g(\tau) \in \mathbb{L}\{\tau\}$ with $f(\tau) = \tau^2 - \tau + T$ and $g(\tau) = \tau - T^2$. Then

$$f(\tau) = \tau^2 - \tau + T = (\tau + (T^2 - 1)^q \tau^0)(\tau - T^2) + (T + T^2(T^2 - 1)^q)\tau^0.$$

In $\overline{\mathbb{L}}$,

$$f(\tau) = (\tau - T^2)(\tau + (T^2 - 1)^{1/q} \tau^0) + (T + T^2(T^2 - 1)^{1/q})\tau^0.$$

If we use the right Euclidean algorithm, we can now find the *right greatest common divisor* of $f(\tau), g(\tau) \in \mathbb{L}\{\tau\}$, which is the monic generator of the left ideal generated by $f(\tau)$ and $g(\tau)$. This polynomial will be denoted by $\operatorname{rgcd}(f(\tau), g(\tau))$.

Definition 4.1.16. Let $f(\tau) \in \mathbb{L}\{\tau\}$ be monic. Then $f(\tau)$ is said to be *prime* or *irreducible* if it has no monic right divisors in $\mathbb{L}\{\tau\}$ other than itself and τ^0.

Definition 4.1.17. Two polynomials $f(\tau), g(\tau) \in \mathbb{L}\{\tau\}$, not both zero, are said to be *right relatively prime* if and only if $\operatorname{rgcd}(f(\tau), g(\tau)) = \tau^0 = 1$.

Lemma 4.1.18. *Let $\mathbb{L}$ be a field of characteristic p. If $f(\tau), g(\tau) \in \mathbb{L}\{\tau\}$, then*

$$rgcd(f(\tau), g(\tau)) = \gcd(f(x), g(x))_{x=\tau}.$$

Proof. Every right hand divisor is also an ordinary divisor of a polynomial. So the (right) Euclidean algorithm in $\mathbb{L}\{\tau\}$ can be considered as the ordinary Euclidean algorithm in $\mathbb{L}(x)$. □

Definition 4.1.19. Let $f(\tau), g(\tau) \in \mathbb{L}\{\tau\}$, not both zero. The *right least common multiple* of $f(\tau)$ and $g(\tau)$, denoted $\text{rlcm}(f(\tau), g(\tau))$, is the monic polynomial of least degree in $\mathbb{L}\{\tau\}$ which is right divisible by both $f(\tau)$ and $g(\tau)$.

Lemma 4.1.20. *The right least common multiple of $f(\tau)$ and $g(\tau)$ exists.*

Proof. The right least common multiple of $f(\tau)$ and $g(\tau)$ is the monic generator of the left ideal which is the intersection of the left ideals generated by $f(\tau)$ and $g(\tau)$. This polynomial exists by Corollary 4.1.12. □

Lemma 4.1.21. *If $f(\tau), g(\tau) \in \mathbb{L}\{\tau\}$, then there exists a polynomial $d(\tau) \in \mathbb{L}\{\tau\}$ with*

$$f(\tau) \cdot g(\tau) = d(\tau) \cdot f(\tau)$$

if and only if rlcm$(f(\tau), g(\tau))$ divides $f(\tau) \cdot g(\tau)$ from the right.

Proof. See [Gos98, Lemma 1.10.5]. □

As before, suppose $\mathbb{L}$ is a field of positive characteristic p. Let $\overline{\mathbb{L}}$ be its algebraic closure and suppose H is a finite additive subgroup of $\overline{\mathbb{L}}$. Define the polynomial

$$g(x) := \prod_{\lambda \in H} (x - \lambda)$$

in $\mathbb{L}[x]$. Let x_0 be another variable and define the polynomial

$$g_0(x) := g(x + x_0) - g(x_0),$$

which is an element of $\mathbb{L}(x_0)[x]$. It annihilates H since H is a subgroup of $(\overline{\mathbb{L}}, +)$. Observe, further, that $\deg_x(g(x)) = \deg_x(g_0(x))$ and both polynomials are monic in x, so they are equal. Hence, $g(x) \in \overline{\mathbb{L}}[x]$ is additive, so it takes the form $\sum_{i=0}^{n} \alpha_i x^{q^i}$ with $\alpha_i \in \mathbb{L}$. Therefore, the corresponding polynomial $g(\tau) = \sum_{i=0}^{n} \alpha_i \tau^i \in \mathbb{L}\{\tau\}$ has kernel H and $\#H = q^{\deg_\tau(g)}$.

Now let $f(\tau) \in \mathbb{L}\{\tau\}$ be a polynomial that also annihilates H. By using Proposition 4.1.11, we can write

$$f(\tau) = m(\tau) \cdot g(\tau) + r(\tau),$$

where $\deg_\tau(r) < \deg_\tau(g)$. Since $f(\tau)$ and $g(\tau)$ both annihilate H, this is also the case for $r(\tau)$. So either $q^{\deg_\tau(r)} \geq \#H$ contradicting $\deg_\tau(r) < \deg_\tau(g)$, or $r(\tau) = 0$.

In summary, we get the following result (see [Mat97, Proposition 1.7]).

Proposition 4.1.22. *Let $\mathbb{L}$ be a field of characteristic p and $\overline{\mathbb{L}}$ be its algebraic closure. If H is a finite subgroup of $\overline{\mathbb{L}}$, then the following properties hold:*

(a) There exists a unique monic polynomial $g(\tau) \in \mathbb{L}\{\tau\}$ such that $H = \ker g$ and $\#H = q^{\deg_\tau(g)}$.

(b) For each polynomial $f(\tau) \in \mathbb{L}\{\tau\}$ annihilating H, there exists a unique polynomial $m(\tau) \in \mathbb{L}\{\tau\}$ such that $f(\tau) = m(\tau) \cdot g(\tau)$.

For a more in-depth discussion of the divisibility properties of the polynomials in $\mathbb{L}\{\tau\}$, see [Gos98] (Chapter 1) and [Ore33a, Ore33b].

4.2 Basic Properties of Drinfeld Modules

Our next goal is to define Drinfeld modules and give some basic properties of these objects. The introductory material presented in this section can be found in [Gos98] (Chapters 3 and 4) and [Ros02] (Chapters 12 and 13). One may also consider [DH87], [Hay92], [Mat97], and [Sal06] (Chapter 13) for good expositions on Drinfeld modules.

For the purposes of this research, we use the classical setting for a Drinfeld module. A more general setting is given in [Gos98, Chapter 4]. We set up the following notation:

$$\begin{aligned}
\mathbb{F}_q &= \text{finite field of } q \text{ elements with } \mathrm{char}(\mathbb{F}_q) = p \\
\mathcal{C} &= \mathbb{P}^1 = \text{projective line over } \mathbb{F}_q \\
\infty &= 1/T, \text{a fixed closed point of } \mathcal{C} \text{ of degree } \deg(\infty) = d_\infty = 1 \text{ over } \mathbb{F}_q \\
\mathbf{A} &= \mathbb{F}_q[T] = \text{polynomial ring in } T \text{ over } \mathbb{F}_q \\
\mathbf{K} &= \mathbb{F}_q(T) = \text{field of fractions of } \mathbf{A};\ \text{the function field of } \mathcal{C} \text{ over } \mathbb{F}_q \\
\nu_\infty &= \text{the valuation in } \mathbf{K} \text{ associated to the prime } \infty \\
\mathbf{K}_\infty &= \mathbb{F}_q((1/T)) = \text{the completion of } \mathbf{K} \text{ with respect to } \nu_\infty \\
\overline{\mathbf{K}}_\infty &= \text{a fixed algebraic closure of } \mathbf{K}_\infty \\
\mathbf{C} &= \text{the completion of } \overline{\mathbf{K}}_\infty \text{ from the canonical extension of } \nu_\infty \text{ from } \mathbf{K}_\infty \text{ to } \overline{\mathbf{K}}_\infty \\
\mathbb{L} &= \text{a field containing } \mathbb{F}_q
\end{aligned}$$

Recall that the basic properties of $\mathbf{A}$ and $\mathbf{K}$ were covered in Chapter 3. We have the following definition.

Definition 4.2.1. $\mathbb{L}$ is called an $\mathbf{A}$-*field* if it comes equipped with an $\mathbb{F}_q$-algebra homomorphism $\gamma : \mathbf{A} \longrightarrow \mathbb{L}$. We call γ the *structure map* from $\mathbf{A}$ to $\mathbb{L}$. The prime ideal $\mathfrak{p}$ which is the kernel of γ is called the $\mathbf{A}$-*characteristic* of $\mathbb{L}$, denoted $\mathrm{char}_{\mathbf{A}}(\mathbb{L})$, i.e., $\mathrm{char}_{\mathbf{A}}(\mathbb{L}) = \mathfrak{p}$. If $\mathfrak{p} = (0)$, we say that $\mathbb{L}$ has *generic* $\mathbf{A}$-*characteristic*; otherwise we say that $\mathfrak{p}$ is *finite* and $\mathbb{L}$ has a *finite* $\mathbf{A}$-*characteristic*.

So it can be seen from this definition that the structure map γ is either containment in $\mathbb{L}$ or reduction modulo a prime ideal. Now consider the ring $\mathbb{L}\{\tau\}$ over $\mathbb{L}$ with τ as the q-th power map. Let $f(\tau) = \sum_{i=0}^{t} a_i \tau^i \in \mathbb{L}\{\tau\}$. Define the map

$$\begin{aligned}
D : \mathbb{L}\{\tau\} &\longrightarrow \mathbb{L} \\
f(\tau) &\longmapsto D(f(\tau)) = a_0.
\end{aligned} \tag{4.5}$$

When translated into the ring of additive polynomials, D applied to $\sum_{i=0} a_i x^{q^i}$ is just differentiation with respect to x. It is clear that D is a homomorphism of $\mathbb{F}_q$-algebras.

For the next definition, we require that $\mathbb{L}$ is an $\mathbf{A}$-field with structure map $\gamma : \mathbf{A} \longrightarrow \mathbb{L}$ and D is the map defined in (4.5).

Definition 4.2.2. Let $\varphi : \mathbf{A} \longrightarrow \mathbb{L}\{\tau\}$ be an $\mathbb{F}_q$-algebra homomorphism. Then φ is called a *Drinfeld* $\mathbf{A}$*-module* (or simply, *Drinfeld module* over $\mathbb{L}$) if and only if the following conditions hold:

1. For all $a \in \mathbf{A}$, $(D \circ \varphi)(a) = \gamma(a)\tau^0$, i.e., the constant term of $\varphi(a)$ is $\gamma(a)\tau^0$.
2. For some $a \in \mathbf{A}$, $\varphi(a) \neq \gamma(a)\tau^0$, i.e., $\varphi(a) \notin \mathbb{L}$ for some $a \in \mathbf{A}$.

For simplicity, we denote the image of $a \in \mathbf{A}$ under φ by φ_a. Note that the second condition in Definition 4.2.2 guarantees that Drinfeld modules are nontrivial. We also remark that $\varphi_\alpha = \alpha\tau^0$, for all $\alpha \in \mathbb{F}_q$. This follows from the fact that φ, as an $\mathbb{F}_q$-algebra homomorphism, sends 1 to τ^0. So

$$\varphi_\alpha = \alpha\varphi_1 = \alpha\tau^0, \qquad \forall\ \alpha \in \mathbb{F}_q.$$

Observe that if B is some field extension of $\mathbb{L}$, then the structure map γ transforms B into an $\mathbf{A}$-module using the standard action

$$a \cdot u = \gamma(a)u, \qquad \text{for } a \in \mathbf{A},\ u \in B. \tag{4.6}$$

The motivation behind the definition of a Drinfeld module is that it turns B into an $\mathbf{A}$-module through the relation

$$a * u := \varphi_a(u),$$

which is a "deformation" of (4.6) since both $a \cdot u$ and $a * u$ have the same linear term $\gamma(a)u$. Moreover, by Definition 4.2.2, $a \cdot u \neq a * u$ for some $a \in \mathbf{A}$, so $a * u$ is a new action. Note that every such extension B of $\mathbb{L}$ is an $\mathbb{L}$-algebra, and that this deformation action can be generalized to any $\mathbb{L}$-algebra, see [Ros02], pp. 220-221.

Example 4.2.3 (The Carlitz Module)**.** Let $\mathbf{A}$ and $\mathbf{K}$ be as defined earlier and $\mathbb{L} = \mathbf{K}$. In this case, let the map $\gamma : \mathbf{A} \longrightarrow \mathbb{L}$ be just inclusion in $\mathbb{L}$. Since $\mathbf{A}$ is generated freely as an $\mathbb{F}_q$-algebra by an element T, it follows that for every element $f \in \mathbb{L}\{\tau\}$, there is a unique homomorphism from $\mathbf{A}$ to $\mathbb{L}\{\tau\}$ which sends T to f provided that the constant term of f is T and $f \notin \mathbf{K}$. The simplest example of such f is $T + \tau$ and the resulting Drinfeld module over $\mathbf{K}$ is called the *Carlitz module*, which we denote by ρ. Hence, $\rho_T = T + \tau$. Note that for higher values of n, ρ_{T^n} can be obtained using (4.4), ρ_T, and the fact that ρ is an $\mathbb{F}_q$-algebra mapping. For instance, let $n = 2$ so

$$\rho_{T^2} = \rho_T \cdot \rho_T = (T + \tau) \cdot (T + \tau) = T^2 + \tau T + T\tau + \tau^2 = T^2 + (T^q + T)\tau + \tau^2.$$

Finally, for an element $a \in \mathbf{A}$ with $a = \sum_{i=0}^{d} a_i T^i$, $\{a_i\} \subseteq \mathbb{F}_q$, and $a_d \neq 0$, we have

$$\rho_a = a\tau^0 + \sum_{i=1}^{d} c_i \tau^i,$$

where $\{c_i\} \subset \mathbf{A}$ and $c_d = a_d$.

Now consider a more general case of a Drinfeld module, i.e., γ is not necessarily the inclusion map. Let $0 \neq a \in \mathbf{A}$. Recall, by Definition 4.2.2, that the constant term of φ_a is equal to $\gamma(a)$; that is, $\varphi_a = \gamma(a)+$ terms divisible by τ. So

$$\varphi_T = \gamma(T) + a_1\tau + a_2\tau^2 + \cdots + a_r\tau^r, \tag{4.7}$$

where $a_i \in \mathbb{L}$ and $a_r \neq 0$ for some $r > 0$. Using this fact and $\varphi_{T^2} = \varphi_T \cdot \varphi_T$, we remark that the constant term of φ_{T^2} is $\gamma(T^2)$ and the highest power of τ in φ_{T^2} is $2r$ with leading coefficient $a_r^{1+q^r}$. Continuing in this manner, we find that for φ_{T^n} the constant term is $\gamma(T^n)$ and the highest power of τ is nr with leading coefficient

$$a_r^{1+q^r+\cdots+q^{n-1}r}.$$

Using these remarks and the fact that φ is a homomorphism of $\mathbb{F}_q$-algebras, we see that for $a \in \mathbf{A}$ the degree in τ of φ_a is $r \deg_T(a)$. Thus,

$$\varphi_a = \gamma(a) + c_1\tau + c_2\tau^2 + \cdots + c_{r\deg_T(a)}\tau^{r\deg_T(a)}, \tag{4.8}$$

where $c_i \in \mathbb{L}$, and $c_{r\deg_T(a)} \neq 0$. It follows that $\deg(\varphi_a(x)) = q^{r\deg_T(a)}$, where

$$\varphi_a(x) = \gamma(a)x + c_1x^q + c_2x^{q^2} + \cdots + c_{r\deg_T(a)}x^{q^{r\deg_T(a)}}.$$

Definition 4.2.4. The number r that satisfies the equation

$$\deg_\tau(\varphi_a) = r\deg_T(a)$$

for all $a \in \mathbf{A}$ is called the *rank* of φ.

Torsion Points

We now look at torsion points associated to a Drinfeld module φ over $\mathbb{L}$. Let $I \subset \mathbf{A}$ be an ideal. Recall that $\mathbf{A}$ is a Dedekind domain, so I may be generated by at most two elements, say $i_1, i_2 \in I$. Moreover, by Proposition 4.1.11, $\mathbb{L}\{\tau\}$ has a right division algorithm so we can find $\mathrm{rgcd}(\varphi_{i_1}, \varphi_{i_2})$. It is the monic generator of the left ideal generated by φ_{i_1} and φ_{i_2}. Let $\overline{\mathbb{L}}$ be a fixed algebraic closure of $\mathbb{L}$.

Definition 4.2.5. Let J be the left ideal in $\mathbb{L}\{\tau\}$ generated by the set $\{\varphi_i \mid i \in I\}$, where $I \subset \mathbf{A}$ is an ideal. Define φ_I as the unique monic generator of the left ideal J.

Definition 4.2.6. Define $\varphi[I] := \{\lambda \in \overline{\mathbb{L}} \mid \varphi_I(\lambda) = 0\} \subset \varphi(\overline{\mathbb{L}})$. It is the finite subgroup of $\varphi(\overline{\mathbb{L}})$ given by the roots of φ_I. In particular, for $0 \neq a \in \mathbf{A}$, we set

$$\varphi[a] := \varphi[(a)] := \{\lambda \in \overline{\mathbb{L}} \mid \varphi_a(\lambda) = 0\}.$$

Note that $\varphi[a]$ is a submodule of the $\mathbf{A}$-module

$$\varphi[\mathbf{A}] := \{\lambda \in \overline{\mathbb{L}} \mid \varphi_a(\lambda) = 0 \text{ for some } a \in \mathbf{A}, a \neq 0\}.$$

The next lemma identifies the $\mathbf{A}$-module structures of these modules.

Lemma 4.2.7. *Let M be an $\mathbf{A}$-module and $a \in \mathbf{A}$ with $a \neq 0$. If for each b dividing a, the submodule $M[b] = \{m \in M \mid bm = 0\}$ has $q^{r\deg_T(b)}$ elements, then*

$$M[a] \cong \mathbf{A}/a\mathbf{A} \oplus \mathbf{A}/a\mathbf{A} \oplus \cdots \oplus \mathbf{A}/a\mathbf{A} \quad r \text{ times.}$$

Proof. Suppose a has prime factorization $a = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t}$, where $\alpha \in \mathbb{F}_q^*$ and the P_i are distinct monic irreducible divisors of a. Then

$$M[a] \cong \oplus_{i=1}^{t} M[P_i^{e_i}].$$

By the Chinese Remainder Theorem, it is enough to consider the case where a is a prime power, i.e., $a = P^e$. So we assume that this is the case.

Consider the field $\mathbf{A}/P\mathbf{A}$ where $\#(\mathbf{A}/P\mathbf{A}) = q^{\deg_T(P)}$. Note that $M[P]$ is a vector space over $\mathbf{A}/P\mathbf{A}$ with $q^{r \deg_T(P)}$ elements, by hypothesis. Hence, the dimension of $M[P]$ over $\mathbf{A}/P\mathbf{A}$ is r. Using the structure of modules over principal ideal domains, we see that $M[P^e]$ must be isomorphic to a sum of r cyclic submodules,

$$M[P^e] \cong \mathbf{A}/P^{f_1}\mathbf{A} \oplus \mathbf{A}/P^{f_2}\mathbf{A} \oplus \cdots \oplus \mathbf{A}/P^{f_r}\mathbf{A},$$

with $f_i \leq e$ for $1 \leq i \leq r$. Now,

$$\#(\mathbf{A}/P^{f_1}\mathbf{A} \oplus \mathbf{A}/P^{f_2}\mathbf{A} \oplus \cdots \oplus \mathbf{A}/P^{f_r}\mathbf{A}) = q^{(f_1+f_2+\cdots+f_r)\deg_T(P)}.$$

On the other hand, by assumption we have $\#M[P^e] = q^{re \deg_T(P)}$. These two cardinalities should be equal, thus $f_i = e$ for $1 \leq i \leq r$. The result follows. □

The Rank of a Drinfeld Module

As before, we assume that $\mathbb{L}$ is an $\mathbf{A}$-field and φ is a Drinfeld module over $\mathbb{L}$. Also, $\overline{\mathbb{L}}$ is a fixed algebraic closure of $\mathbb{L}$. Let $a \in \mathbf{A}$, so $\varphi_a \in \mathbb{L}\{\tau\}$. Define

$$\mu(a) := -\deg_\tau(\varphi_a).$$

Hence, $\mu(0) = \infty$.

Recall Definition 4.2.4. We now give the basis of the definition of the rank of a Drinfeld module. This is the special case $\mathbf{K} = \mathbb{F}_q(T)$ in [Gos98] Lemma 4.5.1 and Proposition 4.5.3.

Proposition 4.2.8. *The rank r of a Drinfeld module φ is a nonzero rational number that satisfies*

$$\mu(a) = rd_\infty \nu_\infty(a) = -r \deg_T(a), \qquad \forall\ a \in \mathbf{A}.$$

Moreover, r is a positive integer.

Proof. For $a, b \in \mathbf{A}$, the map $\mu : \mathbf{A} \longrightarrow \mathbb{Z} \cup \{\infty\}$ satisfies

1. $\mu(a) = \infty$ if and only if $a = 0$,
2. $\mu(ab) = \mu(a) + \mu(b)$, and
3. $\mu(a + b) \geq \min\{\mu(a), \mu(b)\}$.

Since Drinfeld modules are nontrivial, it follows that μ gives rise to a valuation on $\mathbf{K}$ that can only correspond to ∞. So the first assertion follows.

For the second assertion, we let $\mathfrak{P}$ be a prime of $\mathbf{A}$ distinct from the $\mathbf{A}$-characteristic of $\mathbb{L}$. Note that $\mathbf{A}$ has class number 1 as a Dedekind domain. Also, let $a \in \mathbf{A}$ such that $(a) = \mathfrak{P}$. Using the first result of this proposition, we see that the $\mathbf{A}$-module $\varphi[a] \subset \overline{\mathbb{L}}$ has precisely $q^{r \deg_T(a)}$ elements. On the other hand, every $b \in \mathbf{A}$ prime to $\mathfrak{P}$ must act as an automorphism of $\varphi[a]$. Again, we apply the structure of modules over Dedekind domains to get

$$\varphi[a] \cong \oplus_{i=1}^{t} \mathbf{A}/\mathfrak{P}^{f_i}\mathbf{A}$$

for some integers t and f_i, $1 \leq i \leq t$. We proceed as in the proof of Lemma 4.2.7 to get $t = r$ and $f_i = 1$ for all i. This completes the proof of the proposition. □

Corollary 4.2.9. *If $\varphi : \mathbf{A} \longrightarrow \mathbb{L}\{\tau\}$ is a Drinfeld module, then φ is injective.*

Proof. See [Mat97, Proposition 2.3(a)]. □

The Height of a Drinfeld Module

We now define the height of a Drinfeld module. Assume that the $\mathbf{A}$-characteristic of $\mathbb{L}$ is $\mathfrak{p} \neq (0)$. Note that this is not much of a restriction since for $\mathfrak{p} = (0)$, γ is inclusion, so the

smallest nonzero coefficient in φ_a (for a nonzero $a \in \mathbf{A}$) is always the constant coefficient "a". Let $\nu_{\mathfrak{p}} : \mathbf{K}_\infty \longrightarrow \mathbb{Z}$ be the normalized valuation associated to $\mathfrak{p}$. So, for instance, if $a \in \mathbf{K}_\infty$ has a zero at $\mathfrak{p}$ of order t, then $\nu_{\mathfrak{p}}(a) = t$. For each $a \in \mathbf{A}$, define $\omega(a)$ as the smallest integer $t \geq 0$ for which the coefficient of τ^t in φ_a is nonzero. Moreover, define $\omega(0) = \infty$. By abuse of notation, we also use $\mathfrak{p}$ to denote the polynomial generator of the ideal $\mathfrak{p}$. The following result is the special case $\mathbf{K} = \mathbb{F}_q(T)$ in [Gos98] Lemma 4.5.6 and Proposition 4.5.7.

Proposition 4.2.10. *There is a positive rational number h such that*

$$\omega(a) = h\nu_{\mathfrak{p}}(a) \deg_T(\mathfrak{p}) \tag{4.9}$$

for all $a \in \mathbf{A}$. Moreover, h is a positive integer.

Proof. To prove the existence of h, we consider the mapping $a \longmapsto \omega(a)$. This satisfies $\omega(ab) = \omega(a) + \omega(b)$, and $\omega(a+b) \geq \min\{\omega(a), \omega(b)\}$. Furthermore, $\omega(a) \geq 0$ for all $a \in \mathbf{A}$, and $\omega(a) > 0$ if and only if $a \in \mathfrak{p}$. Hence, ω can be extended to a valuation on $\mathbf{K}_\infty$ which must correspond to $\mathfrak{p}$. Thus, the number $h \in \mathbb{Q}$ satisfying (4.9) exists.

For the next assertion, we consider $\varphi[\mathfrak{p}]$, i.e., the $\mathbf{A}/\mathfrak{p}\mathbf{A}$-module of $\mathfrak{p}$-torsion points in a fixed algebraic closure $\overline{\mathbb{L}}$ of $\mathbb{L}$. The elements of $\varphi[\mathfrak{p}]$ are the roots of $\varphi_{\mathfrak{p}}(x) = 0$, where $\varphi_{\mathfrak{p}}$ is the monic generator of the left ideal generated by the set $\{\varphi_a \mid a \in \mathfrak{p}\}$ (see Definitions 4.2.5 and 4.2.6). Write

$$\varphi_{\mathfrak{p}}(\tau) = \alpha\tau^{\omega(\mathfrak{p})} + \text{higher terms},$$

with $\alpha \neq 0$. So

$$\#\varphi[\mathfrak{p}] = q^{\deg_\tau(\varphi_{\mathfrak{p}}) - \omega(\mathfrak{p})}.$$

Alternatively, if $\varphi[\mathfrak{p}]$ is of dimension t as a vector space over $\mathbf{A}/\mathfrak{p}\mathbf{A}$, then

$$\#\varphi[\mathfrak{p}] = q^{t \deg_T(\mathfrak{p})}.$$

Since $\mathbf{A}$ has class number 1, we have $\mathfrak{p} = (a)$ for some $a \in \mathbf{A}$. We see that

$$\begin{aligned} \#\varphi[a] = \#\varphi[\mathfrak{p}] &= q^{(\deg_\tau(\varphi_{\mathfrak{p}}) - \omega(\mathfrak{p}))} \\ &= q^{t \deg_T(\mathfrak{p})}. \end{aligned}$$

From (4.9), we get

$$\begin{aligned} \#\varphi[a] &= q^{r\deg_T(a)-\omega(a)} \\ &= q^{r\deg_T(\mathfrak{p})-h\deg_T(\mathfrak{p})}. \end{aligned}$$

So $h = r - t$ and $h \in \mathbb{Z}$. The result now follows from the fact that r is a positive integer. □

Definition 4.2.11. The positive integer h given in Proposition 4.2.10 is called the *height* of φ.

As we have seen from the proof of Proposition 4.2.10, the rank r and height h of a Drinfeld module φ over an $\mathbf{A}$-field $\mathbb{L}$ can be used to determine the structure of $\varphi[\mathfrak{a}]$ for any ideal $\mathfrak{a}$ of $\mathbf{A}$.

Theorem 4.2.12 (Drinfeld)**.** *Let $\mathbb{L}$ be an $\mathbf{A}$-field with $char_{\mathbf{A}}(\mathbb{L}) = \mathfrak{p}$ and suppose $\mathfrak{a}$ is an ideal of $\mathbf{A}$. If φ is a Drinfeld module over $\mathbb{L}$ of rank r and of height h (if $\mathfrak{p}$ is finite), then the following properties hold:*

(a) If $\mathfrak{a} \nsubseteq \mathfrak{p}$, then $\varphi[\mathfrak{a}]$ is a free $\mathbf{A}/\mathfrak{a}$-module of rank r.

(b) If $\mathfrak{a} = \mathfrak{p}^m$, then $\varphi[\mathfrak{a}]$ is a free $\mathbf{A}/\mathfrak{a}$-module of rank $r - h$.

Proof. See [Mat97, Theorem 2.5]. □

Remark 4.2.13. Let $\mathbb{L}$ and $\mathfrak{p}$ be as in Theorem 4.2.12. A special case of this theorem for $\mathfrak{a} = \mathfrak{q}^e$ with $\mathfrak{q}$ a nonzero prime ideal of $\mathbf{A}$ and integer $e \geq 1$ is as follows:

$$\varphi[\mathfrak{q}^e] \cong \begin{cases} (\mathbf{A}/\mathfrak{q}^e)^r, & \text{if } \mathfrak{q} \neq \mathfrak{p} \\ (\mathbf{A}/\mathfrak{q}^e)^{r-h}, & \text{if } \mathfrak{q} = \mathfrak{p}. \end{cases}$$

4.3 Morphisms of Drinfeld Modules

In this section we present properties of maps between Drinfeld modules. These maps will be used to define the endomorphism ring of a Drinfeld module. Our exposition here is based

on [Gek91], [Gos98] (Chapter 4), [Mat97], and [Ros02] (Chapter 13). The results presented here are analogous to the known properties of morphisms between elliptic curves.

Assume that $\mathbb{L}$ is an $\mathbf{A}$-field and let $\overline{\mathbb{L}}$ be a fixed algebraic closure of $\mathbb{L}$. Let φ and ψ be Drinfeld modules over $\mathbb{L}$, both of rank $r > 0$.

Definition 4.3.1. A *morphism* from φ to ψ over $\mathbb{L}$ is a polynomial $u(\tau) \in \mathbb{L}\{\tau\}$ such that

$$u \cdot \varphi_a = \psi_a \cdot u, \quad \forall\ a \in \mathbf{A}. \tag{4.10}$$

The set of all such morphisms is denoted by $\mathrm{Hom}_{\mathbb{L}}(\varphi, \psi)$ and if $\varphi = \psi$, then we denote $\mathrm{Hom}_{\mathbb{L}}(\varphi, \psi)$ by $\mathrm{End}_{\mathbb{L}}(\varphi)$. A nonzero morphism is called an *isogeny*, and an *isomorphism* if in addition u is invertible, i.e., $u = \varepsilon \in \mathbb{L}^*$. In this case, φ and ψ are called *isogenous* or *isomorphic*, respectively.

Remark 4.3.2. $\mathrm{End}_{\mathbb{L}}(\varphi)$ is a subring of $\mathbb{L}\{\tau\}$ under composition.

Proposition 4.3.3. *Let $u \in \mathbb{L}\{\tau\}$ be a morphism from from φ to ψ. Then u is an isomorphism if and only if* $\deg_\tau(u) = 0$.

Proof. u is an isomorphism if and only if there exists an element $v \in \mathbb{L}\{\tau\}$ such that $u \cdot v = \tau^0$. □

Example 4.3.4. Let φ be a rank r Drinfeld module over the $\mathbf{A}$-field $\mathbb{L}$ and let $u \in \mathbb{L}^*$. Then φ is isomorphic to the Drinfeld module defined by $\psi = u^{-1} \cdot \varphi \cdot u$. Moreover, if φ is determined by (4.7), then

$$\psi_T = \gamma(T) + u^{q-1}a_1\tau + \cdots + u^{q^r-1}a_r\tau^r,$$

where $a_i \in \mathbb{L}$, $a_r \neq 0$.

Denote a morphism u from φ to ψ by $u : \varphi \longrightarrow \psi$.

Definition 4.3.5. Let $u : \varphi \longrightarrow \psi$ be an isogeny of Drinfeld modules over $\mathbb{L}$.

1. u is *separable* if and only if $u(\tau)$ is separable (as a polynomial over $\mathbb{L}$).

2. u is *purely inseparable* if and only if $u(\tau) = \tau^j$ for some $j > 0$.

Proposition 4.3.6. *Let φ and ψ be Drinfeld modules over an $\mathbf{A}$-field $\mathbb{L}$ and $u \in Hom_{\mathbb{L}}(\varphi, \psi)$ an isogeny. Then there exists an isogeny $\widehat{u} \in Hom_{\mathbb{L}}(\psi, \varphi)$ such that*

$$\widehat{u} \cdot u = \varphi_a \tag{4.11}$$

for some nonzero $a \in \mathbf{A}$.

Proof. Let H be the kernel of u in $\overline{\mathbb{L}}$; that is, $H = \{\lambda \in \overline{\mathbb{L}} \mid u \cdot \lambda = u(\lambda^q) = 0\}$. Then H is a finite torsion $\mathbf{A}$-module via φ, so it is annihilated by φ_a for some $a \in \mathbf{A}$. We know from Proposition 4.1.22(b) that there exists a polynomial $\widehat{u} \in \mathbb{L}\{\tau\}$ such that $\varphi_a = \widehat{u} \cdot u$. Since u is an isogeny from φ to ψ we have $u \cdot \varphi_b = \psi_b \cdot u$ for $b \in \mathbf{A}$. Then

$$\widehat{u} \cdot \psi_b \cdot u = \widehat{u} \cdot u \cdot \varphi_b = \varphi_a \cdot \varphi_b = \varphi_{ab} = \varphi_{ba} = \varphi_b \cdot \varphi_a = \varphi_b \cdot \widehat{u} \cdot u$$

in $\mathbb{L}\{\tau\}$. This shows that $\widehat{u} \cdot \psi_b = \varphi_b \cdot \widehat{u}$, and so $\widehat{u} \in \mathrm{Hom}_{\mathbb{L}}(\psi, \varphi)$. □

Corollary 4.3.7. *If $u : \varphi \longrightarrow \psi$ is an isogeny, then*

1. *$u \cdot \widehat{u} = \psi_a$ for some nonzero $a \in \mathbf{A}$.*

2. *the isogeny relation gives rise to an equivalence relation on Drinfeld modules over $\mathbb{L}$.*

Proof.

1. From (4.10) and (4.11) we get

$$u \cdot \widehat{u} \cdot u = u \cdot \varphi_a = \psi_a \cdot u.$$

   Thus $u \cdot \widehat{u} = \psi_a$ by cancellation.

2. Clearly, a Drinfeld module φ is isogenous to itself. In this case $u = \tau^0 = 1$. So reflexivity is satisfied. Next, suppose $u : \varphi \longrightarrow \psi$ is an isogeny. By the preceding

proposition, we see that $\widehat{u} : \psi \longrightarrow \varphi$ is also an isogeny. Thus symmetry is satisfied. Finally, let $u : \varphi \longrightarrow \psi$ and $v : \psi \longrightarrow \sigma$ be isogenies of Drinfeld modules over $\mathbb{L}$. So for $0 \neq a \in \mathbf{A}$, we have $u \cdot \varphi_a = \psi_a \cdot u$ by Definition 4.3.1, $\widehat{v} \cdot v = \psi_a$ by Proposition 4.3.6, and $v \cdot \widehat{v} = \sigma_a$ by part 1 of this corollary. Note that the product of two isogenies is again an isogeny. We need to find an isogeny $w : \varphi \longrightarrow \sigma$ to satisfy transitivity. The only possibility that we can consider is the polynomial $w = v \cdot u \in \mathbb{L}\{\tau\}$ and we can verify that

$$v \cdot u \cdot \varphi_a = v \cdot (u \cdot \varphi_a) = v \cdot \psi_a \cdot u = v \cdot (\widehat{v} \cdot v) \cdot u = (v \cdot \widehat{v}) \cdot v \cdot u = \sigma_a \cdot v \cdot u.$$

Thus isogeny is an equivalence relation on Drinfeld modules over $\mathbb{L}$.

□

Remark 4.3.8. Since $u, \widehat{u} \in \mathbb{L}\{\tau\}$, we see from Proposition 4.3.6 that φ_a is right divisible by u. Similarly, it follows from Corollary 4.3.7 that ψ_a is right divisible by $\widehat{u}$.

Definition 4.3.9. Let $u : \varphi \longrightarrow \psi$ be an isogeny of rank r Drinfeld modules over $\mathbb{L}$. The polynomial $\widehat{u} \in \mathbb{L}\{\tau\}$ that satisfies

$$\widehat{u} \cdot u = \varphi_a \quad \text{and} \quad u \cdot \widehat{u} = \psi_a,$$

for some nonzero $a \in \mathbf{A}$, is called the *dual isogeny* to u.

Additional description of isogenies and endomorphism rings of Drinfeld modules will be presented in the succeeding chapters of this work.

Chapter 5

Drinfeld Modules: Analytic View

As in the elliptic curve case, there is an analytic theory for Drinfeld modules. This is the main focus of this chapter. We show how Drinfeld modules arise from lattices, then determine the coefficients of these modules. A portion of this chapter is also devoted to an exposition on modular functions and modular polynomials for Drinfeld modules.

Throughout this chapter, we use $\mathbf{A}$, $\mathbf{K}$, $\mathbf{K}_\infty$, and $\mathbf{C}$ as defined in Section 4.2. In addition, we use $\mathbf{A}^+ := \{\text{monic polynomials in } \mathbf{A}\}$.

5.1 Lattices and the Exponential Function on $\mathbf{C}$

Let $\mathbf{A}$ and $\mathbf{K}$ be as before. Recall from Section 3.2 that $\mathbf{K}$ is provided with the degree valuation $\nu_\infty : \mathbf{K} \longrightarrow \mathbb{Z} \cup \{\infty\}$ defined by $\nu_\infty(a/b) = \deg_T(b) - \deg_T(a)$ for $a, b \in \mathbf{A}$ with $b \neq 0$ and $\nu_\infty(0) = \infty$. Moreover, recall that $\mathbf{C}$ is the completion of an algebraic closure of the completion $\mathbf{K}_\infty$ of $\mathbf{K}$ at the place $\infty = (1/T)$. Denote the absolute value on $\mathbf{C}$ by "$|\cdot|$". This absolute value is normalized by $|T| = q$. The sets $\mathbf{A}$, $\mathbf{K}$, $\mathbf{K}_\infty$, and $\mathbf{C}$ are the analogues of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, respectively, in the classical case.

Note that $\mathbf{C}$ is algebraically closed (see [Gos98], Proposition 2.1). A function from $\mathbf{C}$ to itself is said to be *entire* if it has a power series representation $\sum a_n z^n$ which converges everywhere (with respect to the extension of ν_∞ to $\mathbf{C}$). The set of zeros of an entire function forms a discrete subset of $\mathbf{C}$. The next two results hold over $\mathbf{C}$ and are very different from the archimedean situation.

Proposition 5.1.1. *If $f(z)$ is a nonconstant entire function on $\mathbf{C}$, then $f(z)$ has at least one zero.*

Proof. See [Gos98, Proposition 2.13]. □

Corollary 5.1.2 ([Ros02])**.** *If $f(z)$ is a nonconstant entire function on $\mathbf{C}$, then $f(z)$ is onto as a map from $\mathbf{C} \longrightarrow \mathbf{C}$.*

Proof. Suppose $c \in \mathbf{C}$. Then $f(z) - c$ is an entire function. So by the previous proposition, this function has a zero, say α. It follows that $f(\alpha) = c$. □

Definition 5.1.3. An $\mathbf{A}$-*lattice* in $\mathbf{C}$ is a discrete, finitely generated $\mathbf{A}$-submodule Λ of $\mathbf{C}$. The *rank* of Λ is its rank as a finitely generated $\mathbf{A}$-module.

The discreteness of a lattice Λ means that the intersection of Λ with any finite ball in $\mathbf{C}$ is finite. We also note that every lattice in $\mathbf{C}$ is an $\mathbb{F}_q$-vector space whose dimension is the rank of the lattice.

One can construct lattices in $\mathbf{C}$ as follows. Let $\{\omega_1, \omega_2, \ldots, \omega_r\}$ be a set of $\mathbf{K}_\infty$-linearly independent elements of $\mathbf{C}$ and $\{I_1, I_2, \ldots, I_r\}$ a set of fractional ideals of $\mathbf{A}$. Then the set

$$\Lambda = I_1\omega_1 + I_2\omega_2 + \cdots + I_r\omega_r$$

is a lattice in $\mathbf{C}$ of rank r. Every lattice in $\mathbf{C}$ has this form. So there is an abundance of lattices in $\mathbf{C}$ and they take on every rank.

Definition 5.1.4. Let Λ_1, Λ_2 be $\mathbf{A}$-lattices of rank r. A *morphism* from Λ_1 to Λ_2 is an element $c \in \mathbf{C}$ such that $c\Lambda_1 \subset \Lambda_2$. If $c\Lambda_1 = \Lambda_2$, then c is called an *isomorphism*. Define

$$\mathrm{Hom}(\Lambda_1, \Lambda_2) := \{c \in \mathbf{C} \mid \ c\Lambda_1 \subseteq \Lambda_2\}.$$

If $\Lambda_1 = \Lambda_2$, then we write $\mathrm{Hom}(\Lambda_1, \Lambda_2) = \mathrm{End}(\Lambda)$.

This definition makes the set of $\mathbf{A}$-lattices of rank r in $\mathbf{C}$ into a category.

Before we continue our description of lattices in $\mathbf{C}$, we consider the next lemma below. Here assume that V is a vector space of finite dimension over some field F. Equip V with the usual sup-norm based on an absolute value on F. A subgroup H of V is said to be *discrete* if and only if there exists a nontrivial neighbourhood N of 0 such that $H \cap N = \{0\}$.

Moreover, suppose F is a local field, $R \subset F$ is a discrete subring with F/R compact, and $\mathcal{F}$ is the quotient field of R. If H is a finitely generated R-module, then the *rank* of H is the dimension of $\mathcal{F} \otimes_R H$. We will use the following lemma in the next section.

Lemma 5.1.5. *Let V be a finite-dimensional vector space over F of dimension r and $H \subset V$ a discrete R-module. Then H is finitely generated over R and its rank is at most r.*

Proof. Set $W = F \cdot H \subseteq V$. Then W is a finitely generated vector space over F. Let $\{w_1', w_2', \ldots, w_n'\}$ be a basis for W. Thus each w_i' can be written as

$$w_i' = \sum_j f_{ij} h_{ij},$$

with $f_{ij} \in F$ and $h_{ij} \in H$. Note that there exists an $\alpha \in R$ such that $\alpha f_{ij} \in R$ for every i, j. Hence, we can now choose another basis $\{w_1, w_2, \ldots, w_n\}$ for W where $w_i = \alpha w_i' \in H$. Let $L = Rw_1 + Rw_2 + \cdots + Rw_n$. Then $L \subseteq H \subseteq W \subseteq V$. By assumption, H is discrete in V, so there exists a neighbourhood N_1 of 0 in V such that $H \cap N_1 = \{0\}$.

We can now find a neighbourhood N of 0 in V such that $N + N = N_1$. So for elements $x, y \in H$,

$$\{N + x\} \bigcap \{N + y\} \neq \emptyset \quad \Longleftrightarrow \quad x = y.$$

It follows that $N + L$ is a neighbourhood of 0 in V/L such that $(N + L) \cap H/L = \{0\}$. So H/L is a discrete subgroup of V/L and also of the compact abelian group

$$W/L = (Fw_1 + Fw_2 + \cdots + Fw_n) \,/\, (Rw_1 + Rw_2 + \cdots + Rw_n).$$

Then H/L is finite and therefore is finitely generated. It also follows that

$$\dim_{\mathcal{F}}(\mathcal{F} \otimes_R L) = \dim_{\mathcal{F}}(\mathcal{F} \otimes_R H) = \dim_{\mathcal{F}}(W),$$

giving the desired result. □

To a lattice Λ in $\mathbf{C}$ we associate the function

$$e_\Lambda(z) = z \prod_{0 \neq \lambda \in \Lambda} \left(1 - \frac{z}{\lambda}\right), \tag{5.1}$$

which is an entire function on $\mathbf{C}$. This follows from the fact that the series

$$\sum_{0 \neq \lambda \in \Lambda} \frac{1}{\lambda}$$

converges absolutely in the ∞-adic topology on $\mathbf{C}$. So the infinite product (5.1) converges for all $z \in \mathbf{C}$. The function $e_\Lambda(z)$ is called the *exponential function* associated to Λ. It is the unique entire function that has its zeros, all simple, at Λ and with leading term z.

The following results show the properties of the exponential function $e_\Lambda(z)$. See, for example, [Ros02] Chapter 13, [Gos98] Sections 4.2 and 4.3, or [Hay92].

Proposition 5.1.6. *Let Λ be a lattice in $\mathbf{C}$. Then e_Λ is additive and $\mathbb{F}_q$-linear; that is,*

$$e_\Lambda(x+y) = e_\Lambda(x) + e_\Lambda(y), \text{ for all } x, y \in \mathbf{C} \tag{5.2}$$

and

$$e_\Lambda(\alpha z) = \alpha e_\Lambda(z), \text{ for all } z \in \mathbf{C}, \ \alpha \in \mathbb{F}_q \tag{5.3}$$

Proof. Let $\Lambda_B = \{\lambda \in \Lambda \mid \nu_\infty(\lambda) \leq B\}$ for each positive integer B. One can check that this is a finite-dimensional $\mathbb{F}_q$-vector space. Then

$$e_\Lambda(z) = \lim_{B \longrightarrow \infty} e_{\Lambda_B}(z)$$

where

$$e_{\Lambda_B}(z) = z \prod_{0 \neq \lambda \in \Lambda_B} \left(1 - \frac{z}{\lambda}\right).$$

It remains to show that $e_{\Lambda_B}(z)$ is an $\mathbb{F}_q$-linear and additive polynomial in z.

Let $V \subset \mathbf{C}$ be a finite $\mathbb{F}_q$-vector space and set

$$f_V(z) = \prod_{v \in V} (z - v).$$

We will show that $f_V(z)$ $\mathbb{F}_q$-linear and additive by applying induction on the dimension of V. If $\dim V = 0$, then $V = \{0\}$. So $f_V(z) = z$, and clearly, the result is true in this case. Now suppose the case is true for vector spaces of dimension less than n and that $\dim V = n$.

Let $V = W + \mathbb{F}_q\omega$, where W is a subspace of V with $\dim W = n-1$ and $\omega \in V - W$. It follows from the definition that

$$f_V(z) = f_W(z) \prod_{0 \neq \alpha \in \mathbb{F}_q} f_W(z - \alpha\omega).$$

Since $\dim W = n-1$, we know that

$$f_W(z - \alpha\omega) = f_W(z) - \alpha f_W(\omega).$$

Then

$$f_V(z) = f_W(z)\left[f_W(z)^{q-1} - \alpha^{q-1} f_W(\omega)^{q-1}\right] = f_W(z)^q - f_W(\omega)^{q-1} f_W(z),$$

where $\alpha^{q-1} = 1$ for $\alpha \in \mathbb{F}_q^*$. The right-hand side of the preceding equation is additive and $\mathbb{F}_q$-linear since $f_W(z)$ is additive and $\mathbb{F}_q$-linear by induction hypothesis, $f_W(\omega)$ is constant, and exponentiation by q is additive and $\mathbb{F}_q$-linear. So $f_V(z)$ is $\mathbb{F}_q$-linear and additive in z. □

Proposition 5.1.7. *Let $\Lambda \subset \mathbf{C}$ be a lattice. Then e_Λ is Λ-periodic.*

Proof. This follows immediately from the fact that $e_\Lambda(z)$ is additive and it has its zeros at Λ. □

Proposition 5.1.8. *Let $\Lambda \subset \mathbf{C}$ be a lattice. Then e_Λ is surjective.*

Proof. This is an easy consequence of Corollary 5.1.2. □

Given the properties of $e_\Lambda(z)$, we can represent it by an everywhere convergent power series

$$e_\Lambda(z) = z + \sum_{i=1}^{\infty} \alpha_i(\Lambda) z^{q^i}, \qquad \alpha_i(\Lambda) \in \mathbf{C}. \tag{5.4}$$

We can do this by considering the partial products of (5.1) over the nonzero elements $\lambda \in \Lambda$ with $\nu_\infty(\lambda)$ less than some bound B. Since the elements λ are the roots of the partial products, they form a finite dimensional $\mathbb{F}_q$-vector space, and each partial product yields an $\mathbb{F}_q$-linear polynomial. From Lemma 4.1.6, it follows that each partial product is of the form $\sum_{i=0}^{n} \alpha_i(\Lambda) z^{q^i}$. By taking the limit as $B \longrightarrow \infty$, we get (5.4). It is clear that this exponential

function has derivative equal to 1. Moreover, $e_\Lambda(z)$ acts as the counterpart of the Weierstrass $\wp$-function in the elliptic curve case, so we have a "Weierstrass uniformization" for Drinfeld modules via this exponential function.

5.2 Construction of Drinfeld Modules over $\mathbf{C}$

In the classical setting, it is known that there is a correspondence (see (2.8)) between elliptic curves over $\mathbb{C}$ and tori $\mathbb{C}/\Lambda$ defined by lattices Λ in $\mathbb{C}$. Each lattice Λ can be used to construct an elliptic curve $\mathbb{C}/\Lambda$ and each elliptic curve $\mathbb{C}/\Lambda$ arises from a lattice Λ in $\mathbb{C}$. In this section, we show that there is a similar phenomenon involving Drinfeld modules; that is, there is a correspondence between lattices of rank r in $\mathbf{C}$ and Drinfeld modules of rank r over $\mathbf{C}$. The construction of such a Drinfeld module can be found, for example, in [DH87], [Gos98], [Hay92], or [Ros02].

Suppose $\Lambda \subseteq \Lambda'$ are two lattices of the same rank in $\mathbf{C}$. Then the function e_Λ maps the finite $\mathbf{A}$-module Λ'/Λ isomorphically to a finite $\mathbb{F}_q$-vector subspace of $\mathbf{C}$. Note that e_Λ can be naturally defined on cosets $\mu + \Lambda$, $\mu \in \Lambda$. Define

$$P(z, \Lambda'/\Lambda) := z \prod_{0 \neq \mu \in \Lambda'/\Lambda} \left(1 - \frac{z}{e_\Lambda(\mu)}\right). \tag{5.5}$$

Proposition 5.2.1. *$P(z, \Lambda'/\Lambda)$ is $\mathbb{F}_q$-linear of degree $\#\Lambda'/\Lambda$ and has initial term z. Furthermore,*

$$e_{\Lambda'}(u) = P(e_\Lambda(u), \Lambda'/\Lambda). \tag{5.6}$$

Proof. Using similar arguments involving the polynomial $f_V(z)$ in the proof of Proposition 5.1.6 shows that $P(z, \Lambda'/\Lambda)$ is $\mathbb{F}_q$-linear. The second assertion follows immediately from the definition of $P(z, \Lambda'/\Lambda)$ given in (5.5).

Next, we show that (5.6) holds. Note that $P(e_\Lambda(u), \Lambda'/\Lambda) = 0$ if and only if $e_\Lambda(\mu) = e_\Lambda(u) + \Lambda$ for some $\mu \in \Lambda'/\Lambda$. Since e_Λ is additive, this is equivalent to $e_\Lambda(u - \mu) \equiv 0 \pmod{\Lambda}$, which is true if and only if $u - \mu \in \Lambda$. Equivalently, $u \in \Lambda'$. Thus $P(e_\Lambda(u), \Lambda'/\Lambda)$

is an entire function with simple zeros at Λ'. Moreover, it has initial term u. These properties characterize $e_{\Lambda'}(u)$, and so we obtain (5.6). □

Proposition 5.2.2. *Let Λ be a lattice in $\mathbf{C}$ and $0 \neq a \in \mathbf{A}$. Then the following equality of entire functions holds.*

$$e_\Lambda(au) = aP(e_\Lambda(u), a^{-1}\Lambda/\Lambda). \tag{5.7}$$

Proof. It follows from Proposition 5.2.1 that

$$e_{a^{-1}\Lambda}(u) = P(e_\Lambda(u), a^{-1}\Lambda/\Lambda). \tag{5.8}$$

So by considering the zero set and the initial term, we see that

$$a^{-1}e_\Lambda(au) = e_{a^{-1}\Lambda}(u). \tag{5.9}$$

By using (5.8) and (5.9), we get (5.7). □

Proposition 5.2.2 gives an important result regarding the exponential function. Furthermore, (5.7) is a fundamental identity for the exponential function. Recall from (5.4) that all the powers of the variable z in e_Λ are of the form z^{q^i}. Thus we can now transition from z to τ where τ is the q-th power map; that is, we use the correspondence $z^{q^i} \longmapsto \tau^i(z)$.

Theorem 5.2.3. *Let Λ be a lattice in $\mathbf{C}$ of rank r and $0 \neq a \in \mathbf{A}$. Define $\varphi_a^\Lambda \in \mathbf{C}\{\tau\}$ by the formula*

$$\varphi_a^\Lambda(z) = aP(z, a^{-1}\Lambda/\Lambda),$$

where τ is the q-th power map. If we assign $0 \longmapsto 0$ and $a \longmapsto \varphi_a^\Lambda$ for nonzero $a \in \mathbf{A}$, then the result is a Drinfeld $\mathbf{A}$-module over $\mathbf{C}$ of rank r.

Proof. Consider $\mathbf{A}$ as a subset of $\mathbf{C}$ through the inclusion

$$\mathbf{A} \longrightarrow \mathbf{K} \longrightarrow \mathbf{K}_\infty \longrightarrow \mathbf{C}.$$

So the required structure map $\gamma : \mathbf{A} \longrightarrow \mathbf{C}$ is just inclusion, and hence, $\gamma(a) = a$ for any $a \in \mathbf{A}$. Now we need to show that $D(\varphi_a^\Lambda) = a$, but this is already clear from the definition of φ_a^Λ.

Next, we prove that φ_a^Λ is a homomorphism, i.e., it satisfies

$$\varphi_{ab}^\Lambda = \varphi_a^\Lambda \varphi_b^\Lambda \qquad \text{and} \qquad \varphi_{a+b}^\Lambda = \varphi_a^\Lambda + \varphi_b^\Lambda$$

for any nonzero $a, b \in \mathbf{A}$. First note that upon using the definition of φ_a^Λ, the fundamental identity given in (5.7) becomes

$$e_\Lambda(az) = \varphi_a^\Lambda(e_\Lambda(z)). \tag{5.10}$$

It follows that

$$\varphi_{ab}^\Lambda(e_\Lambda(z)) = e_\Lambda(abz) = \varphi_a^\Lambda(e_\Lambda(bz)) = \varphi_a^\Lambda(\varphi_b^\Lambda(e_\Lambda(z))).$$

Note that $e_\Lambda(z)$ is surjective, so we can conclude that $\varphi_{ab}^\Lambda = \varphi_a^\Lambda \varphi_b^\Lambda$. Also, by (5.10) and the additivity of e_Λ,

$$\varphi_{a+b}^\Lambda(e_\Lambda(z)) = e_\Lambda((a+b)z) = e_\Lambda(az + bz) = e_\Lambda(az) + e_\Lambda(bz) = \varphi_a^\Lambda(e_\Lambda(z)) + \varphi_b^\Lambda(e_\Lambda(z)).$$

Surjectivity of $e_\Lambda(u)$ on $\mathbf{C}$ implies that $\varphi_{a+b}^\Lambda = \varphi_a^\Lambda + \varphi_b^\Lambda$.

Finally, we show that φ^Λ is of rank r. We do this by showing that $\deg_\tau(\varphi_a^\Lambda) = r \deg_T(a)$. From the definition, we see that the degree of $\varphi_a^\Lambda(z)$ as a polynomial in z is $\#a^{-1}\Lambda/\Lambda$. Since Λ is a lattice in $\mathbf{C}$ of rank r, it is isomorphic to a direct sum of r fractional ideals. For any nonzero fractional ideal I of $\mathbf{A}$, we have

$$a^{-1}I/I \cong a^{-1}\mathbf{A}/\mathbf{A} \cong \mathbf{A}/a\mathbf{A}.$$

Thus $\#a^{-1}\Lambda/\Lambda = q^{r \deg_T(a)}$. It follows that

$$\deg_\tau(\varphi_a^\Lambda) = r \deg_T(a).$$

□

It follows from this theorem that given an $\mathbf{A}$-lattice Λ in $\mathbf{C}$, one can form the Drinfeld $\mathbf{A}$-module φ^Λ where φ_a^Λ for $0 \neq a \in \mathbf{A}$ is defined by the following commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbf{C} & \xrightarrow{e_\Lambda} & \mathbf{C} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle \varphi_a^\Lambda} & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbf{C} & \xrightarrow{e_\Lambda} & \mathbf{C} & \longrightarrow & 0 \end{array}$$

In fact, φ_a^Λ is an additive polynomial and the map $\varphi^\Lambda : a \longmapsto \varphi_a^\Lambda$ defines an $\mathbb{F}_q$-algebra homomorphism of $\mathbf{A}$ into the ring $\mathbf{C}\{\tau\}$, where $\mathbf{C}\{\tau\}$ is the noncommutative ring in τ with the commutation rule

$$\tau z = z^q \tau, \qquad z \in \mathbf{C}. \tag{5.11}$$

So φ^Λ takes values in $\mathbf{C}\{\tau\}$. It follows that for $a \in \mathbf{A}$ with $\deg_T(a) > 0$, we get

$$\varphi_a^\Lambda = \sum_{i=0}^{d} c_i \tau^i, \tag{5.12}$$

where $c_0 = a$, $c_d \neq 0$ and $d = r \deg_T(a)$.

From now on, we use the notation φ in place of φ^Λ if Λ is understood. We go back to the notation φ^Λ if it is necessary to emphasize the association between φ and Λ.

Proposition 5.2.4. *The map $\varphi : \mathbf{A} \longrightarrow \mathbf{C}\{\tau\}$ sending $a \longmapsto \varphi_a$ has the following properties:*

(a) It is $\mathbb{F}_q$-linear.

(b) If $a \in \mathbb{F}_q$, then $\varphi_a = a\tau^0$.

(c) For $a, b \in \mathbf{A}$, $\varphi_{ab} = \varphi_a \varphi_b = \varphi_b \varphi_a = \varphi_{ba}$.

Proof. See [Gos98, Proposition 4.3.2]. □

Let $\gamma : \mathbf{A} \longrightarrow \mathbf{C}$ be the structure map on the $\mathbf{A}$-field $\mathbf{C}$ and note that $D : \mathbf{C}\{\tau\} \longrightarrow \mathbf{C}$ is the map sending a polynomial $\sum c_i \tau^i$ in $\mathbf{C}\{\tau\}$ onto its constant term c_0 (alternatively, in the case of additive polynomials, D applied to a polynomial $\sum c_i X^{q^i}$ is differentiation with respect to X). Let

$$\mathbf{C}\{\{\tau\}\} = \left\{ \sum_{i=0}^{\infty} c_i \tau^i \mid c_i \in \mathbf{C} \right\},$$

it is the ring of *(left) twisted power series* generated by τ over $\mathbf{C}$ with the usual addition and multiplication except for the noncommutativity relation (5.11). We need the following definition for the proof of Theorem 5.2.9 below.

Definition 5.2.5. Let $\psi : \mathbf{K} \longrightarrow \mathbf{C}\{\{\tau\}\}$ be a ring homomorphism such that $D \circ \psi = \gamma$. We call ψ a *formal* $\mathbf{K}$*-module over* $\mathbf{C}$ and say that ψ is *nontrivial* if its image contains a power series which is nonconstant.

Let $0 \neq a \in \mathbf{A}$. If φ is a Drinfeld $\mathbf{A}$-module over $\mathbf{C}$, then $\varphi_a(\tau) = a\tau^0 + \{\text{higher terms}\}$. So φ_a is invertible in $\mathbf{C}\{\{\tau\}\}$. Then φ extends to a nontrivial formal $\mathbf{K}$-module, which we also denote by φ. For the next results, we refer to [Hay92] (or see [Gos98, Section 4.6]).

Lemma 5.2.6. *Let* $f(\tau) = \sum_{j=0}^{\infty} a_j \tau^j \in \mathbf{C}\{\{\tau\}\}$ *with constant term* $D(f) = \alpha := a_0$. *If* α *is transcendental over* $\mathbb{F}_q$, *then there exists a unique power series*

$$\lambda_f = \sum_{i=0}^{\infty} c_i \tau^i \in \mathbf{C}\{\{\tau\}\}$$

with $c_0 = 1$ *such that*

$$\lambda_f \alpha = f \lambda_f. \tag{5.13}$$

Proof. From the definition of $f(\tau)$, we see that (5.13) is equivalent to the recurrence

$$\left(\alpha^{q^i} - \alpha\right) c_i = \sum_{j=1}^{i} a_j \cdot c_{i-j}^{q^j} \tag{5.14}$$

for all $i \geq 1$. If α is transcendental over $\mathbb{F}_q$, then $\alpha^{q^i} - \alpha \neq 0$. So given the initial value $c_0 = 1$, we can find all the coefficients c_i for $i \geq 1$ uniquely by means of the recurrence relation above. □

Corollary 5.2.7. *With assumptions as in Lemma 5.2.6,* $\lambda_f \cdot \mathbf{C} \cdot \lambda_f^{-1}$ *is the centralizer of* $f(\tau)$ *in* $\mathbf{C}\{\{\tau\}\}$.

Proof. It is clear that the centralizer of α in $\mathbf{C}\{\{\tau\}\}$ is $\mathbf{C}$. We also see from (5.13) that

$$\lambda_f \alpha \lambda_f^{-1} = f.$$

So the result follows. □

Proposition 5.2.8. *Let ψ be a formal $\mathbf{K}$-module over $\mathbf{C}$. Then there exists a unique power series*

$$\lambda_\psi = \sum_{i=0}^{\infty} c_i \tau^i \in \mathbf{C}\{\{\tau\}\}$$

with $D(\lambda_\psi) = c_0 = 1$ and

$$\psi_a = \lambda_\psi a \lambda_\psi^{-1}$$

for all $a \in \mathbf{K}$.

Proof. If ψ is trivial, then we let $\lambda_\psi = \tau^0$. Now suppose ψ is nontrivial. Choose an element $z \in \mathbf{K}$ such that $\gamma(z) = \alpha$ is transcendental over $\mathbf{K}$. Let λ_ψ be the power series associated to $f(\tau) = \psi_z$ by Lemma 5.2.6. If $x \in \mathbf{K}$, then

$$\psi_x \psi_z = \psi_{xz} = \psi_z \psi_x.$$

So by Corollary 5.2.7, there exists $y \in \mathbf{C}$ such that

$$\psi_x = \lambda_\psi y \lambda_\psi^{-1}.$$

By comparing the coefficients of τ^0 in this equation, we see that $x = y$.

Finally, the uniqueness follows from Lemma 5.2.6. □

This proposition shows that a Drinfeld $\mathbf{A}$-module φ over $\mathbf{C}$ of generic $\mathbf{A}$-characteristic gives rise to a unique power series $\lambda_\varphi \in \mathbf{C}\{\{\tau\}\}$ with $D(\lambda_\varphi) = 1$. This power series is the analogue of a formal group associated to an elliptic curve.

We have the following result, see [Gos98, Theoren 4.6.9], for example.

Theorem 5.2.9. *Let $L_{\mathbf{A}}(\mathbf{C})$ be the set of $\mathbf{A}$-lattices in $\mathbf{C}$ and $D_{\mathbf{A}}(\mathbf{C})$ the set of Drinfeld $\mathbf{A}$-modules over $\mathbf{C}$. Then the map*

$$\begin{array}{ccc} \delta : L_{\mathbf{A}}(\mathbf{C}) & \longrightarrow & D_{\mathbf{A}}(\mathbf{C}) \\ \Lambda & \longmapsto & \varphi^\Lambda \end{array}$$

is a bijection.

Proof. To show that δ is one-to-one, let Λ and Λ' be two lattices in $\mathbf{C}$ such that $\varphi^\Lambda = \varphi^{\Lambda'}$. We work inside $\mathbf{C}\{\{\tau\}\}$. It is clear that $\mathbf{C}\{\tau\}$ is a subring of $\mathbf{C}\{\{\tau\}\}$. Moreover, every additive power series, such as $e_\Lambda(u)$, can be regarded as an element of $\mathbf{C}\{\{\tau\}\}$ applied to u, with $\tau(u) = u^q$. The fundamental identity given in (5.10) can be expressed as

$$e_\Lambda a = \varphi_a^\Lambda e_\Lambda.$$

Since $\varphi_a^\Lambda = \varphi_a^{\Lambda'}$, it follows that

$$e_{\Lambda'} a = \varphi_a^\Lambda e_{\Lambda'}.$$

Then

$$(e_\Lambda - e_{\Lambda'})a = \varphi_a^\Lambda (e_\Lambda - e_{\Lambda'}). \tag{5.15}$$

We want to show that $e_\Lambda = e_{\Lambda'}$. Suppose, on the contrary, that $e_\Lambda - e_{\Lambda'} \neq 0$. As power series, both e_Λ and $e_{\Lambda'}$ have initial term τ^0. So the first nonvanishing term of $e_\Lambda - e_{\Lambda'}$ is of the form $c\tau^k$, where $0 \neq c \in \mathbf{C}$ and $k > 0$. Upon comparing the coefficients of τ^k on both sides of (5.15), we get

$$ca^{q^k} = ac.$$

This implies that $a^{q^k} = a$ for every $a \in \mathbf{A}$, which is not true if a is nonconstant. So we have a contradiction. Hence $e_\Lambda = e_{\Lambda'}$. As Λ is the set of zeros of $e_\Lambda(z)$ and Λ' is the set of zeros of $e_{\Lambda'}(z)$, it follows that $\Lambda = \Lambda'$. So δ is injective.

Now we show that δ is onto. Let $\varphi \in D_{\mathbf{A}}(\mathbf{C})$ of rank r. As we noted earlier, φ extends to a nontrivial formal $\mathbf{K}$-module, and hence to an element

$$e_\varphi = \sum_{i=0}^{\infty} c_i \tau^i$$

of $\mathbf{C}\{\{\tau\}\}$ with $c_0 = 1$. It follows from Proposition 5.2.8 that

$$\varphi_a e_\varphi = e_\varphi a$$

for all $a \in \mathbf{A}$.

We claim that e_φ is an entire function. Note that e_φ is entire if and only if $c^{1/q^i} \longrightarrow 0$ as $i \longrightarrow \infty$. Pick $a \in \mathbf{A}$ such that $\deg_T(a) > 0$. Then a is transcendental over $\mathbb{F}_q$. Write

$$\varphi_a = a\tau^0 + \sum_{i=1}^{d} a_i \tau^i.$$

Let $n \geq d$. By using (5.14), we get

$$\left(a^{q^n} - a\right) c_n = \sum_{j=1}^{d} a_j \cdot c_{n-j}^{q^j}. \tag{5.16}$$

Let ν_∞ be the ∞-adic valuation on $\mathbf{K}$, which can be uniquely extended to $\mathbf{C}$. By using (5.16), we get

$$\nu_\infty(a) + \frac{\nu_\infty(c_n)}{q^n} \geq \min_{i \leq j \leq d} \left\{ \frac{\nu_\infty(a_j)}{q^n} + q^{j-n} \nu_\infty(c_{n-j}) \right\},$$

or equivalently,

$$\frac{\nu_\infty(c_n)}{q^n} \geq \min_{i \leq j \leq d} \left\{ \frac{\nu_\infty(a_j)}{q^n} + q^{j-n} \nu_\infty(c_{n-j}) \right\} - \nu_\infty(a).$$

Choose v so that $v < \nu_\infty(a) < 0$. So for sufficiently large n, say $n \geq N$, we get

$$\min_{i \leq j \leq d} \left\{ \frac{\nu_\infty(a_j)}{q^n} \right\} < \nu_\infty(a) - v.$$

This implies that

$$\frac{\nu_\infty(c_n)}{q^n} \geq \min_{i \leq j \leq d} \left\{ \frac{\nu_\infty(c_{n-j})}{q^{n-j}} \right\} - v.$$

We apply this relation recursively to get

$$\frac{\nu_\infty(c_n)}{q^n} \longrightarrow \infty \quad \text{as} \quad -nv \longrightarrow \infty.$$

This proves that e_φ is an entire function.

Next, let Λ be the set of zeros of e_φ, i.e., $\ker e_\varphi = \Lambda$. We want to show that Λ is an $\mathbf{A}$-lattice. Since $D(e_\varphi) = c_0 = 1$, it follows that Λ is contained in some separable extension of $\mathbf{K}$. Λ is discrete since $\sum \lambda^{-1}$ is absolutely convergent for $\lambda \in \Lambda$, $\lambda \neq 0$. Moreover, as a function in z, we have

$$\varphi_a(e_\varphi(z)) = e_\varphi(az).$$

It follows that Λ is a discrete $\mathbf{A}$-module.

We still need to show that Λ is finitely generated. Let $V = \mathbf{K}_\infty\Lambda$. This is a vector space over $\mathbf{K}_\infty$, and we claim that it is finitely generated. Suppose it is not. Let $\{\omega_1, \ldots, \omega_s, \ldots\}$ be an infinite set of elements of Λ which are linearly independent over $\mathbf{K}_\infty$. Set

$$V_i = \mathbf{K}_\infty\omega_1 + \mathbf{K}_\infty\omega_2 + \cdots + \mathbf{K}_\infty\omega_i \quad \text{and} \quad \Lambda_i = \Lambda \cap V_i$$

Then each Λ_i is now an $\mathbf{A}$-lattice in a finite dimensional vector space over $\mathbf{K}_\infty$. It follows from Lemma 5.1.5 that Λ_i is finitely generated. Furthermore,

$$a^{-1}\Lambda_i/\Lambda_i \cong (\mathbf{A}/a\mathbf{A})^i.$$

But note that

$$a^{-1}\Lambda_i/\Lambda_i \subseteq a^{-1}\Lambda/\Lambda \cong \varphi[a] \cong (\mathbf{A}/a\mathbf{A})^r,$$

where $\varphi[a]$ is the set of zeros of φ in $\mathbf{C}$. So we get a contradiction once $i > r$. Therefore Λ is a finitely generated lattice of rank r. This completes the proof of the theorem. □

We end this section by stating a correspondence between the set of morphisms from Λ_1 to Λ_2, $\mathrm{Hom}(\Lambda_1, \Lambda_2)$, and the set of morphisms from φ^{Λ_1} to φ^{Λ_2}, $\mathrm{Hom}(\varphi^{\Lambda_1}, \varphi^{\Lambda_2})$.

Theorem 5.2.10. *Let Λ_1 and Λ_2 be $\mathbf{A}$-lattices of rank r in $\mathbf{C}$ and $c \in Hom(\Lambda_1, \Lambda_2)$, $c \in \mathbf{C}^*$. Let*

$$f_c(z) = cP(z; c^{-1}\Lambda_2/\Lambda_1).$$

Then $f_c \in Hom(\varphi^{\Lambda_1}, \varphi^{\Lambda_2})$. Additionally, $Hom(\Lambda_1, \Lambda_2)$ and $Hom(\varphi^{\Lambda_1}, \varphi^{\Lambda_2})$ are isomorphic as abelian groups and as $\mathbb{F}_q$-vector spaces via the map $c \longrightarrow f_c$.

Proof. See [Ros02, Theorem 13.25]. □

These last two results make it possible to determine properties of the category of Drinfeld modules over $\mathbf{C}$ via the category of lattices in $\mathbf{C}$.

5.3 Coefficients of Drinfeld Modules

Suppose φ is a Drinfeld $\mathbf{A}$-module over $\mathbf{C}$ of rank r and Λ the corresponding $\mathbf{A}$-lattice for φ in $\mathbf{C}$ via Theorem 5.2.9. In this section we consider the coefficients of φ and give an explicit formula for them. We refer to [Gek86, Gek88, Gek99] and [Gos78].

Recall from (5.4) that $e_\Lambda(z)$ has a power series expansion

$$e_\Lambda(z) = \sum_{i=0}^{\infty} \alpha_i z^{q^i},$$

where $\alpha_i \in \mathbf{C}$ for $i \geq 0$ and $\alpha_0 = 1$. Since $e'_\Lambda = 1$, there exists a composition inverse for e_Λ given by

$$\log_\Lambda(z) = \sum_{i=0}^{\infty} \beta_i z^{q^i}$$

with a positive radius of convergence. For $a \in \mathbf{A}$ with $\deg_T(a) > 0$, we get from (5.12) that

$$\varphi_a(z) = \sum_{i=0}^{d} c_i z^{q^i}, \qquad c_i = c_i(a, \Lambda).$$

If we apply $\log_\Lambda$ on both sides of (5.10), then

$$a \log_\Lambda(z) = \log_\Lambda(\varphi_a(z)).$$

So for $k \geq 0$,

$$a\beta_k = \sum_{i+j=k} \beta_i c_j^{q^i}. \tag{5.17}$$

If the coefficients c_i are known, then we may compute the β_i recursively, and vice versa.

We need the following definition.

Definition 5.3.1. Let $k \in \mathbb{N}$ such that $k \equiv 0 \pmod{q-1}$. The *Eisenstein series of weight* k for Λ, denoted $E_k(\Lambda)$, is given by

$$E_k(\Lambda) = \sum_{0 \neq \lambda \in \Lambda} \frac{1}{\lambda^k}.$$

Since we are in the non-archimedean setting and Λ is discrete, this series converges for any $k > 0$, but it is equal to zero if $k \not\equiv 0 \pmod{q-1}$. Let $z/e_\Lambda(z) = \sum \gamma_i z^i$. Then

$$\frac{z}{e_\Lambda(z)} = z \sum_{\lambda \in \Lambda} \frac{1}{z-\lambda} = \sum_{\lambda \in \Lambda} \frac{1}{1-\lambda/z} = 1 - \sum_{0 \neq \lambda \in \Lambda} \frac{(z/\lambda)}{1-z/\lambda} = 1 - \sum_{k \geq 1} E_k(\Lambda) z^k.$$

By induction on k, it can be shown that $\gamma_j = \beta_{k-i}^{q^i}$ for $j = q^k - q^i$ (see [Gek86, Lemma 2.9] or [Gos78, Theorem 2.3.4]). Let $E_0(\Lambda) = -1$. Then by using (5.17) we get the following recursion formula:

$$aE_{q^k-1}(\Lambda) = \sum_{i+j=k} E_{q^i-1}(\Lambda) c_j^{q^i}. \tag{5.18}$$

Now let $a = T \in \mathbf{A}$ and define

$$[k] := T^{q^k} - T \in \mathbf{A}, \tag{5.19}$$

i.e., $[k]$ is the product of the monic primes of degree dividing k. By using (5.10) and (5.12), we get

$$e_\Lambda(Tz) = \varphi_T(e_\Lambda(z)) = Te_\Lambda(z) + c_1 e_\Lambda(z)^q + \cdots + c_r e_\Lambda(z)^{q^r},$$

which gives the recursion formula

$$[k]\alpha_k = c_1 \alpha_{k-1}^q + \cdots + c_r \alpha_{k-r}^{q^r} \tag{5.20}$$

for the coefficients $\alpha_k = \alpha_k(\Lambda)$ of $e_\Lambda(z)$ where $\alpha_k = 0$ for $k < 0$ and $\alpha_0 = 1$. This shows that each coefficient α_k is a polynomial in $c_1, \ldots, c_r$.

As in the case of elliptic curves over $\mathbb{C}$, we can write the coefficients $c_i = c_i(T, \Lambda)$ of φ in terms of the Eisenstein series. It can be shown that the coefficient c_k of φ can be uniquely determined by the recursion formula

$$c_k = \sum_{1 \leq i \leq k-1} E_{q^{k-i}-1}(\Lambda) c_i^{q^{k-i}} + [k] E_{q^k-1}(\Lambda) \tag{5.21}$$

(cf. [Gek99], [Gek86, Chapter 2], and [Gos78]). So φ is uniquely determined by the values of $E_k(\Lambda)$.

Drinfeld Modules of Rank 1

We consider the case of rank one Drinfeld modules. It is known that all such Drinfeld modules are isomorphic to the Carlitz module ρ defined by $\rho_T = T + \tau$. Since ρ is of rank one, it corresponds to a rank one lattice in $\mathbf{C}$. Let this lattice be $L = \bar{\pi}\mathbf{A}$ where its *period* $\bar{\pi} \in \mathbf{C}$ is well-defined up to a $(q-1)$-st root of unity. A detailed computation of such an element $\bar{\pi}$ can be found in [Gos98, Chapter 3]. By using (5.21), we get

$$1 = [1]E_{q-1}(L) = [1]\bar{\pi}^{1-q}E_{q-1}(\mathbf{A}).$$

So

$$\bar{\pi}^{q-1} = [1]E_{q-1}(\mathbf{A}) = (T^q - T)\sum_{0\neq a\in\mathbf{A}} \frac{1}{a^{q-1}}, \tag{5.22}$$

and in particular, $|\bar{\pi}^{q-1}| = |[1]| = q^q$. Now define

$$F_k := [k][k-1]^q \cdots [1]^{q^k-1}, \tag{5.23}$$

so F_k is the product of all monic polynomials in $\mathbf{A}$ of degree k. From (5.20) we see that the coefficients of e_L are of the form

$$\alpha_k(L) = \frac{1}{F_k}. \tag{5.24}$$

Moreover, we can also determine the coefficients of ρ_a for an arbitrary nonzero element $a \in \mathbf{A}$. Suppose

$$\rho_a = \sum_{i=0}^{\deg_T(a)} \beta_i(a)\tau^i. \tag{5.25}$$

Since

$$\rho_{aT} = \rho_a\rho_T = \rho_T\rho_a$$

in $\mathbf{C}\{\tau\}$, we can determine the β_i via the recursion formula (see [Gek88, (4.4)])

$$\beta_i = \frac{\beta_{i-1}^q - \beta_{i-1}}{[i]}, \tag{5.26}$$

for $i \geq 1$ with $\beta_0 = a$ and

$$\deg_T(\beta_i) = (\deg_T(a) - i)q^i \leq \frac{q^{\deg_T(a)} - q^i}{q-1} \tag{5.27}$$

for $0 \leq i \leq \deg_T(a)$ (see [Gek88, (4.5)]).

Drinfeld Modules of Rank 2

Finally, we look into the rank two case. Consider the lattice $\Lambda = \mathbf{A}\omega_1 + \mathbf{A}\omega_2$ corresponding to a Drinfeld module $\varphi = \varphi^\Lambda$ of rank two. For $a = T \in \mathbf{A}$, write

$$\varphi_T = T + g\tau + \Delta\tau^2,$$

or equivalently,

$$\varphi_T(X) = TX + gX^q + \Delta X^{q^2}, \tag{5.28}$$

where $g, \Delta \in \mathbf{C}$ and $\Delta \neq 0$. By using (5.21) we can write g and Δ as

$$\begin{aligned} g &= g(\Lambda) = [1]E_{q-1}(\Lambda), \\ \Delta &= \Delta(\Lambda) = E_{q-1}(\Lambda)g^q + [2]E_{q^2-1}(\Lambda) \\ &= [1]^q E_{q-1}^{q+1}(\Lambda) + [2]E_{q^2-1}(\Lambda). \end{aligned} \tag{5.29}$$

5.4 Modular Forms in $\mathbf{C}$

In this section we give a description of the analogue of the j-invariant in the Drinfeld module case. For most of the material presented here we refer to [Gek83, Gek86, Gek88, Gek99] and [Gos80a].

We continue to use $\mathbf{A}$, $\mathbf{K}$, $\mathbf{K}_\infty$, and $\mathbf{C}$ as defined before and focus on Drinfeld modules φ of rank $r = 2$. From the coefficients used in (5.28) we have the following definition.

Definition 5.4.1. Let φ be a Drinfeld $\mathbf{A}$-module of rank two. The *j-invariant* of φ is given by

$$j = j(\varphi) = \frac{g^{q+1}}{\Delta}.$$

Remark 5.4.2.

1. If we replace Λ by some similar lattice $c\Lambda$, with $0 \neq c \in \mathbf{C}$, then the pair (g, Δ) is replaced by $(c^{1-q}g, c^{1-q^2}\Delta)$. However, the same value of j is obtained. Let $\varphi = \varphi^\Lambda$ and $\varphi' = \varphi^{\Lambda'}$. Then we have the following equivalent statements:

(a) φ and φ' are isomorphic Drinfeld modules.

(b) ϕ and ϕ' have the same j-invariant.

(b) There exists $c \in \mathbf{C}^*$ such that $\Lambda' = c\Lambda$, i.e., Λ and Λ' are homothetic.

2. We can treat the j-invariant as an isomorphism invariant of Drinfeld modules. So if φ is associated to $\Lambda = [1, z]$, then we can write

$$j(\varphi) = j(\Lambda) = j(z) = j(c\Lambda), \quad \text{for all } c \in \mathbf{C}^*.$$

3. Instead of considering g, Δ and j as functions of (ω_1, ω_2), we can restrict to pairs of the form $(1, z)$ by taking $z = \omega_2/\omega_1$. Since Λ is discrete, it follows that the set $\{\omega_1, \omega_2\}$ is linearly independent over $\mathbf{K}_\infty$. Hence z is contained in

$$\Omega := \mathbf{C} - \mathbf{K}_\infty, \tag{5.30}$$

and so we can consider lattices of the form $\Lambda = \mathbf{A} + z\mathbf{A}$.

The set Ω in the previous remark is called the *Drinfeld upper half plane*. It is the counterpart of the upper half plane in the classical case. The group $\mathrm{GL}_2(\mathbf{K}_\infty)$ acts on Ω by fractional linear transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{az + b}{cz + d}.$$

Note that two elements $z, z' \in \Omega$ define similar lattices (hence, they give isomorphic Drinfeld modules) if and only if they are equivalent by $\Gamma := \mathrm{GL}_2(\mathbf{A})$. So we obtain an isomorphism

$$\begin{array}{ccc} \Gamma\backslash\Omega & \xrightarrow{\cong} & \mathbf{C} \\ z & \longmapsto & j(z), \end{array}$$

where the quotient $\Gamma\backslash\Omega$ is the set of isomorphism classes of rank two Drinfeld modules over $\mathbf{C}$.

The next concept that we introduce captures the idea of measuring distance "to infinity". The *imaginary part* of an element $z \in \mathbf{C}$, denoted by $|z|_i$ is defined as

$$|z|_i := \inf_{x \in \mathbf{K}_\infty} |z - x| = \min_{x \in \mathbf{K}_\infty} |z - x|,$$

where the absolute value $|\cdot|$ is normalized by $|T| = q$. So $|z|_i = 0$ if and only if $z \in \mathbf{K}_\infty$ and

$$|\theta z|_i = \frac{|\det \theta|}{|cz + d|^2} |z|_i, \qquad \theta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{K}_\infty).$$

Let M be an element of the value set $q^{\mathbb{Q}}$ of $\mathbf{C}$ and define $\Omega_M := \{z \in \Omega \mid |z|_i \geq M\}$. To briefly describe Ω, we have the following proposition. We refer the reader to [GvdP80, Section IV.1] for a proof.

Proposition 5.4.3. *Ω is a connected admissible open subspace of the rigid analytic space $\mathbb{P}^1(\mathbf{C})$. Each Ω_M is an open admissible subspace of Ω. Furthermore, $GL_2(\mathbf{K}_\infty)$ acts as an analytic automorphism group on Ω.*

For additional structural properties of Ω, see for example, [Ste97], [vdP97], and [vdPT97].

From now on, let $\Lambda = \mathbf{A} + z\mathbf{A}$, $z \in \Omega$. Since Ω is a rigid analytic space, the functions $E_k(z) := E_k(\Lambda)$ are holomorphic on Ω. Moreover, from the equality $E_k(c\Lambda) = c^{-k} E_k(\Lambda)$ with $c \in \mathbf{C}^*$ we get

$$E_k\left(\frac{az + b}{cz + d}\right) = (cz + d)^k E_k(z)$$

for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

Let L be a rank one lattice in $\mathbf{C}$ and $\bar{\pi}$ be its period. As we are interested in Laurent series expansions of *Drinfeld modular forms*, we define

$$t(z) := \frac{1}{e_L(\bar{\pi})} = \frac{1}{\bar{\pi} e_{\mathbf{A}}(z)}, \tag{5.31}$$

where L is the lattice that corresponds to the Carlitz module. This value acts as the canonical uniformizer "at infinity". It replaces q = $\exp(2\pi i z)$ and the factor $\bar{\pi}$ is introduced for

normalizing purposes, as does $2\pi i$ in the classical case. As a way of measuring distance to infinity, we have the next result.

Lemma 5.4.4. *There exists a constant $1 < M_0 \in \mathbb{R}$ such that $|z|_i \leq -\log_q |t(z)| \leq M_0|z|_i$. Furthermore, for $M > 1$, t induces an isomorphism from $\mathbf{A}\backslash\Omega_M$ to some punctured ball $B_n - \{0\}$.*

Proof. See [Gek88, 5.5 and 5.6]. □

We can now define modular forms in the Drinfeld module case.

Definition 5.4.5. Let k be a nonnegative integer and m a residue class $\pmod{q-1}$. A function $f : \Omega \longrightarrow \mathbf{C}$ is called a *modular function of weight k* and *type m* for Γ if it satisfies the following conditions:

(i) $f(\theta z) = (\det \theta)^{-m}(cz+d)^k f(z)$ for $\theta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, $z \in \Omega$;

(ii) f is holomorphic on Ω; and

(iii) f is holomorphic at infinity.

The last condition entails that f has a Laurent series expansion $f(z) = \tilde{f}(t(z))$ with respect to t. Here $\tilde{f}(X) = \sum a_i X^i$ is a power series with positive radius of convergence. This power series exists since f is Γ-invariant by part(i). The order of vanishing of f at infinity is defined to be that of $\tilde{f}$.

Example 5.4.6. Let $\mathbf{M}_{k,m}$ denote the vector space of modular forms of weight k and type m over $\mathbf{C}$. Also let $\Lambda = \mathbf{A} + z\mathbf{A}$ for $z \in \Omega$.

1. For a positive integer k such that $k \equiv 0 \pmod{q-1}$, the function

$$z \longmapsto E_k(z) = E_k(\Lambda) = \sum_{0 \neq a,b \in \mathbf{A}} \frac{1}{(az+b)^k}$$

is a modular form and is contained in $\mathbf{M}_{k,0}$.

2. Let $0 \neq a \in \mathbf{A}$ and φ^{Λ} be the Drinfeld module corresponding to Λ. Then from (5.12), we can write

$$\varphi_a^{\Lambda}(X) = \sum_{i=0}^{2\deg_T a} c_i(a,\Lambda) X^{q^i}.$$

By letting z vary on Ω, the coefficient $c_i(a,z) := c_i(a,\Lambda)$ becomes a function in z. Each $c_i(a,z)$ is contained in $\mathbf{M}_{k,0}$ where $k = q^i - 1$. As a consequence, we get the functions $g \in \mathbf{M}_{q-1,0}$ and $\Delta \in \mathbf{M}_{q^2-1,0}$ for $a = T$ and $i = 1, 2$. Note that g and Δ play the role of the classical functions g_2, g_3 and Δ, respectively.

As we have noted earlier in Remark 5.4.2, j is an invariant (under isomorphism) for rank two Drinfeld modules φ defined by (5.28). Two such Drinfeld modules given by pairs (g, Δ) and (g', Δ') are isomorphic if and only if

$$\frac{g^{q+1}}{\Delta} = \frac{g'^{q+1}}{\Delta'}.$$

This implies that the holomorphic Γ-invariant function

$$\begin{array}{rcl} j : \Omega & \longrightarrow & \mathbf{C} \\ z & \longmapsto & \frac{g(z)^{q+1}}{\Delta(z)} \end{array}$$

identifies the quotient $\Gamma\backslash\Omega$ with the affine line $\mathbf{C} = \mathbb{A}^1(\mathbf{C})$ both analytically and set-theoretically (see [Gek99], p.496).

t-expansions

Our aim is to determine a *t-expansion* for the modular function j, which is the analogue of the q-expansion in the classical case. Here ρ denotes the Carlitz module over $\mathbf{C}$. Let $0 \neq a \in \mathbf{A}$ and define the *a-th inverse cyclotomic polynomial* $f_a(X) \in \mathbf{A}[X]$ by

$$f_a(X) := \rho_a(X^{-1}) X^{|a|}, \tag{5.32}$$

where ρ_a is considered as a polynomial in X; that is, by replacing τ by X^q in (5.25). Clearly, $f_a(X)$ is of degree $|a| - 1$, it has a as its leading coefficient, and $f_a(0)$ is equal to the

leading coefficient of a. In particular, f_a is a polynomial in X^{q-1}. For $a, b \in \mathbf{A}^+$ with $\deg_T(b) < \deg_T(a)$, the following properties hold (see [Gek88]):

(i) $f_{a+b} = f_a + X^{q^{\deg_T(a)} - q^{\deg_T(b)}} f_b$;

(ii) $\prod_{c \in \mathbb{F}_q} f_{aT+c} = f_{aT}^q - X^k f_{aT}$, where $k = (q^{\deg_T(a)+1} - 1)(q-1)$; and

(iii) $f_{aT} = f_a^q + TX^k f_a$, where $k = q^{\deg_T(a)}(q-1)$.

The reason for considering the Carlitz module ρ at this point is that we have to determine the t-expansion for j inside the abelian extension $\mathbf{K}(\lambda_a)$, where λ_a is a generator of the set of roots of the cylotomic polynomial $\rho_a(X)/X$. This is similar to the classical case scenario.

Recall the definition of $t(z)$ given in (5.31). For simplicity, let $t = t(z)$. Now we determine the t-expansion of the Eisenstein series given in Example 5.4.6.1. For $0 \neq a \in \mathbf{A}$, let

$$t_a = t(az) = \frac{1}{e_L(\bar{\pi} a z)},$$

where $L = \bar{\pi}\mathbf{A}$ is the rank one lattice associated to ρ. This is the counterpart of the q-expansion in the case of classical modular forms. We have

$$t_a = \frac{1}{e_L(\bar{\pi} a z)} = \frac{1}{\rho_a(e_L(\bar{\pi} z))} = \frac{1}{\rho_a(t^{-1})} = \frac{t^{|a|}}{\rho_a(t^{-1}) t^{|a|}} = \frac{t^{|a|}}{f_a(t)}, \tag{5.33}$$

as a power series in t with coefficients in $\mathbf{A}$. Here $|a| = q^{\deg_T(a)}$. For $E_k(z)$ we get

$$\begin{aligned} E_k(z) &= \sum_{0 \neq a, b \in \mathbf{A}} \frac{1}{(az+b)^k} \\ &= \sum_{0 \neq b \in \mathbf{A}} \frac{1}{b^k} - \sum_{a \in \mathbf{A}^+} \sum_{b \in \mathbf{A}} \frac{1}{(az+b)^k} \\ &= \bar{\pi}^k E_k(L) - \bar{\pi}^k \sum_{a \in \mathbf{A}^+} \sum_{b \in \mathbf{A}} \frac{1}{(\bar{\pi} a z + \bar{\pi} b)^k}, \end{aligned}$$

where $E_k(L) \in \mathbf{K}$. So

$$\bar{\pi}^{-k} E_k(z) = E_k(L) - \sum_{a \in \mathbf{A}^+} \sum_{b \in \mathbf{A}} \frac{1}{(\bar{\pi} a z + \bar{\pi} b)^k}, \tag{5.34}$$

from which we obtain

$$\begin{aligned} k = q-1: \quad & \bar{\pi}^{-k} E_{q-1}(z) = [1]^{-1} - \sum_{a \in \mathbf{A}^+} t_a^{q-1} \\ k = q^2-1: \quad & \bar{\pi}^{-k} E_{q^2-1}(z) = -([1][2])^{-1} - \sum_{a \in \mathbf{A}^+} \left(t_a^{q^2-1} - [1]^{-1} t_a^{q^2-q} \right) \end{aligned} \tag{5.35}$$

(see [Gek88, Section 6]). For each fixed exponent i of t in (5.34), only a finite number of a contribute. So upon dividing by $\bar{\pi}$ to their respective weights, the t-expansion E_k gets rational coefficients.

There is a special value of the Eisenstein series known as the *normalized Eisenstein series* of weight $q^k - 1$. This is defined by

$$g_k := (-1)^{k+1} \bar{\pi}^{1-q^k} F_k E_{q^k-1}(z) \tag{5.36}$$

as a modular form or as a formal power series in t, where F_k is given in (5.23). This value has the following properties

Proposition 5.4.7.

1. *g_k has constant term equal to 1.*
2. *g_k has coefficients in $\mathbf{A}$.*
3. *g_k is obtained by using the following recursion formula:*

$$g_0 = 1, \ g_1 = g, \ \text{and } g_k = -[k-1] g_{k-2} \Delta^{q^{k-2}} + g_{k-1} g^{q^{k-1}} \text{ for } k \geq 2, \tag{5.37}$$

where $[k]$ is given in (5.19)

Proof. See [Gek88, Proposition 6.9]. □

Observe that the expansions given in (5.35) involve only powers of t which are divisible by $q-1$. Define $s := t^{q-1}$. By combining (5.29) and (5.35) we get the following t-expansions (or s-expansions) for g and Δ (cf. [BL97]).

Theorem 5.4.8 ([Gek88])**.** *The modular functions $g(z)$ and $\Delta(z)$ have the following t-expansions*[1]*:*

$$\bar{\pi}^{1-q} g(z) = [1]\left([1]^{-1} - \sum_{a\in\mathbf{A}^+} t_a^{q-1}\right) \tag{5.38}$$

$$= 1 - [1]s - [1]s^{q^2-q+1} + [1]s^{q^2} - [1]\left([1]+\alpha\right)s^{q^2+1} + \textit{higher terms}$$

$$\bar{\pi}^{1-q^2}\Delta(z) = [2]\left(-\left([1][2]\right)^{-1} - \sum_{a\in\mathbf{A}^+}\left(t_a^{q^2-1} - [1]^{-1}t_a^{q^2-q}\right)\right) + [1]^q\left([1]^{-1} - \sum_{a\in\mathbf{A}^+} t_a^{q-1}\right)^{q+1} \tag{5.39}$$

$$= -s + s^q - [1]s^{q+1} - s^{q^2-q+1} + s^{q^2} - \left([1] - [1]^q + \alpha\right)s^{q^2+1} + \textit{higher terms},$$

where $\alpha = 1$ if $q = 2$ and $\alpha = 0$ otherwise.

By using the result in [Gek88, Remark 6.6 and Proposition 6.7], it can be shown that j can be written as

$$j(z) = \sum_{i=0}^{\infty} a_i s^{i-1}, \qquad a_0 = -1, \qquad a_i \in \mathbf{A} \tag{5.40}$$

(cf. [BL97]).

Example 5.4.9. By directly manipulating the t-expansions of $g(z)$ and $\Delta(z)$ using SAGE [S$^+$17], we get some examples of j-invariants given in Table 5.1.

Remark 5.4.10. Since we are dealing with infinite series, we can compute the s-expansion of $j(z)$ up to a certain precision only; that is, we can only compute the first N terms of this invariant. To guarantee that we obtained the correct coefficient a_i of s^{i-1} in the preceding example, we had to use a sufficient number of monic elements of $\mathbf{A}$ in our computation. We revisit the calculation of this invariant in Chapter 8.

Finally, note that modular functions which are holomorphic both on Ω and at infinity are constants. So we get an analogue of [Lan87, Theorem 2, Ch. 5 §2] in the following theorem.

[1] *The t-expansion of $g(z)$ given in [BL97, Theorem 1.2] contains some (probably, typographical) errors which we have corrected here.*

q	$j(z)$
2	$\frac{1}{s}+(T^2+T+1)+(T^4+T^2)s+(T^6+T^5+T^4+T^3+T^2+T)s^2+(T^8+T^6+T^5$ $+T^3+1)s^4+(T^4+T^2)s^5+(T^6+T^5+T^3+T^2)s^6+(T^4+T^2)s^7+(T^4+T^2)s^8$ $+(T^8+T^2)s^9+(T^{10}+T^9+T^6+T^5+T^4+T)s^{10}+$ higher terms
3	$\frac{2}{s}+(T^3+2T)+2s+(T^9+T^3+T)s^2+(2T^{12}+T^{10}+T^4+2T^2+2)s^3+(T^9+2T^3)s^4$ $+(T^{12}+2T^{10}+2T^6+T^4)s^5+(T^{15}+T^{13}+T^{11}+T^9+2T^7+2T^5+2T^3+2T)s^6$ $(2T^{18}+T^{12}+T^{10}+2T^4)s^9+$ higher terms
5	$\frac{4}{s}+(T^5+4T)+4s^3+(T^{25}+T^5+3T)s^4+(4T^{30}+T^{26}+T^6+4T^2)s^5+4s^7+(T^{25}$ $+2T^5+2T)s^8+(3T^{30}+2T^{26}+4T^{10}+4T^6+2T^2)s^9+(T^{35}+3T^{31}+T^{27}+4T^{11}$ $+2T^7+4T^3)s^{10}+$ higher terms

Table 5.1: j-invariants for $q = 2, 3$, and 5

Theorem 5.4.11 ([Bae92])**.** *Let f be a modular function which is holomorphic on Ω, and with an s-expansion*

$$f = \sum_{i=-k}^{\infty} c_i s^i.$$

Then f is a polynomial in $j(z)$ with coefficients in the $\mathbf{A}$-module generated by the coefficients c_i.

Corollary 5.4.12 ([BL97])**.** *Let f be a modular function which is holomorphic on Ω, and with s-expansion*

$$f = \sum_{i=-k}^{\infty} c_i s^i.$$

Then f can be written as

$$f = \sum_{i=0}^{k} b_i j(z)^i.$$

Proof. Choose the coefficients b_i such that the s-expansion of

$$f - \sum_{i=0}^{k} b_i j(z)^i$$

is $O(s)$, i.e., the expansion of is the form $as +$ higher terms with $a \neq 0$. So by Theorem 5.4.11, we get the desired result. □

5.5 Modular Polynomial for j

We continue to present properties of the j-invariant corresponding to a Drinfeld module φ of rank two over $\mathbf{C}$. In particular, we look into the integrality of j when φ has complex multiplication, i.e., when $\mathrm{End}(\varphi)$ is strictly larger than $\mathbf{A}$, and then consider the *modular polynomial* associated to this j-invariant. Most of the material presented in this section can be found in [Bae92] and [BL97].

Let $M_2(\mathbf{A})$ denote the set of 2×2 matrices with entries in $\mathbf{A}$. An element $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{A})$ is called *primitive* if $\gcd(a, b, c, d) = 1$. For $\mathfrak{n} \in \mathbf{A}^+$, define the sets

$$\triangle_{\mathfrak{n}} := \{\alpha \in M_2(\mathbf{A}) \mid \det \alpha = \mu\mathfrak{n} \text{ for some } \mu \in \mathbb{F}_q^*\}$$

and

$$\triangle_{\mathfrak{n}}^* := \{\alpha \in \triangle_n \mid \alpha \text{ is primitive}\}.$$

Then, as in the classical case, the group $\Gamma = \mathrm{GL}_2(\mathbf{A}) = \{\theta \in M_2(\mathbf{A}) \mid \det \theta \in \mathbb{F}_q^*\}$ acts on $\triangle_{\mathfrak{n}}^*$ by left (or right) multiplication. For the rest of this section we assume that $a, d, \mathfrak{n} \in \mathbf{A}^+$, unless otherwise stated.

Theorem 5.5.1. *Γ acts left transitively on the right Γ-cosets, and also right transitively on the left Γ-cosets of $\triangle_{\mathfrak{n}}^*$.*

Proof. The proof is the same as the classical one. See [Lan87, Theorem 1, Ch. 5 §1]. □

It can be verified that the set

$$S_{\mathfrak{n}} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbf{A}) \mid ad = \mathfrak{n}, \gcd(a, b, d) = 1, \deg_T(b) < \deg_T(d), \text{and } a, d \in \mathbf{A}^+ \right\} \tag{5.41}$$

is the complete set of distinct left Γ-coset representatives of $\triangle_{\mathfrak{n}}^*$. Let $\mathrm{N}(\mathfrak{n}) = \#S_{\mathfrak{n}}$. Similar to the classical setting, we have

$$\mathrm{N}(\mathfrak{n}) = |\mathfrak{n}| \prod_{p|\mathfrak{n}} \left(1 + \frac{1}{|p|}\right) = q^{\deg_T(\mathfrak{n})} \prod_{p|\mathfrak{n}} \left(1 + \frac{1}{q^{\deg_T(p)}}\right). \tag{5.42}$$

Let $\theta_i \in S_{\mathsf{n}}$. So Γ acts on $j \circ \theta_i$ transitively. Define

$$\Phi_{\mathsf{n}}(X) = \prod_{i=1}^{\mathrm{N}(\mathsf{n})} (X - j \circ \theta_i).$$

Similar to the classical situation, the coefficients of this polynomial are holomorphic on Ω, invariant under Γ, and are meromorphic at infinity. It follows from Theorem 5.4.11 that the coefficients of $\Phi_{\mathsf{n}}(X)$ are polynomials in j, i.e., these coefficients are in $\mathbf{A}[j]$.

Let

$$\theta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_{\mathsf{n}}$$

and consider the expansion of $j \circ \theta$. Let

$$u := u(z) = t(z/\mathsf{n}) = e_L(\bar{\pi} z/\mathsf{n})^{-1}.$$

Let $\rho[\mathsf{n}]$ be the kernel of ρ_{n}, i.e., $\rho[\mathsf{n}] = \{c \in \mathbf{C} \mid \rho_{\mathsf{n}}(c) = 0\}$. Suppose λ_{n} is a generator of $\rho[\mathsf{n}]$, and denote by $\mathbf{A}[\lambda_{\mathsf{n}}]$ the ring generated by λ_{n} over $\mathbf{A}$.

Lemma 5.5.2 ([Bae92])**.** *If $ad = \mathsf{n}$, then $t(az/d)$ is a power series in u with coefficients in $\mathbf{A}$.*

Proof. Note that $\rho_a(X) \in \mathbf{A}[X]$, so it follows from definition that $f_a(X) \in \mathbf{A}[X]$. By (5.33), we have

$$t\left(\frac{az}{d}\right) = \frac{t(z/d)^{|a|}}{f_a(t(z/d))},$$

which is a power series in $t(z/d)$ with coefficients in $\mathbf{A}$. This follows from the fact that the constant term of $f_a(X)$ is a unit in $\mathbf{A}$. Recall that $a \in \mathbf{A}^+$ and $f_a(0)$ is the leading coefficient of a. Then we only need to show that $t(z/d)$ is a power series in u with coefficients in $\mathbf{A}$. Note that $d = \mathsf{n}/a$. By using (5.33) one more time, we get

$$t\left(\frac{z}{d}\right) = t\left(\frac{az}{\mathsf{n}}\right) = \frac{t(z/\mathsf{n})^{|a|}}{f_a(t(z/\mathsf{n}))}.$$

By following the same argument as above, we get the desired result. □

Corollary 5.5.3 ([Bae92]). *Let* $\theta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_{\mathsf{n}}$. *Then* $j \circ \theta \in \mathbf{A}[\lambda_{\mathsf{n}}][[u]]$.

Proof. By definition,

$$\begin{aligned} t\left(\frac{az+b}{d}\right) &= \left(e_L\left(\frac{\bar{\pi}az+\bar{\pi}b}{d}\right)\right)^{-1} = \left(e_L\left(\frac{\bar{\pi}az}{d}\right) + e_L\left(\frac{\bar{\pi}b}{d}\right)\right)^{-1} \\ &= \left(\frac{1}{t(az/d)} + e_L\left(\frac{\bar{\pi}b}{d}\right)\right)^{-1} = \frac{t(az/d)}{1+e_L(\bar{\pi}b/d)t(az/d)} \\ &= \sum_{i=0}^{\infty}(-1)^i e_L\left(\frac{\bar{\pi}b}{d}\right)^i t\left(\frac{az}{d}\right)^{i+1} \end{aligned}$$

and

$$t\left(\frac{az+b}{d}\right)^{-1} = e_L\left(\frac{\bar{\pi}az+\bar{\pi}b}{d}\right) = e_L\left(\frac{\bar{\pi}az}{d}\right) + e_L\left(\frac{\bar{\pi}b}{d}\right) = t\left(\frac{az}{d}\right)^{-1} + e_L\left(\frac{\bar{\pi}b}{d}\right),$$

where $t(az/d)$ is a power series in u by the previous lemma. From (5.40), we get

$$j \circ \theta = -\left(\frac{1}{t((az+b)/d)}\right)^{q-1} + \sum_{i=0}^{\infty} a_i \left(t\left(\frac{az+b}{d}\right)^{q-1}\right)^{i-1},$$

where $a_i \in \mathbf{A}$. Since $e_L(\bar{\pi}b/d) \in \rho[\mathsf{n}]$, it follows that $j \circ \theta$ is a Laurent series in u with coefficients in $\mathbf{A}[\lambda_{\mathsf{n}}]$. □

We can give a more precise form of the u-expansion for $j \circ \theta$. From (5.33) we get

$$t\left(\frac{az}{d}\right) = t\left(a^2\frac{z}{\mathsf{n}}\right) = \frac{u^{|a|^2}}{f_{a^2}(u)}. \tag{5.43}$$

So

$$t\left(\frac{az+b}{d}\right) = \sum_{i=0}^{\infty}(-1)^i e_L\left(\frac{\bar{\pi}b}{d}\right)^i \left(\frac{u^{|a|^2}}{f_{a^2}(u)}\right)^{i+1}$$

and

$$\begin{aligned} s\left(\frac{az+b}{d}\right)^{-1} &= e_L\left(\frac{\bar{\pi}az+\bar{\pi}b}{d}\right)^{q-1} = \left[e_L\left(\frac{\bar{\pi}az}{d}\right) + e_L\left(\frac{\bar{\pi}b}{d}\right)\right]^{q-1} \\ &= \left[\frac{1}{t\,(az/d)} + e_L\left(\frac{\bar{\pi}b}{d}\right)\right]^{q-1} = \left[\frac{f_{a^2}(u)}{u^{|a|^2}} + e_L\left(\frac{\bar{\pi}b}{d}\right)\right]^{q-1} \\ &= u^{-|a|^2(q-1)}\left[f_{a^2}(u) + e_L\left(\frac{\bar{\pi}b}{d}\right)u^{|a|^2}\right]^{q-1}. \end{aligned}$$

Substitute θz into (5.40) to obtain

$$j\left(\frac{az+b}{d}\right) = s\left(\frac{az+b}{d}\right)^{-1}\sum_{i=0}^{\infty} a_i s\left(\frac{az+b}{d}\right)^{i} = s\left(\frac{az+b}{d}\right)^{-1}\sum_{i=0}^{\infty} a_i t\left(\frac{az+b}{d}\right)^{(q-1)i},$$

which can be written as

$$j\left(\frac{az+b}{d}\right) = u^{-|a|^2(q-1)}\sum_{k=0}^{\infty} a_k u^k. \tag{5.44}$$

Let $\mathbf{A}((t))$ be the ring of formal Laurent series in t with coefficients in $\mathbf{A}$.

Proposition 5.5.4 ([Bae92])**.** *Each coefficient of $\Phi_{\mathfrak{n}}(X)$ has t-expansion in $\mathbf{A}((t))$.*

Proof. Let $m \in (\mathbf{A}/(\mathfrak{n}))^*$. For $\lambda_{\mathfrak{n}} \in \rho[\mathfrak{n}]$, the automorphism σ_m on $\mathbf{K}(\lambda_{\mathfrak{n}})$ is defined by

$$\sigma_m(\lambda_{\mathfrak{n}}) := \rho_m(\lambda_{\mathfrak{n}}).$$

Extend this automorphism to $\mathbf{K}(\lambda_{\mathfrak{n}})((u))$. Observe that in (5.43) the polynomial $f_{a^2}(X)$ is in $\mathbf{A}[X]$. Apply σ_m to the value of $t((az+b)/d)$ from the proof of Corollary 5.5.3 to obtain

$$\sigma_m\left(t\left(\frac{az+b}{d}\right)\right) = \sum_{i=0}^{\infty}(-1)^i e_L\left(\frac{\bar{\pi}br}{d}\right)^{i} t\left(\frac{az}{d}\right)^{i+1}.$$

Note that we can write

$$e_L\left(\frac{\bar{\pi}br}{d}\right) = e_L\left(\frac{\bar{\pi}b'}{d}\right),$$

where $b' \in \mathbf{A}$ such that $b' \equiv br \pmod{d}$ and $\deg_T(b') < \deg_T(d)$. It follows that $(j\circ\theta)^{\sigma_m} = j\circ\theta'$ for

$$\theta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \quad \text{and} \quad \theta' = \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix}.$$

So σ_m merely permutes the functions $j\circ\theta_i$, $\theta_i \in S_{\mathfrak{n}}$. This implies that the coefficients of $\Phi_{\mathfrak{n}}(X)$ are invariant under σ_m, and hence, the t-expansions of these coefficients are contained in $\mathbf{A}((t))$. □

Analogous to the q-expansion principle in the classical case, we know that the coefficients of $\Phi_{\mathfrak{n}}(X)$ are polynomials in $\mathbf{A}[j]$. So $\Phi_{\mathfrak{n}}$ can be viewed as a polynomial in X and j with coefficients in $\mathbf{A}$. So $\Phi_n(X,j) \in \mathbf{A}[X,j]$. We now get the analogue of the modular polynomial in the classical case. We call this the *Drinfeld modular polynomial of order* $\mathfrak{n}$ for j.

Theorem 5.5.5 ([Bae92]). *The modular polynomial $\Phi_{\mathsf{n}}(X, j)$ has the following properties.*

(i) It is irreducible over $\mathbf{C}(j)$, and has degree $\mathrm{N}(\mathsf{n})$.

(ii) Φ_{n} satisfies $\Phi_{\mathsf{n}}(X, j) = \Phi_{\mathsf{n}}(j, X)$.

(iii) If $\deg_T(\mathsf{n})$ is odd, then $\Phi_{\mathsf{n}}(j, j)$ is a polynomial in j of degree > 1 with leading coefficient ± 1.

Proof. The proofs of parts (i) and (ii) are the same as in the classical situation, see [Lan87, pp. 55-56].

To prove part (iii), assume that $\deg_T(\mathsf{n})$ is odd and let $\theta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \triangle_{\mathsf{n}}^*$ with $ad = \mathsf{n}$. Then $\deg_T(a) \neq \deg_T(d)$. From (5.33), we get

$$t^{-1} = t\left(\mathsf{n} \cdot \frac{z}{\mathsf{n}}\right)^{-1} = \frac{f_{\mathsf{n}}(u)}{u^{|\mathsf{n}|}}$$

and

$$t\left(\frac{az}{d}\right)^{-1} = t\left(a^2 \cdot \frac{z}{\mathsf{n}}\right)^{-1} = \frac{f_{a^2}(u)}{u^{|a|^2}},$$

where $|\mathsf{n}| = q^{\deg_T(\mathsf{n})}$ and $|a|^2 = q^{2\deg_T(a)}$. It follows that the u-expansion of j starts with $u^{-(q-1)q^{\deg_T(\mathsf{n})}}$ while that of $j \circ \theta$ starts with $u^{-(q-1)q^{2\deg_T a}}$. Since $\deg_T(\mathsf{n})$ is odd, $\deg_T(\mathsf{n}) \neq 2\deg_T(a)$. So the term with negative degree in $j - j \circ \theta$ starts with $u^{-(q-1)q^{\deg_T(\mathsf{n})}}$ or $-u^{-(q-1)q^{2\deg_T(a)}}$. So the u-expansion for $\Phi_{\mathsf{n}}(j, j)$ starts with c_m/u^m for some integer m with $c_m = \pm 1$. Hence

$$\Phi_{\mathsf{n}}(j, j) = c_m j^m + \cdots$$

is a polynomial in j with leading coefficient ± 1. □

Corollary 5.5.6 ([Bae92]). *For $\theta \in M_2(\mathbf{K})$, the function $j \circ \theta$ is integral over $\mathbf{A}[j]$.*

Proof. We can assume that $\theta \in M_2(\mathbf{A})$, i.e., θ is integral. Suppose $\det \theta = \mathsf{n}$. Then $j \circ \theta$ is a root of $\Phi_{\mathsf{n}}(X)$ which has leading coefficient 1, and is contained in $\mathbf{A}[j, X]$. □

The next result, known as the *Kronecker congruence relation*, gives a factorization of the modular polynomial $\Phi_\ell(X, j)$ where $\ell \in \mathbf{A}^+$ is irreducible. The detailed proof of this result is given in [Bae92]. It is very similar to the proof of this congruence relation in the classical case, see [Lan87, pp. 57-58].

Theorem 5.5.7 ([Bae92])**.** *Let $\ell \in \mathbf{A}^+$ be an irreducible polynomial of degree d. Then*

$$\Phi_\ell(X, j) \equiv (X - j^{q^d})(X^{q^d} - j) \pmod{\ell}. \tag{5.45}$$

In what follows, denote by $\sqrt{\mathsf{n}}$ any root of $X^2 - \mathsf{n} = 0$.

Theorem 5.5.8 ([Bae92])**.** *Let $\mathsf{n} \in \mathbf{A}^+$ be square-free of odd degree. If $z \in \mathbf{K}(\sqrt{\mathsf{n}})$, then $j(z)$ is integral over $\mathbf{A}$.*

Proof. Let $F = \mathbf{K}(z)$ and $\mathcal{O}_F = \mathbf{A}\omega + \mathbf{A}$ be the ring of regular functions (away from ∞) in F. So we can write $\sqrt{\mathsf{n}}\omega = a\omega + b$ and $\sqrt{\mathsf{n}} = c\omega + d$ with $a, b, c, d \in \mathbf{A}$. So the matrix

$$\theta' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is primitive with $\det \theta' = ad - bc = -\mathsf{n}$ and $\theta'\omega = \omega$. Put

$$\theta = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \theta'.$$

Then $\theta\omega = -\omega$ and $j(-\omega) = j(\omega)$. It follows that $j(\omega)$ is a root of $\Phi_{\mathsf{n}}(X, X) \in \mathbf{A}[X]$. By Theorem 5.5.5(iii), $j(\omega)$ is integral over $\mathbf{A}$. Now $\mathbf{K}(z) = \mathbf{K}(\omega)$, so there exists a primitive matrix $\alpha \in M_2(\mathbf{A})$ such that $z = \alpha\omega$. So by construction, $j(z)$ is a root of the polynomial $\Phi_{\det \alpha}(X, j(\omega))$. This implies that $j(z)$ is integral over $\mathbf{A}[j(\omega)]$. Hence $j(z)$ is integral over $\mathbf{A}$. □

Note that in this theorem, the field $F = \mathbf{K}(\sqrt{\mathsf{n}})$ is imaginary quadratic since the prime ∞ does not split. This theorem also holds for a square-free polynomial n of the following types:

1. $\deg_T(\mathsf{n})$ is odd and n is not necessarily monic.

2. $\deg_T(\mathsf{n})$ is even and n has leading coefficient contained in $\mathbb{F}_q - \mathbb{F}_q^2$, where $\mathbb{F}_q - \mathbb{F}_q^2$ is the set of non-squares in $\mathbb{F}_q$.

A proof of this assertion is given in [Bae92], pp.128-129. As for the second type of polynomial here, the leading coefficient of $\phi_{\mathsf{n}}(j, j)$ is in $\mathbb{F}_q$.

As in the classical case, the modular polynomial can be used to determine isogenies of Drinfeld modules. Let M be a finite $\mathbf{A}$-module. Then M is called *cyclic of degree* $\mathsf{n} \in \mathbf{A}$ if M is isomorphic to the cyclic module $\mathbf{A}/(\mathsf{n})$.

Theorem 5.5.9 ([Bae92])**.** *Let φ and φ' be Drinfeld modules of rank two over $\mathbf{C}$. Then there exists an isogeny $u : \varphi \longrightarrow \varphi'$ with cyclic kernel of degree $\mathsf{n} \in \mathbf{A}$ if and only if $j(\varphi')$ is a root of the equation*

$$\Phi_{\mathsf{n}}(X, j(\varphi)) = 0.$$

Proof. The proof is the same as in the classical case, see Theorem 2.3.18 or [Lan87, Theorem 5, Ch. 5 §3]. □

Expansions involving $\mathsf{n} = \ell$

We continue to use the notation $\mathbf{A}$, $\mathbf{K}$, $\mathbf{K}_\infty$, and $\mathbf{C}$ as in Section 5.1. Recall that the absolute value on $\mathbf{C}$ is normalized by $|T| = q$. Define a valuation on $\mathbf{C}$ by $\nu(x) = \log_q |x|$.

In what follows, we assume that $\ell \in \mathbf{A}^+$ is irreducible. Let $L = \bar{\pi}\mathbf{A} \subset \mathbf{C}$ be the rank one lattice associated to the Carlitz module $\rho_T = T + \tau$. Write

$$\rho_\ell(X) = \sum_{i=0}^{\deg_T(\ell)} \beta_i X^{q^i}, \tag{5.46}$$

where $\beta_i \in \mathbf{A}$. Let φ be the rank two Drinfeld module associated to the lattice $\Lambda = \mathbf{A} + z\mathbf{A}$ for $z \in \Omega$.

Lemma 5.5.10 ([BL97]). *For $a \in \mathbf{A}$ such that $\deg_T(a) < \deg_T(\ell)$, we have*

$$\prod_{\deg_T(a)<\deg_T(\ell)} \left(X + e_L\left(\frac{z+a}{\ell}\right)\right) = e_L(z) + \rho_\ell(X). \tag{5.47}$$

Proof.

$$\begin{aligned}\prod_{\deg_T(a)<\deg_T(\ell)} \left(X + e_L\left(\frac{z+a}{\ell}\right)\right) &= \prod_{\deg_T(a)<\deg_T(\ell)} \left(X + e_L\left(\frac{z}{\ell}\right) + e_L\left(\frac{a}{\ell}\right)\right) \\ &= \rho_\ell\left(X + e_L\left(\frac{z}{\ell}\right)\right) \\ &= \rho_\ell(X) + \rho_\ell\left(e_L\left(\frac{z}{\ell}\right)\right) \\ &= \rho_\ell(X) + e_L(z),\end{aligned}$$

where the last equality follows from (5.10). □

Corollary 5.5.11 ([BL97]). *Any elementary symmetric polynomial of $\{t((z+a)/\ell) \mid \deg_T(a) < \deg_T(\ell)\}$ takes the form bt for some polynomial $b \in \mathbf{A}$.*

Proof. Suppose f is a symmetric polynomial of $\{t((z+a)/\ell)\}$ such that $f \neq \prod t\left((z+a)/\ell\right)$. Then

$$f = \frac{h}{\prod e_L\left((z+a)/\ell\right)} = ht,$$

where h is a symmetric polynomial of $\{e_L((z+a)/\ell)\}$ and $h \neq \prod e_L\left((z+a)/\ell\right)$. □

The next corollary follows from the application of Newton's formulas [Gek88, p. 674] for power sums of the zeros of (5.47).

Corollary 5.5.12 ([BL97]).

$$\sum_{\deg_T(a)<\deg_T(\ell)} e_L\left(\frac{z+a}{\ell}\right) = \begin{cases} 0, & \text{if } \deg_T(\ell) \geq 2 \\ \beta_0 = \ell, & \text{if } \deg_T(\ell) = 1. \end{cases}$$

Proposition 5.5.13 ([BL97]).

$$\sum_{\deg_T(a)<\deg_T(\ell)} j\left(\frac{z+a}{\ell}\right)$$

has a holomorphic t-expansion of the form $\sum_{i=0}^{\infty} c_i t^i$, where $c_i \in \mathbf{A}$.

Proof. From the s-expansion of the j-invariant given in (5.40), we get

$$\sum_{\deg_T(a)<\deg_T(\ell)} j\left(\frac{z+a}{\ell}\right) = a_0 \sum_{\deg_T(a)<\deg_T(\ell)} e_L\left(\frac{z+a}{\ell}\right)^{q-1} + \sum_{i=1}^{\infty}\left(a_i \sum_{\deg_T(a)<\deg_T(\ell)} t\left(\frac{z+a}{\ell}\right)^{(q-1)(i-1)}\right)$$

By applying the Newton formulas to the symmetric polynomial obtained in Corollary 5.5.11, we see that

$$\sum_{\deg_T(a)<\deg_T(\ell)} t\left(\frac{z+a}{\ell}\right)^{(q-1)(i-1)} \in \mathbf{A}[t]$$

for $i \geq 2$. Moreover, there are only finitely many i such that t^v appears for a fixed v. The result now follows from Corollary 5.5.12. □

In the following proposition $\beta_{\deg_T(\ell)-1}$ (see (5.26) is obtained from (5.46) and S_ℓ is the complete set of Γ-coset representatives of $\triangle_\ell^*$. Recall that for $\theta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_\ell$, with $\deg_T(b) < \deg_T(d)$, we have $\theta(z) = \frac{az+b}{d}$.

Proposition 5.5.14 ([BL97])**.** *Write $\beta = \beta_{\deg_T(\ell)-1}$. Then $\nu(\beta) = q^{\deg_T(\ell)-1}$ and*

$$\sum_{\theta \in S_\ell} j(\theta z) = -s^{-q^{\deg_T(\ell)}} + \beta s^{-q^{\deg_T(\ell)-1}(q-1)} + \textit{higher terms.}$$

Proof. The first result follows from the fact that $\nu(\beta_i) = \log_q |\beta_i| = (\deg_T(\ell) - i)q^i$. To obtain the second result, we use (5.33) and the s-expansion of j given in (5.40). Then

$$\begin{aligned} j(\ell z) &= -s(\ell z)^{-1} + \sum_{i=1}^{\infty} a_i s(\ell z)^{i-1} \\ &= -\left(\frac{f_\ell(t)}{t^{|\ell|}}\right)^{q-1} + \sum_{i=1}^{\infty} a_i \left(\frac{t^{|\ell|}}{f_\ell(t)}\right)^{(q-1)(i-1)}. \end{aligned}$$

But

$$\begin{aligned} \left(\frac{f_\ell(t)}{t^{|\ell|}}\right)^{q-1} &= \left(\frac{\rho_\ell(t^{-1})t^{|\ell|}}{t^{|\ell|}}\right)^{q-1} = \rho_\ell(t^{-1})^{q-1} \\ &= \left(\beta_0 t^{-1} + \beta_1 t^{-q} + \cdots + \beta t^{-q^{\deg_T(\ell)-1}} + t^{-q^{\deg_T(\ell)}}\right)^{q-1} \\ &= t^{-q^{\deg_T(\ell)}(q-1)} + (q-1)\beta t^{-q^{\deg_T(\ell)-1}(q-1)^2} + \text{higher terms.} \end{aligned}$$

Thus

$$\begin{aligned} j(\ell z) &= -\left(\frac{1}{t^{q-1}}\right)^{q^{\deg_T(\ell)}} - (q-1)\beta\left(\frac{1}{t^{q-1}}\right)^{q^{\deg_T(\ell)-1}(q-1)} + \text{higher terms} \\ &= -s^{-q^{\deg_T(\ell)}} + \beta s^{-q^{\deg_T(\ell)-1}(q-1)} + \text{higher terms.} \end{aligned}$$

The desired result now follows from Proposition 5.5.13. □

By using Proposition 5.5.14 and Corollary 5.4.12, we obtain

$$\sum_{\theta \in S_\ell} j(\theta z) = j(z)^{q^{\deg_T(\ell)}} + \beta j(z)^{q^{\deg_T(\ell)-1}(q-1)} + h, \tag{5.48}$$

where h is a polynomial in $j(z)$ and $\deg(h) < q^{\deg_T(\ell)-1}(q-1)$.

Example 5.5.15. Consider the case $\ell = T \in \mathbf{A}$. Let $q = 3$. Then the Carlitz module is given by $\rho_T(X) = TX + X^3$ and the cyclotomic function field is given by $\mathbf{K}(\lambda_T)$, where $\lambda_T = \sqrt{-T}$ is a root of $X^2 + T = 0$. The complete set of Γ-coset representatives of $\triangle_T^*$ is the set

$$S_T = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & T \end{pmatrix}, \begin{pmatrix} T & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & T \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & T \end{pmatrix} \right\}.$$

We find a power series expansion for $\sum_{\theta \in S_T} j(\theta z)$ in terms of u using Proposition 5.5.14. Here $Y = e_L(\bar{\pi} z/T)$ and $a_0 = -1 \equiv 2 \pmod 3$.

$$\begin{aligned} j(z) &= \sum_{i=0}^{\infty} a_i s^{i-1} = \sum_{i=0}^{\infty} a_i \left[\frac{u^3}{f_T(u)}\right]^{2(i-1)} \\ &= a_0(u^{-6} + 2Tu^{-4} + T^2u^{-2}) + a_1 + \text{higher terms} \\ j\left(\frac{z}{T}\right) &= \sum_{i=0}^{\infty} a_i u^{2(i-1)} = a_0u^{-2} + a_1 + \text{higher terms} \\ j(Tz) &= \sum_{i=0}^{\infty} a_i \left[\frac{u^9}{f_{T^2}(u)}\right]^{2(i-1)} \\ &= a_0[u^{-18} + (2T^3 + 2T)u^{-12} + 2T^2u^{-10} + (T^6 + 2T^4 + T^2)u^{-6} + (2T^5 + 2T^3)u^{-4} \\ &\quad + T^4u^{-2}] + a_1 + \text{higher terms} \end{aligned}$$

$$j\left(\frac{z+1}{T}\right) = \sum_{i=0}^{\infty} a_i \left[\frac{u}{1+Yu}\right]^{2(i-1)} = a_0[u^{-2} + 2Yu^{-1} + Y^2] + a_1 + \text{higher terms}$$

$$j\left(\frac{z+2}{T}\right) = \sum_{i=0}^{\infty} a_i \left[\frac{u}{1+2Yu}\right]^{2(i-1)} = a_0[u^{-2} + Yu^{-1} + Y^2] + a_1 + \text{higher terms}$$

Then by (5.48), we get

$$\sum_{\theta \in S_T} j(\theta z) = j(z)^3 - 2Tj(z)^2 + T^2 j(z).$$

Chapter 6

Morphisms of Rank Two Drinfeld Modules

This chapter focuses on morphisms between rank two Drinfeld modules. In particular, we consider properties of isogenies and endomorphism rings of Drinfeld modules over finite fields. Further, we delve into the characteristic polynomial of the Frobenius endomorphism and give a description of the coefficients of this polynomial. Then we look into the features of the automorphism group of Drinfeld modules, and determine how these modules behave under reduction. Finally, we review the action of ideals on Drinfeld modules.

Most of the results presented in this chapter are prior work with the exception of our method of finding linear isogenies between Drinfeld modules (see Proposition 6.1.6), which is new and original, and a few minor results that we will point out as we go further in the chapter.

Throughout this chapter we continue to use the notations $\mathbf{A}$, $\mathbf{A}^+$, $\mathbf{K}$, $\mathbf{K}_\infty$, and $\mathbf{C}$, which were introduced at the beginning of Section 4.2. We also use the following additional notations.

$\mathfrak{p}$ = a (maximal) prime ideal in $\mathbf{A}$;

$P = P(T)$ = monic irreducible polynomial generator of $\mathfrak{p}$

$d = \deg_T(P)$

$\mathbb{F}_\mathfrak{p} = \mathbf{A}/\mathfrak{p}$, a finite residue field

$\mathbb{L}$ = a field equipped with a structure morphism $\gamma : \mathbf{A} \longrightarrow \mathbb{L}$ as an $\mathbf{A}$-algebra

6.1 Isogenies of Drinfeld Modules

In this section we give additional properties of nonzero morphisms, i.e., isogenies, of Drinfeld modules. As in Chapter 4, let τ be the q-th power map , i.e., $\tau : \alpha \longmapsto \alpha^q$ with $\alpha \in \mathbb{L}$, and let $\mathbb{L}\{\tau\}$ be the twisted polynomial ring with commutation rule given in (4.4). Throughout this section we assume that φ is a rank two Drinfeld $\mathbf{A}$-module over $\mathbb{L}$ given by

$$\begin{aligned} \varphi : \mathbf{A} &\longrightarrow \mathbb{L}\{\tau\} \\ a &\longmapsto \varphi_a. \end{aligned}$$

It is uniquely determined by the image of T, and we write this as

$$\varphi_T = \gamma(T) + g\tau + \Delta\tau^2, \tag{6.1}$$

with $g, \Delta \in \mathbb{L}$ and $\Delta \neq 0$. For ease of notation, we will sometimes use $\varphi = (g, \Delta)$ to represent φ as determined by (6.1). Recall that for $0 \neq a \in \mathbf{A}$, the set of a-torsion points of φ is the set

$$\varphi[a] = \varphi[(a)] = \{\lambda \in \overline{\mathbb{L}} \mid \varphi_a(\lambda) = 0\} = \ker \varphi_a.$$

Suppose ψ is another Drinfeld module of rank two defined over $\mathbb{L}$. Similar to φ, it is also uniquely determined by $\psi_T = \gamma(T) + g'\tau + \Delta'\tau^2$, where $g', \Delta' \in \mathbb{L}$ and $\Delta' \neq 0$. As shown in Section 4.3, the morphisms between φ and ψ are polynomials in $\mathbb{L}\{\tau\}$.

Let $u \in \mathbb{L}\{\tau\}$ be a separable isogeny from φ to ψ; that is, $u = \sum_{i=0}^{m} u_i\tau^i$, with $u_0 \neq 0$ and $u_i \in \mathbb{L}$ for $0 \leq i \leq m$. The kernel of this isogeny over $\overline{\mathbb{L}}$, denoted $\ker u/\overline{\mathbb{L}}$, is a finite $\mathbf{A}$-submodule of $\overline{\mathbb{L}}$. So we can always find a nonzero $a \in \mathbf{A}$ that annihilates $\ker u/\overline{\mathbb{L}}$, i.e., $a \cdot \ker u/\overline{\mathbb{L}} = 0$.

Proposition 6.1.1. *Let $u : \varphi \longrightarrow \psi$ be a separable isogeny of Drinfeld modules over $\mathbb{L}$. If $0 \neq a \in \mathbf{A}$ such that $a \cdot \ker u/\overline{\mathbb{L}} = 0$, then there exists an isogeny $v : \psi \longrightarrow \varphi$ such that*

(a) $v \cdot u = \varphi_a$ with $\ker v/\overline{\mathbb{L}} = u(\varphi[a])$, and

(b) $u \cdot v = \psi_a$ with $\ker u/\overline{\mathbb{L}} = v(\psi[a])$.

Proof. See [DH87](4.1) for part (a) and [Tra03, Proposition 1.19] for part (b). □

Remark 6.1.2. If u is a separable isogeny from φ to ψ, then we can choose v to be separable as well. Moreover, the polynomial v in the preceding proposition is the dual isogeny to u (see Definition 4.3.9).

Now consider a purely inseparable isogeny. Recall that this is of the form $\tau^j \in \mathbb{L}\{\tau\}$ for some integer $j > 0$. Note that $\tau^j \cdot \varphi_a = \varphi_a \cdot \tau^j$ in $\mathbb{L}\{\tau\}$ if and only if the coefficients of φ_a are in $\mathbb{F}_{q^j}$. So a purely inseparable isogeny exists only if the $\mathbf{A}$-characteristic of $\mathbb{L}$, $\mathrm{char}_{\mathbf{A}}(\mathbb{L})$, is finite. In what follows, the symbol $\mathrm{Spec}(R)$ represents the set of prime ideals of a ring R.

Proposition 6.1.3. *If $u : \varphi \longrightarrow \psi$ is a purely inseparable isogeny of Drinfeld modules over $\mathbb{L}$, then*

$$\ker u = Spec\left(\frac{\mathbb{L}[T]}{(T^{q^j})}\right).$$

Proof. See [DH87](4.2). □

We now define a term pertaining to the degree of isogenies of Drinfeld modules (cf. [Sch95], p. 54).

Definition 6.1.4. Let $\mathfrak{n} \in \mathbf{A}^+$ be nonconstant and let φ and ψ be Drinfeld modules of rank two over an $\mathbf{A}$-field $\mathbb{L}$. An isogeny $u : \varphi \longrightarrow \psi$ is called an $\mathfrak{n}$-*isogeny* if $\ker u / \overline{\mathbb{L}}$, i.e., the elements of $\overline{\mathbb{L}}$ annihilated by u, is a free rank one $\mathbf{A}$-submodule of $\varphi[\mathfrak{n}]$. We say that u is an isogeny of *degree* $\mathfrak{n}$.

Denote the degree of an isogeny u by $\deg_{isog}(u)$ to differentiate it from the degree $\deg_\tau(u)$ as a polynomial in τ.

Remark 6.1.5.

(a) A necessary condition for the definition of an $\mathfrak{n}$-isogeny is the existence of another element $v \in \mathbb{L}\{\tau\}$ such that $v \cdot u = \varphi_{\mathfrak{n}}$ with $\deg_\tau(v) = \deg_\tau(u) = \deg_T(\mathfrak{n})$. Moreover, this condition is sufficient if $\deg_T(\mathfrak{n}) = 1$. Note that Proposition 4.3.6 guarantees the existence of such v, i.e., $v = \widehat{u}$.

(b) $\varphi[\mathfrak{n}]$ only depends on the ideal in $\mathbf{A}$ generated by $\mathfrak{n}$. So u is an isomorphism if and only if $(\mathfrak{n}) = (1)$.

The next result gives a method of constructing a separable monic isogeny $u \in \mathbb{L}\{\tau\}$ between rank two Drinfeld modules φ and ψ over $\mathbb{L}$ with $\deg_\tau(u) = 1$. We use some properties of additive polynomials given in [Ore33a, Theorem 3]. Recall that $\mathbb{L}$ is equipped with a structure map $\gamma : \mathbf{A} \longrightarrow \mathbb{L}$, where γ is either inclusion or reduction modulo a prime $P \in \mathbf{A}$. Let $\mathfrak{n} = T + \varepsilon \in \mathbf{A}$ with $\varepsilon \in \mathbb{F}_q$. Here we identify $\mathfrak{n}$ with $\mathfrak{n} \pmod P$ in the finite $\mathbf{A}$-characteristic case.

Proposition 6.1.6. *Let $\alpha \in \mathbb{L}^*$, $u = \tau - \alpha \in \mathbb{L}\{\tau\}$ and $\mathfrak{n} = T + \varepsilon \in \mathbf{A}$, where $\varepsilon \in \mathbb{F}_q$. Let φ be a rank two Drinfeld module such that $\varphi_\mathfrak{n} = \mathfrak{n} + g\tau + \Delta\tau^2$, with $g \in \mathbb{L}$ and $\Delta \in \mathbb{L}^*$. Then u is an $\mathfrak{n}$-isogeny from φ to a rank two Drinfeld module ψ if and only if α is a root of $r(X) := \Delta X^{q+1} + gX + \mathfrak{n}$ and the image of $\varphi_\mathfrak{n}$ under u is $\psi_\mathfrak{n} = \mathfrak{n} + g'\tau + \Delta'\tau^2$, where $g' = g^q - \alpha\Delta + \alpha^{q^2}\Delta^q$ and $\Delta' = \Delta^q$. Moreover, the dual isogeny $\widehat{u} : \psi \longrightarrow \varphi$ is the polynomial $v = \Delta\tau + g + \Delta\alpha^q \in \mathbb{L}\{\tau\}$.*

Proof. Suppose $u = \tau - \alpha$ is an isogeny from φ such that $\deg_{isog}(u) = \mathfrak{n}$. So $\varphi_\mathfrak{n}$ is right divisible by u; that is, there exists a polynomial $v \in \mathbb{L}\{\tau\}$ such that $\varphi_\mathfrak{n} = v \cdot u$. Here $v = \widehat{u} \in \mathbb{L}\{\tau\}$. We claim that v is of the form $\Delta\tau - \beta$, with $\beta \in \mathbb{L}$. Note that $\varphi_\mathfrak{n}$ is of degree 2 in terms of τ and has leading coefficient Δ. Since u is linear in τ and monic, it follows that v is also linear in τ and has leading coefficient Δ. We have

$$\varphi_\mathfrak{n} = \Delta\tau^2 + g\tau + \mathfrak{n} = (\Delta\tau - \beta) \cdot (\tau - \alpha) = \Delta\tau^2 - (\Delta\alpha^q + \beta)\tau + \beta\alpha.$$

By comparing coefficients, one gets

$$g = -\Delta\alpha^q - \beta \quad \text{and} \quad \beta\alpha = \mathfrak{n}.$$

So $\beta = -g - \Delta\alpha^q$. Furthermore, $\Delta\alpha^q + g + \beta = 0$. Therefore,

$$0 = \alpha(\Delta\alpha^q + g + \beta) = \Delta\alpha^{q+1} + g\alpha + \beta\alpha = \Delta\alpha^{q+1} + g\alpha + \mathfrak{n},$$

which shows that α is a root of $r(X)$.

By assumption, u is an isogeny from φ to another Drinfeld module ψ. Let the image of φ_{n} under u be $\psi_{\mathsf{n}} = \Delta'\tau^2 + g'\tau + \mathsf{n}$. We need to determine Δ' and g'. Since u is an isogeny, we have

$$\begin{aligned} u \cdot \varphi_{\mathsf{n}} &= \psi_{\mathsf{n}} \cdot u \\ (\tau - \alpha) \cdot (\Delta\tau^2 + g\tau + \mathsf{n}) &= (\Delta'\tau^2 + g'\tau + \mathsf{n}) \cdot (\tau - \alpha) \qquad (6.2) \\ \Delta^q\tau^3 + (g^q - \Delta\alpha)\tau^2 + (\mathsf{n}^q - g\alpha)\tau - \mathsf{n}\alpha &= \Delta'\tau^3 + (g' - \Delta'\alpha^{q^2})\tau^2 + (\mathsf{n} - g'\alpha^q)\tau - \mathsf{n}\alpha. \end{aligned}$$

Therefore $\Delta' = \Delta^q$ and $g' = g^q - \Delta\alpha + \Delta^q\alpha^{q^2}$.

As for the converse, let $\alpha \in \overline{\mathbb{L}}$ be a root of $r(X)$. We want to show that $u = \tau - \alpha$ is an isogeny of degree n from φ to ψ. First, we need to verify that $u \cdot \varphi_{\mathsf{n}} = \psi_{\mathsf{n}} \cdot u$ holds for $\varphi_{\mathsf{n}} = \Delta\tau^2 + g\tau + \mathsf{n}$ and $\psi_{\mathsf{n}} = \Delta^q\tau^2 + (g^q - \Delta\alpha + \Delta^q\alpha^{q^2})\tau + \mathsf{n}$. As in (6.2),

$$u \cdot \varphi_{\mathsf{n}} = \Delta^q\tau^3 + (g^q - \Delta\alpha)\tau^2 + (\mathsf{n}^q - g\alpha)\tau - \mathsf{n}\alpha,$$

while substituting the values of Δ' and g' into the right-hand side of (6.2) gives

$$\begin{aligned} \psi_{\mathsf{n}} \cdot u &= \Delta^q\tau^3 + (g^q - \Delta\alpha + \Delta^q\alpha^{q^2} - \Delta^q\alpha^{q^2})\tau^2 + (\mathsf{n} - (g^q - \Delta\alpha + \Delta^q\alpha^{q^2})\alpha^q)\tau - \mathsf{n}\alpha \\ &= \Delta^q\tau^3 + (g^q - \Delta\alpha)\tau^2 + (\mathsf{n} - g^q\alpha^q + \Delta\alpha^{q+1} - \Delta^q\alpha^{q^2+q})\tau - \mathsf{n}\alpha. \end{aligned}$$

So we need to show that

$$\mathsf{n} - g^q\alpha^q + \Delta\alpha^{q+1} - \Delta^q\alpha^{q^2+q} = \mathsf{n}^q - g\alpha. \qquad (6.3)$$

Note that

$$\begin{aligned} \mathsf{n} - g^q\alpha^q + \Delta\alpha^{q+1} - \Delta^q\alpha^{q^2+q} - (\mathsf{n}^q - g\alpha) &= \mathsf{n} - g^q\alpha^q + \Delta\alpha^{q+1} - \Delta^q\alpha^{q^2+q} - \mathsf{n}^q + g\alpha \\ &= \Delta\alpha^{q+1} + g\alpha + \mathsf{n} - (\Delta^q\alpha^{q^2+q} + g^q\alpha^q + \mathsf{n}^q) \\ &= \Delta\alpha^{q+1} + g\alpha + \mathsf{n} - (\Delta\alpha^{q+1} + g\alpha + \mathsf{n})^q \\ &= r(\alpha) - r(\alpha)^q = 0, \end{aligned}$$

since α is a root of $r(X)$. So (6.3) is obtained. Hence, $u : \varphi \longrightarrow \psi$ is an isogeny. By Proposition 4.3.6, there exists $v \in \mathbb{L}\{\tau\}$ such that $\varphi_{\mathfrak{n}} = v \cdot u$. As noted above, we have $\deg_\tau(u) = \deg_\tau(v) = 1$. Moreover, $\deg_T(\mathfrak{n}) = 1$ as well. It follows from Remark 6.1.5 that $\deg_{isog}(u) = \mathfrak{n}$. This completes the proof. □

Remark 6.1.7.

(a) If α satisfies Proposition 6.1.6, then α is a $(q-1)$-st power of a root of $\varphi_{\mathfrak{n}}(X)$.

(b) We can obtain an alternate expression for g' in (6.2), namely

$$g' = \frac{\mathfrak{n} + g\alpha - \mathfrak{n}^q}{\alpha^q},$$

which can be easily shown to equal $g^q - \Delta\alpha + \Delta^q\alpha^{q^2}$ since α is a root of $r(X)$.

(c) A similar result for T-isogenies is given in [Sch95].

(d) At this point, we do not know if Proposition 6.1.6 can be generalized to higher degree isogenies of Drinfeld modules over $\mathbb{L}$. We have done some preliminary computations, but even for $\deg_T(\mathfrak{n}) = 2$ alone, the computations already required complicated symbolic computation.

1. Another method of constructing isogenies of Drinfeld modules over finite fields is given in [Yu95b, Section 2] using *kernel lattices*.

Example 6.1.8. Let $q = 3$ and $\mathbb{L} = \mathbb{F}_{\mathfrak{p}} = \mathbf{A}/\mathfrak{p}$, with $P(T) = T^5 + 2T + 1$. Some $\mathfrak{n}$-isogenies of Drinfeld modules obtained by using Proposition 6.1.6 are given below.

(a) T-isogeny: The isogeny $u = \tau - (T^3 + 2T + 2)$ sends the Drinfeld module $\varphi = (T^2, T^3)$ to $\psi = (2T^4 + T^2, 2T^4 + T + 2)$. Its dual is given by $\widehat{u} = (2T^4 + T^2, 2T^4 + T + 2)$. Here $\alpha = T^3 + 2T + 2$ is a root of the polynomial $r(X) = T^3X^4 + T^2X + T$.

(b) $(T+1)$-isogeny: We have an isogeny $u = \tau - (T^2 + 2)$ from $\varphi = (T^2, T^2 + 2T)$ to $\psi = (2T^4 + 2T + 2, 2T^3 + T^2 + 2T)$ with dual $\widehat{u} = (T^2 + 2T)\tau + T^4 + T^3 + T^2 + T$. In this case, $\alpha = T^2 + 2$ is a root of $r(X) = (T^2 + 2T)X^4 + T^2X + T + 1$.

(c) $(T+2)$-isogeny: Consider the Drinfeld module $\varphi = (T^3, T^4+1)$ and construct the polynomial $r(X) = (T^4+1)X^4 + T^3X + T + 2$. This polynomial has $\alpha = T^3 + T$ as a root, so the isogeny $u = \tau - (T^3+T)$ sends φ to the Drinfeld module $\psi = (2T^4+1, T^4+T^3+T^2+1)$. Here $\widehat{u} = (T^4+1)\tau + T^3 + 2T^2 + 2T + 1$.

The Dual Isogeny

We conclude this section by giving additional properties of the dual isogeny, see Definition 4.3.9. Recall from Proposition 4.3.6 that for every isogeny $u \in \mathrm{Hom}_{\mathbb{L}}(\varphi, \psi)$, there exists an isogeny $\widehat{u} \in \mathrm{Hom}_{\mathbb{L}}(\psi, \varphi)$ that satisfies

$$\widehat{u} \cdot u = \varphi_a \quad \text{and} \quad u \cdot \widehat{u} = \psi_a,$$

for some nonzero $a \in \mathbf{A}$.

Notice that this gives an analogue of the multiplication-by-m map for elliptic curves, i.e., φ_a takes the role of $[m]$, where m is the degree of an isogeny between two elliptic curves.

Lemma 6.1.9. *Let $u : \varphi \longrightarrow \psi$ be an isogeny of Drinfeld modules such that $\deg_{isog}(u) = \mathfrak{n} \in \mathbf{A}$. Then the dual isogeny $\widehat{u} : \psi \longrightarrow \varphi$ such that $\widehat{u} \cdot u = \varphi_{\mathfrak{n}}$ is unique.*

Proof. Suppose there exists another isogeny $\widehat{u}' : \psi \longrightarrow \varphi$ such that $\widehat{u}' \cdot u = \varphi_{\mathfrak{n}}$. Then

$$(\widehat{u} - \widehat{u}')u = \widehat{u} \cdot u - \widehat{u}' \cdot u = \varphi_{\mathfrak{n}} - \varphi_{\mathfrak{n}} = 0.$$

By definition of an isogeny, u is nonzero. It follows that $\widehat{u} - \widehat{u}' = 0 \in \mathbb{L}\{\tau\}$ if and only if $\widehat{u} = \widehat{u}'$. □

We mention, at this point, that an analogue of the Weil pairing has been constructed for Drinfeld modules in [vdH04]. Here we give a brief discussion on this nondegenerate pairing because we need some of its features to characterize sums of dual isogenies in Theorem 6.1.11. Suppose $a \in \mathbf{A}^+$ is prime to $\mathrm{char}_{\mathbf{A}}(\mathbb{L})$. Write $a = \sum_{i=0}^{k} a_i T^i$, with $a_k = 1$. Let φ be a rank two Drinfeld module determined by (6.1) and let ϑ be the rank one Drinfeld module such

that $\vartheta_T = \gamma(T) - \Delta\tau$. Moreover, assume that $u \in \mathbb{L}\{\tau\}$ is an isogeny from φ to another rank two Drinfeld module ψ with $\widehat{u}$ as its dual. As before, $\varphi[a]$ and $\vartheta[a]$ are the kernels of φ_a and ϑ_a, respectively. The Weil pairing introduced in [vdH04, Proposition 7.3] induces a pairing

$$\begin{aligned} e_a : \varphi[a] \times \varphi[a] &\longrightarrow \vartheta[a] \\ (x, y) &\longmapsto \sum_{i=0}^{k-1} \left(\sum_{j=0}^{k-i-1} a_{i+j+1} T^j \right) f_j(x, y), \end{aligned}$$

where $f_j(x, y) = x\varphi_{T^j}(y)^q - x^q \varphi_{T^j}(y)$.

Proposition 6.1.10. *With the notations as above, the pairing e_a has the following properties:*

1. *Bilinearity:*

$$e_a(x_1 + x_2, y) = e_a(x_1, y) + e_a(x_2, y),$$
$$e_a(x, y_1 + y_2) = e_a(x, y_1) + e_a(x, y_2).$$

2. *Galois equivariance: For $\sigma \in \mathrm{Gal}(\overline{\mathbb{L}}/\mathbb{L})$,*

$$e_a(x^\sigma, y^\sigma) = e_a(x, y)^\sigma.$$

3. *Compatibility: Let $b \in \mathbf{A}$ such that b is prime to $char_{\mathbf{A}}(\mathbb{L})$. For $x \in \varphi[ab]$ and $y \in \varphi[a]$,*

$$b\ e_{ab}(x, y) = e_a(\varphi_b(x), y).$$

4. *Duality:*

$$e_a(\widehat{u}(u(x)), y) = e_a(u(x), u(y)).$$

Proof. It is clear that $f_j(x_1 + x_2, y) = f_j(x_1, y) + f_j(x_2, y)$ for $x_1, x_2, y \in \varphi[a]$. Also, as φ_{T^j} is an additive polynomial, it follows immediately that $f_j(x, y_1 + y_2) = f_j(x, y_1) + f_j(x, y_2)$ for $x, y_1, y_2 \in \varphi[a]$. Therefore, e_a is bilinear.

See [vdH04, Proposition 5.4] for the last three properties. □

We use some properties of this pairing in the proof of the next result regarding dual isogenies. We mention that this result may already be known to experts in the field, but we could not find any proof in the literature. So we included a proof here for completeness. This result is the analogue of Theorem 2.1.9. Note that the product of two isogenies is again an isogeny, i.e., nonzero. On the other hand, the sum of two isogenies, $u+v$, is an isogeny if and only if $u \neq -v$ for $u, v \in \mathrm{Hom}_{\mathbb{L}}(\varphi, \psi)$.

Theorem 6.1.11. *Let $u : \varphi \longrightarrow \psi$ be an isogeny of rank two Drinfeld modules over an $\mathbf{A}$-field $\mathbb{L}$.*

(a) Let $\deg_{isog}(u) = \mathfrak{n}$. Then $\widehat{u} \cdot u = \varphi_{\mathfrak{n}}$ and $u \cdot \widehat{u} = \psi_{\mathfrak{n}}$.

(b) Let $v : \psi \longrightarrow \sigma$ be another isogeny of rank two Drinfeld modules. Then $\widehat{v \cdot u} = \widehat{u} \cdot \widehat{v}$.

(c) Let $w : \varphi \longrightarrow \psi$ be another isogeny of rank two Drinfeld modules with $w \neq -u$. Then $\widehat{u+w} = \widehat{u} + \widehat{w}$.

(d) For all $a \in \mathbf{A}$, $\widehat{\varphi_a} = \varphi_a$ and $\deg_{isog}(\varphi_a) = a^2$.

(e) $\deg_{isog}(\widehat{u}) = \deg_{isog}(u)$.

(f) $\widehat{\widehat{u}} = u$.

Proof.

(a) This follows from Proposition 4.3.6, Corollary 4.3.7.1, and Remark 6.1.5.

(b) Let $\deg_{isog}(v) = \mathfrak{m} \in \mathbf{A}$. Necessarily, there exists $\widehat{v} \in \mathbb{L}\{\tau\}$ such that $\widehat{v} \cdot v = \psi_{\mathfrak{m}}$. Moreover, we know from Definition 4.3.1 that $u \cdot \varphi_{\mathfrak{m}} = \psi_{\mathfrak{m}} \cdot u$. So

$$(\widehat{u} \cdot \widehat{v}) \cdot (v \cdot u) = \widehat{u} \cdot \psi_{\mathfrak{m}} \cdot u = \widehat{u} \cdot u \cdot \varphi_{\mathfrak{m}} = \varphi_{\mathfrak{n}} \cdot \varphi_{\mathfrak{m}} = \varphi_{\mathfrak{nm}}.$$

However, we know that $\widehat{(v \cdot u)}$ is the unique dual isogeny to $v \cdot u$ such that $\widehat{(v \cdot u)} \cdot (v \cdot u) = \varphi_{\mathfrak{nm}}$. The desired equality follows.

(c) Note that $w \neq -u$ so $u+w$ is an isogeny from φ to ψ. Let $a \in \mathbf{A}$ be prime to $\mathrm{char}_{\mathbf{A}}(\mathbb{L})$. Suppose $x, y \in \varphi[a]$, then by using the bilinear and dual properties of e_a we obtain the equality

$$\begin{aligned}
e_a(\widehat{(u+w)} \cdot (u+w)(x), y) &= e_a((u+w)(x), (u+w)(y)) \\
&= e_a((u+w)(x), u(y) + w(y)) \\
&= e_a((u+w)(x), u(y)) + e_a((u+w)(x), w(y)) \\
&= e_a(u(x), u(y)) + e_a(w(x), u(y)) + e_a(u(x), w(y)) \\
&\quad + e_a(w(x), w(y)) \\
&= e_a(\widehat{u}(u(x)), y) + e_a(\widehat{u}(w(x)), y) + e_a(\widehat{w}(u(x)), y) \\
&\quad + e_a(\widehat{w}(w(x)), y) \\
&= e_a((\widehat{u} \cdot u + \widehat{u} \cdot w + \widehat{w} \cdot u + \widehat{w} \cdot w)(x), y) \\
&= e_a((\widehat{u} + \widehat{w}) \cdot (u+w)(x), y).
\end{aligned}$$

So

$$\widehat{(u+w)} \cdot (u+w) = (\widehat{u} + \widehat{w}) \cdot (u+w),$$

and dividing this equation by $u+w$ from the right gives $\widehat{u+w} = \widehat{u} + \widehat{w}$.

(d) Let $\deg_{isog}(\varphi_a) = \mathsf{b} \in \mathbf{A}$. Note that $\widehat{\varphi_a}$ is the unique polynomial in $\mathbb{L}\{\tau\}$ such that $\widehat{\varphi_a} \cdot \varphi_a = \varphi_{\mathsf{b}}$, and by Remark 6.1.5 we have $\deg_\tau(\varphi_a) = \deg_\tau(\widehat{\varphi_a}) = \deg_T(\mathsf{b})$. Now

$$\varphi_a \cdot \widehat{\varphi_a} \cdot \varphi_a = \varphi_a \cdot \varphi_{\mathsf{b}} = \varphi_{a\mathsf{b}} = \varphi_{\mathsf{b}a} = \varphi_{\mathsf{b}} \cdot \varphi_a.$$

Divide this equation by φ_a from the right to get $\varphi_a \cdot \widehat{\varphi_a} = \varphi_{\mathsf{b}}$. It follows that

$$\varphi_a \cdot \widehat{\varphi_a} = \varphi_{\mathsf{b}} = \widehat{\varphi_a} \cdot \varphi_a.$$

So $\widehat{\varphi_a} = \varphi_a$. Furthermore, $\varphi_{\mathsf{b}} = \varphi_a^2 = \varphi_a \cdot \varphi_a = \varphi_{a^2}$, which shows that $\mathsf{b} = a^2$.

(e) Suppose $\deg_{isog}(u) = \mathsf{n}$, so that $\widehat{u} \cdot u = \varphi_{\mathsf{n}}$. As $\deg_{isog}(\varphi_{\mathsf{n}}) = \mathsf{n}^2$ from part (d), we get

$$\mathsf{n}^2 = \deg_{isog}(\varphi_{\mathsf{n}}) = \deg_{isog}(\widehat{u} \cdot u) = \deg_{isog}(\widehat{u}) \deg_{isog}(u) = \deg_{isog}(\widehat{u})\ \mathsf{n}.$$

This shows that $\deg_{isog}(\widehat{u}) = \mathsf{n}$.

(f) As before, let $\deg_{isog}(u) = \mathsf{n}$. We apply parts (a), (b), and (d) to get

$$\widehat{u} \cdot u = \varphi_{\mathsf{n}} = \widehat{\varphi_{\mathsf{n}}} = \widehat{\widehat{u} \cdot u} = \widehat{u} \cdot \widehat{\widehat{u}}.$$

So $\widehat{u} \cdot u - \widehat{u} \cdot \widehat{\widehat{u}} = \widehat{u} \cdot (u - \widehat{\widehat{u}}) = 0$. Since $\widehat{u} \neq 0$, it follows that $\widehat{\widehat{u}} = u$.

□

6.2 The Endomorphism Ring

Here we identify $\mathbf{A}$ with the subring $\varphi(\mathbf{A}) \subset \mathbb{L}\{\tau\}$. Our aim in this section is to describe the basic properties of the endomorphism ring $\mathrm{End}_{\mathbb{L}}(\varphi)$ of a rank two Drinfeld module φ over $\mathbb{L}$. We have

$$\mathrm{End}_{\mathbb{L}}(\varphi) = \{u \in \mathbb{L}\{\tau\} \mid u\varphi = \varphi u\}.$$

This endomorphism ring becomes an $\mathbf{A}$-module via φ. Moreover, as $\mathrm{End}_{\mathbb{L}}(\varphi) \subseteq \mathbb{L}\{\tau\}$, $\mathrm{End}_{\mathbb{L}}(\varphi)$ is torsion-free.

Lemma 6.2.1. *For any $a \in \mathbf{A}$, φ_a is an endomorphism of φ.*

Proof. Let $b \in \mathbf{A}$. By commutativity in $\mathbf{A}$ we get

$$\varphi_a \varphi_b = \varphi_{ab} = \varphi_{ba} = \varphi_b \varphi_a.$$

Thus, $\varphi_a \in \mathrm{End}_{\mathbb{L}}(\varphi)$. □

Hence, if we identify $\mathbf{A}$ with $\varphi(\mathbf{A})$ we get the next result.

Corollary 6.2.2. $\mathbf{A}$ *is a subring of* $\mathrm{End}_{\mathbb{L}}(\varphi)$.

Note that φ_a is always an endomorphism of φ for any $\mathbf{A}$-characteristic of $\mathbb{L}$. We give another endomorphism of φ in the next result where the $\mathbf{A}$-characteristic of $\mathbb{L}$ is finite. Let

$[\mathbb{F}_\mathfrak{p} : \mathbb{F}_q] = d$, where $\mathfrak{p} = (P)$ and $d = \deg_T(P)$. Assume that $\mathbb{L}$ is an extension of $\mathbb{F}_\mathfrak{p}$ of degree m. Then

$$n := [\mathbb{L} : \mathbb{F}_q] = [\mathbb{L} : \mathbb{F}_\mathfrak{p}][\mathbb{F}_\mathfrak{p} : \mathbb{F}_q] = md. \tag{6.4}$$

So $\#\mathbb{L} = q^n$, and $\mathbb{L}$ contains $\mathbb{F}_q$ via the structure map $\gamma : \mathbf{A} \longrightarrow \mathbb{L}$. Define $F := \tau^n$, i.e., F is the map that sends α to α^{q^n} for every $\alpha \in \overline{\mathbb{L}}$.

Lemma 6.2.3. *If $\mathbb{L}$ has finite $\mathbf{A}$-characteristic, i.e., $char_\mathbf{A}(\mathbb{L}) \neq (0)$, then $F \in \mathrm{End}_\mathbb{L}(\varphi)$.*

Proof. Note that

$$\begin{aligned} F\varphi_T &= F\gamma(T) + Fg\tau + F\Delta\tau^2 \\ &= \gamma(T)^{q^n}\tau^n + g^{q^n}\tau^{n+1} + \Delta^{q^n}\tau^{n+2} \\ &= \gamma(T)F + g\tau F + \Delta\tau^2 F, \qquad \text{since } \gamma(T), g, \Delta \in \mathbb{L} \\ &= \varphi_T F. \end{aligned}$$

So F commutes with φ_T. This is also true for any $a \in \mathbf{A}$, i.e., F commutes with $\varphi(\mathbf{A}) \subset \mathbb{L}\{\tau\}$, and hence $F \in \mathrm{End}_\mathbb{L}(\varphi)$. □

Definition 6.2.4. F is called the *Frobenius endomorphism* associated to φ.

The Tate Module

Now suppose $\mathrm{char}_\mathbf{A}(\mathbb{L}) = \mathfrak{p} \neq (0)$, so $\mathfrak{p}$ is finite. Let $\mathfrak{a}$ be an ideal prime to $\mathfrak{p}$. Define the $\mathbf{A}$-module of $\mathfrak{a}$-torsion points to be

$$\varphi[\mathfrak{a}] = \bigcap_{a \in \mathfrak{a}, a \neq 0} \varphi[a].$$

By Remark 4.2.13, $\varphi[\mathfrak{a}]$ is isomorphic to the $\mathbf{A}$-module $(\mathbf{A}/\mathfrak{a})^2$.

Throughout this subsection, let $\mathfrak{l} \subset \mathbf{A}$ be a nonzero prime ideal distinct from the $\mathbf{A}$-characteristic $\mathfrak{p}$ of $\mathbb{L}$. Let S be a complete set of representatives for $\mathbf{A}/\mathfrak{l}$, i.e. $S = \{a \in \mathbf{A} \mid$

$\deg_T(a) < \deg(\mathfrak{l})\}$. We denote the $\mathfrak{l}$-adic completions of $\mathbf{K}$ and $\mathbf{A}$ by $\mathbf{K}_\mathfrak{l}$ and $\mathbf{A}_\mathfrak{l}$, respectively. Then

$$\mathbf{K}_\mathfrak{l} = \left\{ \pi_\mathfrak{l}^m \sum_{i=0}^{\infty} s_i \pi_\mathfrak{l}^i \mid m \in \mathbb{Z}, s_i \in S \right\} \quad \text{and} \quad \mathbf{A}_\mathfrak{l} = \left\{ \sum_{i=0}^{\infty} s_i \pi_\mathfrak{l}^i \mid s_i \in S \right\},$$

where $\pi_\mathfrak{l}$ is a uniformizing parameter at $\mathfrak{l}$. Define

$$\varphi[\mathfrak{l}^\infty] := \varinjlim_n \varphi[\mathfrak{l}^n].$$

Then

$$\varphi[\mathfrak{l}^\infty] \cong \left(\varinjlim_n \mathbf{A}/\mathfrak{l}^n \right)^2 \cong \left(\varinjlim_n \mathfrak{l}^{-n}\mathbf{A}/\mathbf{A} \right)^2 \cong \left(\mathbf{K}_\mathfrak{l}/\mathbf{A}_\mathfrak{l}\right)^2.$$

We have the following definition (see [Gek91] or [Hay92]).

Definition 6.2.5. The $\mathfrak{l}$-*adic Tate module* of φ is given by

$$T_\mathfrak{l}(\varphi) = \mathrm{Hom}_{\mathbf{A}_\mathfrak{l}}(\mathbf{K}_\mathfrak{l}/\mathbf{A}_\mathfrak{l}, \varphi[\mathfrak{l}^\infty]).$$

Note that

$$T_\mathfrak{l}(\varphi) \cong \varprojlim_n \varphi[\mathfrak{l}^n], \tag{6.5}$$

where the inverse limit is taken with respect to the multiplication by $\pi_\mathfrak{l}$ maps

$$\varphi[\mathfrak{l}^{n+1}] \xrightarrow{\pi_\mathfrak{l}} \varphi[\mathfrak{l}^n].$$

Here $\pi_\mathfrak{l} = \varphi_\ell$, where $\ell \in \mathbf{A}^+$ is the generator of $\mathfrak{l}$.

By (6.5), we can consider $T_\mathfrak{l}(\varphi)$ as the set of infinite tuples $(a_1, a_2, a_3, \ldots)$, where $a_n \in \varphi[\mathfrak{l}^n]$ and $\pi_\mathfrak{l} a_{n+1} = a_n$. Addition is defined componentwise. To define multiplication of a vector by an $\mathfrak{l}$-adic polynomial, we define it componentwise. On the ith component, we reduce the $\mathfrak{l}$-adic polynomial modulo $\mathfrak{l}^i$ and multiply the ith component by this residue. This multiplication is well defined, and provides an action of $\mathbf{A}_\mathfrak{l}$ on $T_\mathfrak{l}(\varphi)$.

Moreover, each $\varphi[\mathfrak{l}^n]$ is an $(\mathbf{A}/\mathfrak{l}^n)$-module, so $T_\mathfrak{l}(\varphi)$ has a natural structure as an $\mathbf{A}_\mathfrak{l}$-module. It is a free $\mathbf{A}_\mathfrak{l}$-module of rank two. From (6.5), we get

$$T_\mathfrak{l}(\varphi) \cong \varprojlim_n (\mathbf{A}/\mathfrak{l}^n)^2 = \mathbf{A}_\mathfrak{l} \times \mathbf{A}_\mathfrak{l}. \tag{6.6}$$

Now if we consider the P-torsion points, we see that either $T_{\mathfrak{p}}(\varphi) \cong \{0\}$ or $T_{\mathfrak{p}}(\varphi) \cong \mathbf{A}_{\mathfrak{p}}$. Similar to the elliptic curve case, we have the following natural homomorphisms

(a) $\delta_{\mathfrak{l}} : \mathrm{Gal}(\overline{\mathbb{L}}/\mathbb{L}) \longrightarrow \mathrm{Aut}(T_{\mathfrak{l}}(\varphi)) \cong \mathrm{GL}_2(\mathbf{A}_{\mathfrak{l}})$ and

(b) $\iota_{\mathfrak{l}} : \mathrm{End}_{\mathbb{L}}(\varphi) \otimes_{\mathbf{A}} \mathbf{A}_{\mathfrak{l}} \longrightarrow \mathrm{End}_{\mathbf{A}_{\mathfrak{l}}}(T_{\mathfrak{l}}(\varphi))$.

We give an additional description of the map $\iota_{\mathfrak{l}}$. Let u be a morphism of rank two Drinfeld modules φ and ψ. Then u induces the following homomorphisms

$$u_{\mathfrak{l}} : T_{\mathfrak{l}}(\varphi) \longrightarrow T_{\mathfrak{l}}(\psi) \quad \text{and} \quad u_{\mathfrak{p}} : T_{\mathfrak{p}}(\varphi) \longrightarrow T_{\mathfrak{p}}(\psi),$$

where $u_{\mathfrak{l}}$ sends a vector $(a_1, a_2, \ldots)$ to the vector $(u_{\mathfrak{l}}a_1, u_{\mathfrak{l}}a_2, \ldots)$, and $u_{\mathfrak{p}}$ acts similarly. The following result is the analogue of [Lan87, Theorem 2, Ch. 13 §1].

Theorem 6.2.6. *If $u_1, u_2, \ldots, u_r \in \mathrm{End}_{\mathbb{L}}(\varphi)$ are linearly independent over $\mathbf{A}$, then they are also linearly independent over $\mathbf{A}_{\mathfrak{l}}$ when considered as endomorphisms of $T_{\mathfrak{l}}(\varphi)$.*

Proof. Suppose

$$\lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_r u_r = 0,$$

where $\lambda_i \in \mathbf{A}_{\mathfrak{l}}$. It suffices to show that $\pi_{\mathfrak{l}}$ divides each λ_i. Let

$$\lambda_i = m_i + \pi_{\mathfrak{l}} d_i,$$

with $d_i \in \mathbf{A}_{\mathfrak{l}}$ and $m_i \in \mathbf{A}$. Then we need to show that $\pi_{\mathfrak{l}}$ divides m_i for all i. Since $\mathrm{End}_{\mathbb{L}}(\varphi)$ is closed under addition, we see that the morphism

$$u = \sum_{i=1}^{r} m_i u_i = \sum_{i=1}^{r} (-\pi_{\mathfrak{l}} d_i + \lambda_i) u_i = \sum_{i=1}^{r} -\pi_{\mathfrak{l}} d_i u_i + \sum_{i=1}^{r} \lambda_i u_i = -\pi_{\mathfrak{l}} \sum_{i=1}^{r} d_i u_i$$

is an element of $\mathrm{End}_{\mathbb{L}}(\varphi)$. Since u acts on φ, we see that it annihilates $\varphi[\mathfrak{l}]$. Hence u is of the form $u = \pi_{\mathfrak{l}} v$ for some $v \in \mathrm{End}_{\mathbb{L}}(\varphi)$. But note, however, that the u_i generate a space

$$V = \mathbf{K}u_1 + \mathbf{K}u_2 + \cdots + \mathbf{K}u_r$$

over $\mathbf{K}$. Moreover, $V \cap \mathrm{End}_{\mathbb{L}}(\varphi)$ is a lattice of rank r in this subspace. Thus, without loss of generality, it suffices to show that a basis of this lattice is linearly independent over $\mathbf{A}_{\mathfrak{l}}$. In other words, we can assume that the u_i themselves form a basis for this lattice. But then this implies that $v \in \mathbf{A}u_1 + \mathbf{A}u_2 + \cdots + \mathbf{A}u_r$. Thus $\pi_{\mathfrak{l}}$ divides m_i for all i. This completes the proof. □

Corollary 6.2.7. *The map*

$$\begin{aligned} \iota_{\mathfrak{l}} : \mathrm{End}(\varphi) \otimes_{\mathbf{A}} \mathbf{A}_{\mathfrak{l}} &\longrightarrow \mathrm{End}_{\mathbf{A}_{\mathfrak{l}}}(T_{\mathfrak{l}}(\varphi)) \\ u &\longmapsto u_{\mathfrak{l}} \end{aligned}$$

is injective.

The next result is an important analogy between rank two Drinfeld modules and elliptic curves. We adapt the proof for the elliptic curve case in [Sil09], p. 91.

Theorem 6.2.8. $\mathrm{End}_{\mathbb{L}}(\varphi)$ *is a free* $\mathbf{A}$*-module of rank at most 4.*

Proof. As pointed out earlier, $\mathrm{End}_{\mathbb{L}}(\varphi)$ is an $\mathbf{A}$-module via φ and is torsion-free. We now have

$$\mathrm{rank}_{\mathbf{A}}(\mathrm{End}_{\mathbb{L}}(\varphi)) = \mathrm{rank}_{\mathbf{A}_{\mathfrak{l}}}(\mathrm{End}_{\mathbb{L}}(\varphi) \otimes_{\mathbf{A}} \mathbf{A}_{\mathfrak{l}})$$

since tensoring does not change the rank.

Next, observe that by choosing an $\mathbf{A}_{\mathfrak{l}}$-basis for $T_{\mathfrak{l}}(\varphi)$ we get $\mathrm{End}_{\mathbf{A}_{\mathfrak{l}}}(T_{\mathfrak{l}}(\varphi)) \cong M_2(\mathbf{A}_{\mathfrak{l}})$ from (6.6), where $M_2(\mathbf{A}_{\mathfrak{l}})$ is the additive group of 2×2 matrices with entries from $\mathbf{A}_{\mathfrak{l}}$. The rank of $M_2(\mathbf{A}_{\mathfrak{l}})$ over $\mathbf{A}_{\mathfrak{l}}$ is 4. By Corollary 6.2.7, we see that

$$\mathrm{rank}_{\mathbf{A}_{\mathfrak{l}}}(\mathrm{End}_{\mathbb{L}}(\varphi) \otimes_{\mathbf{A}} \mathbf{A}_{\mathfrak{l}}) \leq \mathrm{rank}_{\mathbf{A}_{\mathfrak{l}}}(\mathrm{End}_{\mathbf{A}_{\mathfrak{l}}}(T_{\mathfrak{l}}(\varphi))) = 4.$$

The desired result follows. □

Note that $\mathrm{End}_{\mathbb{L}}(\varphi)$ is a discrete submodule of the vector space $\mathcal{D} := \mathrm{End}_{\mathbb{L}}(\varphi) \otimes_{\mathbf{A}} \mathbf{K}$. We have the following result in the rank two case of Drinfeld modules.

Proposition 6.2.9. *$\mathcal{D}$ is a division algebra of dimension at most 4 over $\mathbf{K}$.*

Proof. Note that for every endomorphism $u \in \mathrm{End}_{\mathbb{L}}(\varphi)$, there exists a dual endomorphism $\widehat{u}$ satisfying $\widehat{u} \cdot u = \varphi_a$ for some $a \in \mathbf{A}$. So if $\mathrm{End}_{\mathbb{L}}(\varphi)$ is tensored with $\mathbf{K}$, every nonzero endomorphism becomes invertible. Hence $\mathcal{D}$ is a division algebra. The bound on the dimension of $\mathcal{D}$ over $\mathbf{K}$ is a consequence of Theorem 6.2.8. □

Remark 6.2.10. As $\mathrm{End}_{\mathbb{L}}(\varphi)$ is torsion-free, we have the following embeddings

$$\mathrm{End}_{\mathbb{L}}(\varphi) \hookrightarrow \mathcal{D} \hookrightarrow \mathrm{End}_{\mathbb{L}}(\varphi) \otimes_{\mathbf{A}} \mathbf{K}_{\infty}.$$

6.3 The Characteristic Polynomial of Frobenius

Let $\varphi = (g, \Delta)$ be a Drinfeld module of rank $r = 2$ over an $\mathbf{A}$-field $\mathbb{L}$ where $\mathbb{L}$ is an extension of $\mathbb{F}_{\mathfrak{p}}$ of degree m as given in (6.4) with Frobenius endomorphism $F = \tau^n$ acting on $T_{\mathfrak{l}}(\varphi)$ for some prime $\mathfrak{l} \neq \mathfrak{p} = \mathrm{char}_{\mathbf{A}}(\mathbb{L})$. F is integral over $\mathbf{A}$, hence it satisfies a polynomial equation over $\mathbf{A}$. Therefore it has a uniquely determined minimal polynomial $M_{\varphi}(X) \in \mathbf{A}[X]$. It has a 2×2 matrix representation via an $\mathfrak{l}$-adic basis of $T_{\mathfrak{l}}(\varphi)$. So its *characteristic polynomial* is given by

$$P_{\varphi}(X) := X^2 - aX + b.$$

We describe the coefficients $a = a(\varphi)$ and $b = b(\varphi)$ of P_{φ} in this section using the method given in [Gek83], [Gek91], and [Gek08]. The coefficients a and b of $P_{\varphi}(X)$ are called the *Frobenius trace* and *norm*, respectively.

Now consider $\mathcal{D}$. Let $\mathbb{L}(\tau)$ be the division ring of fractions of $\mathbb{L}\{\tau\}$. Consider $\varphi : \mathbf{A} \longrightarrow \mathbb{L}\{\tau\}$ as an embedding so that the quotient field $\mathbf{K}$ of $\mathbf{A}$ is contained in $\mathbb{L}(\tau)$. So we have the embeddings

$$\mathbf{K} \hookrightarrow \mathcal{D} \hookrightarrow \mathbb{L}(\tau).$$

Next, define E to be the subfield of $\mathcal{D}$ generated by F over $\mathbf{K}$, i.e., $E := \mathbf{K}(F)$. Recall that F commutes with φ, so E is commutative even though $\mathbf{K}\{\tau\} \subset \mathbb{L}(\tau)$ is not commutative

in general. Also let $E_\infty = \mathbf{K}_\infty(F)$. Recall that $\deg_T(P) = d$ and $\mathrm{char}_{\mathbf{A}}(\mathbb{L}) = \mathfrak{p} = (P)$. Then φ_P modulo P is of the form

$$\varphi_P = h_d\tau^d + h_{d+1}\tau^{d+1} + \cdots + h_{2d}\tau^{2d}, \quad h_i \in \mathbb{L}. \tag{6.7}$$

(see [Gek83]), p. 178). So τ divides φ_P, and this implies that F divides φ_P^s for $s \gg 0$. Thus F lies above P in the extension $E/\mathbf{K}$. Let $\mathfrak{P}$ be a prime of E that divides F (so $\mathfrak{P}$ also lies above P). Note that $\mathfrak{P}$ is unique since E embeds into $\mathbb{L}(\tau)$. This follows from [Rei03, Theorem 32.15] (see also [Gos98, Theorem 4.11.33]). Under the same reasoning, there is also only one place of E above ∞.

What we have discussed, so far, is contained in the following general result stated in [Dri74] and completely proved in [Gek91] (see [GS97] also).

Theorem 6.3.1. *Let φ be a Drinfeld module of rank r over $\mathbb{L}$. Let E be the subfield of $\mathcal{D}$ obtained by adjoining F to $\mathbf{K}$ with $r_1 = [E : \mathbf{K}]$. Then the following results hold.*

1. *r/r_1 is an integer s.*
2. *$\mathcal{D}$ is a central division ring over E of degree s^2.*
3. *There exists a unique prime $\mathfrak{P}$ of E that divides F, and this prime lies above P.*
4. *There exists a unique prime ∞_E in E that lies above the place ∞ of $\mathbf{K}$.*
5. *$\mathcal{D}$ splits at primes distinct from $\mathfrak{P}$ and ∞ and has invariants $1/s$ and $-1/s$ at $\mathfrak{P}$ and ∞, respectively.*

The next three results are true for any rank $r \geq 1$. We only consider the rank two case.

Lemma 6.3.2 ([Gek91], Lemma 3.3 and Corollary 3.4)**.** *Let F be the Frobenius endomorphism of φ having $M_\varphi(X)$ as its minimal polynomial over $\mathbf{K}$ as a field element. Let $P_\varphi(X)$ be its characteristic polynomial as an endomorphism of $T_\mathfrak{l}(\varphi)$. Then $P_\varphi(X) = M_\varphi(X)^s$ with $s = 2/[E : \mathbf{K}]$, and consequently, $P_\varphi(X)$ has coefficients in $\mathbf{A}$ independent of $\mathfrak{l}$.*

It is now possible to classify isogeny classes of Drinfeld modules over $\mathbb{L}$.

Theorem 6.3.3 ([Gek91], Theorem 3.5)**.** *Let φ and ψ be Drinfeld modules of rank two over $\mathbb{L}$. Then the following are equivalent:*

(a) φ and ψ are $\mathbb{L}$-isogenous;

(b) $\mathcal{D}$ and $\mathrm{End}_{\mathbb{L}}(\psi) \otimes \mathbf{K}$ are F-isomorphic $\mathbf{K}$-algebras;

(c) $M_\varphi = M_\psi$; and

(d) $P_\varphi = P_\psi$.

The next result gives a description of the coefficients a and b of $P_\varphi(X)$. We continue to assume that $\mathbb{L}$ is an $\mathbf{A}$-field such that $[\mathbb{L} : \mathbb{F}_\mathfrak{p}] = m$, $[\mathbb{F}_\mathfrak{p} : \mathbb{F}_q] = d$, $\#\mathbb{L} = q^n$, and $n = md$.

Theorem 6.3.4 ([Gek91], Theorem 5.1)**.** *With the notations as above, the following are obtained:*

(i) $(b) = (P_\varphi(0)) = \mathfrak{p}^m$. Hence $\mathfrak{p}^m$ is a principal ideal and $b = \varepsilon P^m$ with $\varepsilon = \mathrm{sgn}(b) \in \mathbb{F}_q^*$.

(ii) Let ω_i be the roots of $P_\varphi(X)$ for $i = 1, 2$. Then $|\omega_i| = q^{n/2}$ in an extension of $\mathbf{K}_\infty$, and hence $|a| \leq q^{n/2}$.

The fact that $|\omega_i| = q^{n/2}$, i.e., $\deg(\omega_i) = n/2$ for $i = 1, 2$ in this theorem corresponds to the Riemann hypothesis and the bound on $\deg(a)$ corresponds to the Hasse bound for elliptic curves defined over finite fields. Moreover, part(i) of this theorem gives a restriction on which finite field extensions have Drinfeld modules over them. The next result is also true for arbitrary rank r.

As indicated in Theorem 6.3.4(i), the constant term of the characteristic polynomial $P_\varphi(X)$ is $b = \varepsilon P^m$. An explicit formula for ε is given in the following result.

Theorem 6.3.5 ([Gek08], Theorem 2.11)**.** *Let $\varphi = (g, \Delta)$ be a rank two Drinfeld module defined over $\mathbb{L}$. Then the constant term b of the characteristic polynomial $P_\varphi(X)$ of the*

Frobenius $F = \tau^n$ is $b = \varepsilon P^m$, where

$$\varepsilon = (-1)^n N_{\mathbb{F}_q}^{\mathbb{L}}(\Delta)^{-1}. \tag{6.8}$$

We mention that a general approach for finding the constant term of the characteristic polynomial of Frobenius for arbitrary rank r Drinfeld modules is fully discussed in [HY00].

Remark 6.3.6. If $\mathbb{L} = \mathbb{F}_{\mathfrak{p}}$, i.e., $m = 1$, in the previous theorem, then $N_{\mathbb{F}_q}^{\mathbb{L}}(\alpha)$ is the residue symbol $\left(\frac{\alpha}{P}\right)_{q-1}$ for $\alpha \in \mathbb{L}$. In this case, (6.8) becomes

$$\varepsilon = (-1)^d \left(\frac{\Delta}{P}\right)_{q-1}^{-1}. \tag{6.9}$$

Now we determine a formula for the trace of Frobenius modulo P. As before, let $\deg_T(P) = d$. Define the *Hasse invariant* of φ to be the coefficient $H(\varphi) := h_d$ in (6.7).

Lemma 6.3.7 ([Gek83], Lemma 5.2)**.** *Let $P_\varphi(X) = X^2 - aX + b$ be the characteristic polynomial of F and $\varepsilon = \operatorname{sgn}(b)$. Then*

$$\varepsilon\, N_{\mathbb{F}_{\mathfrak{p}}}^{\mathbb{L}}(H(\varphi)) \equiv a \pmod{P}. \tag{6.10}$$

Proof. Let $\varphi_a = \sum a_i \tau^i$ and $\varphi_b = \sum b_i \tau^i$. So $a_0 \equiv a \pmod{P}$. Because $P_\varphi(F) = 0$ over $\mathbb{L}$, we get

$$F^2 - \varphi_a F + \varphi_b = 0 \tag{6.11}$$

in $\mathbb{L}\{\tau\}$. It follows that $a_0 = b_{dm}$.

Note that $b = \varepsilon P^m$ from Theorem 6.3.4, so we have

$$\varphi_b = \varepsilon\, (\varphi_P)^m = \varepsilon\, (H\tau^d + \cdots)^m = \varepsilon\, H^{1+q^d+\cdots+q^{(m-1)d}} \tau^{md} + \cdots = \varepsilon\, N_{\mathbb{F}_{\mathfrak{p}}}^{\mathbb{L}}(H)\tau^{dm} + \cdots,$$

where we used H is place of $H(\varphi)$ for ease of notation. □

We see from Lemma 6.3.7 that $H(\varphi)$ satisfies

$$\gamma(a) = \varepsilon\, N_{\mathbb{F}_{\mathfrak{p}}}^{\mathbb{L}}(H(\varphi)).$$

As a consequence, the Frobenius trace $a(\varphi)$ is fully determined via $H(\varphi)$ if $\mathbb{L} = \mathbb{F}_{\mathfrak{p}}$ because in this case $\deg(a) \leq n/2 = d/2$ and a is determined by its residue class $\gamma(a)$ modulo P. Now, let $g_k(\varphi)$ be the normalized Eisenstein series of weight $q^k - 1$ on φ given in (5.36). Then $H(\varphi)$ satisfies the "*Deligne congruence*"

$$H(\varphi) \equiv g_d(\varphi) \pmod{P}$$

This gives rise to the following result.

Proposition 6.3.8 ([Gek08], Proposition 3.7)**.** *Let $\varphi = (g, \Delta)$ be a Drinfeld module over $\mathbb{F}_{\mathfrak{p}}$ and consider $[k]$ as an element of $\mathbb{F}_{\mathfrak{p}}$. Then the Hasse invariant $H(\varphi)$ is equal to $g_d(\varphi)$, with $d = [\mathbb{F}_{\mathfrak{p}} : \mathbb{F}_q]$, via the recursion formula* (5.37)*.*

This gives a simple way of computing the Frobenius trace $a(\varphi) \in \mathbf{A}$ of a Drinfeld module φ over $\mathbb{F}_{\mathfrak{p}}$. As we will only deal with $\mathbb{L} = \mathbb{F}_{\mathfrak{p}}$ in the latter part of this work, we will employ this method to find $a(\varphi)$, i.e., we use

$$a \equiv \varepsilon \cdot g_d(\varphi) \pmod{P}. \tag{6.12}$$

We refer the reader to [Gek08, Section 3] for the computation of $a(\varphi)$ when $\mathbb{L}$ is a finite extension of $\mathbb{F}_{\mathfrak{p}}$ of degree $m > 1$.

Theorem 6.3.9. *Let $\varphi = (g, \Delta)$ be a rank two Drinfeld module defined over a finite $\mathbf{A}$-field $\mathbb{L} = \mathbb{F}_{\mathfrak{p}}$, where $\deg_T(P) = d$. Then the characteristic polynomial of the Frobenius endomorphism $F = \tau^d$ is*

$$P_\varphi(X) = X^2 - (-1)^d \left(\frac{\Delta}{P}\right)_{q-1}^{-1} g_d(\varphi) X + (-1)^d \left(\frac{\Delta}{P}\right)_{q-1}^{-1} P.$$

Proof. This follows from Theorem 6.3.5, Remark 6.3.6 and Proposition 6.3.8. □

Remark 6.3.10. The formula for $P_\varphi(X)$ in the previous theorem was already stated, without proof, in [HY00]. It is also interesting to note that the preceding theorem clearly draws the difference between the characteristic polynomials of the Frobenius in the Drinfeld module

case and in the elliptic curve case. Here the sign of the constant term of $P_\varphi(X)$ can vary, which is not the case for elliptic curves. Moreover, the norm and trace of Frobenius have signs that depend on the leading coefficient Δ of φ.

Example 6.3.11. Let $\varphi = (g, \Delta)$ be a Drinfeld module over $\mathbb{L} = \mathbb{F}_\mathfrak{p}$. We give several examples of characteristic polynomials of the Frobenius endomorphism using Theorem 6.3.9 given $q = 3$ and a prime $P \in \mathbf{A}$.

(a) $P = T^2 + 2T + 2$

$$P_\varphi(X) = \begin{cases} X^2 - 2TX + 2P, & \text{for } \varphi = (1, T) \\ X^2 - X + P, & \text{for } \varphi = (0, T+1) \\ X^2 + P, & \text{for } \varphi = (T, T+1) \end{cases}$$

(b) $P = T^3 + 2T + 1$

$$P_\varphi(X) = \begin{cases} X^2 + 2TX - P, & \text{for } \varphi = (1, T^2) \\ X^2 + 2(2T+2)X - 2P, & \text{for } \varphi = (T, T) \\ X^2 - 2P, & \text{for } \varphi = (0, T+1) \end{cases}$$

Remark 6.3.12. $H(\varphi) \equiv 0 \pmod{P}$ implies that φ_P is purely inseparable, i.e., φ has no nontrivial P-torsion points over extensions of $\mathbb{L}$.

We can now define a classification of Drinfeld modules

Definition 6.3.13. Let $\mathrm{char}_\mathbf{A}(\mathbb{L}) = \mathfrak{p} \neq (0)$ and φ a rank two Drinfeld module over $\mathbb{L}$. We say that φ is *supersingular* if and only if $\varphi[P]$ is trivial. If this is not the case, then we say that φ is *ordinary*.

We end this section by recalling the following type of elements in a fixed algebraic closure $\overline{\mathbf{K}}$ of $\mathbf{K}$. Let π be an element of $\overline{\mathbf{K}}$ and, as before, let $E = \mathbf{K}(\pi)$. Here, π is called a *Weil number* of rank r over the $\mathbf{A}$-field $\mathbb{L}$ if it satisfies the following properties (see [Yu95b]):

1. π is integral over $\mathbf{A}$.

2. There is a unique place of E which is a zero of π, and this place lies above P.

3. There is a unique place of E lying above ∞.

4. Let $|\ |_\infty$ be the unique extension to E of the normalized absolute value $|\ |$ of $\mathbf{K}$ associated to ∞. Then $|\pi|_\infty = q^{1/r}$.

5. $[E : \mathbf{K}]$ divides r.

Note that the Frobenius endomorphism $F = \tau^n$ over $\mathbb{L}$, when considered as a field element of an extension of $\mathbf{K}$ in $\overline{\mathbf{K}}$, satisfies these conditions. So it is an example of a Weil number for $\mathbb{L}$ of rank r, see [GS97], p. 77. The next result is stated in [Dri74].

Theorem 6.3.14. *The map between the set of $\mathbb{L}$-isogeny classes of Drinfeld modules of rank r over $\mathbb{L}$ and the set of conjugacy classes of Weil numbers of rank r for $\mathbb{L}$ is a bijection.*

Proof. See [Yu95b, Theorem 3]. □

By this theorem, we call a Weil number π supersingular if the corresponding isogeny class of Drinfeld modules is supersingular. The injection in this theorem sends the isogeny class of a Drinfeld module φ to the roots of the minimal polynomial $M_\varphi(X)$ of its Frobenius.

Remark 6.3.15.

(1) If π is a Weil number of rank two, then $N_{\mathbf{K}}^E(\pi)$ generates the ideal $\mathfrak{p}^{m[E:\mathbf{K}]/2}$. In particular, if there is a rank two Drinfeld module over $\mathbb{L}$, then $\mathfrak{p}^m$ is principal.

(2) The minimal polynomial of a Weil number π of rank two over $\mathbf{K}$, when π is considered as an element of a field extension of $\mathbf{K}$ in its algebraic closure $\overline{\mathbf{K}}$, takes one of the forms below (see [GS97] pp. 85 - 86, or [Yu95b, Proposition 4]). Note that cases (b) and (c) do not occur in the number field case.

   (a) $X^2 - aX + \varepsilon P^m$ with $\gcd(a, P) = 1$ for $a \in \mathbf{A}$,

   (b) $X^2 + \varepsilon P^m$ if m is odd,

(c) $X^2 + \varepsilon_0 P^{m/2} X + \varepsilon P^m$ if m is even and d is odd, and

(d) $X + \varepsilon P^{m/2}$ if m is even.

Here $\varepsilon \in \mathbb{F}_q^*$ and $\varepsilon_0 \in \mathbb{F}_q$, and the coefficients are such that $M_\varphi(X)$ remains irreducible over $\mathbf{K}_\infty$. So for cases (a) to (c), we have the following additional conditions, respectively.

(a) $2\deg(a) < dm$ or $2\deg(a) = dm$ and $X^2 - a_0 X + \varepsilon$ is irreducible over $\mathbb{F}_q$ with $a_0 = \operatorname{sgn}(a)$,

(b) d is odd or $-\varepsilon$ is not a square in $\mathbb{F}_q^*$, and

(c) $X^2 + \varepsilon_0 X + \varepsilon$ is irreducible over $\mathbb{F}_q$.

(3) Note that the Hasse invariant in cases (b) - (d) are all $0 \pmod P$. It is clear from Definition 6.3.13 that we have an ordinary Drinfeld module in case (a) and supersingular ones in cases (b) to (d). Moreover, in these four cases, we can also characterize the primes P and ∞ in the extension $\mathbf{K}(\pi)$ of $\mathbf{K}$ in $\overline{\mathbf{K}}$ as given in Table 6.1.

Case	P	∞
(a)	split	inert
(b)	ramified	ramified or inert
(c)	ramified	inert
(d)	ramified	ramified

Table 6.1: Behaviour of the primes P and ∞ under the possible forms of $M_\varphi(X)$

Remark 6.3.16. Let φ and ψ be isogenous rank two Drinfeld modules over $\mathbb{L}$. Observe that φ is supersingular if and only if ψ is supersingular. To see this, first note that if φ is supersingular, then its minimal polynomial must be of one of the forms (b) - (d) given in Remark 6.3.15(2), in which case the Hasse invariant is $0 \pmod P$. Now, as φ and ψ are isogenous, they have the same minimal polynomial by Theorem 6.3.3. So $H(\psi) \equiv 0 \pmod P$ also. It follows from Remark 6.3.12 that $\psi[P]$ is trivial, so ψ is supersingular. The converse is proved similarly.

6.4 Classification of the Endomorphism Ring

In this section, we assume that φ is a rank two Drinfeld module over a finite $\mathbf{A}$-field $\mathbb{L}/\mathbb{F}_{\mathfrak{p}}$, unless otherwise stated. So far, by Theorem 6.2.8, we know that $\mathrm{End}_{\mathbb{L}}(\varphi)$ is a free $\mathbf{A}$-module of rank at most 4. Moreover, it has an anti-involution $u \longmapsto \widehat{u}$. It is also clear that $\widehat{u} \cdot u$ or $u \cdot \widehat{u}$ is 0 if and only if u is the zero morphism.

As before, let $\mathcal{D} = \mathrm{End}_{\mathbb{L}}(\varphi) \otimes_{\mathbf{A}} \mathbf{K}$ and $F = \tau^n$. Our goal in this section is to classify the type of the endomorphism ring $\mathrm{End}_{\mathbb{L}}(\varphi)$ of φ. In view of Theorem 6.3.3, we see that the behaviour of $\mathrm{End}_{\mathbb{L}}(\varphi)$ depends on the isogeny class of φ. Furthermore, from Lemma 6.3.2, we know that the characteristic polynomial $P_{\varphi}(X)$ of the Frobenius endomorphism F is a power of its minimal polynomial $M_{\varphi}(X)$. Thus, we will be guided by the possible forms of $M_{\varphi}(X)$ given in Remark 6.3.15 and the fact that $1 \leq \dim_{\mathbf{K}}(\mathcal{D}) \leq 4$. It is clear that if $\dim_{\mathbf{K}}(\mathcal{D}) = 1$, then $\mathcal{D} = \mathbf{K}$ and $\mathrm{End}_{\mathbb{L}}(\varphi) = \mathbf{A}$. The other two cases for the dimension of $\mathcal{D}$ need a little bit of work. We follow Deuring's method for elliptic curves (see, for instance, [Lan87, Section 13.2]) and Gekeler's (see [Gek91, GS97]) and Yu's (see [Yu95b]) methods for classifying endomorphism rings of Drinfeld modules of rank two.

It is interesting to note that in the elliptic curve case, we only have one type of supersingularity, and in this case the endomorphism ring of a supersingular elliptic curve is always a maximal order in a quaternion algebra. As for the Drinfeld module case, we consider several types of supersingularity (see Remark 6.3.15(2)) based on the characteristic polynomial of the Frobenius associated to φ. Moreover, if φ is supersingular, then $\mathrm{End}_{\mathbb{L}}(\varphi)$ may or may not be a maximal order in a quaternion algebra (see, for instance, [Yu95b, Proposition 5]). The following result gives equivalent conditions for supersingularity of a rank two Drinfeld module φ over $\mathbb{L}$.

Theorem 6.4.1. *Let φ be a Drinfeld module of rank two over $\mathbb{L}$ with Frobenius endomorphism F. The following conditions are equivalent:*

(a) $\varphi[P]$ is trivial.

(b) $H(\varphi) = 0$.

(c) φ_P *is inseparable.*

(d) The height and rank of φ *are equal.*

Proof. See, for example, [Jun00, Proposition 3.3.2] □

If the conditions in this theorem hold, then $\mathcal{D} \neq \mathbf{K}$, i.e., $[\mathcal{D} : \mathbf{K}] \neq 1$. In this case, we have two cases: (1) $[\mathcal{D} : \mathbf{K}] = 2$, so $\mathrm{End}_{\mathbb{L}}(\varphi)$ is an order in an imaginary quadratic field, or (2) $[\mathcal{D} : \mathbf{K}] = 4$, so $\mathrm{End}_{\mathbb{L}}(\varphi)$ is a maximal order in a quaternion algebra over $\mathbf{K}$ ramified at P and ∞. See [Yu95b, Propositions 4 and 5]. Case (1) corresponds to cases (b) and (c) in Remark 6.3.15(2), and these conditions do not have counterparts in the elliptic curve case.

Case (a) of Remark 6.3.15(2) remains to be considered. This is the ordinary case and is the main focus of this thesis. We give results in the next theorem which are very similar to those for ordinary elliptic curves over finite fields given in [Lan87, Theorem 5, Ch. 13 §2].

Theorem 6.4.2. *Let* $\mathfrak{p} \neq (0)$ *be the* $\mathbf{A}$*-characteristic of a finite field* $\mathbb{L}$ *and let* φ *be an ordinary Drinfeld module of rank two over* $\mathbb{L}$*. Suppose* $T_{\mathfrak{p}}(\varphi) \neq 0$*. Then the following statements hold.*

(i) The Frobenius endomorphism F *is a nontrivial endomorphism of* φ*.*

(ii) The $\mathbf{A}$*-module* $\varphi[P]$ *is isomorphic to* $\mathbf{A}/\mathfrak{p}$*. Thus* $T_{\mathfrak{p}}(\varphi) \cong \mathbf{A}_{\mathfrak{p}}$*.*

(iii) $\mathcal{D}$ *is an imaginary quadratic function field, and* $\mathrm{End}_{\mathbb{L}}(\varphi)$ *is an order* $\mathcal{O}$ *in* $\mathcal{D}$*.*

(iv) The prime P *splits completely in* $\mathcal{D}$*.*

(v) The prime P *does not divide the conductor* f *of* $\mathcal{O}$*.*

Proof. Suppose F is a trivial endomorphism of φ, i.e., $F \in \mathbf{A}$. Then every power F^e of F lies in $\mathbf{A}$. Let $e = 1$. Then φ_F is purely inseparable, whose divisor (F) must be a power of $\mathfrak{p}$. Thus φ is supersingular, and we have a contradiction. Now (i) follows.

By Theorem 4.2.12, $\varphi[P] \cong (\mathbf{A}/\mathfrak{p})^{r-h}$, where $r = 2$ and the height h of φ needs to be determined in this case. Since φ is ordinary, the Frobenius trace is not divisible by P. So by Lemma 6.3.7, the Hasse invariant $H(\varphi)$ is nonzero modulo P. From equation (6.7), we see that $H(\varphi) = h_d$ and $d = \deg(P)$ is the least nonnegative integer for which the coefficient of τ^d in φ_P is nonzero. Using Proposition 4.2.10 yields

$$\omega(P) = d = h\nu_P(P)d.$$

As $\nu_P(P) = 1$, we obtain $h = 1$. So (ii) is now proved.

The representation of $\mathrm{End}_{\mathbb{L}}(\varphi)$ on $T_{\mathfrak{p}}(\varphi)$ is faithful, i.e., it is injective. So this gives an embedding of $\mathrm{End}(\varphi)$ into $\mathbf{A}_{\mathfrak{p}}$, which implies that $\mathrm{End}_{\mathbb{L}}(\varphi) = \mathcal{O}$ is commutative. Consequently, $\mathrm{End}_{\mathbb{L}}(\varphi)$ is of rank two over $\mathbf{A}$. It follows that $\mathcal{D}$ is a quadratic function field. It is imaginary based on the restrictions given in Remark 6.3.15(2)(a). This gives (iii).

By Remark 6.3.15(2)(a), we see that $\mathcal{D}$ has discriminant $D_{\mathcal{D}} = a^2 - 4\varepsilon P^m$ with $\gcd(a, P) = 1$. By using the quadratic residue symbol for function fields, we get

$$\left(\frac{D_{\mathcal{D}}}{P}\right) = \left(\frac{a^2}{P}\right) = 1.$$

So P splits in $\mathcal{D}$, which shows (iv).

Finally, let f be the conductor of $\mathcal{O}$. As an $\mathbf{A}$-order, $\mathcal{O}$ can be written as $\mathcal{O} = \mathbf{A} + f\mathcal{O}_{\mathcal{D}}$, where $\mathcal{O}_{\mathcal{D}}$ is the maximal order in $\mathcal{D}$. Hence we can write the Frobenius and its conjugate as

$$F = g + f\alpha \quad \text{and} \quad \overline{F} = g + f\overline{\alpha},$$

respectively, for some $\alpha \in \mathcal{O}_{\mathcal{D}}$ and a polynomial $g \in \mathbf{A}$. Then

$$\overline{F}F \equiv g^2 \pmod{f\mathcal{O}_{\mathcal{D}}}.$$

As $\mathcal{O}_{\mathcal{D}}$ admits an embedding in $\mathbf{A}_{\mathfrak{p}}$ from the representation of $T_{\mathfrak{p}}(\varphi)$, it follows that P divides g^2. If P divides f and P divides g^2, and hence P divides g, then P divides F or $\overline{F}$. So one of those is a trivial endomorphism of φ. This contradicts part(a). Thus, P does not divide f. □

6.5 The Automorphism Group

We present the automorphism group of a rank two Drinfeld module $\varphi = (g, \Delta)$ defined over an $\mathbf{A}$-field $\mathbb{L}$. Recall that the j-invariant $j(\varphi)$ of φ is defined as

$$j = j(\varphi) = \frac{g^{q+1}}{\Delta}.$$

Proposition 6.5.1. *If $j_0 \in \mathbb{L}$, then there exists a rank two Drinfeld module over $\mathbb{L}$ with j-invariant j_0.*

Proof. If $j_0 = 0$, then φ such that $\varphi_T = \gamma(T) + \Delta\tau^2$ with $\Delta \neq 0$, is a rank two Drinfeld module with j-invariant $j = 0/\Delta = j_0$. If $j_0 \neq 0$, then φ such that $\varphi_T = \gamma(T) + \tau + j_0^{-1}\tau^2$ is a rank two Drinfeld module with j-invariant

$$j = \frac{1^{q+1}}{j_0^{-1}} = j_0.$$

□

This result implies that the j-invariant gives a bijection between elements of $\mathbb{L}$ and $\overline{\mathbb{L}}$-isomorphism classes of Drinfeld modules defined over $\mathbb{L}$. Such is also the case for elliptic curves defined over finite fields. The following result is stated in [Gek08].

Proposition 6.5.2. *Let $\varphi = (g, \Delta)$ and $\varphi' = (g', \Delta')$ be rank two Drinfeld modules over $\mathbb{L}$. Then φ and φ' are isomorphic over $\overline{\mathbb{L}}$ if and only if there exists $c \in \mathbb{L}^*$ such that $g' = gc^{q-1}$ and $\Delta' = \Delta c^{q^2-1}$.*

Proof. Note that φ and φ' are isomorphic if and only if there exists $u \in \mathbb{L}^*$ such that $u\varphi'_T = \varphi_T u$. Thus

$$u\gamma(T) + ug'\tau + u\Delta'\tau^2 = \gamma(T)u + g\tau u + \Delta\tau^2 u = \gamma(T)u + gu^q\tau + \Delta u^{q^2}\tau^2,$$

which holds if and only if $ug' = gu^q$ and $u\Delta' = \Delta u^{q^2}$. Equivalently, we get $c = u \in \mathbb{L}^*$ such that $g' = gc^{q-1}$ and $\Delta' = \Delta c^{q^2-1}$. □

Remark 6.5.3.

1. Proposition 6.5.2 is equivalent to saying that two rank two Drinfeld modules $\varphi = (g, \Delta)$ and $\varphi' = (g', \Delta')$ are isomorphic over $\overline{\mathbb{L}}$ if and only if the following conditions are satisfied

   (a) $j(\varphi) = j(\varphi')$ and

   (b) g'/g is a $(q-1)$-st power in $\mathbb{L}$, if $j(\varphi) = j(\varphi') \neq 0$, and

   Δ'/Δ is a (q^2-1)-st power in $\mathbb{L}$, if $j(\varphi) = j(\varphi') = 0$.

2. Notice that if $\varphi = (g, \Delta)$ is replaced with $(c^{q-1}g, c^{q^2-1}\Delta)$ where $c \in \mathbb{L}^*$, then $H(\varphi)$ is multiplied by c^{q^d-1}. So the norm $N^{\mathbb{L}}_{\mathbb{F}_\mathfrak{p}}(H(\varphi))$ in (6.10) depends only on the $\mathbb{L}$-isomorphism class of φ.

Proposition 6.5.4 ([Gek08])**.** *The automorphism group of a rank two Drinfeld module $\varphi = (g, \Delta)$ over $\mathbb{L}$ is*

$$Aut_{\mathbb{L}}(\varphi) = \begin{cases} \mathbb{F}_q^*, & \text{if } j \neq 0 \text{ or } \mathbb{L} \not\supseteq \mathbb{F}_{q^2} \\ \mathbb{F}_{q^2}^*, & \text{otherwise.} \end{cases}$$

Proof. Let $u \in \mathbb{L}^*$ be an automorphism of φ. Then $u\varphi_T = \varphi_T u$, i.e.,

$$u\gamma(T) + ug\tau + u\Delta\tau^2 = \gamma(T)u + gu^q\tau + \Delta u^{q^2}\tau^2.$$

Note that $ug = gu^q$ if and only if $1 = u^{q-1}$, i.e., u is a $(q-1)$st root of unity. Similarly, $u\Delta = \Delta u^{q^2}$ if and only if $1 = u^{q^2-1}$, i.e., u is a (q^2-1)st root of unity. The result follows. □

Now assume that $\mathbb{L}$ is an extension of $\mathbb{F}_\mathfrak{p}$ of degree m and $[\mathbb{L} : \mathbb{F}_q] = n$ as in (6.4). The next result follows from Propositions 6.5.2 and 6.5.4.

Proposition 6.5.5 ([Gek08], Proposition 1.6)**.** *There are $q^n(q^n-1)$ rank two Drinfeld modules over $\mathbb{L}$ and the number of isomorphism classes of such modules is*

$$(q^n-1)(q-1) + \#(\mathbb{L}^*/\mathbb{L}^{*q^2-1}).$$

Corollary 6.5.6 ([Gek08], Corollary 1.7)**.**

$$\sum \frac{1}{Aut_{\mathbb{L}}(\varphi)} = q^n = \#\mathbb{L},$$

where the sum runs through all the isomorphism classes of φ *over* $\mathbb{L}$*.*

6.6 Reduction and Lifting of Drinfeld Modules

Our objective in this section is to give an analouge of the Deuring Lifting Theorem for Drinfeld modules. The material we present here is a summary of prior work given in [BK92]. Fix the rank of Drinfeld modules here to be $r = 2$.

Assume that $\mathbb{L}$ is an $\mathbf{A}$-field with $\mathbf{A}$-characteristic $\mathfrak{p} \neq (0)$. Let φ be an ordinary Drinfeld module defined over $\mathbb{L}$. Then $\mathcal{D} = \mathrm{End}_{\mathbb{L}}(\varphi) \otimes_{\mathbf{A}} \mathbf{K}$ is isomorphic to an imaginary quadratic function field extension $\mathcal{K}$ of $\mathbf{K}$, and $\mathrm{End}_{\mathbb{L}}(\varphi)$ is isomorphic to an order $\mathcal{O}$ of $\mathcal{K}$. There are two isomorphisms

$$\theta_1, \theta_2 : \mathcal{K} \longrightarrow \mathcal{D}$$

such that $\theta_i(a) = \varphi_a$ for $a \in \mathbf{A}$. Note also that $\mathcal{K}$ is a subfield of $\mathbf{C}$.

Now if φ is defined over $\mathbf{C}$, then an isomorphism $\theta : \mathcal{K} \longrightarrow \mathcal{D}$ is called *normalized* if $D \circ \theta(\alpha) = \alpha$ for $\alpha \in \mathcal{O}$, where D is the map from $\mathbb{L}\{\tau\}$ to $\mathbb{L}$ defined in (4.5). If this condition is satisfied, then the pair (φ, θ) is called a *normalized pair*.

Proposition 6.6.1.

1. *Let* (φ, θ) *and* (φ', θ') *be normalized pairs and* $u : \varphi \longrightarrow \varphi'$ *be a homomorphism. Then*

$$u \cdot \theta(\alpha) = \theta'(\alpha) \cdot u, \qquad \text{for } \alpha \in \mathcal{O}.$$

2. *Let* (φ, θ) *be a normalized pair. If* σ *is an isomorphism, fixing* $\mathcal{K}$*, of the field over which* φ *and all elements of* $\mathrm{End}_{\mathbb{L}}(\varphi)$ *are defined, then the pair* $(\varphi^\sigma, \theta^\sigma)$ *is also normalized.*

3. *If* (φ, θ) *is normalized and* φ *is defined over* $\mathcal{L} \subset \mathbf{C}$*, then every element of* $\mathrm{End}_{\mathcal{L}}(\varphi)$ *is defined over* $\mathcal{K}\mathcal{L}$*.*

Proof. See [BK92, Proposition 2.2] □

At this point, assume that $\mathcal{L}$ is a finite extension of the function field $\mathbf{K}$. Let φ be a Drinfeld module of rank two over $\mathcal{L}$. Suppose $\mathfrak{P} \neq (0)$ is a prime ideal of the maximal order $\mathcal{O}_{\mathcal{L}}$ of $\mathcal{L}$. If φ_a, for $a \in \mathbf{A}$, has integral coefficients at $\mathfrak{P}$ and $\operatorname{sgn}(\varphi_a)$ is a $\mathfrak{P}$-adic unit, then we can perform *reduction modulo* $\mathfrak{P}$ to obtain a rank two Drinfeld module over the residue field $\mathcal{L}_{\mathfrak{P}} := \mathcal{O}_{\mathcal{L}}/\mathfrak{P}$. For the remaining part of this section, we denote reduction modulo $\mathfrak{P}$ by a bar.

Definition 6.6.2. Let φ be a Drinfeld module of rank two over $\mathcal{L}$ and $\mathfrak{P}$ a prime ideal of $\mathcal{O}_{\mathcal{L}}$. We say that φ has *good reduction* at $\mathfrak{P}$ if and only if there exists a Drinfeld module $\overline{\varphi}$ of rank two where $\overline{\varphi} \cong \varphi$ over $\mathcal{L}$ and $\overline{\varphi_a}$ has integral coefficients at $\mathfrak{P}$.

Suppose φ is a Drinfeld module over the function field $\mathcal{L}$ with good reduction, $\overline{\varphi}$, at a prime ideal $\mathfrak{P}$ of $\mathcal{O}_{\mathcal{L}}$. Note that endomorphisms of φ can also be reduced modulo $\mathfrak{P}$ (see [Gek83, Lemma 3.3]. Suppose (φ, θ) is a normalized pair, and let $V = \operatorname{End}_{\mathcal{L}}(\overline{\varphi}) \otimes_{\mathbf{A}} \mathbf{K}$. Define the map

$$\overline{\theta} : \mathcal{K} \longrightarrow V$$

via $\overline{\theta}(\alpha) = \overline{\theta(\alpha)}$. Then we get the following result which can be proved in a manner similar to the classical case, see [Lan87, Section 13.4], since V is either an imaginary quadratic field or a noncommutative division algebra of degree 4 over $\mathbf{K}$.

Proposition 6.6.3. *Let $\mathcal{D}$ be an imaginary quadratic extension of $\mathbf{K}$. If an element of V commutes with all elements of $\overline{\operatorname{End}_{\mathbb{L}}(\varphi)}$, i.e., with all the reduced endomorphisms of φ, then it lies in $\overline{\mathcal{D}}$.*

Proof. See [BK92, Proposition 2.3]. □

Let $\mathfrak{p} = \mathfrak{P} \cap \mathbf{K}$ and $\mathcal{L}_{\mathfrak{P}}$ be the residue field at $\mathfrak{P}$. Suppose $\mathfrak{p} = (P)$ and $\deg_T(P) = d$. The following theorem gives the behaviour of φ under reduction.

Theorem 6.6.4 ([BK92])**.** *Let φ be a Drinfeld module defined over a function field $\mathcal{L}$, and suppose φ has good reduction $\overline{\varphi}$ at a prime $\mathfrak{P}$ of $\mathcal{O}_{\mathcal{L}}$. Suppose $\mathrm{End}_{\mathcal{L}}(\varphi) \cong \mathcal{O}$, where $\mathcal{O}$ is an order of an imaginary quadratic field extension $\mathcal{K}$ of $\mathbf{K}$ with $\mathcal{K} \subseteq \mathcal{L}$. Then we have the following cases:*

(1) $\overline{\varphi}$ is supersingular if and only if P does not split in $\mathcal{K}$.

(2) Suppose P splits in $\mathcal{K}$, and let f be the conductor of $\mathcal{O}$. If P does not divide f, then the reduction map $u \longmapsto \overline{u}$ is an isomorphism of $\mathrm{End}_{\mathcal{L}}(\varphi)$ onto $\mathrm{End}_{\mathcal{L}}(\overline{\varphi})$. In this case, $\overline{\varphi}$ is ordinary.

Proof. See [BK92, Theorem 3.1] □

Suppose the second case in the previous theorem holds. Fix a prime $\mathfrak{P}$ of $\mathcal{L}$ that lies above P such that $\mathcal{L}_{\mathfrak{P}} \simeq \mathbb{F}_{\mathfrak{p}}$. We can now state the analogue of Deuring's Lifting Theorem for Drinfeld modules.

Theorem 6.6.5. *Let $\mathcal{O}$, $\mathcal{K}$, $\mathcal{L}$, P, and $\mathfrak{P}$ be as above. Let φ_0 be an ordinary Drinfeld module of rank two defined over a finite extension of $\mathbb{F}_{\mathfrak{p}}$, and $u_0 \neq 0$ be an endomorphism of φ_0. Then there exists a Drinfeld module φ defined over a function field $\mathcal{L}$, an endomorphism u of φ, and a good reduction of φ at a place $\mathfrak{P}$ lying above P, such that φ_0 is isomorphic to $\overline{\varphi}$ and u corresponds to $\overline{u}$ under the isomorphism.*

Proof. See [BK92, Theorem 3.4]. □

This lifting theorem shows that the method given in Theorem 6.6.4 for obtaining an ordinary Drinfeld module with complex multiplication is basically the only way. In other words, a Drinfeld module over a finite field can be obtained by reducing a Drinfeld module with complex multiplication in the generic characteristic.

Definition 6.6.6. The Drinfeld module φ in Theorem 6.6.5 is called the *canonical lift* of φ_0.

Next, let $\mathcal{J}$ be the set of all j-invariants $j(\varphi)$ of Drinfeld modules φ over $\mathbf{C}$ with complex multiplication, i.e., the endomorphism rings of such Drinfeld modules strictly contain $\mathbf{A}$. Let $\mathcal{K}_j$ be the imaginary quadratic extension of $\mathbf{K}$ isomorphic to the endomorphism algebra corresponding to $j \in \mathcal{J}$. For each prime ideal $\mathfrak{p}$ of $\mathbf{A}$, let $\mathcal{J}_\mathfrak{p}$ be the set of all $j \in \mathcal{J}$ such that P splits completely in $\mathcal{K}_j$ and P does not divide the conductor of the ring $\mathcal{O}_j$ of endomorphisms of a Drinfeld module φ with invariant j. Let $\overline{\mathbf{K}}$ be the algebraic closure of $\mathbf{K}$ in $\mathbf{C}$ and $\overline{\mathbb{F}}_\mathfrak{p}$ the algebraic closure of $\mathbb{F}_\mathfrak{p} = \mathbf{A}/\mathfrak{p}$. Suppose $\mathfrak{P}$ is a place of $\overline{\mathbf{K}}$ lying above P. Let $J_{ord} \subset \overline{\mathbb{F}}_\mathfrak{p}$ be the set of ordinary j-invariants in characteristic $\mathfrak{p}$. Then we obtain a map

$$\mathcal{J}_\mathfrak{p} \longrightarrow J_{ord}$$

denoted by the usual bar,

$$j \longmapsto \overline{j}$$

into the set of ordinary j-invariants in characteristic $\mathfrak{p}$ since in this case the ordinary j-invariants over $\mathbf{A}$ are all integral ([Gek83, Satz 4.3]). Finally, we get the next result, which is an analogue of one of Deuring's results for Drinfeld modules.

Theorem 6.6.7 ([BK92])**.** *The map $\mathcal{J}_\mathfrak{p} \longrightarrow J_{ord}$ is a bijection of $\mathcal{J}_\mathfrak{p}$ with the set of ordinary j-invariants in characteristic $\mathfrak{p}$.*

Proof. See [BK92, Theorem 3.5]. □

6.7 Action of the Ideal Class Group

Throughout this section, we assume that all lattices under consideration are of rank two. Now consider a rank two ordinary Drinfeld module φ over $\mathbf{C}$ with $\mathcal{O}_\varphi = \mathrm{End}(\varphi)$, an order in an imaginary quadratic extension $\mathcal{K}$ of $\mathbf{K}$ with $\mathcal{K} \subset \mathbf{C}$. This order is determined using the following result, which is a reformulation of Lemma 3.4.1 for rank two Drinfeld modules.

Lemma 6.7.1. *Let φ be the Drinfeld module associated to the lattice $[1, z]$ such that z has minimal polynomial $aX^2 + bX + c$, where $a, b, c \in \mathbf{A}$ and $\gcd(a, b, c) = 1$. Then $\mathcal{O}_\varphi$ is the order with discriminant $b^2 - 4ac$.*

As φ has complex multiplication, it can be considered as a rank one Drinfeld module on $\mathcal{O}_\varphi$ in the sense of Hayes, see [Hay79]. We determine the action of the ideal class group $\mathcal{C}l(\mathcal{O}_\varphi) = \mathcal{I}(\mathcal{O}_\varphi)/\mathcal{P}(\mathcal{O}_\varphi)$ (see Definition 3.4.2) on

$$\mathcal{DM}(\mathcal{O}_\varphi) = \frac{\{\text{Drinfeld modules } \psi \text{ over } \mathbf{C} \text{ with } \mathrm{End}(\psi) \simeq \mathcal{O}_\varphi\}}{\text{isomorphism over } \mathbf{C}},$$

which is the isomorphism class of Drinfeld modules over $\mathbf{C}$ with endomorphism ring $\mathcal{O}_\varphi$. Note that $\mathcal{DM}(\mathcal{O}_\varphi)$ is in bijection with the set of homothetic rank two $\mathbf{A}$-lattices Λ in $\mathbf{C}$ for which $\mathrm{End}(\varphi^\Lambda) = \mathcal{O}_\varphi$, where φ^Λ is the Drinfeld module associated to Λ (see Theorem 5.2.9).

Let $\mathfrak{a} \in \mathcal{I}(\mathcal{O}_\varphi)$ and let $\mathfrak{i}_{\mathfrak{a},\varphi}$ be the left ideal of $\mathbf{C}\{\tau\}$ generated by the polynomials φ_a, $a \in \mathfrak{a}$. Since $\mathbf{C}\{\tau\}$ is a left principal ideal domain (see Corollary 4.1.12), there exists a unique monic polynomial $\varphi_\mathfrak{a} \in \mathbf{C}\{\tau\}$ such that $\mathfrak{i}_{\mathfrak{a},\varphi} = (\varphi_\mathfrak{a})$, and

$$\varphi_\mathfrak{a} = u_1 \cdot \varphi_{a_1} + u_2 \cdot \varphi_{a_2} + \cdots + u_k \cdot \varphi_{a_k}$$

for suitable elements $a_1, a_2, \ldots, a_k \in \mathfrak{a}$ and polynomials $u_1, u_2, \ldots, u_k \in \mathbf{C}\{\tau\}$. If $\mathfrak{a}$ is principal, i.e., $\mathfrak{a} = (a)$, then $\varphi_\mathfrak{a} = \mathrm{sgn}(a)^{-1}\varphi_a$ is the unique monic polynomial that generates $\mathfrak{i}_{\mathfrak{a},\varphi}$. So there exists a unique Drinfeld module φ' for which

$$\varphi_\mathfrak{a} \cdot \varphi = \varphi' \cdot \varphi_\mathfrak{a}$$

(see [BK92], p. 273). Denote φ' by $\mathfrak{a} * \varphi$. Via $*$, we see that $\varphi_\mathfrak{a} : \varphi \longrightarrow \varphi'$ is an isogeny.

Note that $\mathcal{O}_\varphi$ is a finitely-generated $\mathbf{A}$-module of rank $2 = [\mathcal{K} : \mathbf{K}]$. So every $\mathcal{O}_\varphi$-ideal $\mathfrak{a}$ is also a finitely generated $\mathbf{A}$-module. If $\mathfrak{a}$ is an invertible fractional $\mathcal{O}_\varphi$-ideal, then $\mathfrak{a}$ is also a lattice in $\mathbf{C}$ via the embedding $\mathfrak{a} \subset \mathcal{K} \subset \mathbf{C}$. To emphasize the association of rank two Drinfeld modules and rank two lattices in $\mathbf{C}$, we go back to the notation φ^Λ (see Theorem 5.2.9) to denote that φ is associated to the lattice Λ.

Lemma 6.7.2. *Let $\mathfrak{a}$ be an invertible fractional $\mathcal{O}_\varphi$-ideal and let φ^Λ be the Drinfeld module associated to the lattice $\Lambda \subset \mathbf{C}$ with $\mathrm{End}(\varphi^\Lambda) = \mathcal{O}_\varphi$. Then $\mathfrak{a}\Lambda$ is a lattice in $\mathbf{C}$ and $\mathrm{End}(\varphi^{\mathfrak{a}\Lambda}) = \mathcal{O}_\varphi$.*

Proof. Note that $\mathcal{O}_\varphi\Lambda = \Lambda$ because $\mathrm{End}(\varphi^\Lambda) = \mathcal{O}_\varphi$. Since $\mathfrak{a}$ is an invertible fractional ideal, we can choose a polynomial $d \in \mathbf{A}^+$ such that $d\mathfrak{a} \subset \mathcal{O}_\varphi$. So $d\mathfrak{a}\Lambda \subset \Lambda$. It follows that $\mathfrak{a}\Lambda \subset d^{-1}\Lambda$, so $\mathfrak{a}\Lambda$ is discrete. Now choose a polynomial $a \in \mathbf{A}^+$ so that $a\mathcal{O}_\varphi \subset \mathfrak{a}$. Then $a\Lambda \subset \mathfrak{a}\Lambda$, so $\mathfrak{a}\Lambda$ spans $\mathbf{C}$. Hence, $\mathfrak{a}\Lambda$ is a lattice.

Now suppose $\alpha \in \mathcal{O}_\varphi$, then $\alpha\mathfrak{a} \subseteq \mathfrak{a}$. So $\alpha\mathfrak{a}\Lambda \subseteq \mathfrak{a}\Lambda$, which implies that $\mathcal{O}_\varphi \subseteq \mathrm{End}(\varphi^{\mathfrak{a}\Lambda})$. Next, take $\beta \in \mathrm{End}(\varphi^{\mathfrak{a}\Lambda})$. Then we have

$$\beta\mathfrak{a}\Lambda \subseteq \mathfrak{a}\Lambda.$$

Since $\mathfrak{a}$ is invertible, we can multiply by $\mathfrak{a}^{-1}$ to get $\beta\Lambda \subseteq \Lambda$. Therefore, $\beta \in \mathcal{O}_\varphi$. This completes the proof. □

Lemma 6.7.3. *Let $\mathfrak{a}$, $\mathfrak{b}$ be invertible $\mathcal{O}_\varphi$-ideals. Let φ^Λ be a Drinfeld module over $\mathbf{C}$. Then*

$$\varphi^\Lambda_{\mathfrak{a}\mathfrak{b}} = (\mathfrak{b} * \varphi^\Lambda_{\mathfrak{a}}) * \varphi^\Lambda_{\mathfrak{b}} \qquad \textit{and} \qquad \mathfrak{a} * (\mathfrak{b} * \varphi^\Lambda) = (\mathfrak{a}\mathfrak{b}) * \varphi^\Lambda.$$

Proof. See [Hay79, Theorem 3.10]. □

The following result gives the lattice associated to $\mathfrak{a} * \varphi^\Lambda$ (see [BK92, Lemma 4.2]).

Lemma 6.7.4. *Let φ^Λ be a Drinfeld module over $\mathbf{C}$, then $\mathfrak{a}*\varphi^\Lambda$ is isomorphic to the Drinfeld module associated to the lattice $\mathfrak{a}^{-1}\Lambda$.*

Proof. See [Hay79, Proposition 5.10 and Equations (5.15) and (5.18)]. □

Let $[\mathfrak{a}]$ be the ideal class of an $\mathcal{O}_\varphi$-ideal $\mathfrak{a}$ in $\mathcal{C}l(\mathcal{O}_\varphi)$.

Theorem 6.7.5. *Let $\Lambda \subset \mathbf{C}$ be a lattice with $\mathrm{End}(\varphi^\Lambda) = \mathcal{O}_\varphi$, an order in an imaginary quadratic function field $\mathcal{K}$. Let $\mathfrak{a}$ and $\mathfrak{b}$ be invertible $\mathcal{O}_\varphi$-ideals. Then*

(i) $\varphi^{\mathfrak{a}\Lambda} \simeq \varphi^{\mathfrak{b}\Lambda}$ *if and only if* $[\mathfrak{a}] = [\mathfrak{b}]$ *in* $\mathcal{C}l(\mathcal{O}_\varphi)$.

(ii) $\mathcal{C}l(\mathcal{O}_\varphi)$ *acts on* $\mathcal{DM}(\mathcal{O}_\varphi)$ *by*

$$\mathfrak{a} * \varphi^\Lambda = \varphi^{\mathfrak{a}^{-1}\Lambda}, \tag{6.13}$$

and this action is simply transitive.

Proof. Recall from Remark 5.4.2 that the isomorphism class of $\varphi^{\mathfrak{a}\Lambda}$ is completely determined by the homothethy class of $\mathfrak{a}\Lambda$, i.e., $\varphi^{\mathfrak{a}\Lambda} \simeq \varphi^{\mathfrak{b}\Lambda}$ if and only if

$$\mathfrak{a}\Lambda = c\mathfrak{b}\Lambda \tag{6.14}$$

for some $c \in \mathbf{C}^*$. Multiply both sides of this equation by $\mathfrak{a}^{-1}$ to get

$$\Lambda = c\mathfrak{a}^{-1}\mathfrak{b}\Lambda.$$

Recall that $\mathcal{O}_\varphi\Lambda = \Lambda$, so $c\mathfrak{a}^{-1}\mathfrak{b} \subset \mathcal{O}_\varphi$. Similarly, if we multiply (6.14) by $c^{-1}\mathfrak{b}^{-1}$, then

$$\Lambda = c^{-1}\mathfrak{b}^{-1}\mathfrak{a}\Lambda.$$

So $c^{-1}\mathfrak{b}^{-1}\mathfrak{a} \subset \mathcal{O}_\varphi$ as well. It follows that $c\mathfrak{a}^{-1}\mathfrak{b} = c^{-1}\mathfrak{b}^{-1}\mathfrak{a} = \mathcal{O}_\varphi$. Hence, $\mathfrak{a} = c\mathfrak{b}$ and $c \in \mathcal{K}^*$. So $[\mathfrak{a}] = [\mathfrak{b}]$. This completes the proof of (i).

Observe that by homothety, $\mathfrak{a} * \varphi^\Lambda$ only depends on the ideal class of $\mathfrak{a}$. By Lemmas 6.7.3 and 6.7.4, we see that the definition $\mathfrak{a} * \varphi^\Lambda = \varphi^{\mathfrak{a}^{-1}\Lambda}$ gives a group action of $\mathcal{C}l(\mathcal{O}_\varphi)$ on $\mathcal{DM}(\mathcal{O}_\varphi)$.

Now let $\varphi^\Lambda, \varphi^{\Lambda'} \in \mathcal{DM}(\mathcal{O}_\varphi)$. To show that $\mathcal{C}l(\mathcal{O}_\varphi)$ acts transitively on $\mathcal{DM}(\mathcal{O}_\varphi)$, we have to find an invertible fractional $\mathcal{O}_\varphi$-ideal $\mathfrak{a}$ such that $\mathfrak{a} * \varphi^\Lambda = \varphi^{\Lambda'}$, i.e., such that $\mathfrak{a}^{-1}\Lambda$ is homothetic to Λ'. Now suppose $\{\omega_1, \omega_2\}$ is an $\mathbf{A}$-basis of Λ, then we can let $\mathfrak{a}_1 = c\Lambda = [1, z]$, where $c = \frac{1}{\omega_1}$ and $z = \frac{\omega_2}{\omega_1}$. Clearly, $\mathfrak{a}_1$ is a finitely generated $\mathcal{O}_\varphi$-submodule of $\mathcal{K}$. So it is a fractional $\mathcal{O}_\varphi$-ideal. Its inverse is

$$\mathfrak{a}_1^{-1} = \{\alpha \in \mathcal{K} \mid \alpha\frac{1}{\omega_1}\Lambda \subseteq \mathcal{O}_\varphi\} = \{\alpha \in \mathcal{K} \mid \alpha = \omega_1 a,\ a \in \mathbf{A}\}.$$

Similarly, we apply homothety to Λ' to get an invertible fractional ideal $\mathfrak{a}_2 = d\Lambda'$ for some $d \in \mathbf{C}^*$. Then

$$\mathfrak{a}_2\mathfrak{a}_1^{-1}\Lambda = dc^{-1}\Lambda'.$$

Now if we let $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2^{-1}$, then $\mathfrak{a} * \varphi^{\Lambda} = \varphi^{\Lambda'}$. This shows that the action is transitive.

Finally, the action is simply transitive, as a consequence of part (i). This completes the proof of (ii). $\square$

Chapter 7

Isogeny Volcanoes of Ordinary Drinfeld Modules

In this chapter we present results regarding graphs that arise from isogenies of ordinary rank two Drinfeld modules defined over finite fields. In order to characterize such graphs, we formulate an analogue of Kohel's Theorem in the Drinfeld module case. Then we give results pertaining to isogeny volcanoes for Drinfeld modules. The results we present here are new.

Throughout this chapter we let q be a power of an odd prime $p \in \mathbb{Z}$, $\mathbf{A} = \mathbb{F}_q[T]$, and $\mathfrak{p} \neq (0)$ a prime ideal in $\mathbf{A}$. We use $P(T)$, or simply P, to denote the monic irreducible polynomial that generates the ideal $\mathfrak{p}$. Fix the $\mathbf{A}$-field $\mathbb{L} = \mathbb{F}_\mathfrak{p} = \mathbf{A}/\mathfrak{p}$, so we are in the finite characteristic case, i.e., $\mathrm{char}_\mathbf{A}(\mathbb{L}) = \mathfrak{p} \neq (0)$. As before, let $|a| = q^{\deg_T(a)}$ for $a \in \mathbf{A}$. We also use the notations $\mathbf{A}^+$, $\mathbf{K}$, $\mathbf{K}_\infty$ and $\mathbf{C}$ as defined earlier.

7.1 Analogue of Kohel's Theorem for Drinfeld Modules

Throughout this section assume that $[\mathbb{F}_\mathfrak{p} : \mathbb{F}_q] = d$, so $\mathbb{F}_\mathfrak{p}$ has q^d elements. Let φ be an ordinary Drinfeld module of rank two over $\mathbb{F}_\mathfrak{p}$, and denote this condition by $\varphi/\mathbb{F}_\mathfrak{p}$. We also identify $\mathbf{A}$ with $\varphi(\mathbf{A})$. So we use the notation φ_a (instead of a) only where it is desirable to emphasize φ_a as a morphism of Drinfeld modules.

It was shown in Theorem 6.4.2 that the endomorphism ring of φ is an order $\mathcal{O}_\varphi := \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\varphi)$ in an imaginary quadratic function field $\mathcal{K}$. Similar to the classical case, $\mathcal{O}_\varphi$ contains $\mathbf{A}$ because of multiplication-by-a maps. Note that the Frobenius endomorphism $F = \tau^d$ is always an element of $\mathcal{O}_\varphi - \mathbf{A}$ in finite characteristic $\mathfrak{p}$. Thus

$$\mathbf{A} \subset \mathbf{A}[F] \subseteq \mathcal{O}_\varphi.$$

The minimal polynomial of F in our setting is of the form $M_\varphi(X) = X^2 - aX + \varepsilon P$,

where $\gcd(a, P) = 1$ for $a \in \mathbf{A}$ and $\varepsilon \in \mathbb{F}_q^*$ such that $2\deg(a) < d$ or $2\deg(a) = d$ and $X^2 - a_0X + \varepsilon$ is irreducible over $\mathbb{F}_q$ with $a_0 = \operatorname{sgn}(a)$, so $M_\varphi(X)$ remains irreducible over $\mathbf{K}_\infty$ (see Remark 6.3.15, [Yu95b], or [GS97]). Since the characteristic polynomial $P_\varphi(X)$ is a power of $M_\varphi(X)$, it follows that $P_\varphi(X) = M_\varphi(X)$. Moreover, a and εP are the Frobenius trace and norm, respectively, in this case. Hence F satisfies $P_\varphi(F) = F^2 - aF + \varepsilon P = 0$. Then

$$\det(F^2 - aF + \varepsilon P) = \det(0) = 0,$$

and so $F^2 - aF + \varepsilon P$ is the zero morphism in $\mathcal{O}_\varphi$. Moreover, $\mathbf{A}[F]$ has discriminant

$$D_F := a^2 - 4\varepsilon P, \tag{7.1}$$

and embeds into the imaginary quadratic function field

$$\mathcal{K} := \mathbf{K}\left(\sqrt{a^2 - 4\varepsilon P}\right).$$

Let $\mathcal{O}_\mathcal{K}$ be the integral closure of $\mathbf{A}$ in $\mathcal{K}$, i.e., $\mathcal{O}_\mathcal{K}$ is the maximal order of $\mathcal{K}$. Thus, we get the inclusions

$$\mathbf{A}[F] \subseteq \mathcal{O}_\varphi \subseteq \mathcal{O}_\mathcal{K}. \tag{7.2}$$

We use the following terminology in the entire chapter.

Definition 7.1.1. We call $\mathbf{A}[F]$ the *Frobenius order* and $\mathcal{O}_\varphi$ the *endomorphism order*. The conductors of these orders will be called *Frobenius conductor* and *endomorphism conductor*, respectively, and their discriminants *Frobenius discriminant* and *endomorphism discriminant*, respectively. The discriminant of the maximal order $\mathcal{O}_\mathcal{K}$ (or of the field $\mathcal{K}$) will be termed *fundamental discriminant*.

Let $D_\mathcal{K}$ denote the discriminant of the field $\mathcal{K}$, and recall that $\mathcal{O}_\mathcal{K} = [1, D_\mathcal{K}] = \mathbf{A} + \mathbf{A}\sqrt{D_\mathcal{K}}$. By Definition 3.2.5, the conductor of an order in $\mathcal{K}$ is a monic polynomial in $\mathbf{A}$. Now let $f_\varphi \in \mathbf{A}$ be the endomorphism conductor. Thus, by Proposition 3.2.4, we can write

$$\mathcal{O}_\varphi = [1, f_\varphi\sqrt{D_\mathcal{K}}] = \mathbf{A} + f_\varphi\mathcal{O}_\mathcal{K}.$$

Let D_φ be the discriminant of $\mathcal{O}_\varphi$. Then D_φ and $D_\mathcal{K}$ are related via the equation

$$D_\varphi = 4f_\varphi^2 D_\mathcal{K},$$

(see (3.2)) where the factor 4 is a unit since $\mathrm{char}(\mathbb{F}_q) = p \neq 2$. Denote the conductor of $\mathbf{A}[F]$ by f_F. Thus, we can similarly write

$$D_F = 4f_F^2 D_\mathcal{K} \quad \text{and} \quad \mathbf{A}[F] = [1, f_F\sqrt{D_\mathcal{K}}] = \mathbf{A} + f_F\mathcal{O}_\mathcal{K}.$$

It follows from the inclusion $\mathbf{A}[F] \subseteq \mathcal{O}_\varphi$ that f_φ divides f_F. Since $\mathcal{O}_\varphi$ is determined by f_φ, there is a finite number of possibilities for $\mathcal{O}_\varphi$. These are the rings of the form $\mathcal{O} = \mathbf{A} + f\mathcal{O}_\mathcal{K}$, where $f \mid f_F$. Now consider the case where $f_F = 1$. Then it is clear that $\mathbf{A}[F] = \mathcal{O}_\mathcal{K}$. It follows from (7.2) that $\mathcal{O}_\varphi = \mathcal{O}_\mathcal{K}$ in this case. The other possibility is that the monic polynomial f_F is not equal to 1, and hence $\deg(f_F) \geq 1$. Since $\mathbf{A}$ is a unique factorization domain, we can write

$$f_F = \prod_{i=1}^{s} \ell_i^{e_i},$$

where $\ell_1, \ell_2, \ldots, \ell_s \in \mathbf{A}$ are distinct finite primes and $e_1, e_2, \ldots, e_s$ are positive integers (here, it is assumed that all the $\ell_i \in \mathbf{A}^+$). Likewise, we can write

$$f_\varphi = \prod_{i=1}^{s} \ell_i^{d_i},$$

where the exponents d_i satisfy $0 \leq d_i \leq e_i$ since $f_\varphi \mid f_F$. By Lemma 3.2.7, we see that the conductor of $\mathbf{A}[F]$ in $\mathcal{O}_\varphi$ is f_F/f_φ. Table 7.1 shows the indices associated to the orders $\mathbf{A}[F]$, $\mathcal{O}_\varphi$, and $\mathcal{O}_\mathcal{K}$ (see Proposition 3.2.6) as compared to those in the elliptic curve case (see Figure 2.1). Notice that in the Drinfeld module case, these indices are all powers of q.

Elliptic Curve Case	**Drinfeld Module Case**
$[\mathcal{O}_K : \mathbb{Z}[\pi]] = f_\pi$	$[\mathcal{O}_\mathcal{K} : \mathbf{A}[F]] = \lvert f_F \rvert$
$[\mathcal{O}_K : \mathcal{O}_E] = f_E$	$[\mathcal{O}_\mathcal{K} : \mathcal{O}_\varphi] = \lvert f_\varphi \rvert$
$[\mathcal{O}_E : \mathbb{Z}[\pi]] = f_\pi/f_E$	$[\mathcal{O}_\varphi : \mathbf{A}[F]] = \lvert f_F/f_\varphi \rvert$

Table 7.1: Indices of Orders

Our main goal in this section is to classify isogenies of rank two ordinary Drinfeld modules. In particular, we examine isogenies of degree ℓ, where ℓ is a prime in $\mathbf{A}$. We determine the type and number of ℓ-isogenies to or from a given ordinary Drinfeld module. Alongside with this, we also characterize endomorphism rings of Drinfeld modules locally, i.e., with respect to ℓ.

We follow closely what has been done in the elliptic curve case, see Section 2.4. Here, however, we cannot treat the conductors as indices of groups since they are polynomials. So their absolute values are the appropriate group indices. We note that if a prime ℓ divides the conductor f_φ, then $|\ell|$ divides $|f_\varphi|$.

Assume that φ and ψ are ordinary Drinfeld modules of rank two over $\mathbb{F}_\mathfrak{p}$, and let $\mathcal{O}_\psi := \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi)$ with conductor $f_\psi \in \mathbf{A}$. First, we determine the relationship between $\mathcal{O}_\varphi$ and $\mathcal{O}_\psi$ given an isogeny $u : \varphi \longrightarrow \psi$.

Lemma 7.1.2. *If $u : \varphi \longrightarrow \psi$ is an isogeny of Drinfeld modules with dual isogeny $\widehat{u} : \psi \longrightarrow \varphi$, then $\widehat{u}\mathcal{O}_\psi u \subseteq \mathcal{O}_\varphi$. Similarly, $u\mathcal{O}_\varphi\widehat{u} \subseteq \mathcal{O}_\psi$.*

Proof. Let $0 \neq v \in \mathcal{O}_\psi$. Then we have the isogenies $u : \varphi \longrightarrow \psi$, $v : \psi \longrightarrow \psi$, and $\widehat{u} : \psi \longrightarrow \varphi$. Hence the isogeny $\widehat{u} \cdot v \cdot u$ is in $\mathcal{O}_\varphi$.

The other inclusion is similarly proved. □

The following result is the analogue of Lemma 2.4.1 (or [Koh96, Proposition 21]) for Drinfeld modules.

Lemma 7.1.3. *Let $u : \varphi \longrightarrow \psi$ be an ℓ-isogeny of ordinary Drinfeld modules over $\mathbb{F}_\mathfrak{p}$. Then exactly one of the following holds:*

(a) $f_\psi/f_\varphi = \ell$, in particular, f_φ divides f_ψ, equivalently, $\mathcal{O}_\psi \subset \mathcal{O}_\varphi$.

(b) $f_\varphi/f_\psi = \ell$, in particular, f_ψ divides f_φ, equivalently, $\mathcal{O}_\varphi \subset \mathcal{O}_\psi$.

(c) $\mathcal{O}_\varphi = \mathcal{O}_\psi$.

Proof. Note that both φ and ψ are ordinary, so both of their endomorphism rings contain $\mathbf{A}[F]$. Thus, we obtain the embbedings in Figure 7.1. We determine the relationship between the orders $\mathcal{O}_\varphi$ and $\mathcal{O}_\psi$. We lift the Drinfeld modules φ and ψ to $\mathbf{C}$ using Theorem 6.6.5, and also call these lifts φ and ψ, respectively. By Theorem 6.6.4, these lifts are also ordinary Drinfeld modules. Let Λ_1 and Λ_2 be the lattices in $\mathbf{C}$ associated to φ and ψ, respectively. Write

$$\mathcal{O}_1 = \mathrm{End}(\Lambda_1) \quad \text{and} \quad \mathcal{O}_2 = \mathrm{End}(\Lambda_2),$$

where the $\mathrm{End}(\Lambda_i)$ are as defined in Definition 5.1.4. By Theorem 5.2.10, we have

$$\mathcal{O}_\varphi \cong \mathcal{O}_1 \quad \text{and} \quad \mathcal{O}_\psi \cong \mathcal{O}_2. \tag{7.3}$$

Since these are quadratic orders, we can write

$$\mathcal{O}_1 = \mathbf{A} + z_1\mathbf{A} \quad \text{and} \quad \mathcal{O}_2 = \mathbf{A} + z_2\mathbf{A}, \quad \text{for some } z_1, z_2 \in \Omega,$$

where Ω is the Drinfeld upper half plane in (5.30).

Let $\ell = \alpha\widehat{\alpha} = \widehat{\alpha}\alpha$ with $\alpha, \widehat{\alpha} \in \mathbf{C}$ be such that $\alpha \in \mathrm{Hom}(\Lambda_1, \Lambda_2)$ and $\widehat{\alpha} \in \mathrm{Hom}(\Lambda_2, \Lambda_1)$, with the corresponding maps $\alpha \longmapsto u$ and $\widehat{\alpha} \longmapsto \widehat{u}$ in Theorem 5.2.10. We apply Lemma 7.1.2 to $\mathcal{O}_1$ and $\mathcal{O}_2$ using the morphisms $\alpha : \Lambda_1 \longrightarrow \Lambda_2$ and $\widehat{\alpha} : \Lambda_2 \longrightarrow \Lambda_1$ to obtain $\widehat{\alpha}\mathcal{O}_2\alpha \subseteq \mathcal{O}_1$ and $\alpha\mathcal{O}_1\widehat{\alpha} \subseteq \mathcal{O}_2$. So

$$\widehat{\alpha}z_2\alpha = \widehat{\alpha}\alpha z_2 = \alpha\widehat{\alpha}z_2 = \ell z_2 \in \mathcal{O}_1, \qquad \text{and similarly,} \qquad \alpha z_1\widehat{\alpha} = \alpha\widehat{\alpha}z_1 = \widehat{\alpha}\alpha z_1 = \ell z_1 \in \mathcal{O}_2$$

which implies three possible cases: $\mathcal{O}_1 \subset \mathcal{O}_2$, $\mathcal{O}_2 \subset \mathcal{O}_1$, or $\mathcal{O}_1 = \mathcal{O}_2$. By Lemma 7.1.2, we obtain

$$\widehat{\alpha}(\alpha\mathcal{O}_1\widehat{\alpha})\alpha \subseteq \widehat{\alpha}\mathcal{O}_2\alpha \subseteq \mathcal{O}_1 \quad \Longrightarrow \quad \ell^2\mathcal{O}_1 \subseteq \ell\mathcal{O}_2 \subseteq \mathcal{O}_1.$$

By using (7.3), we obtain three possibilities:

$$\ell^2 f_\varphi = \ell f_\psi, \quad \ell f_\psi = \ell f_\varphi, \quad \ell f_\psi = f_\varphi.$$

The result now follows. □

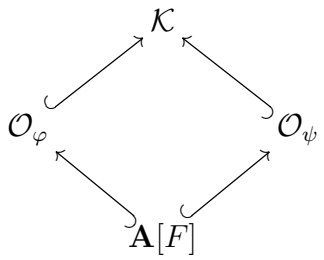


Figure 7.1: Embeddings of orders in $\mathcal{K}$

Definition 7.1.4. Let $u : \varphi \longrightarrow \psi$ be an ℓ-isogeny of ordinary Drinfeld modules. Then u is

(a) *ascending* ($\uparrow$) if $f_\varphi / f_\psi = \ell$, in this case $\mathcal{O}_\varphi \subset \mathcal{O}_\psi$.

(b) *descending* ($\downarrow$) if $f_\psi / f_\varphi = \ell$, in this case $\mathcal{O}_\psi \subset \mathcal{O}_\varphi$.

(c) *horizontal* ($\rightarrow$) if $\mathcal{O}_\varphi = \mathcal{O}_\psi$.

In addition to these results, we will use j-invariants and the modular polynomial $\Phi_\ell(X, Y)$ to classify ℓ-isogenies. Recall from Theorem 5.5.9 that two Drinfeld modules φ and ψ are ℓ-isogenous if and only if their j-invariants satisfy

$$\Phi_\ell(j(\varphi), j(\psi)) = 0.$$

Moreover, from Theorem 5.5.5, we know that $\Phi_\ell(X, Y)$ is of degree $\mathrm{N}(\ell) = |\ell| + 1$ in each variable, where $|\ell| = q^{\deg_T(\ell)}$. This gives us a bound on the number of ℓ-isogenies from a given Drinfeld module.

Note that Deuring's lifting theorem (Theorem 6.6.5) is also crucial in our classification since we are looking into orders of an imaginary quadratic function field $\mathcal{K} \subset \mathbf{C}$. We also require Lemma 6.7.1 which gives the endomorphism ring of a Drinfeld module over $\mathbf{C}$.

Now let $Q \in \mathbf{A}^+$ be an irreducible polynomial prime to P. We also require the Kronecker symbol $\chi_\mathcal{K}(Q)$ (see Definition 3.5.1) in our classification because we need know how primes decompose in $\mathcal{O}_\mathcal{K}$. We show that we can use the quadratic residue symbol $\left(\frac{\cdot}{Q}\right)$ (see Definition 3.1.12) in place of the Kronecker symbol in the classification theorem below. Note that q is

odd, so $|Q| = q^{\deg_T(Q)}$ is also odd. Hence, $2 \mid |Q| - 1$. Thus, we can consider the quadratic residue symbol. Let $\mathbb{F}_Q := \mathbf{A}/(Q)$. For $a \in \mathbb{F}_\mathfrak{p}^*$, a not divisible by Q, we have

$$\left(\frac{a}{Q}\right) = a^{\frac{|Q|-1}{2}} \in \mathbb{F}_Q^*/\mathbb{F}_Q^{*2} = \{\pm 1\} \subset \mathbb{Z}.$$

So we can interpret $\left(\frac{a}{Q}\right)$ as an integer. Its value is (a) 1 if a is a square $\pmod{Q}$, or (b) 0 if $Q \mid a$, or (c) -1 if a is not a square $\pmod{Q}$. These values correspond to the cases where Q splits, or ramifies, or is inert, respectively, in $\mathcal{O}_\mathcal{K}$.

We now have the following classification of ℓ-isogenies. This is the analogue of Kohel's result, Theorem 2.4.4, for Drinfeld modules. Here we adapt the proof in the elliptic curve case given in [Gal99]. Note that the technique used in the elliptic curve case works here since we can also lift Drinfeld modules to $\mathbf{C}$. We also exclude the case $j(\varphi) = 0$. This exclusion will be discussed at the end of the next section.

Theorem 7.1.5. *Let φ be an ordinary rank two Drinfeld module over a finite $\mathbf{A}$-field $\mathbb{F}_\mathfrak{p}$ with $j(\varphi) \neq 0$ and endomorphism ring $\mathcal{O}_\varphi$ in an imaginary quadratic function field $\mathcal{K}$. Let $\ell \in \mathbf{A}^+$ be an irreducible polynomial prime to P, and let $\left(\frac{D_\varphi}{\ell}\right)$ be the quadratic residue symbol.*

(1) If ℓ does not divide f_φ, then φ has $1 + \left(\frac{D_\varphi}{\ell}\right)$ horizontal ℓ-isogenies.

(2) If ℓ divides f_φ, then φ has one ascending ℓ-isogeny.

(3) If ℓ does not divide f_F/f_φ, then φ has no descending ℓ-isogeny.

(4) If ℓ does not divide f_φ and ℓ divides f_F/f_φ, then φ has $|\ell| - \left(\frac{D_\varphi}{\ell}\right)$ descending ℓ-isogenies.

(5) If ℓ divides f_φ and ℓ divides f_F/f_φ, then φ has $|\ell|$ descending ℓ-isogenies.

Proof. By using the Deuring lifting theorem (see Theorem 6.6.5), we can lift φ from $\mathbb{F}_\mathfrak{p}$ to $\mathcal{L} \subset \mathbf{C}$ with its endomorphism ring preserved, where $\mathcal{L}$ is a finite extension of $\mathcal{K}$. Let $\widetilde{\varphi}$ be the canonical lift of φ over $\mathcal{L}$. Then $\mathrm{End}_\mathcal{L}(\widetilde{\varphi}) = \mathcal{O}_\varphi$ is an order in $\mathcal{K}$. Note that $\widetilde{\varphi}$ is associated to a rank two lattice Λ in $\mathbf{C}$.

Let $\Lambda = [1, \beta]$ such that β has minimal polynomial $aX^2 + bX + c$, with $a, b, c \in \mathbf{A}$ and $\gcd(a, b, c) = 1$. Then $\mathrm{End}_{\mathbf{C}}(\widetilde{\varphi})$ is the order with discriminant $D = b^2 - 4ac = D_\varphi = 4f_\varphi^2 D_{\mathcal{K}}$. By using the quadratic formula, we get

$$\beta = \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$

It follows from (5.42) and Theorem 5.5.5 that there are $|\ell| + 1$ Drinfeld modules which are ℓ-isogenous to $\widetilde{\varphi}$ in $\mathbf{C}$. These are determined by the lattices $\Lambda_i = [1, \alpha_i\beta]$ for $0 \leq i \leq |\ell|$, where $\alpha_i \in S_\ell$ (see (5.41)). So let $\alpha_i = \begin{pmatrix} 1 & n_i \\ 0 & \ell \end{pmatrix}$ for $0 \leq i \leq |\ell| - 1$, where $n_i \in \mathbf{A}$ and $\deg_T(n_i) < \deg_T(\ell)$, and $\alpha_{|\ell|} = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$. Let $\widetilde{\varphi}_i$ be the Drinfeld module associated to Λ_i.

Suppose $i = |\ell|$. Then $\ell\beta$ is a root of $aX^2 + \ell bX + \ell^2 c$. Consider the following cases:

1. $\gcd(a, \ell b, \ell^2 c) = 1$: Then Lemma 6.7.1 is applicable. So $\mathrm{End}_{\mathbf{C}}(\widetilde{\varphi}_{|\ell|})$ has discriminant $\ell^2 D$. Then its conductor is $f_{\widetilde{\varphi}_{|\ell|}} = \ell f_\varphi$. So $\mathrm{End}_{\mathbf{C}}(\widetilde{\varphi}_{|\ell|}) \subset \mathcal{O}_\varphi$, which results in a descending ℓ-isogeny.

2. $\gcd(a, \ell b, \ell^2 c) \neq 1$: Then $\ell \mid a$.

   If $\ell \nmid b$, then let $a' = a/\ell$. In this case, $\ell\beta$ has minimal polynomial $a'X^2 + bX + \ell c$. It follows that $\mathrm{End}_{\mathbf{C}}(\widetilde{\varphi}_{|\ell|})$ has discriminant D. So $\mathrm{End}_{\mathbf{C}}(\widetilde{\varphi}_{|\ell|}) = \mathcal{O}_\varphi$, and we get a horizontal isogeny.

   If $\ell \mid b$, then $\ell \mid D$. Let $b' = b/\ell$. If $\ell \mid f_\varphi$, then it follows that $\ell^2 \mid a$ since $D = b^2 - 4ac$. So let $a' = a/\ell^2$. In this case, $\ell\beta$ has minimal polynomial $a'X^2 + b'X + c$, and $\mathrm{End}_{\mathbf{C}}(\widetilde{\varphi}_{|\ell|})$ has discriminant D/ℓ^2 and conductor $f_{\widetilde{\varphi}_{|\ell|}} = f_\varphi/\ell$. Therefore, $\mathcal{O}_\varphi \subset \mathrm{End}_{\mathbf{C}}(\widetilde{\varphi}_{|\ell|})$. This gives an ascending ℓ-isogeny.

Now consider the Drinfeld modules $\widetilde{\varphi}_i$ for $i = 0, 1, \ldots, |\ell| - 1$. Let $\omega_i = \alpha_i\beta = \frac{\beta + n_i}{\ell}$ for a particular i. Then

$$\omega = \frac{2an_i - b + \sqrt{b^2 - 4ac}}{2a\ell}$$

is a root of $a\ell^2X^2 + \ell(b - 2an_i)X + (an_i^2 - bn_i + c)$. Let $m = an_i^2 - bn_i + c$. We need to consider two cases here:

A. $\gcd(a\ell^2, \ell(b - 2an_i), m) = 1$: In this case, by Lemma 6.7.1, $\mathrm{End}_{\mathbf{C}}(\widetilde{\varphi}_i)$ has discriminant $\ell^2 D$, so $f_{\widetilde{\varphi}_i} = \ell f_\varphi$, and $\mathrm{End}_{\mathbf{C}}(\widetilde{\varphi}_i) \subset \mathcal{O}_\varphi$. Therefore, we found a descending ℓ-isogeny.

B. $\gcd(a\ell^2, \ell(b - 2an_i), m) \neq 1$: This condition holds if and only if $\ell \mid m$. So we need to determine the number of solutions of $m \equiv 0 \pmod{\ell}$. If we consider m as a polynomial in n_i, then its discriminant is equal to D.

   If $\ell \mid a$ and $\ell \mid b$, then $m \equiv 0 \pmod{\ell}$ if and only if $\ell \mid c$. This contradicts the assumption that $\gcd(a, b, c) = 1$. Therefore, $m \equiv 0 \pmod{\ell}$ has no solution. Also, if ℓ divides both a and b, then ℓ divides $D = 4f_\varphi^2 D_{\mathcal{K}}$. If $\ell \mid f_\varphi$, then we already have obtained a single ascending ℓ-isogeny above. If $\ell \mid D_{\mathcal{K}}$ but $\ell \nmid f_\varphi$, then ℓ ramifies in $\mathcal{O}_{\mathcal{K}}$. Note that we already found a single horizontal ℓ-isogeny above.

   If $\ell \mid a$ but $\ell \nmid b$, then $\left(\frac{D_{\mathcal{K}}}{\ell}\right) = 1$ i.e., ℓ splits in $\mathcal{O}_{\mathcal{K}}$. So $m \equiv 0 \pmod{\ell}$ has two solutions. We already found one horizontal isogeny above. The other horizontal isogeny is obtained when $n_i \equiv c/b \pmod{\ell}$. Therefore, we obtain two horizontal ℓ-isogenies.

   If $\ell \nmid a$, then m is a quadratic polynomial. It has a repeated root if and only if $\ell \mid D$. This is the ramified case presented above, which gave a single horizontal ℓ-isogeny. Now, if m has two distinct roots, then we have two horizontal ℓ-isogenies. In this case, ℓ splits in $\mathcal{O}_{\mathcal{K}}$. Finally, if ℓ is inert in $\mathcal{O}_{\mathcal{K}}$, then $m \equiv 0 \pmod{\ell}$ has no solution. So each n_i, for $i = 0, 1, \ldots, |\ell| - 1$, will contribute a descending ℓ-isogeny. In this case we get a total of $|\ell|$ descending ℓ-isogenies.

To complete the proof, we have to reduce the Drinfeld modules $\widetilde{\varphi}_i$, for $i = 0, 1, \ldots, |\ell|$, to the residue field $\mathcal{O}_{\mathcal{L}}/\mathfrak{P} \cong \mathbb{F}_{\mathfrak{p}}$, where $\mathfrak{P}$ is a place above $\mathfrak{p}$ (see Theorem 6.6.5). These Drinfeld modules will be defined over $\mathbb{F}_{\mathfrak{p}}$ if and only if their endomorphism rings contain $\mathbf{A}[F]$. This completes the proof. □

We summarize the results from this theorem in Table 7.2. Here we use the quadratic symbol $\left(\frac{D_K}{\ell}\right)$ since $\left(\frac{D_\varphi}{\ell}\right) = \left(\frac{D_K}{\ell}\right)$ if $\ell \nmid f_\varphi$.

$\left(\frac{D_K}{\ell}\right)$	Case		Number of Isogenies			
			$\rightarrow$	$\uparrow$	$\downarrow$	Total
0	$\ell \nmid f_\varphi$	$\ell \nmid f_F/f_\varphi$	1	0	0	1
		$\ell \mid f_F/f_\varphi$	1	0	$\lvert\ell\rvert$	$\lvert\ell\rvert+1$
	$\ell \mid f_\varphi$	$\ell \nmid f_F/f_\varphi$	0	1	0	1
		$\ell \mid f_F/f_\varphi$	0	1	$\lvert\ell\rvert$	$\lvert\ell\rvert+1$
1	$\ell \nmid f_\varphi$	$\ell \nmid f_F/f_\varphi$	2	0	0	2
		$\ell \mid f_F/f_\varphi$	2	0	$\lvert\ell\rvert-1$	$\lvert\ell\rvert+1$
	$\ell \mid f_\varphi$	$\ell \nmid f_F/f_\varphi$	0	1	0	1
		$\ell \mid f_F/f_\varphi$	0	1	$\lvert\ell\rvert$	$\lvert\ell\rvert+1$
-1	$\ell \nmid f_\varphi$	$\ell \nmid f_F/f_\varphi$	0	0	0	0
		$\ell \mid f_F/f_\varphi$	0	0	$\lvert\ell\rvert+1$	$\lvert\ell\rvert+1$
	$\ell \mid f_\varphi$	$\ell \nmid f_F/f_\varphi$	0	1	0	1
		$\ell \mid f_F/f_\varphi$	0	1	$\lvert\ell\rvert$	$\lvert\ell\rvert+1$

Table 7.2: Number and type of ℓ-isogenies of an ordinary rank two Drinfeld module φ

7.2 Isogeny Volcanoes of Drinfeld Modules

In this section we examine the structure of the graphs arising from isogenies of rank two Drinfeld modules defined over $\mathbb{F}_\mathfrak{p}$. This exploration will be guided by the classification theorem discussed in the previous section (Theorem 7.1.5) and Section 2.4.2. We give particular attention to isogenies of ordinary Drinfeld modules.

Throughout this section, let $\ell \in \mathbf{A}^+$ be an irreducible polynomial prime to P. Similar to the elliptic curve case, we define an ℓ-isogeny graph, denoted $G_\ell(\mathbb{F}_\mathfrak{p})$, as a graph with vertex set $\mathbb{F}_\mathfrak{p}$ and edges (j_1, j_2) if $\Phi_\ell(j_1, j_2) = 0$ and with multiplicity equal to the multiplicity of j_2 as a root of $\Phi_\ell(j_1, Y)$ for $j_1, j_2 \in \mathbb{F}_\mathfrak{p}$. We also treat these edges in bijection with the multiplicity of j_1 as a root of $\Phi_\ell(X, j_2)$. This means that $G_\ell(\mathbb{F}_\mathfrak{p})$ may contain loops or multiple edges. If we fix $\mathbb{F}_\mathfrak{p}$ and vary ℓ, then we get the same vertex set $\mathbb{F}_\mathfrak{p}$ but different edge sets because the edges depend on ℓ-isogenies.

Suppose $\varphi/\mathbb{F}_\mathfrak{p}$ is ordinary with Frobenius endomorphism F_φ and j-invariant $j(\varphi) \neq 0$. The case $j(\varphi) = 0$ corresponds to j-invariants 0 and 1728 for elliptic curves. It will be discussed separately later in this section. Let $P_\varphi(X) = X^2 - aX + b$ be the characteristic polynomial of the Frobenius endomorphism of φ, where $a = a(\varphi)$ and $b = b(\varphi)$ are the Frobenius trace and norm, respectively. Note that there are other Drinfeld modules with the same characteristic polynomial, namely those which are isogenous to φ over $\mathbb{F}_\mathfrak{p}$, see Theorem 6.3.3. Suppose ψ is one such Drinfeld module. Then its Frobenius endomorphism, F_ψ, must also be a root of $P_\varphi(X) = X^2 - aX + b$. So either $F_\varphi = F_\psi$ or $F_\varphi = \overline{F}_\psi$, where $\overline{F}_\psi$ is the conjugate of F_ψ in $\mathcal{K}$. Since F_φ and F_ψ may just differ by conjugation, we have $\mathbf{A}[F_\psi] = \mathbf{A}[\overline{F}_\psi]$. So we can fix one as F to obtain the order $\mathbf{A}[F]$. We now introduce the notation $P_{a,b}$ to signify that the characteristic polynomial is determined by a and b and we consider all Drinfeld modules over $\mathbb{F}_\mathfrak{p}$ whose Frobenius has characteristic polynomial $P_{a,b}$.

By Theorem 6.4.2, the endomorphism ring $\mathcal{O}_\varphi$ of φ is an order in an imaginary quadratic function field $\mathcal{K}$. Due to the set inclusions in (7.2), we see that the endomorphism conductor f_φ divides the Frobenius conductor f_F. This is also the case for any ordinary Drinfeld module $\psi/\mathbb{F}_\mathfrak{p}$ with the same characteristic polynomial $P_{a,b}$, i.e., $f_\psi \mid f_F$. Now recall from Proposition 6.5.1 that for every $j \in \mathbb{F}_\mathfrak{p}$, there exists a rank two Drinfeld module $\varphi/\mathbb{F}_\mathfrak{p}$ such that $j(\varphi/\mathbb{F}_\mathfrak{p}) = j$. Define

$$j_{a,b}(\mathbb{F}_\mathfrak{p}) := \{j(\varphi/\mathbb{F}_\mathfrak{p}) \mid \varphi/\mathbb{F}_\mathfrak{p} \text{ has characteristic polynomial } P_{a,b}\} \tag{7.4}$$

to be the set of $\overline{\mathbb{F}}_\mathfrak{p}$-isomorphism classes of Drinfeld modules $\varphi/\mathbb{F}_\mathfrak{p}$ with characteristic polynomial $P_{a,b}$. We know from Theorem 6.3.3 that two Drinfeld modules, say $\varphi/\mathbb{F}_\mathfrak{p}$ and $\psi/\mathbb{F}_\mathfrak{p}$, are isogenous over $\mathbb{F}_\mathfrak{p}$ if and only if they have the same characteristic polynomial. Therefore, this set is an isogeny class. We can also write

$$j_{a,b}(\mathbb{F}_\mathfrak{p}) = \bigsqcup_{\mathbf{A}[F] \subseteq \mathcal{O}_\varphi \subseteq \mathcal{O}_\mathcal{K}} j_{\mathcal{O}_\varphi}(\mathbb{F}_\mathfrak{p}),$$

where

$$j_{\mathcal{O}_\varphi}(\mathbb{F}_\mathfrak{p}) = \{j(\psi/\mathbb{F}_\mathfrak{p}) \mid \psi/\mathbb{F}_\mathfrak{p} \text{ has endomorphism ring } \mathcal{O}_\psi \cong \mathcal{O}_\varphi\}.$$

Notice that $P_{a,b}$ and $P_{-a,b}$ have the same splitting field $\mathcal{K} = \mathbf{K}(\sqrt{a^2 - 4b})$. Suppose $\varphi/\mathbb{F}_\mathfrak{p} = (g_\varphi, \Delta_\varphi)$ and $\psi/\mathbb{F}_\mathfrak{p} = (g_\psi, \Delta_\psi)$ have characteristic polynomials $P_{a,b}$ and $P_{-a,b}$, respectively. It follows from Proposition 6.3.8 and Theorem 6.3.9 that $H(\psi) = -H(\varphi)$ and $\Delta_\varphi \equiv \Delta_\psi \pmod{\mathfrak{p}}$. Then, via (5.29) and (5.37), we see that $j(\varphi/\mathbb{F}_\mathfrak{p}) = j(\psi/\mathbb{F}_\mathfrak{p})$. So the isogeny class that contains $j(\varphi/\mathbb{F}_\mathfrak{p})$ must also contain $j(\psi/\mathbb{F}_\mathfrak{p})$ and vice versa.

7.2.1 Isogeny Graphs

Assume that $\varphi/\mathbb{F}_\mathfrak{p}$ and $\psi/\mathbb{F}_\mathfrak{p}$ are ordinary Drinfeld modules such that $j(\varphi), j(\psi) \neq 0$. Let $\mathcal{O}_\varphi$ and $\mathcal{O}_\psi$ be the endomorphism orders of $\varphi/\mathbb{F}_\mathfrak{p}$ and $\psi/\mathbb{F}_\mathfrak{p}$, respectively. Suppose $u : \varphi \longrightarrow \psi$ is an ℓ-isogeny. It follows from Lemma 7.1.3 that one of two things can happen: either (1) the conductors of $\mathcal{O}_\varphi$ and $\mathcal{O}_\psi$ are equal or (2) one conductor divides the other and the quotient is equal to ℓ. So u has to fall into one of the types of isogenies given in Definition 7.1.4. Note that isogenies of Drinfeld modules have duals, see Definition 4.3.9. Moreover, an isogeny and its dual have the same degree as shown in Theorem 6.1.11. So the set of j-invariants of Drinfeld modules over $\mathbb{F}_\mathfrak{p}$ with characteristic polynomial $P_{\pm a,b}$ can be represented as an undirected graph. The vertices of this graph are the j-invariants (i.e., the elements of $\mathbb{F}_\mathfrak{p}$) and its edges represent the ℓ-isogenies of Drinfeld modules representing two vertices. This graph is a connected component of $G_\ell(\mathbb{F}_\mathfrak{p})$, and its shape depends on the number of roots of the modular polynomial $\Phi_\ell(j(\varphi), Y)$.

Recall from Remark 6.3.16 that if a Drinfeld module is supersingular, then any Drinfeld module isogenous to it is also supersingular. So $G_\ell(\mathbb{F}_\mathfrak{p})$ contains ordinary and supersingular components. Our concern here is to study the structure of ordinary components of $G_\ell(\mathbb{F}_\mathfrak{p})$ not containing $j = 0$. We now describe basic properties of these components. The analogue of the next lemma in the elliptic curve case is given in [Fou01, Lemma 6.1.6].

Lemma 7.2.1. *Let $u : \varphi \longrightarrow \psi$ be an ℓ-isogeny of Drinfeld modules with dual $\widehat{u}$. Then*

(a) u is horizontal if and only if $\widehat{u}$ is horizontal.

(b) u is ascending if and only if $\widehat{u}$ is descending.

Proof. This follows immediately from the definition of the dual isogeny and Lemma 7.1.3. □

Recall that the set of invertible $\mathcal{O}_\varphi$-ideals is a multiplicative group. It induces an action of $\mathcal{C}l(\mathcal{O}_\varphi)$ on the isomorphism class of Drinfeld modules with endomorphism ring $\mathcal{O}_\varphi$ in the generic characteristic case, where the action is as given in (6.13) (see Theorem 6.7.5). We can also use the same action on Drinfeld modules in the finite characteristic case by lifting them to $\mathbf{C}$. So a horizontal isogeny is obtained from the action of an invertible $\mathcal{O}_\varphi$-ideal $\mathfrak{l}$ of norm ℓ. If $\ell \mid f_\varphi$, then no such ideal exist. If $\ell \nmid f_\varphi$, then we say that $\mathcal{O}_\varphi$ is *ℓ-maximal*.

Now we examine $\mathbf{A}[F]$. If it is ℓ-maximal, i.e., $\ell \nmid f_F$, then $\mathcal{O}_\varphi$ is also ℓ-maximal since $\mathbf{A}[F] \subseteq \mathcal{O}_\varphi$. So $\ell \nmid f_\varphi$ and hence $\ell \nmid f_F/f_\varphi$. The following result follows immediately from Theorem 7.1.5. A similar result holds in the elliptic curve case, see [Fou01, Lemma 6.1.2].

Lemma 7.2.2. *Let φ be an ordinary Drinfeld module such that $\mathbf{A}[F]$ is ℓ-maximal. If there exists an ℓ-isogeny u from φ to another Drinfeld module ψ, then u is horizontal.*

Now we consider the existence of vertical (ascending or descending) isogenies. These isogenies exist if and only if $\mathbf{A}[F]$ is not ℓ-maximal, i.e., $\ell \mid f_F$. Suppose $u : \varphi \longrightarrow \psi$ is an ℓ-isogeny. Then, by Lemma 7.1.3, one of the following conditions holds:

(a) $\mathbf{A}[F] \subseteq \mathcal{O}_\psi \subset \mathcal{O}_\varphi \subseteq \mathcal{O}_\mathcal{K}$ (u is descending; $f_\psi/f_\varphi = \ell$)

(b) $\mathbf{A}[F] \subseteq \mathcal{O}_\varphi \subset \mathcal{O}_\psi \subseteq \mathcal{O}_\mathcal{K}$ (u is ascending; $f_\varphi/f_\psi = \ell$).

From these inclusions, we can determine $\nu_\ell(f_\varphi)$ or $\nu_\ell(f_\psi)$, where ν_ℓ is the ℓ-adic valuation on $\mathbf{A}$. Recall that $\nu_\ell(a) = n \in \mathbb{N}$ for $a \in \mathbf{A}$, $a \neq 0$, if $\ell^n \mid a$ but $\ell^{n+1} \nmid a$; in this case, we say that ℓ^n *exactly divides* a and denote this by $\ell^n \parallel a$. Additionally, $\nu_\ell(a) = \infty$ if $a = 0$. It is clear that $\nu_\ell(a) = 0$ if and only if $\ell \nmid a$. Consider the first case above where $f_\psi = \ell f_\varphi$. Suppose $\nu_\ell(f_F) = n$ and $\nu_\ell(f_\varphi) = m$, then $\nu_\ell(f_\psi) = m + 1$ and $\nu_\ell(f_F/f_\psi) = n - (m + 1)$.

Definition 7.2.3 (cf. Definition 2.4.7)**.** The *level* of a Drinfeld module φ (or its j-invariant $j(\varphi)$) in a connected component of an ℓ-isogeny graph is the ℓ-adic valuation $\nu_\ell(f_\varphi)$ of the endomorphism conductor f_φ.

The elliptic curve case analogue of the following lemma is given in [Fou01, Lemma 6.1.3] (see Lemma 2.4.8).

Lemma 7.2.4. *Let $\nu_\ell(f_F) = n \geq 1$. If $\ell \nmid f_F/f_\varphi$, then the unique ℓ-isogeny $u : \varphi \longrightarrow \psi$ of φ in Table 7.2 is such that $\ell \mid f_F/f_\psi$; that is, $\nu_\ell(f_\psi) = n - 1$.*

Proof. By Table 7.2, we see that the unique isogeny φ is ascending. So $f_\varphi/f_\psi = \ell$. By hypothesis, $\ell \nmid f_F/f_\varphi$, so if $\nu_\ell(f_F) = n$, then $\nu_\ell(f_\varphi) = n$. This implies that $\ell \mid (f_F/f_\psi)$. From this, we conclude that $\nu_\ell(f_\psi) = n - 1$. □

In the following lemma, let ϱ be a rank two Drinfeld module over $\mathbb{F}_\mathfrak{p}$ with $\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\varrho) = \mathcal{O}_\varrho$. The proof we present here is similar to the elliptic curve case, see [Fou01, Lemma 6.1.4]. Here, however, we can no longer treat the conductors as indices of groups because the conductors here are polynomials rather than integers.

Lemma 7.2.5. *Let $u : \varphi \longrightarrow \psi$ be a descending ℓ-isogeny and suppose $\ell \mid f_F$. If $\ell \mid f_F/f_\psi$, then for any ℓ-isogeny $v : \psi \longrightarrow \varrho$, $\mathcal{O}_\varrho \neq \mathcal{O}_\varphi$ if and only if v is descending. Moreover, there are $|\ell|$ isogenies of this type.*

Proof. By assumption, u is descending. So $f_\psi/f_\varphi = \ell$ and hence $\ell \mid f_\psi$. We combine this result with the assumption that $\ell \mid f_F/f_\psi$. By using Table 7.2, we see that ψ has one ascending and $|\ell|$ descending ℓ-isogenies and no horizontal ℓ-isogenies.

Now suppose $v : \psi \longrightarrow \varrho$ is an ascending ℓ-isogeny. Then $f_\psi/f_\varrho = \ell$. Since $f_\psi/f_\varphi = \ell$ as well, it follows that $f_\varrho = f_\varphi$, or equivalently, $\mathcal{O}_\varrho = \mathcal{O}_\varphi$.

On the other hand, if $v : \psi \longrightarrow \varrho$ is a descending ℓ-isogeny, then $f_\varrho/f_\psi = \ell$. Now $f_\psi/f_\varphi = \ell$, so $f_\varrho = \ell^2 f_\varphi$, which implies that $\mathcal{O}_\varrho \neq \mathcal{O}_\varphi$.

So any ℓ-isogeny satisfying the hypothesis of this lemma is descending and there are $|\ell|$ of these isogenies. $\square$

The following result is analogous to Lemma 2.4.10. We give a proof similar to that for the elliptic curve case, see [Fou01, Lemma 6.1.5].

Lemma 7.2.6. *Suppose $\ell \mid f_F$. If there exist two ℓ-isogenies of a Drinfeld module φ to another Drinfeld module ψ, different up to isomorphism, then these are both horizontal ℓ-isogenies. Furthermore, $\mathcal{O}_\varphi$ is ℓ-maximal and ℓ splits in $\mathcal{O}_\varphi$.*

Proof. We claim that ℓ does not divide f_φ. Suppose, on the contrary, that $\ell \mid f_\varphi$. We claim that φ has no horizontal isogenies. We prove this claim by using the relationship between ℓ and f_F/f_φ.

If $\ell \nmid f_F/f_\varphi$, then by referring to Table 7.2, we see that φ admits only one ascending ℓ-isogeny up to isomorphism. So φ has no horizontal isogenies in this case.

If, on the other hand, $\ell \mid f_F/f_\varphi$, then we see from Table 7.2 that φ has one ascending and $|\ell|$ descending ℓ-isogenies. So if there exist two ℓ-isogenies from φ to ψ, then both of these isogenies should be descending. For if one is ascending, then the other must be descending since φ admits only one ascending ℓ-isogeny. In this case we have $f_\psi/f_\varphi = \ell$ and $f_\varphi/f_\psi = \ell$, which is not possible. Upon establishing that both isogenies are descending, we see that $f_\psi/f_\varphi = \ell$. So $\mathcal{O}_\psi$ is not ℓ-maximal. Then ψ has exactly one ascending ℓ-isogeny, and if $\ell \mid f_F/f_\psi$, then Table 7.2 shows that ψ has $|\ell|$ descending ℓ-isogenies. However, we see from Lemma 7.2.1 that the duals of these descending isogenies are ascending. Note that these duals are different up to isomorphism. This contradicts the fact that ψ has only one ascending ℓ-isogeny. So ℓ cannot divide f_φ, i.e., $\mathcal{O}_\varphi$ is ℓ-maximal.

Now $\ell \nmid f_\varphi$ and $\ell \mid f_F$, so $\ell \mid f_F/f_\varphi$. In this case, $\left(\frac{D_\varphi}{\ell}\right) = \left(\frac{D_\mathcal{K}}{\ell}\right)$. From Table 7.2, we see that φ has $1 + \left(\frac{D_\mathcal{K}}{\ell}\right)$ horizontal and $|\ell| - \left(\frac{D_\mathcal{K}}{\ell}\right)$ descending ℓ-isogenies since $\ell \mid f_F$.

Similar to the scenarios considered above, we see that these two isogenies cannot be both descending or one horizontal and the other descending. Hence both must be horizontal.

Furthermore, it also follows that $\left(\frac{D_K}{\ell}\right) = 1$; that is, ℓ splits in $\mathcal{O}_\varphi$. This completes the proof. □

We use this series of lemmas to describe the ℓ-isogeny graph of ordinary Drinfeld modules with characteristic polynomial $P_{\pm a,b}$. Similar to the elliptic curve case, each ordinary connected component of $G_\ell(\mathbb{F}_\mathfrak{p})$ is an isogeny volcano (G, C) in the sense of Definition 2.4.11. The crater C consists of the ℓ-isogenies for which $\mathcal{O}_\varphi$ is ℓ-maximal and is a regular graph of degree at most 2, while the rest of the structure of G consists of isomorphism classes of Drinfeld modules for which $\mathcal{O}_\varphi$ is not ℓ-maximal. Again, we mention that G is a connected component of $G_\ell(\mathbb{F}_\mathfrak{p})$ with at most one cycle.

7.2.2 Structure of ℓ-Isogeny Volcanoes of Drinfeld Modules

As before, we assume $\ell \in \mathbf{A}^+$ is an irreducible polynomial prime to P and let $\varphi/\mathbb{F}_\mathfrak{p}$ be an ordinary Drinfeld module with j-invariant $j(\varphi) \neq 0$. Let $\mathcal{N}_\ell(\varphi)$ be the number of roots of the modular polynomial $\Phi_\ell(j(\varphi), Y)$ in $\mathbb{F}_\mathfrak{p}$. We determine some properties of $\mathcal{O}_\varphi$ using $\mathcal{N}_\ell(\varphi)$ and Table 7.2. These properties are summarized in Table 7.3.

$\mathcal{N}_\ell(\varphi)$	**Type**	**Case**	$\left(\frac{D_\varphi}{\ell}\right)$	$\left(\frac{D_F}{\ell}\right)$
0	none	$\ell \nmid f_\varphi$ and $\ell \nmid f_F/f_\varphi$	-1	-1
2	$\rightarrow$	$\ell \nmid f_\varphi$ and $\ell \nmid f_F/f_\varphi$	$+1$	$+1$
1	$\rightarrow$	$\ell \nmid f_\varphi$ and $\ell \nmid f_F/f_\varphi$	0	0
	$\uparrow$	$\ell \mid f_\varphi$ and $\ell \nmid f_F/f_\varphi$	0	0
$\lvert\ell\rvert + 1$	$1 + \left(\frac{D_\varphi}{\ell}\right)$ $\rightarrow$ $\lvert\ell\rvert - \left(\frac{D_\varphi}{\ell}\right)$ $\downarrow$	$\ell \nmid f_\varphi$ and $\ell \mid f_F/f_\varphi$	unknown	0
	1 $\uparrow$ $\lvert\ell\rvert$ $\downarrow$	$\ell \mid f_\varphi$ and $\ell \mid f_F/f_\varphi$	0	0

Table 7.3: Properties of $\mathcal{O}_\varphi$ based on the number and type of ℓ-isogenies of $\varphi/\mathbb{F}_\mathfrak{p}$

The case $\mathcal{N}_\ell(\varphi) = |\ell| + 1$

Let G be an ordinary connected component of an ℓ-isogeny graph $G_\ell(\mathbb{F}_\mathfrak{p})$, and let H be the horizontal subgraph of G; that is, H is the subgraph obtained by deleting all edges corresponding to vertical isogenies in G and vertices joined by these edges which are not in H. We give additional properties of G.

Lemma 7.2.7. *Every horizontal ℓ-isogeny in G connects two Drinfeld modules with ℓ-maximal endomorphism rings.*

Proof. Suppose G contains a horizontal ℓ-isogeny $u : \varphi \longrightarrow \psi$. Then by definition, it follows that $\mathcal{O}_\varphi = \mathcal{O}_\psi$. So the correspoding conductors of these orders are equal and must have the same ℓ-adic valuation. We see from Table 7.2 that φ admits a horizontal ℓ-isogeny only when $\ell \nmid f_\varphi$. So $\nu_\ell(f_\varphi) = 0$. □

Corollary 7.2.8. *Every horizontal ℓ-isogeny in G is at level 0.*

Proof. This immediately follows from Lemma 7.2.7 and Definition 7.2.3. □

Lemma 7.2.9. *Every cycle in $G_\ell(\mathbb{F}_\mathfrak{p})$ contains horizontal ℓ-isogenies only.*

Proof. Let C be a cycle of length $s \geq 3$ in an ℓ-isogeny graph given by the sequence

$$j(\varphi_1) \longrightarrow j(\varphi_2) \longrightarrow \cdots \longrightarrow j(\varphi_{s-1}) \longrightarrow j(\varphi_s) \longrightarrow j(\varphi_1)$$

of ℓ-isogenies of Drinfeld modules, where the $j(\varphi_i)$ are distinct for $i \in \{1, 2, \ldots, s\}$. Let $\mathcal{O}_{\varphi_i} = \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\varphi_i)$ for $i \in \{1, 2, \ldots, s\}$. Suppose C contains horizontal and non-horizontal ℓ-isogenies. Then there exists a vertex in C, say $j(\varphi_i)$ for some $i \in \{1, 2, \ldots, s\}$, that admits both a horizontal and a non-horizontal ℓ-isogeny. Consider the subgraph $j(\varphi_{i-1}) \longrightarrow j(\varphi_i) \longrightarrow j(\varphi_{i+1})$ of C where $j(\varphi_{i-1}) \longrightarrow j(\varphi_i)$ is a horizontal ℓ-isogeny and $j(\varphi_i) \longrightarrow j(\varphi_{i+1})$ is a vertical ℓ-isogeny. By Definition 7.1.4 and Lemma 7.2.7, we see that $\mathcal{O}_{\varphi_{i-1}} = \mathcal{O}_{\varphi_i}$ and $\mathcal{O}_{\varphi_{i-1}}$ and $\mathcal{O}_{\varphi_i}$ are both ℓ-maximal. Since $j(\varphi_i)$ admits a horizontal ℓ-isogeny, we see from Table

7.2 that $\ell \nmid f_{\varphi_i}$. Moreover, we also gather from Table 7.2 that if $j(\varphi_i) \longrightarrow j(\varphi_{i+1})$ is vertical, then it can only be a descending ℓ-isogeny. So by Definition 7.1.4, $\ell \mid f_{\varphi_{i+1}}/f_{\varphi_i}$. Thus $\mathcal{O}_{\varphi_{i+1}}$ is not ℓ-maximal.

We now consider the other parts of C. In particular, we first analyze the ℓ-isogeny $j(\varphi_{i+1}) \longrightarrow j(\varphi_{i+2})$.

Suppose $j(\varphi_{i+1}) \longrightarrow j(\varphi_{i+2})$ is a horizontal ℓ-isogeny. Then Definition 7.1.4 and Lemma 7.2.7 imply that $\mathcal{O}_{\varphi_{i+1}} = \mathcal{O}_{\varphi_{i+2}}$ and these endomorphism rings are both ℓ-maximal. This contradicts $\mathcal{O}_{\varphi_{i+1}}$ being not ℓ-maximal. So $j(\varphi_{i+1}) \longrightarrow j(\varphi_{i+2})$ cannot be a horizontal ℓ-isogeny.

Suppose $j(\varphi_{i+1}) \longrightarrow j(\varphi_{i+2})$ is an ascending ℓ-isogeny. Since the $j(\varphi_k)$ are distinct for $k \in \{1, 2, \ldots, s\}$, $j(\varphi_{i+1})$ admits two ascending ℓ-isogenies: $j(\varphi_{i+1}) \longrightarrow j(\varphi_{i+2})$ and the dual of $j(\varphi_i) \longrightarrow j(\varphi_{i+1})$. By referring to Table 7.2, we see that this is not possible since a Drinfeld module can only admit at most one ascending ℓ-isogeny. Thus $j(\varphi_{i+1}) \longrightarrow j(\varphi_{i+2})$ cannot be an ascending ℓ-isogeny.

Since the first two cases are not possible, we conclude that $j(\varphi_{i+1}) \longrightarrow j(\varphi_{i+2})$ is a descending ℓ-isogeny.

We do the same analysis for the remaining part of C given by the subsequence

$$j(\varphi_{i+2}) \longrightarrow j(\varphi_{i+3}) \longrightarrow \ldots \longrightarrow j(\varphi_{s-1}) \longrightarrow j(\varphi_s) \longrightarrow j(\varphi_1) \longrightarrow \cdots \longrightarrow j(\varphi_{i-1})$$

of ℓ-isogenies. We obtain the same result for each of these isogenies; that is, each ℓ-isogeny in this subsequence is descending. In particular, the ℓ-isogeny $j(\varphi_{i-2}) \longrightarrow j(\varphi_{i-1})$ is descending. So $\ell \mid f_{\varphi_{i-1}}/f_{\varphi_{i-2}}$, which implies that $\mathcal{O}_{\varphi_{i-1}}$ is not ℓ-maximal. But note that $\mathcal{O}_{\varphi_i} = \mathcal{O}_{\varphi_{i-1}}$, so $\mathcal{O}_{\varphi_i}$ is also not ℓ-maximal. This is a contradiction. Hence all the ℓ-isogenies contained in C are horizontal. □

In what follows, we assume that $\mathbf{A}[F]$ is not ℓ-maximal and $\mathcal{N}_\ell(\varphi) = |\ell| + 1$.

Lemma 7.2.10. *Let H be the horizontal subgraph of G. If H has size at least 3, then H is a simple cycle and is the unique cycle in G.*

Proof. Suppose that size$(H) = s \geq 3$. Then H must be a series of ℓ-isogenies of Drinfeld modules

$$j(\varphi_1) \longrightarrow j(\varphi_2) \longrightarrow \cdots \longrightarrow j(\varphi_{s-1}) \longrightarrow j(\varphi_s) \longrightarrow j(\varphi_{s+1}),$$

where each $j(\varphi_i) \longrightarrow j(\varphi_{i+1})$ is a horizontal ℓ-isogeny for $i \in \{1, 2, \ldots, s\}$. Let $j(\varphi) \in H$, so $j(\varphi)$ is one of the $j(\varphi_i)$ in the series. By Lemma 7.2.7, $\mathcal{O}_\varphi$ is ℓ-maximal. In this case, $\ell \nmid f_\varphi$. By assumption, $\mathbf{A}[F]$ is not ℓ-maximal. So it follows that $\ell \mid f_F/f_\varphi$.

If $\ell \nmid f_\varphi$ and $\ell \mid f_F/f_\varphi$, then we obtain three possibilities for Drinfeld modules based on Table 7.2. These are shown in Figure 7.2. Since $s \geq 3$, the case given in Figure 7.2(c) must hold. So $j(\varphi)$ admits two horizontal ℓ-isogenies. This is also the case for each $j(\varphi_i)$ in H. In particular, $j(\varphi_{s+1})$ admits two horizontal ℓ-isogenies. But size$(H) = s$, so $j(\varphi_{s+1}) = j(\varphi_1)$ and the $j(\varphi_i)$ are distinct for $i = 1, 2, \ldots, s$. So H is a simple cycle.

For uniqueness, suppose H' is another cycle in G, where H' is of size at least 3. By Lemma 7.2.9, H' consists of horizontal ℓ-isogenies only. Recall that H is the horizontal subgraph of G, this implies that the edge set of H' is a subset of the edge set of H. Since H' is a cycle, it is connected and so it has no isolated vertices. Hence, its vertex set is also a subset of the vertex set of H. It follows that H' is a subgraph of H, and hence, H' is a subcycle of H. But the only subcycle of a cycle is itself. This implies that $H' = H$. □

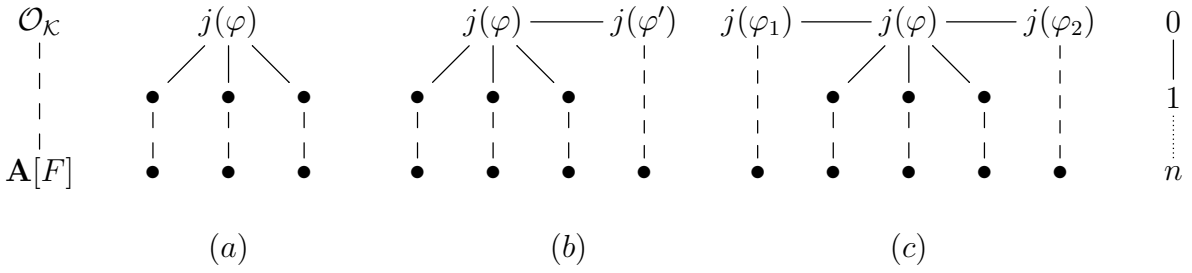


Figure 7.2: Drinfeld modules such that $\ell \nmid f_\varphi$ and $\ell \mid f_F/f_\varphi$

Corollary 7.2.11. *Any ordinary connected component of $G_\ell(\mathbb{F}_\mathfrak{p})$ is a volcano with its horizontal subgraph as its crater.*

As in the elliptic curve case, we call any connected component of $G_\ell(\mathbb{F}_\mathfrak{p})$ an *ℓ-isogeny volcano*. We can determine the type of the crater of a volcano in terms of the decomposition of ℓ in the maximal order $\mathcal{O}_\mathcal{K}$ of an imaginary quadratic function field $\mathcal{K}$.

Remark 7.2.12. As we have seen in part (1) of Theorem 7.1.5, the number of invertible $\mathcal{O}_\varphi$-ideals that give rise to horizontal ℓ-isogenies is

$$1 + \left(\frac{D_\mathcal{K}}{\ell}\right) = \begin{cases} 0, & \text{if } \ell \text{ is inert in } \mathcal{O}_\mathcal{K} \\ 1, & \text{if } \ell \text{ is ramified in } \mathcal{O}_\mathcal{K} \\ 2, & \text{if } \ell \text{ splits in } \mathcal{O}_\mathcal{K}. \end{cases}$$

Lemma 7.2.13. *The crater of an isogeny volcano can be one of the following:*

1. *a simple cycle*
2. *a double edge*
3. *a single vertex with two loops*
4. *a single vertex with a loop*
5. *a simple edge*
6. *a single vertex with no loops*

Proof. The first three forms are obtained when ℓ splits in $\mathcal{O}_\mathcal{K}$. See Table 7.2, Lemma 7.2.10, and the preceding remark. If ℓ is ramified in $\mathcal{O}_\mathcal{K}$, then there is only one horizontal ℓ-isogeny (see Table 7.2) and so the crater either a single vertex with a loop or a simple edge. Finally, if ℓ is inert in $\mathcal{O}_\mathcal{K}$, then there are no horizontal isogenies (see Table 7.2). So the crater must be a single vertex with no loops. □

Lemma 7.2.14. *Let $G \subset G_\ell(\mathbb{F}_\mathfrak{p})$ be an isogeny volcano with crater H and $\varphi/\mathbb{F}_\mathfrak{p}$ a Drinfeld module such that $j(\varphi) \in H$. If H is a simple cycle, then the size of H is the order of the ideal class of $\mathfrak{l}$ in $\mathcal{C}l(\mathcal{O}_\varphi)$, where $\mathfrak{l}$ is a prime ideal of norm ℓ in $\mathcal{O}_\varphi$.*

Proof. First we recall that an invertible fractional $\mathcal{O}_\varphi$-ideal $\mathfrak{a}$ can be considered as lattice in $\mathbf{C}$ via the embedding $\mathfrak{a} \subset \mathcal{K} \subset \mathbf{C}$. Now suppose H is a simple cycle of length s. Let $\widetilde{\varphi}_0$ be canonical lift of $\varphi/\mathbb{F}_\mathfrak{p}$ to $\mathbf{C}$, so $\widetilde{\varphi}_0$ is associated to a lattice $\mathfrak{a}_0$ whose order is $\mathcal{O}_\varphi$, where $\mathfrak{a}_0$ is an invertible fractional $\mathcal{O}_\varphi$-ideal. We consider the canonical lift of each Drinfeld module in H to $\mathbf{C}$. Then we get the cycle

$$\widetilde{\varphi}_0 \longrightarrow \widetilde{\varphi}_1 \longrightarrow \cdots \longrightarrow \widetilde{\varphi}_s \simeq \widetilde{\varphi}_0,$$

where $\widetilde{\varphi}_i$ is the Drinfeld module associated to the (ideal) lattice $\mathfrak{a}_i$ whose order is also $\mathcal{O}_\varphi$ since $\widetilde{\varphi}_i$ is also in H. Since each of the isogenies in this cycle is an ℓ-isogeny, it follows that $\mathfrak{a}_i = \mathfrak{a}_{i+1}\mathfrak{l}$ where $\mathfrak{l}$ is a prime ideal of norm ℓ in $\mathcal{O}_\varphi$. This implies that

$$\mathfrak{a}_0 = \mathfrak{a}_s\mathfrak{l}^s.$$

As $\widetilde{\varphi}_s \simeq \widetilde{\varphi}_0$, they have the same j-invariant. We see from Remark 5.4.2 that $\mathfrak{a}_0$ and $\mathfrak{a}_s$ are homothetic lattices in $\mathbf{C}$. So $\mathfrak{a}_0$ and $\mathfrak{a}_s$ are equivalent as ideals and it follows that $\mathfrak{l}^s$ is a principal ideal of $\mathcal{O}_\varphi$. We claim that s is the least positive integer k such that $\mathfrak{l}^k$ is principal. Suppose there exists an integer $i < s$ such that $\mathfrak{l}^i$ is principal. Then $\mathfrak{a}_0$ and $\mathfrak{a}_i$ are homothethic and hence have the same j-invariant. This results in a subcycle of H of length $i < s$, which contradicts the fact that H length s. Therefore s is the order in the class of $\mathfrak{l}$ in $\mathcal{C}l(\mathcal{O}_\varphi)$. □

Remark 7.2.15. The inert, ramified, and split scenarios for ℓ correspond to the order of the ideal class of $\mathfrak{l}$ being 1, 2, or at least 3, which corresponds to one, two, or more than two elements in each coset of $\mathcal{C}l(\mathcal{O}_\varphi)/\langle\mathfrak{l}\rangle$. This in turn, corresponds to the two-loop vertex, double edge, and simple cycle shape of the horizontal subgraph. We saw in Section 2.4 that this is also the case for ordinary elliptic curves over finite fields.

Lemma 7.2.16. *Suppose $\nu_\ell(f_F) \geq 1$. If ℓ splits (respectively, ramifies, or is inert) in $\mathcal{O}_\mathcal{K}$, then every vertex in the crater of an isogeny volcano admits $|\ell|-1$ (respectively, $|\ell|$, or $|\ell|+1$) descending ℓ-isogenies.*

Proof. Let $j(\varphi)$ be a vertex in the crater of an isogeny volcano. Then the endomorphism ring $\mathcal{O}_\varphi$ of φ is ℓ-maximal. As in the proof of Lemma 7.2.10, we see that $\ell \nmid f_\varphi$ and $\ell \mid f_F/f_\varphi$. So, by Table 7.3, φ has $1 + \left(\frac{D_\mathcal{K}}{\ell}\right)$ horizontal and $|\ell| - \left(\frac{D_\mathcal{K}}{\ell}\right)$ descending ℓ-isogenies. So if ℓ splits in $\mathcal{O}_\mathcal{K}$, then φ admits two horizontal and $|\ell| - 1$ descending ℓ-isogenies. If ℓ ramifies in $\mathcal{O}_\mathcal{K}$, then φ admits one horizontal and $|\ell|$ descending ℓ-isogenies. If ℓ is inert in $\mathcal{O}_\mathcal{K}$, then φ has no horizontal ℓ-isogenies, and $|\ell| + 1$ descending ℓ-isogenies. □

Definition 7.2.17 (cf. Definition 2.4.13)**.** The valuation $n := \nu_\ell(f_F)$ is called the *height* of an ℓ-isogeny volcano of Drinfeld modules. All Drinfeld modules at level n make up the *floor* of the isogeny volcano.

Similar to the elliptic curve case, we can detect whether or not a vertex lies on the floor of an isogeny volcano. We count the number of edges coming from $j(\varphi)$, i.e., the number of roots of the modular polynomial $\Phi_\ell(j(\varphi), Y)$ in $\mathbb{F}_\mathfrak{p}$ counted with multiplicity. If $n = 0$, the crater coincides with the floor of the volcano. So $j(\varphi)$ has degree at most 2. If $n > 0$, then $\mathbf{A}[F]$ is not ℓ-maximal. Accordingly, we see from Table 7.2 that $j(\varphi)$ is of degree 1 or $|\ell| + 1$. So if $j(\varphi)$ is on the floor, it only admits one ℓ-isogeny. Therefore, we have shown the following result.

Lemma 7.2.18. *If a vertex j is on the floor of an isogeny volcano, then it has degree 1 except when the isogeny volcano is the crater only.*

In the following results, we note that if the height $\nu_\ell(f_F)$ of an isogeny volcano G is at least one, then G is not equal to its crater.

Lemma 7.2.19. *Let G be an isogeny volcano of height $n \geq 1$. Then all descending ℓ-isogenies of G have pairwise distinct targets.*

Proof. Suppose there exist two distinct descending ℓ-isogenies from level k of G, $0 \leq k < n$, with the same target, say $u_1 : j(\varphi_1) \longrightarrow j(\varphi_3)$ and $u_2 : j(\varphi_2) \longrightarrow j(\varphi_3)$. Then $f_{\varphi_3}/f_{\varphi_1} = \ell$ and $f_{\varphi_3}/f_{\mathcal{O}_{\varphi_2}} = \ell$. In either case, $\mathcal{O}_{\varphi_3}$ is not ℓ-maximal. By Lemma 7.2.1, the duals of u_1 and

u_2 are both ascending. Then φ_3 admits two ascending ℓ-isogenies which are different up to isomorphism. By Table 7.2, however, we see that φ_3 can only have one ascending ℓ-isogeny. Thus no two descending isogenies in G have the same target. □

Corollary 7.2.20. *Let G be a volcano of height $n \geq 1$. Then the sides (as defined in Definition 2.4.11) of G do not contain cycles, multiple edges, or loops, and are hence trees with roots on the crater.*

Let G be a volcano of height $n \geq 1$. We can traverse G by creating paths from a vertex j of G. By a *path*, we mean a sequence of distinct vertices in G. So backtracking is not allowed. Similar to the elliptic curve case, we can create descending and ascending paths from j.

Definition 7.2.21. We call a sequence of j-invariants of ℓ-isogenous Drinfeld modules

$$j(\varphi) = j(\varphi_0) \longrightarrow j(\varphi_1) \longrightarrow \cdots \longrightarrow j(\varphi_m) \tag{7.5}$$

a *descending path* if each edge $j(\varphi_i) \longrightarrow j(\varphi_{i+1})$, for $i = 0, 1, \ldots, m-1$, represents a descending ℓ-isogeny and $\ell \nmid f_F/f_{\varphi_m}$. It is a *maximal descending path* if $\nu_\ell(f_{\varphi_0}) = 0$. In this case, $j(\varphi_0)$ is on the crater of G. Next, we call a sequence of j-invariants of ℓ-isogenous Drinfeld modules

$$j(\varphi) = j(\varphi_0) \longrightarrow j(\varphi_{-1}) \longrightarrow \cdots \longrightarrow j(\varphi_{-m}) \tag{7.6}$$

an *ascending path* if each edge $j(\varphi_{-i}) \longrightarrow j(\varphi_{-(i+1)})$, for $i = 0, 1, \ldots, m-1$, represents an ascending ℓ-isogeny. It is a *maximal ascending path* if $\nu_\ell(f_{\varphi_0}) = n$. In this case, $j(\varphi_0)$ is on the floor of G.

For the next result, we use the same convention for counting degrees of vertices in a volcano as in the elliptic curve case, see Section 2.4. We still continue to assume that $\mathbf{A}[F]$ is not ℓ-maximal.

Theorem 7.2.22. *Let $G_\ell(\mathbb{F}_\mathfrak{p})$ be the ℓ-isogeny graph of Drinfeld modules over $\mathbb{F}_\mathfrak{p}$ and $\varphi/\mathbb{F}_\mathfrak{p}$ an ordinary Drinfeld module with $j(\varphi) \neq 0$. Then the connected component of $G_\ell(\mathbb{F}_\mathfrak{p})$ containing $j(\varphi)$ with horizontal subgraph H is a volcano G, all of whose sides are maximal trees and with internal vertices all of degree $|\ell| + 1$.*

Proof. Note that each side of G is a tree, since it is a connected graph with no cycles. See Corollary 7.2.20. What remains to be shown is that each tree descending from a root in the crater is a maximal tree (i.e. all leaves are at the same level) and all of its internal vertices are of degree $|\ell| + 1$.

Consider an arbitrary tree in G, say T, with root $j(\varphi_0)$ in H. If ℓ splits in $\mathcal{O}_\mathcal{K}$, then $j(\varphi_0)$ is in a cycle or in a double edge, or it is a vertex with two loops. We see from Table 7.3 that $j(\varphi_0)$ admits two horizontal and $|\ell| - 1$ descending ℓ-isogenies. Also from Lemma 7.2.16, we see that if ℓ ramifies in $\mathcal{O}_\mathcal{K}$ (i.e. the crater is a simple edge), then $j(\varphi_0)$ admits one horizontal and $|\ell|$ descending ℓ-isogenies. Now, if ℓ is inert in $\mathcal{O}_\mathcal{K}$ (i.e the crater is a single vertex without loops), then $j(\varphi_0)$ has no horizontal and $|\ell| + 1$ descending ℓ-isogenies. All of these possibilities show that $j(\varphi_0)$ admits $|\ell| + 1$ ℓ-isogenies.

Now take an internal vertex of T different from $j(\varphi_0)$, say $j(\varphi)$, and suppose $j(\varphi)$ is at level $k \neq 0$ of G. Then $\ell \mid f_\varphi$. By assumption, $\mathbf{A}[F]$ is not ℓ-maximal. Thus $\ell \mid f_F/f_\varphi$. So we have the case shown in Figure 7.3. Referring to Table 7.2, we see that φ admits one ascending and $|\ell|$ descending ℓ-isogenies. Hence $j(\varphi)$ is also of degree $|\ell| + 1$.

Finally, we determine the level of each leaf of T. Let $j(\varphi_m)$ be a leaf of T. We take a descending path of ℓ-isogenies

$$j(\varphi_0) \longrightarrow j(\varphi_1) \longrightarrow j(\varphi_2) \longrightarrow \cdots \longrightarrow j(\varphi_{m-1}) \longrightarrow j(\varphi_m),$$

where $j(\varphi_0)$ is the root of T. So this path is a maximal descending path of length m. By Definition 7.2.21, we know that $\ell \nmid f_F/f_{\varphi_m}$. Moreover, $j(\varphi_m)$ is a leaf, so its endomorphism ring $\mathcal{O}_{\varphi_m}$ is not ℓ-maximal. This means that if the height of the volcano is n, then $j(\varphi_m)$

is at level n and so $m = n$. So each leaf of T is at level n. This completes the proof of the theorem. □

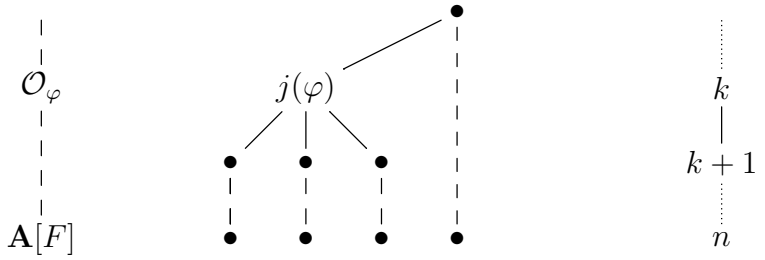


Figure 7.3: Drinfeld module φ such that $\ell \mid f_\varphi$ and $\ell \mid f_F/f_\varphi$

The next series of results can be used to locate a Drinfeld module in an isogeny volcano. These results are analogous to those in the elliptic curve case (see Lemmas 2.4.19, 2.4.20, and 2.4.22). We adapt the proofs given for elliptic curves, see [Fou01, Lemmas 6.2.1, 6.2.2, and 6.2.4].

Lemma 7.2.23. *Consider the descending path given in* (7.5)*. If $j(\varphi)$ is at level k, then $j(\varphi_i)$ is at level $k + i$.*

Proof. We use induction to prove this result. Clearly, the base case $i = 0$ holds. Let $j(\varphi)$ be at level k and suppose the result is true for integers $0 \leq s < k$. Note that each $j(\varphi_s) \longrightarrow j(\varphi_{s+1})$ is a descending ℓ-isogeny. By the inductive hypothesis, $j(\varphi_s)$ is located at level $k+s$, so $\ell^{k+s} \parallel f_{\varphi_s}$. Since $j(\varphi_s) \longrightarrow j(\varphi_{s+1})$ is descending, it follows that $\ell^{k+s+1} \parallel f_{\varphi_{s+1}}$. So $j(\varphi_{s+1})$ is at level $k + (s + 1)$. □

Lemma 7.2.24. *Let φ be a Drinfeld module and let G be an ℓ-isogeny volcano of Drinfeld modules containing $j(\varphi)$. Let P be a descending path of length m starting from $j(\varphi)$. If G is of height n, then $j(\varphi)$ is at level $n - m$.*

Proof. Let $j(\varphi)$ be at level k of G. Since P is descending and starts at $j(\varphi)$, it is of the form given in (7.5). By Lemma 7.2.23, φ_m is located at level $k+m$. By definition of a descending

path, we know that $\ell \nmid f_F/f_{\varphi_m}$. In other words, if the height of the volcano is n, then φ_m is at level n. It follows that $n = k + m$, so $k = n - m$. □

Lemma 7.2.25. *Let G be an ℓ-isogeny volcano of Drinfeld modules. Let $P \subset G$ be an ascending path starting at $j(\varphi) \in G$. If $j(\varphi)$ is at level k, then $j(\varphi_{-i})$ is at level $k - i$.*

Proof. The proof is similar to that of Lemma 7.2.24 using the sequence (7.6). □

What we have done so far is to determine the behaviour of an isogeny volcano when $\mathcal{N}_\ell(\varphi) = |\ell| + 1$, where $\mathcal{N}_\ell(\varphi)$ is the number of roots of the polynomial $\Phi_\ell(j(\varphi), Y)$ in $\mathbb{F}_\mathfrak{p}$. In this case, $\mathbf{A}[F]$ is not ℓ-maximal and $j(\varphi)$ can either be a vertex on the crater or on the side but not on the floor of a volcano. We now consider the case $\mathcal{N}_\ell(\varphi) \neq |\ell| + 1$.

The case $\mathcal{N}_\ell(\varphi) \neq |\ell| + 1$

1. $\mathcal{N}_\ell(\varphi) = 0$. It is clear from Table 7.2 that $\varphi/\mathbb{F}_\mathfrak{p}$ admits no ℓ-isogeny and ℓ is inert in $\mathcal{O}_\mathcal{K}$. Moreover, $\ell \nmid f_F$ so $\mathbf{A}[F]$ is ℓ-maximal. The resulting graph is just the vertex $j(\varphi)$.

2. $\mathcal{N}_\ell(\varphi) = 1$. In this case, $\varphi/\mathbb{F}_\mathfrak{p}$ admits only one ℓ-isogeny. As shown in Table 7.2, this isogeny can be horizontal or ascending. So $\mathbf{A}[F]$ may or may not be ℓ-maximal. Let $u : \varphi \longrightarrow \psi$ be the single isogeny of $\varphi/\mathbb{F}_\mathfrak{p}$. Consider the following cases:

   (a) $\mathcal{N}_\ell(\psi) = 1$. Suppose that $\mathbf{A}[F]$ is not ℓ-maximal i.e., $\ell \mid f_F$. Then $\ell \mid f_\varphi$ and $\ell \nmid f_F/f_\varphi$. Then u is ascending (see Table 7.2). It follows from Lemma 7.2.4 that $\ell \mid f_F/f_\psi$. Then $\mathcal{N}_\ell(\psi) = |\ell| + 1$ (see Table 7.3), which leads to a contradiction. So $\mathbf{A}[F]$ must be ℓ-maximal and u is horizontal. The resulting graph is therefore a simple edge. We can also see from Table 7.2 that ℓ ramifies in $\mathcal{O}_\mathcal{K}$.

   (b) $\mathcal{N}_\ell(\psi) = |\ell| + 1$. Suppose that $\mathbf{A}[F]$ is ℓ-maximal, i.e., $\ell \nmid f_F$. Then $\ell \nmid f_\varphi$ and $\ell \nmid f_F/f_\varphi$. Table 7.3 shows that u is a horizontal isogeny and $\left(\frac{D_\varphi}{\ell}\right) = 0$. So $f_\psi = f_\varphi$. It follows that $\ell \nmid f_\psi$, $\ell \nmid f_F/f_\psi$ and $\left(\frac{D_\psi}{\ell}\right) = 0$. This implies that

$\mathcal{N}_\ell(\psi) = 1 + \left(\frac{D_\psi}{\ell}\right) = 1$, which is a contradiction. So $\mathbf{A}[F]$ is not ℓ-maximal and u is ascending. In this case, we see from Table 7.3 that ℓ ramifies in $\mathcal{O}_\mathcal{K}$ and φ is a leaf on a side.

3. $\mathcal{N}_\ell(\varphi) = 2$. Table 7.3 shows that ℓ splits in $\mathcal{O}_\mathcal{K}$ and $\mathbf{A}[F]$ is ℓ-maximal since $\ell \nmid f_F$. By Lemma 7.2.2, any ℓ-isogeny in this case is horizontal. So the resulting graph is a simple cycle.

7.2.3 Components containing $j = 0$

We give a separate (but brief) treatment for connected components of $G_\ell(\mathbb{F}_\mathfrak{p})$ containing $j(\varphi) = 0$. We mention the reasons behind this.

If $\varphi/\mathbb{F}_\mathfrak{p}$ has j-invariant $j(\varphi) = 0$ and $\deg_T(P)$ is even, then its endomorphism ring is already known to be isomorphic to $\mathbb{F}_{q^2}[T]$ (see [BK92]). Moreover, recall from Proposition 6.5.4 that φ has extra automorphisms. So we cannot distinguish Drinfeld modules which are isogenous to φ over $\mathbb{F}_\mathfrak{p}$ or from those which are isogenous to φ over some algebraic closure of $\mathbb{F}_\mathfrak{p}$.

It is also known that $\varphi/\mathbb{F}_\mathfrak{p}$ with j-invariant $j(\varphi) = 0$ is supersingular when $\deg_T(P(T))$ is odd, and ordinary when $\deg_T(P(T))$ is even (see [Gek83]). Note that we have completely excluded supersingular components from the beginning of this chapter.

Chapter 8

Algorithms and Computational Results

This chapter is devoted to the computational aspects of this research. We present algorithms for computing j-invariants, modular polynomials, and isogeny volcanoes for rank two Drinfeld modules, and establish the complexity of each algorithm in terms of operations in $\mathbb{F}_q$. Then we conclude this chapter with some examples of computing endomorphism rings and explicit isogenies of Drinfeld modules. All the results presented here are new, unless otherwise stated.

Notation:

$$\begin{aligned}
\mathbf{A}[[s]] &= \text{ring of formal power series in } s \text{ with coefficients in } \mathbf{A} \\
\mathbf{A}^+ &= \{\text{monic polynomials in } \mathbf{A}\} \\
\mathbf{A}_m^+ &= \{a \in \mathbf{A}^+ \mid \deg_T(a) = m\} \\
\mathbf{A}_{\leq m}^+ &= \{a \in \mathbf{A}^+ \mid \deg_T(a) \leq m\} \\
P &= P(T) \in \mathbf{A}^+ \text{ irreducible with } \deg_T(P) = d > 1 \\
\mathfrak{p} &= (P(T)) \\
\mathbb{F}_\mathfrak{p} &= \mathbf{A}/\mathfrak{p} = \text{an } \mathbf{A}\text{-field equipped with structure morphism } \gamma : \mathbf{A} \longrightarrow \mathbb{F}_\mathfrak{p} \\
\varphi, \psi &= \text{rank two Drinfeld modules from } \mathbf{A} \text{ to } \mathbb{F}_\mathfrak{p}\{\tau\}
\end{aligned}$$

8.1 Polynomial Operations

In this section we present some preliminaries on how we count the number of operations required to run an algorithm. Our end goal is to express the cost of an algorithm in terms of operations in the finite field $\mathbb{F}_q$, where q is a power of a prime $p \in \mathbb{Z}$.

The algorithms that we present in the succeeding sections involve polynomials over co-

efficient rings $\mathbb{F}_q$, $\mathbb{F}_\mathfrak{p}$, or $\mathbf{A}$. If the coefficients are also polynomials themselves, we also take into account in our analysis the size (in terms of degrees) of the coefficients involved and the number of arithmetic operations required on these coefficients. In this section we use $\mathcal{R}$ to denote a generic coefficient ring, and specify it as the need arises. We assume that $\mathcal{R}$ is a unique factorization domain.

The operations that we require on the polynomials involved in the algorithms include addition, subtraction, multiplication, division, raising to powers, evaluation, and root-finding. Table 8.1 summarizes the the required operations for the algorithms in this chapter.

Algorithm	**Operations on Polynomials**
Algorithm 8.2.11	addition/subtraction, multiplication, division, and raising to powers
Algorithm 8.3.2	addition/subtraction, multiplication, and raising to powers
Algorithm 8.4.1	polynomial evaluation and root-finding
Algorithm 8.5.1	polynomial evaluation and root-finding
Algorithm 8.5.4	addition, multiplication, raising to powers, and root-finding
Algorithm 8.5.7	addition, multiplication, and raising to powers

Table 8.1: Required polynomial operations for algorithms

It is known that addition of two polynomials of degree at most n with coefficients in $\mathcal{R}$ costs at most $n+1$ or $O(n)$ $\mathcal{R}$-operations as $n \longrightarrow \infty$. Subtraction costs the same as addition. Now let f and g be polynomials over $\mathcal{R}$ of degrees n and m, respectively. Let $M(n,m)$ be the number of $\mathcal{R}$-operations required to multiply f and g. Let $M(n) = M(n,n)$. Naive (or schoolbook) multiplication costs nm additions and $(n+1)(m+1)$ multiplications, giving a total cost of $M(n,m) = 2nm + n + m + 1$ $\mathcal{R}$-operations. So multiplying two polynomials of degree at most n costs $2n^2 + 2n + 1$ or $O(n^2)$ $\mathcal{R}$-operations in the naive way. See, for example, [vzGG03], p. 33. Using fast multiplication techniques, the cost of multiplying two polynomials of degree at most n can be decreased to $O(n \log n)$ ([vzGG03, Corollary 8.19]) via the Fast Fourier Transform (FFT) algorithm or to $O(n \log n \log\log n)$ or $O^\sim(n)$ $\mathcal{R}$-operations ([vzGG03, Theorem 8.22]) using the Schönhage-Strassen algorithm, where the $O^\sim$ notation is used to suppress logarithmic factors ($h = O^\sim(n)$ means $h = O(n(\log n)^k)$ for

some constant k). As for division, we assume that g is monic and $n \geq m \geq 0$. Dividing f by g using naive division (with remainder) costs at most $2m(n-m+1) = 2m(\deg(Q)+1)$ additions and multiplications in $\mathcal{R}$, where Q is the quotient when f is divided by g. In many applications $n < 2m$, so the cost of division is at most $2m^2 + O(m)$ $\mathcal{R}$-operations. This is basically the same as multiplying two polynomials of degree at most m in the naive way. See [vzGG03], p. 38. The cost of division (with remainder) can be improved to $O(M(m))$ $\mathcal{R}$-operations using Newton iteration (see [vzGG03, Theorem 9.6]). Clearly, multiplication and division are more expensive than addition and subtraction.

As for raising to powers, we have to consider the type of powers required. We have to raise polynomials to the q-th power in Algorithm 8.2.11. If $\mathcal{R} = \mathbb{F}_q$, then $f(T)^q = f(T^q)$ for $f(T) \in \mathcal{R}[T]$ since the (additive) q-th power map fixes elements of $\mathbb{F}_q$. So, in this case, we only need to shift the exponents of the variable T in $f(T)$. If $\mathcal{R} = \mathbf{A}$, then $g(X)^q = \sum_{i=0}^{n} g_i(T^q)X^{qi}$ for $g(X) \in \mathbf{A}[X]$. Again, we only have to shift the degrees of the variables in this case. In Algorithm 8.3.2 we have to raise polynomials to the e-th power for all integers $2 \leq e \leq k$, $k \in \mathbb{N}$. We need the coefficients of each power $g(X)^e$, so we have to use repeated multiplication to determine the products $g(X)^2 = g(X)g(X), g(X)^3 = g(X)^2g(X), \ldots, g(X)^k = g(X)^{k-1}g(X)$. The product $g(X)^{e-1}g(X)$ requires $M((e-1)\deg(g(X)), \deg(g(X))$ $\mathcal{R}$-operations for $e = 2, \ldots, k$. As for Algorithms 8.5.4 and 8.5.7, we have to raise elements of $\mathbb{F}_{\mathfrak{p}}$ to the q^i-th power for some $i \in \mathbb{N}$, i.e., we compute the i-th iterate of the Frobenius map. Note that we can treat the elements of $\mathbb{F}_{\mathfrak{p}}$ as polynomials of degree at most d by using a polynomial basis to represent elements in $\mathbb{F}_{\mathfrak{p}}$. It was shown in [GP02, Section 3] that computing α^{q^i}, for $\alpha \in \mathbb{F}_{\mathfrak{p}}$ and a positive integer i, using a $d \times d$ matrix costs $d(d-1)$ multiplications and $(d-1)^2$ additions in $\mathbb{F}_q$. This complexity is roughly the same as one multiplication in $\mathbb{F}_{\mathfrak{p}}$ (or $d^2 + O(d)$ $\mathbb{F}_q$-multiplications) assuming no fast convolution techniques are implemented in $\mathbb{F}_q$. In some special types of finite fields, this complexity can be improved to $O(d)$ operations in $\mathbb{F}_q$, see for example [HMV04, Section

2.4.3].

Lemma 8.1.1. *Raising an element of $\mathbb{F}_\mathfrak{p}$ to the q^i-th power for $i \in \mathbb{N}$ costs $O(M(d))$ $\mathbb{F}_q$-multiplications as $d \longrightarrow \infty$.*

To determine the cost of $\mathbb{F}_\mathfrak{p}$-operations in terms of $\mathbb{F}_q$-operations, we use the following results.

Lemma 8.1.2. *Let $P \in \mathbf{A}^+$ with $\deg_T(P) = d$. One multiplication in $\mathbb{F}_\mathfrak{p} = \mathbf{A}/(P)$ costs $O(M(d))$ arithmetic operations in $\mathbb{F}_q$ as $d \longrightarrow \infty$.*

Proof. See [vzGG03, Corollary 9.7]. □

Similarly, we have the following result for division (see [vzGG03], p. 258).

Lemma 8.1.3. *Under the same hypothesis in Lemma 8.1.2, one division in $\mathbb{F}_\mathfrak{p}$ costs $O(M(d))$ $\mathbb{F}_q$-operations as $d \longrightarrow \infty$.*

Next, we consider the cost of polynomial evaluation in Algorithms 8.4.1 and 8.5.1 for polynomials over a coefficient ring $\mathcal{R}$. We can use Horner's method to evaluate a polynomial of degree n using $O(n)$ operations in $\mathcal{R}$ (n multiplication and n additions, minus one addition for each zero coefficient), see [Knu81], p. 467. This is asymptotically faster than any multiplication algorithm.

Let $R(n)$ be the number of operations required to compute all the roots in $\mathcal{R}$ of a degree n polynomial $f(X) \in \mathcal{R}[X]$. We let $\mathcal{R} = \mathbb{F}_\mathfrak{p}$ in this case since we only need to find roots of polynomials over $\mathbb{F}_\mathfrak{p}$ for Algorithms 8.4.1, 8.5.1, and 8.5.4. A probabilistic root-finding algorithm given in [Rab80] finds all roots of a degree n polynomial over $\mathcal{R}$ using $O(dn \log n \log\log n \log q)$ or $O^\sim(dn \log q)$ $\mathcal{R}$-operations by letting q^d take the place of p^n in his formula. This algorithm finds the roots of $f(X)$ by computing a sequence of greatest common divisors

$$h_1(X) = \gcd(f(X), X^{q^d-1} - 1), f_2(X) = \gcd(h_1(X), X^{\frac{q^d-1}{2}} - 1), \ldots,$$

until a linear factor of $f(X)$ is found. We can bound $R(n)$ using the complexity of Rabin's algorithm.

8.2 Computation of j-invariants

The results we present in this section apply to any prime power $q \in \mathbb{Z}$. As we saw in Chapter 5, the j-invariant is the key element in the construction of modular polynomials for Drinfeld modules. We mention that the resulting coefficients of the Eisenstein series E_k in this case are more complicated than the function $\sigma_k(n)$ in the classical case (see (2.11)). These coefficients involve the polynomials given in (5.19), (5.23), and (5.32). So computing the Laurent series expansion of the j-invariant in the Drinfeld module case is quite difficult. This is in contrast to the elliptic curve case where this is fairly easy.

In order to obtain j, we require computations involving formal power series up to a certain precision. Generically, we let this precision be $\mathcal{N}$. By computing to precision $\mathcal{N}$ here, we mean to say that for a power series

$$P(s) = \sum_{i=0}^{\infty} p_i s^i \in \mathbf{A}[[s]],$$

we compute the coefficients of s^i, $i = 0, 1, \ldots, \mathcal{N}$, in P. In other words, we want to determine the truncated series

$$P(s) \pmod{s^{\mathcal{N}+1}}.$$

Let

$$P_{\mathcal{N}}(s) := \sum_{i=0}^{\mathcal{N}} p_i s^i.$$

For the precision of j, we specifically use N to denote this precision, where $N \in \mathbb{N}$. Our goal in this section is to develop an algorithm for computing the j-invariant to precision N. Since j is a Laurent series in s (see (5.40)), by computing j to precision N, we mean computing

$$sj \in \mathbf{A}[[s]] \pmod{s^{N+2}}.$$

As we can see from Definition 5.4.1, we can compute the quotient g^{q+1}/Δ to determine the j-invariant, where g and Δ are given in (5.38) and (5.39), respectively. Recall t_a as given in (5.33). The series expansions of g and Δ involve t_a for polynomials $a \in \mathbf{A}^+$, and t_a is a power series in $t = t(z)$ (see (5.31)) with coefficients in $\mathbf{A}$. As in Section 5.4, let $s = t^{q-1}$. So we consider g and Δ as formal power series in s. Here we determine up to what precision g and Δ should be computed for the calculation of the s-expansion of j to precision N. This approximation of the j-invariant will be used to compute modular polynomials in the next section.

In order to determine the s-expansions for g and Δ, we need to compute t_a^{q-1}, $t_a^{q^2-q}$, and $t_a^{q^2-1}$ (see (5.38) and (5.39)). Notice that the last two values can be obtained by raising t_a^{q-1} to q-th and $(q+1)$-st powers, respectively. So we determine an s-expansion for t_a^{q-1}. If $a = 1$, then $t_1^{q-1} = s$. Now consider polynomials $a \in \mathbf{A}^+$ for which $\deg_T(a) = m \geq 1$. We use (5.32) to obtain

$$t_a^{q-1} = \left(\frac{t^{|a|}}{f_a(t)}\right)^{q-1} = \frac{(t^{q-1})^{q^m}}{(\rho_a(t^{-1})t^{|a|})^{q-1}} = \frac{(t^{q-1})^{q^m}}{\left(\sum_{i=0}^{m-1} \beta_i t^{q^m-q^i} + 1\right)^{q-1}} = \frac{s^{q^m}}{\left(\sum_{i=0}^{m-1} \beta_i s^{\frac{q^m-q^i}{q-1}} + 1\right)^{q-1}}, \tag{8.1}$$

where f_a is the a-th inverse cyclotomic polynomial (see 5.32), ρ is the Carlitz module and each β_i is obtained by using one of the recursive formulae given in (5.26) or (A.1). Let

$$r_a(s) := \sum_{i=0}^{m-1} \beta_i s^{\frac{q^m-q^i}{q-1}}, \tag{8.2}$$

and let $r_a(s)_i$ be its i-th term. Then

$$\begin{aligned} t_a^{q-1} &= \frac{s^{q^m}}{(1+r_a(s))^{q-1}} = \frac{s^{q^m}(1+r_a(s))}{(1+r_a(s))^q} = \frac{s^{q^m}(1+r_a(s))}{1+r_a(s)^q} \\ &= s^{q^m}(1+r_a(s)) \sum_{i=0}^{\infty} (-r_a(s)^q)^i. \end{aligned} \tag{8.3}$$

The smallest exponent of s in $r_a(s)$ is $\deg_s(r_a(s)_{m-1}) = (q^m - q^{m-1})/(q-1) = q^{m-1}$. Thus,

$$t_a^{q-1} = s^{q^m} + \beta_{m-1} s^{q^m+q^{m-1}} + \cdots \tag{8.4}$$

Consider the sum

$$\sum_{a\in\mathbf{A}^+} t_a^{q-1} = B_0 + B_1 + B_2 + \cdots = \sum_{i=0}^{\infty} c_i s^i, \tag{8.5}$$

where $B_m = \sum_{a\in\mathbf{A}_m^+} t_a^{q-1}$ and $c_i \in \mathbf{A}$. Recall that $[i] = T^{q^i} - T$. The values of B_m are as follows:

$$\begin{aligned} B_0 &= s, \\ B_1 &= s^{q^2-q+1}\left(1 - s^{q-1} + [1]s^q\right)^{1-q}, \\ B_m &= s^k + \cdots, \qquad\qquad k = \frac{q^{2m+1}+1}{q+1} \text{ for } m \geq 2. \end{aligned} \tag{8.6}$$

See [Gek88], pp. 692–694. We need (8.5) in the computation of g and Δ. Suppose (8.5) is required to precision $\mathcal{N}$. We have to use monic polynomials only up to a certain degree in our computation. We must compute B_m for m with

$$\deg_s(B_m) = \frac{q^{2m+1}+1}{q+1} \leq \mathcal{N}.$$

From this inequality, we obtain

$$\lambda_{\mathcal{N}} := \left\lfloor \frac{\log_q(\mathcal{N}q + \mathcal{N} - 1) - 1}{2} \right\rfloor \tag{8.7}$$

as the largest value of m. Thus, we have to use all polynomials in $\mathbf{A}^+_{\leq\lambda_{\mathcal{N}}}$ to compute (8.5). So if g and Δ are required to precisions N_g and N_Δ, respectively, then we use the bounds

$$\lambda_g := \lambda_{N_g} \quad \text{and} \quad \lambda_\Delta := \lambda_{N_\Delta}$$

for the degrees of the monic polynomials that should be used in the computations of g and Δ, respectively.

From (5.38), write

$$g(s) = 1 - [1]\sum_{a\in\mathbf{A}^+} t_a^{q-1}. \tag{8.8}$$

We now have the following result.

Lemma 8.2.1. *It suffices to sum over all polynomials in* $\mathbf{A}^+_{\leq \lambda_g}$ *to obtain* g *to precision* N_g*, i.e.,*

$$g(s) \equiv 1 - [1] \sum_{a \in \mathbf{A}^+_{\leq \lambda_g}} t_a^{q-1} \pmod{s^{N_g+1}}.$$

Example 8.2.2. Let $q = 3$. Suppose we need to compute g to precision $N_g = 10$, i.e., $g_{10}(s)$. Then, from (8.7) and Lemma 8.2.1, we need to include all polynomials $a \in \mathbf{A}^+$ of degree up to

$$\lambda_g = \left\lfloor \frac{\log_3(39) - 1}{2} \right\rfloor = 1.$$

The coefficients of $s^0, \ldots, s^{10}$ in $g_{10}(s)$ are then determined using B_0 and B_1.

Remark 8.2.3. Note that if we compute g to precision N_g, then we also get g^{q+1} to precision N_g since $\mathbf{A}[[s]]/s^{N_g+1}$ is a ring.

Now consider Δ. Note that

$$\begin{aligned}
\left([1]^{-1} - \sum_{a \in \mathbf{A}^+} t_a^{q-1}\right)^{q+1} &= \left([1]^{-1} - \sum_{a \in \mathbf{A}^+} t_a^{q-1}\right)^{q} \left([1]^{-1} - \sum_{a \in \mathbf{A}^+} t_a^{q-1}\right) \\
&= [1]^{-q-1} - [1]^{-q} \sum_{a \in \mathbf{A}^+} t_a^{q-1} - [1]^{-1} \sum_{a \in \mathbf{A}^+} t_a^{q^2-q} \\
&\quad + \left(\sum_{a \in \mathbf{A}^+} t_a^{q^2-q}\right)\left(\sum_{a \in \mathbf{A}^+} t_a^{q-1}\right).
\end{aligned}$$

So (5.39) becomes

$$\begin{aligned}
\Delta = -[2] \sum_{a \in \mathbf{A}^+} \left(t_a^{q^2-1} - [1]^{-1} t_a^{q^2-q}\right) - \sum_{a \in \mathbf{A}^+} t_a^{q-1} \\
- [1]^{q-1} \sum_{a \in \mathbf{A}^+} t_a^{q^2-q} + [1]^q \left(\sum_{a \in \mathbf{A}^+} t_a^{q^2-1}\right),
\end{aligned} \tag{8.9}$$

where $[2][1]^{-1} = T^{q^2-q} + T^{q^2-2q+1} + \cdots + T^{q-1} + 1$ and $[1]^{q-1} = T^{q^2-q} + T^{q^2-2q+1} + \cdots + T^{q-1}$. As noted above, we have to use all monic polynomials of degree $m \leq \lambda_\Delta$ to compute Δ to precision N_Δ. We now have the following result.

Lemma 8.2.4. *It suffices to sum over all polynomials in* $\mathbf{A}^+_{\leq \lambda_\Delta}$ *to compute* Δ *to precision* N_Δ*, i.e.,*

$$\Delta(s) \equiv -[2] \sum_{a \in \mathbf{A}^+_{\leq \lambda_\Delta}} \left(t_a^{q^2-1} - [1]^{-1} t_a^{q^2-q} \right) - \sum_{a \in \mathbf{A}^+_{\leq \lambda_\Delta}} t_a^{q-1} - [1]^{q-1} \sum_{a \in \mathbf{A}^+_{\leq \lambda_\Delta}} t_a^{q^2-q} + [1]^q \left(\sum_{a \in \mathbf{A}^+_{\leq \lambda_\Delta}} t_a^{q^2-1} \right) \pmod{s^{N_\Delta+1}}.$$

To compute j to precision N (equivalently, $sj \pmod{s^{N+2}}$), we divide $g^{q+1} \pmod{s^{N+2}}$ by $\Delta \pmod{s^{N+3}}$. The precisions of g^{q+1} and Δ differ by 1 since the initial term of Δ is $-s$ (see Theorem 5.4.8). By Remark 8.2.3, $g \pmod{s^{N+2}}$ has to be computed to get $g^{q+1} \pmod{s^{N+2}}$. Thus, we obtain the following lemma.

Lemma 8.2.5. *The* s*-expansions of* g *and* Δ *have to be computed to precisions* $N_g = N+1$ *and* $N_\Delta = N+2$*, respectively, for the computation of the* s*-expansion of the* j*-invariant to precision* N*.*

Before we present the algorithm for computing j-invariants, we give some additional properties of the coefficients of g, g^{q+1}, Δ, $1/\Delta$, and j. Let $\mathcal{S}$ be the set of power series

$$\mathcal{S} = \left\{ \sum c_k s^k \mid c_k \in \mathbf{A} \text{ and } \deg_T(c_k) \leq k \right\}.$$

Also, let

$$\mathcal{S}^* = \{ R \in \mathbf{A}[[s]] \mid R = aR' \text{ for some } a \in \mathbf{A}, R' \in \mathcal{S} \}$$

be the $\mathbf{A}$-submodule of $\mathbf{A}[[s]]$ generated by $\mathcal{S}$. See [Gek88], p. 683.

Lemma 8.2.6. $\mathcal{S}$ *is closed under addition and multiplication. Moreover, if* $P(s) = 1 + \cdots \in \mathcal{S}$*, then* $1/P(s) \in \mathcal{S}$*.*

Let $a \in \mathbf{A}^+$ such that $\deg_T(a) = m$, so $a = \sum_{i=0}^m \alpha_i T^i$ with $\alpha_m = 1$. Recall $r_a(s)$ as defined in (8.2). Define

$$h_a(s) := 1 + r_a(s), \tag{8.10}$$

which is obtained from the a-th inverse cyclotomic polynomial $f_a(t)$ using the substitution $s = t^{q-1}$. We consider $h_a(s)$ as a power series in s. Since $\deg_s(r_a(s)) = (q^m - 1)/(q - 1)$, we can write $h_a(s)$ as

$$h_a(s) = \sum_{k=0}^{(q^m-1)/(q-1)} c_k s^k,$$

where $c_k \in \mathbf{A}$ and $c_k = \beta_i$ for $k = (q^m - q^i)/(q - 1)$ for integers from $i = m$ down to $i = 0$, and $c_k = 0$, otherwise. In particular, $c_0 = \beta_m = \alpha_m = 1$ and $c_{(q^m-1)/(q-1)} = \beta_0$. Moreover,

$$\deg_T(c_k) = \deg_T(\beta_i) = q^i(m - i) \leq k = \frac{q^m - q^i}{q - 1}$$

by (5.27). Another way to see this inequality is by noting that the maximum value of $q^i(m-i)$ and the minimum value of $\frac{q^m-q^i}{q-1}$, both equal to q^{m-1}, are obtained when $i = m-1$. We now have shown the following lemma.

Lemma 8.2.7. *For $a \in \mathbf{A}^+$, $h_a(s) \in \mathcal{S}$.*

Proposition 8.2.8.

(a) $\Delta/s, (g-1)/[1] \in \mathcal{S}$.

(b) $g, \Delta \in \mathcal{S}^*$.

Proof. See [Gek88, Proposition 6.7]. □

Write

$$g(s) = \sum_{i=0}^{\infty} g_i s^i, \qquad \Delta(s) = \sum_{i=0}^{\infty} \Delta_i s^{i+1}, \tag{8.11}$$

$$g(s)^{q+1} = \sum_{i=0}^{\infty} w_i s^i, \qquad 1/\Delta = \sum_{i=0}^{\infty} v_i s^{i-1}, \qquad \text{and} \qquad j(s) = \sum_{i=0}^{\infty} a_i s^{i-1} \tag{8.12}$$

where $g_i, \Delta_i, w_i, v_i, a_i \in \mathbf{A}$. The following result is presented in [BL97, Section 3].

Lemma 8.2.9. *With notations as above,*

$$\deg_T(g_i),\ \deg_T(\Delta_i),\ \deg_T(w_i),\ \deg_T(v_i),\ \deg_T(a_i) \leq qi.$$

Recall that our aim in this section is to formulate an algorithm for computing the j-invariant to precision N. By Lemma 8.2.5, let $N_g = N + 1$ and $N_\Delta = N + 2$. Note that $N_\Delta > N_g$ implies that $\lambda_\Delta \geq \lambda_g$. Define

$$\lambda := \lambda_\Delta = \left\lfloor \frac{\log_q((N+2)q + N + 1) - 1}{2} \right\rfloor. \tag{8.13}$$

The following lemma follows easily from the definition of λ using elementary calculations, see (A.5).

Lemma 8.2.10. *With λ defined above, we have*

$$q^\lambda < 3\sqrt{N}.$$

The following algorithm determines the j-invariant to the required precision N.

Algorithm 8.2.11. Computing the j-Invariant

Input: A prime power $q \in \mathbb{Z}$ and precision $N \in \mathbb{N}$.

Output: The s-expansion of the j-invariant to precision N.

1. Compute λ as given in (8.13)
2. Compute t_a^{q-1}, $t_a^{q^2-1}$, and $t_a^{q^2-q} \pmod{s^{N+3}}$ for all $a \in \mathbf{A}^+_{\leq\lambda}$.
3. Compute $g \pmod{s^{N+2}}$.
4. Compute $g^{q+1} \pmod{s^{N+2}}$.
5. Compute $\Delta \pmod{s^{N+3}}$.
6. Compute the coefficients a_i of $j = g^{q+1}/\Delta$ for i from 0 to $N + 1$.
7. Return
$$j_N(s) = \sum_{i=0}^{N+1} a_i s^{i-1}.$$

To prove the next result, we note that

$$\#\mathbf{A}^+_{\leq\lambda} = \sum_{i=0}^{\lambda} q^i = \frac{q^{\lambda+1} - 1}{q - 1} < \frac{q^{\lambda+1}}{q - 1} < \frac{3q\sqrt{N}}{q - 1}, \tag{8.14}$$

where the last inequality follows from Lemma 8.2.10. Recall that $M(n)$ is the number of ring operations required to multiply two polynomials both of degree n with coefficients from a unique factorization domain as in the previous section. As noted in the previous section, the cost of computing q-th powers of polynomials in $\mathbf{A}$ is negligible since we just need to shift the powers of T. It follows that the cost of computing

$$F(s)^q = \left(\sum_{i=0}^{\infty} f_i(T) s^i \right)^q = \sum_{i=0}^{\infty} f_i(T^q) s^{qi}$$

for any power series $F(s) = \sum_{i=0}^{\infty} f_i(T) s^i$, with $f_i(T) \in \mathbf{A}$, is also negligible.

Note that Algorithm 8.2.11 takes as input q and the precision N, and both of these values can tend to ∞. If N is fixed and $q \longrightarrow \infty$ then a complexity an expression like $M(qN)$ inside an $O()$ estimate can be replaced by $O(M(q))$. If q is fixed and $N \longrightarrow \infty$, then we write $M(qN) = O(M(N))$. But if both go simultaneously to ∞, then we need to keep the explicit dependency $M(qN)$.

Theorem 8.2.12. *Algorithm 8.2.11 correctly computes the j-invariant to precision N in*

$$O\left(\sqrt{N} M(N)^2 + M(N) M(qN) \right)$$

operations in $\mathbb{F}_q$, as $q, N \longrightarrow \infty$.

Proof. The correctness of Algorithm 8.2.11 follows from Theorem 5.4.8 and Lemma 8.2.5. As for its run time, we determine the cost of each step in terms of operations in $\mathbb{F}_q$. We show that Steps 2 and 6 are the dominant ones requiring $O(\sqrt{N} M(N)^2)$ and $O(M(N) M(qN))$ $\mathbb{F}_q$-operations, respectively.

Step 1. Negligible.

Step 2. Let $\deg_T(a) = m$ for $a \in \mathbf{A}^+_{\leq \lambda}$, so $m \leq \lambda$. Recall $h_a(s)$ as defined in (8.10). We see from (8.1), (8.2), and (8.10) that we need to determine each coefficient β_i of $h_a(s)$ to obtain t_a^{q-1}. From Remark A.2.5, the cost of computing the β_i is at most $m^2 q^{m-1}$

multiplications in $\mathbb{F}_q$. Since $m \leq \lambda$ and $\#\mathbf{A}^+_{\leq\lambda} < 3q\sqrt{N}/(q-1)$ from (8.14), it follows that the cost of computing the β_i for all $a \in \mathbf{A}^+_{\leq\lambda}$ is

$$\lambda^2 q^{\lambda-1}\frac{3q\sqrt{N}}{q-1} = \lambda^2 q^{\lambda}\frac{3\sqrt{N}}{q-1} < \lambda^2\frac{9N}{q-1} \leq \left(\frac{\log 3\sqrt{N}}{\log q}\right)^2 \frac{9N}{q-1} \tag{8.15}$$

multiplications in $\mathbb{F}_q$, where the last inequality follows from Lemma 8.2.10.

By definition of $h_a(s)$, we can write t_a^{q-1} as

$$t_a^{q-1} = \frac{s^{q^m}}{h_a(s)^{q-1}}.$$

Notice that for the nonzero terms in $h_a(s)$, the smallest exponent of s is q^{m-1}. Moreover, the coefficients β_i of $h_a(s)$ satisfy

$$\deg_T(\beta_i) \leq q^{m-1} \leq q^{\lambda-1}$$

for $a \in \mathbf{A}^+_{\leq\lambda}$, see (5.27). The cost of computing

$$\frac{1}{h_a(s)^{q-1}} = \frac{h_a(s)}{h_a(s)^q}$$

is roughly that of multiplying $h_a(s)$ by $h_a(s)^q \pmod{s^{N+3}}$. Now

$$\deg_s(h_a(s)) = \frac{q^m-1}{q-1} \leq \frac{q^\lambda-1}{q-1} < q^\lambda < 3\sqrt{N}$$

and

$$\deg_s\left(h_a(s)\right)^q \pmod{s^{N+3}} \leq \min\{N+2, 3q\sqrt{N}\},$$

so computing the quotient $h_a(s)/h_a(s)^q$ requires $M(3\sqrt{N}, \min\{N+2, 3q\sqrt{N}\})$ multiplications in $\mathbf{A}$. The largest degree of any coefficient of $h_a(s)$ is $q^{m-1} \leq q^{\lambda-1} < 3\sqrt{N}/q$ by Lemma 8.2.10 and the largest degree of any coefficient of $h_a(s)^q$ is $q^m \leq q^\lambda < 3\sqrt{N}$. So computing t_a^{q-1} for all $a \in \mathbf{A}^+_{\leq\lambda}$ costs at most

$$\frac{3q\sqrt{N}}{q-1}\, M\left(3\sqrt{N}, \min\left\{N+2, 3q\sqrt{N}\right\}\right) M\left(\frac{3\sqrt{N}}{q}, 3\sqrt{N}\right) \tag{8.16}$$

multiplications in $\mathbb{F}_q$, where $3q\sqrt{N}/(q-1)$ comes from (8.14).

Next, we have

$$t_a^{q^2-q} = (t_a^{q-1})^q \quad \text{and} \quad t_a^{q^2-1} = (t_a^{q-1})^{q+1} = t_a^{q^2-q} t_a^{q-1}.$$

So computing $t_a^{q^2-q}$ is just raising t_a^{q-1} to the q-th power. As noted earlier, the cost of raising a power series to the q-th power is negligible. As for $t_a^{q^2-1}$, we have to multiply $t_a^{q^2-q}$ by t_a^{q-1}. Both have degree $N+2$ in s, giving $M(N+2)$ multiplications in $\mathbf{A}$. Note that $h_a(s) \in \mathcal{S}$ by Lemma 8.2.7 for all $a \in \mathbf{A}^+_{\leq\lambda}$. So

$$\frac{1}{h_a(s)},\ \frac{1}{h_a(s)^{q-1}},\ \left(\frac{1}{h_a(s)^{q-1}}\right)^q \in \mathcal{S}$$

by Lemma 8.2.6. The largest degree of any coefficient of t_a^{q-1} is $N+2$, and the same degree bound also holds for any coefficient of $t_a^{q^2-q}$ by Lemma 8.2.6. Therefore, by (8.14) the cost of computing $t_a^{q^2-1}$ for all $a \in \mathbf{A}^+_{\leq\lambda}$ is

$$\frac{3q\sqrt{N}}{q-1}\ M(N+2)^2 \tag{8.17}$$

multiplications in $\mathbb{F}_q$.

Observe that (8.17) asymptotically dominates both (8.15) and (8.16). It follows that the asymptotic cost of Step 2 arises from (8.17).

Step 3. We see from (8.8) that each term in $\sum_{a\in\mathbf{A}^+_{\leq\lambda_g}} t_a^{q-1} \pmod{s^{N+2}}$ has to be multiplied by $[1] = T^q - T$. This can be done by shifting the degrees of T in the coefficients of the sum, changing signs, and doing $O(N)$ additions. So this step is negligible.

Step 4. Note that $g^{q+1} = g^q g$. So we multiply $g^q \pmod{s^{N+2}}$ by $g \pmod{s^{N+2}}$, requiring $M(N+1)$ multiplications in $\mathbf{A}$. The largest degree of any coefficient of $g \pmod{s^{N+2}}$ and of $g^q \pmod{s^{N+2}}$ is $q(N+1)$ by Lemma 8.2.9. So this step costs a total of

$$M(N+1)M(q(N+1))$$

multiplications in $\mathbb{F}_q$.

Step 5. We see from (8.9) that the cost of computing $\Delta \pmod{s^{N+3}}$ is asymptotically the same as that for g, i.e., we just need to do shifts, change in signs, and $O(N)$ additions.

Step 6. Let Δ and g^{q+1} be represented as in (8.11) and (8.12), respectively. The asymptotic cost of computing

$$\frac{g^{q+1} \pmod{s^{N+2}}}{\Delta \pmod{s^{N+3}}}$$

is asymptotically the same as multiplying $g^{q+1} \pmod{s^{N+2}}$ by $\Delta \pmod{s^{N+3}}$, giving $M(N+1, N+2)$ multiplications in $\mathbf{A}$. The largest degree of any coefficient of $g^{q+1} \pmod{s^{N+2}}$ is $q(N+1)$ by Lemma 8.2.9. Similarly, the largest degree of any coefficient of $\Delta \pmod{s^{N+3}}$ is $q(N+2)$. Thus, the total cost of this step is

$$M(N+1, N+2)M(q(N+1), q(N+2))$$

$\mathbb{F}_q$-multiplications. Asymptotically, Steps 4 and 6 have the same complexity.

Combining the costs of Steps 2 and 6 gives the complexity of this algorithm. It requires

$$O\left(\sqrt{N}M(N)^2 + M(N)M(qN)\right)$$

multiplications in $\mathbb{F}_q$, as $q, N \longrightarrow \infty$. □

Remark 8.2.13.

(1) We require a total space of $O(qN^2)$ elements in $\mathbb{F}_q$ to store the $N+2$ coefficients of j since the largest degree of any coefficient of $sj \pmod{s^{N+2}}$ is $q(N+1)$.

(2) The value of λ in (8.7) is optimal. If we only use polynomials of degree less than λ in our computation of j, then we get some errors on some of its coefficients as we observed in our computations.

(3) For naive multiplication, the complexity of Algorithm 8.2.11 is $O(N^4(\sqrt{N}+q^2))$. If fast convolution techniques are allowed, this complexity becomes $O^{\sim}(N^2(\sqrt{N}+q))$ for any positive integer k, as $q, N \longrightarrow \infty$.

To end this section, we mention that we computed j-invariants using code in SAGE [S+17] for $q = 2, 3, 5, 7$ using $\mathbf{A}^+_{\leq 1}$ and $\mathbf{A}^+_{\leq 2}$, and for all other prime powers less than 100 using $\mathbf{A}^+_{\leq 1}$.

8.3 Computation of Drinfeld Modular Polynomials

Throughout this section, let q be a prime power in $\mathbb{Z}$. We assume that φ is a rank two Drinfeld module over $\mathbf{C}$, unless otherwise stated. Let $\ell \in \mathbf{A}^+$ be an irreducible polynomial. Recall that the modular polynomial $\Phi_\ell(X, Y)$ for $j(\varphi)$ was introduced in Section 5.5, and we have seen in Section 7.1 that it plays a fundamental role in the classification of isogenies of Drinfeld modules. Similar to the elliptic curve case, the roots of $\Phi_\ell(X, Y)$ are pairs $(j(\varphi), j(\psi))$ of j-invariants of ℓ-isogenous rank two Drinfeld modules φ and ψ (see Theorem 5.5.9).

As far as the author knows, there are two known algorithms for the computation of modular polynomials for rank two Drinfeld modules. One is given in [Sch95], which only computes $\Phi_T(X, Y)$. The other one is given in [BL97]. This is the algorithm we used in the computation of modular polynomials for our isogeny volcanoes. It uses the coefficients of the j-invariant's s-expansion and some linear algebra. We present a detailed complexity analysis for this algorithm.

It is necessary to repeat some of the arguments presented in [BL97] to motivate the derivation of the algorithm. Recall that $\Phi_\ell(X, Y)$ is a symmetric bivariate polynomial of degree $|\ell| + 1$ with coefficients in $\mathbf{A}$, see Theorem 5.5.5. Write this polynomial as

$$\Phi_\ell(X, Y) = X^{|\ell|+1} + Y^{|\ell|+1} + \sum_{\mu=0}^{|\ell|} \sum_{\nu=0}^{|\ell|} w_{\mu,\nu} X^\mu Y^\nu. \tag{8.18}$$

So we need to compute the coefficients $w_{\mu,\nu} \in \mathbf{A}$ for $0 \leq \mu, \nu \leq |\ell|$. It follows from Theorem 5.5.5(ii) that $w_{\mu,\nu} = w_{\nu,\mu}$. Thus, (8.18) can be reformulated as

$$\Phi_\ell(X, Y) = X^{|\ell|+1} + Y^{|\ell|+1} + \sum_{\mu=0}^{|\ell|} \sum_{\nu=0}^{\mu} w_{\mu,\nu} X^\mu Y^\nu + \sum_{\mu=1}^{|\ell|} \sum_{\nu=0}^{\mu-1} w_{\mu,\nu} X^\nu Y^\mu. \tag{8.19}$$

We determine the values of $w_{\mu,\nu}$ from the coefficients of the equation

$$\Phi_\ell(j(\ell z), j(z)) = 0. \tag{8.20}$$

Recall from (5.40) that $j(z) = \sum_{i=0}^{\infty} a_i s^{i-1}$, with $a_0 = -1$. Suppose j has been precomputed using Algorithm 8.2.11, i.e., the a_i are already known up to a certain precision. Then we can determine the powers $j(z)^e$ from $j(z)$ for $2 \le e \le |\ell| + 1$. Define $a_i(e)$ by

$$j(z)^e =: \sum_{i=0}^{\infty} a_i(e) s^{i-e},$$

where $a_0(e) = \pm 1$ and $a_i(1) = a_i$.

Now we compute $j(\ell z)$ by replacing s with $s(\ell z)$ in $j(z)$. Thus, we have to determine t_ℓ^{q-1}. Using (8.3), we can write

$$s(\ell z) = t_\ell^{q-1} = s^{|\ell|}(1 + r_\ell(s)) \sum_{k=0}^{\infty} (-r_\ell(s)^q)^k$$

where $r_\ell(s) = \sum_{i=0}^{\deg_T(\ell)-1} \beta_i s^{\frac{q^{\deg_T(\ell)} - q^i}{q-1}}$ as defined in (8.2). Now we get

$$j(\ell z) = \sum_{i=0}^{\infty} a_i s(\ell z)^{i-1} = s^{-|\ell|}(1 + r_\ell(s))^{q-1} \sum_{i=0}^{\infty} a_i \left(s^{|\ell|}(1 + r_\ell(s)) \sum_{k=0}^{\infty} (-r_\ell(s)^q)^k \right)^i.$$

Write

$$j(\ell z) = \sum_{i=0}^{\infty} b_i s^{i-|\ell|},$$

where the first $|\ell|$ coefficients $b_0, b_1, \ldots, b_{|\ell|-1}$ are the coefficients of $(1 + r_\ell(s))^{q-1}$ and the remaining coefficients are obtained from the coefficients $a_1, a_2, \ldots$ of $j(z)$ and the coefficients β_i of $r_\ell(s)$. Clearly, $b_0 = a_0 = -1$. Define $b_i(e)$ by

$$j(\ell z)^e =: \sum_{i=0}^{\infty} b_i(e) s^{i-e|\ell|},$$

where $b_0(e) = \pm 1$ and $b_i(1) = b_i$.

Now define the sets

$$W := \{(\mu, \nu) \mid 0 \le \mu \le |\ell|,\ 0 \le \nu \le \mu\} \tag{8.21}$$

and

$$V := \{(k,h) \mid 0 \leq k \leq |\ell|,\ k \leq h \leq |\ell|\}. \tag{8.22}$$

W is the set of all pairs (μ,ν) for which we need to compute $w_{\mu,\nu}$. V, on the other hand, is the set of all pairs (k,h) that gives the indices $i = k|\ell| + h$ of the coefficients $a_i(e)$ and $b_i(e)$ which are needed for the calculation of $w_{\mu,\nu}$. One may check that

$$\#W = \#V = \frac{(|\ell|+1)(|\ell|+2)}{2}. \tag{8.23}$$

Introduce the usual lexicographic order on W by defining

$$(\mu,\nu) < (\mu',\nu') \qquad \text{if and only if} \quad \mu < \mu', \quad \text{or} \quad \mu = \mu',\ \nu < \nu'.$$

We also use the analogous lexicographic order on V. So the elements of W and V are ordered from the "smallest" pair to the "biggest" pair.

Remark 8.3.1. We have the following relationships between the elements of W and V (see [BL97, Lemmas 4.1 and 4.2 and Propositions 4.3 and 4.4]):

(a) $(k,h) \in V$ if and only if $(|\ell|-k, |\ell|-h) \in W$.

(b) $(k,h) < (k',h')$ if and only if $(|\ell|-k, |\ell|-h) > (|\ell|-k', |\ell|-h')$.

(c) $k|\ell| + h - |\ell|^2 - |\ell| + \mu|\ell| + \nu \geq 0$ if and only if $(\mu,\nu) \geq (|\ell|-k, |\ell|-h)$ for $(\mu,\nu) \in W$ and $(k,h) \in V$. Define the set

$$R_i = \{(\mu,\nu) \in W \mid (\mu,\nu) \geq (|\ell|-k, |\ell|-h)\}$$

for $i = k|\ell| + h$ where $(k,h) \in V$.

(d) The set

$$S = \{(\mu,\nu) \in W \mid 0 \leq \nu \leq \mu \leq |\ell| \text{ and } i - |\ell|^2 - |\ell| + \nu|\ell| + \mu \geq 0\}$$

is a subset of R_i.

By expanding (8.20), we get

$$\begin{aligned}0 = \Phi_\ell(j(\ell z), j(z)) = s^{-|\ell|(|\ell|+1)} \sum_{i=0}^{\infty} b_i(|\ell|+1)s^i + s^{-(|\ell|+1)} \sum_{i=0}^{\infty} a_i(|\ell|+1)s^i \\ + \sum_{\mu=0}^{|\ell|} \sum_{\nu=0}^{\mu} w_{\mu,\nu} \left(s^{-\mu|\ell|-\nu} \sum_{i=0}^{\infty} c_i(\nu,\mu)s^i \right) \\ + \sum_{\mu=1}^{|\ell|} \sum_{\nu=0}^{\mu-1} w_{\mu,\nu} \left(s^{-\nu|\ell|-\mu} \sum_{i=0}^{\infty} c_i(\mu,\nu)s^i \right),\end{aligned}$$

where

$$c_i(\mu,\nu) := \sum_{n=0}^{i} a_n(\mu) b_{i-n}(\nu) \tag{8.24}$$

with particular values $c_i(\mu,0) = a_i(\mu)$, $c_i(0,\nu) = b_i(\nu)$, $c_0(0,0) = 1$, and $c_i(\mu,\nu) = 0$ for $i < 0$. The coefficients of $s^{-|\ell|(|\ell|+1)+i}$ are all zero for all $i \geq 0$. Thus we get a system of equations

$$\begin{aligned}b_i(|\ell|+1) + a_{i-|\ell|^2+1}(|\ell|+1)) + \sum_{\mu=0}^{|\ell|} \sum_{\nu=0}^{\mu} w_{\mu,\nu} c_{i-|\ell|^2-|\ell|+\mu|\ell|+\nu}(\nu,\mu) \\ + \sum_{\mu=1}^{|\ell|} \sum_{\nu=0}^{\mu-1} w_{\mu,\nu} c_{i-|\ell|^2-|\ell|+\nu|\ell|+\mu}(\mu,\nu) = 0\end{aligned} \tag{8.25}$$

for $i = k|\ell| + h$, $(k,h) \in V$, where $a_{i-|\ell|^2+1}(|\ell|+1) := 0$ if $i - |\ell|^2 + 1 < 0$. Let

$$c_{i,\mu,\nu}(\nu,\mu) := c_{i-|\ell|^2-|\ell|+\mu|\ell|+\nu}(\nu,\mu) \qquad \text{and} \qquad c_{i,\nu,\mu}(\mu,\nu) := c_{i-|\ell|^2-|\ell|+\nu|\ell|+\mu}(\mu,\nu). \tag{8.26}$$

Then the system (8.25) can be represented via matrices as

$$DX = B.$$

Here X and B are the $\#W \times 1$ matrices

$$X = \begin{pmatrix} w_{|\ell|,|\ell|} \\ \vdots \\ w_{\mu,\mu} \\ \vdots \\ w_{0,0} \end{pmatrix} \qquad \text{and} \qquad B = - \begin{pmatrix} b_0(|\ell|+1) + a_{-|\ell|^2+1}(|\ell|+1) \\ \vdots \\ b_{k|\ell|+h}(|\ell|+1) + a_{k|\ell|+h-|\ell|^2+1}(|\ell|+1) \\ \vdots \\ b_{|\ell|^2+|\ell|}(|\ell|+1) + a_{|\ell|+1}(|\ell|+1) \end{pmatrix},$$

respectively, with (μ, ν) going through all the elements of W in reversed lexicographic order and (k, h) through all the elements of V in lexicographic order (see Remark 8.3.1(a) – (b)). Define

$$I := \{i \in \mathbb{Z} \mid i = k|\ell| + h,\ (k, h) \in V\} \tag{8.27}$$

and introduce an order on this set according to the lexicographic order on V. So the elements of I are integers ordered from least to greatest. Note that $\#I = \#V$ as well. Let $m, n \in \mathbb{Z}$ such that $1 \leq m \leq \#V$ and $1 \leq n \leq \#W$ (with $\#V = \#W$), and define

$$\begin{aligned} (\mu_n, \nu_n) &:= n\text{-th element of } W \text{ (in reversed lexicographic order)}, \\ (k_m, h_m) &:= m\text{-th element of } V\text{(in lexicographic order), and} \\ i_m &:= k_m|\ell| + h_m = m\text{-th element of } I. \end{aligned} \tag{8.28}$$

Then $D = (d_{m,n})$ is a $\#W \times \#W$ matrix whose entries are

$$d_{m,n} = \begin{cases} c_{i_m,\mu_n,\nu_n}(\nu_n, \mu_n), & \text{if} \quad \mu_n = \nu_n, \\ c_{i_m,\mu_n,\nu_n}(\nu_n, \mu_n) + c_{i_m,\nu_n,\mu_n}(\mu_n, \nu_n), & \text{if} \quad \mu_n \neq \nu_n. \end{cases} \tag{8.29}$$

We use Remark 8.3.1 to determine which indices will give $d_{m,n} = 0$. It follows from this remark that D is a lower triangular matrix. So for each row m, we need to determine the entries $d_{m,1}, d_{m,2}, \ldots, d_{m,m}$. The diagonal entries of D, i.e., the $d_{m,m}$, are of the form $c_0(\mu, \nu)$ since the diagonal entries in D have $(\mu_m, \nu_m) = (|\ell| - k_m, |\ell| - h_m)$. Since $a_0(\mu_m) = \pm 1$ and $b_0(\nu_m) = \pm 1$, it follows that $c_0(\mu_n, \nu_n) = \pm 1$. Based on the entries of B and D, we need to determine the following coefficients:

$$\begin{aligned} &a_i(\mu),\ b_i(\nu), && \text{for } 0 \leq \mu, \nu \leq |\ell|, \\ &a_{i-|\ell|^2+1}(|\ell| + 1), \\ &b_i(|\ell| + 1), \\ &c_{i,\mu,\nu}(\nu, \mu), && \text{for } 0 \leq \mu, \nu \leq |\ell|, \\ &c_{i,\nu,\mu}(\mu, \nu), && \text{for } 0 \leq \mu, \nu \leq |\ell| \text{ and } \mu \neq \nu, \end{aligned} \tag{8.30}$$

where $i = k|\ell| + h \in I$ as (k, h) runs through all the elements of V in lexicographic order. Finally, since D is a lower triangular matrix, we solve for the coefficients $w_{\mu,\nu}$ from $DX = B$ via forward substitution.

We summarize the procedure presented above in the next algorithm. This method assumes that the s-expansions of $j(z)$ and $j(\ell z)$ have been precomputed up to a certain precision. Note that only a sufficient number of coefficients of $j(z)$ and $j(\ell z)$ is needed to perform this algorithm. We will prove later that we require $sj(z)$ to precision $N + 1$ and $s^{|\ell|}j(\ell z)$ to precision $N - |\ell| + 1$, where $N = |\ell|^2 + |\ell| - 1$.

Algorithm 8.3.2. Computing the Modular Polynomial $\Phi_\ell(X, Y)$

Input: A prime $\ell \in \mathbf{A} = \mathbb{F}_q[T]$, $|\ell|$, $N = |\ell|^2 + |\ell| - 1$, and $sj(z)$ and $s^{|\ell|}j(\ell z)$ to precisions $N + 1$ and $N - |\ell| + 1$, respectively.

Output: The coefficients $w_{\mu,\nu}$ of the modular polynomial $\Phi_\ell(X, Y)$.

1. Construct the sets W, V, and I as defined in (8.21), (8.22), and (8.27), respectively.
2. For e from 2 to $|\ell| + 1$:
   (a) Calculate $s^e j(z)^e \pmod{s^{N+2}}$.
   (b) Calculate $s^{e|\ell|} j(\ell z)^e \pmod{s^{N+2}}$.
3. //Compute $B = -(b_{m,1})_{1 \le m \le \#W}$:
   For $m := 1$ to $\#W$: Let i_m be as defined in (8.28).
   If $i_m - |\ell|^2 + 1 < 0$, then $b_{m,1} \longleftarrow b_{i_m}(|\ell| + 1)$.
   Else, $b_{m,1} \longleftarrow b_{i_m}(|\ell| + 1) + a_{i_m - |\ell|^2 + 1}(|\ell| + 1)$.
4. //Compute $D = (d_{m,n})_{1 \le m,n \le \#W}$:
   For $m := 1$ to $\#W$ and $n := 1$ to $\#W$: Let i_m and (μ_n, ν_n) be as defined in (8.28).
   If $n \le m$, then for (μ_n, ν_n) in W:
   If $\mu_n = \nu_n$, then compute $c_{i_m,\mu_n,\nu_n}(\nu_n, \mu_n)$ and $d_{m,n} \longleftarrow c_{i_m,\mu_n,\nu_n}(\nu_n, \mu_n)$.

Else, compute $c_{i_m,\mu_n,\nu_n}(\nu_n,\mu_n) + c_{i_m,\nu_n,\mu_n}(\mu_n,\nu_n)$ and

$d_{m,n} \longleftarrow c_{i_m,\mu_n,\nu_n}(\nu_n,\mu_n) + c_{i_m,\nu_n,\mu_n}(\mu_n,\nu_n)$.

Else, $d_{m,n} \longleftarrow 0$.

5. Solve $DX = B$ for $X = (w_{\mu,\nu})_{(\mu,\nu)\in W}$.

6. Return X.

Now we establish the complexity of Algorithm 8.3.2; we show that Step 4 is the dominant step in the algorithm. We determine its complexity as $|\ell| \longrightarrow \infty$. There are three possible cases for $|\ell|$ to tend to ∞: (a) $\deg_T(\ell) \longrightarrow \infty$, (b) $q \longrightarrow \infty$, or (c) both $\deg_T(\ell) \longrightarrow \infty$ and $q \longrightarrow \infty$. Our analysis applies equally to all these three cases. As before, let $M(m,n)$ (and $M(n)$ if $m = n$) be the number of ring multiplications required to multiply polynomials of degrees m and n, respectively, with coefficients from a given ring.

The first step of the algorithm is negligible compared to the other steps. We look into the cost of Step 2. First we show that the precision we specified for $j(z)$ is the right one for the algorithm. We consider $j(z)^e$. Set $j(z)^0 = 1$ and examine the powers for $2 \le e \le |\ell| + 1$. We compute

$$j(z)^2 = j(z)j(z), \quad j(z)^3 = j(z)^2 j(z), \quad ..., \quad j(z)^{|\ell|+1} = j(z)^{|\ell|} j(z).$$

As the ith coefficient of $j(z)^e$ can be written as

$$a_i(e) = \sum_{k=0}^{i} a_k(e-1)a_{i-k} \tag{8.31}$$

and the index i has maximum value $|\ell|^2 + |\ell|$ (by definition of I), it is enough to precompute the first $|\ell|^2 + |\ell| + 1$ coefficients $a_0, a_1, \ldots, a_{|\ell|^2+|\ell|}$ of $j(z)$ (i.e., precompute $j(z)$ to precision $N = |\ell|^2 + |\ell| - 1$, or equivalently, $sj(z)$ to precision $N+1$, or $sj(z) \pmod{s^{N+2}}$). Now we determine the cost of Step 2(a). By Lemma 8.2.9, the coefficients a_i of $j(z)$ satisfy $|a_i| \le q^{qi}$. Moreover, $|a_i(e)| \le q^{qi}$ (see [BL97, Lemma 3.1]). Thus, a_i and $a_i(e)$ are at most of degree qi for each i. Since the largest value of i is $|\ell|^2 + |\ell|$, the biggest bound on the degree of $a_i(e)$

is therefore $q(|\ell|^2+|\ell|)$. Using the first $|\ell|^2+|\ell|+1$ coefficients of $sj(z)$, we now write it as the truncated power series

$$sj(z) \equiv \sum_{i=0}^{N+1} a_i s^i \pmod{s^{N+2}},$$

so we can now treat it as a polynomial of degree $N+1$ in s. In order to get the coefficients $a_i(2)$ of j^2 for $0 \le i \le |\ell|^2+|\ell|$, we have to compute $s^2 j(z)^2$. This requires $M(N+1)$ multiplications in $\mathbf{A}$ involving polynomials of degree at most $q(N+1)$, which gives a total cost of

$$M(N+1)M(q(N+1)) \tag{8.32}$$

multiplications in $\mathbb{F}_q$. We go on to compute the remaining powers $j^3 = j^2 j$, ..., $j^{|\ell|+1} = j^{|\ell|} j$. Note that for each of these powers we have to multiply $s^{e-1}j(z)^{e-1}$ by $sj(z)$ (both of degree $N+1$ in s) to get the required coefficients of $j(z)^e$ for $e = 3, \ldots, |\ell|+1$. The degrees of the coefficients of $s^{e-1}j(z)^{e-1}$ and $sj(z)$ are again bounded by $q(N+1)$. So the cost of computing each remaining power is the same as (8.32). The total cost of Step 2(a) is therefore equal to

$$|\ell| M(N+1)M(q(N+1)). \tag{8.33}$$

As for $j(\ell z)$, we also need to precompute its first $|\ell|^2+|\ell|+1$ coefficients (i.e., precompute $j(\ell z)$ to precision $N-|\ell|+1 = |\ell|^2$, or equivalently, $s^{|\ell|}j(\ell z) \pmod{s^{N+2}}$). Write

$$s^{|\ell|} j(\ell z) \equiv \sum_{i=0}^{N+1} b_i s^i \pmod{s^{N+2}}.$$

Similar to the case of the powers of $j(z)$, we obtain $j(\ell z)^e$ by computing

$$(s^{|\ell|} j(\ell z))^e = (s^{|\ell|} j(\ell z))^{e-1} (s^{|\ell|} j(\ell z))$$

for $e = 2, \ldots, |\ell|+1$. Both $(s^{|\ell|}j(\ell z))^{e-1}$ and $s^{|\ell|}j(\ell z)$ are of degree $N+1$ in s with coefficients in $\mathbf{A}$ of degrees less than $q(|\ell|^2+|\ell|)$, so the cost of multiplying these polynomials is the same as (8.32). It follows that the cost of Step 2(b) is the same as Step 2(a) given in (8.33).

Now determine the storage requirement for Step 2. Note that the $a_i(e)$ and $b_i(e)$ are at most of degree qi. This means that we need to store $qi+1$ elements of $\mathbb{F}_q$ for the i-th coefficient. So for $1 \le e \le |\ell|+1$ and $0 \le i \le |\ell|^2+|\ell|$, we need to keep at most

$$2\left(|\ell|+1\right)\sum_{i=0}^{|\ell|^2+|\ell|}(qi+1) = 2\left(|\ell|+1\right)\left[q\left(\frac{(|\ell|^2+|\ell|)(|\ell|^2+|\ell|+1)}{2}\right)+|\ell|^2+|\ell|+1\right]$$
$$= \left(|\ell|+1\right)\left(|\ell|^2+|\ell|+1\right)\left(q(|\ell|^2+|\ell|)+2\right)$$

lements in $\mathbb{F}_q$.

Step 3 is negligible since it only costs at most $\#W$ additions. Storing the entries of B requires a space of $\#W(q(|\ell|^2+|\ell|)+1)$ elements in $\mathbb{F}_q$.

Now consider Step 4. Recall that D is a $\#W \times \#W$ lower triangular matrix. By (8.29), we have to compute at most

$$2\left(\#W+(\#W-1)+(\#W-2)+\cdots+2+1\right) = \#W\left(\#W+1\right)$$

values of $c_{i_m,\mu_n,\nu_n}(\nu_n,\mu_n)$ and $c_{i_m,\nu_n,\mu_n}(\mu_n,\nu_n)$. For the moment, let

$$f_1 = i_m - |\ell|^2 - |\ell| + \mu_n|\ell| + \nu_n \quad \text{and} \quad f_2 = i_m - |\ell|^2 - |\ell| + \nu_n|\ell| + \mu_n.$$

From (8.26) and (8.24), we see that computing $c_{f_1}(\nu_n,\mu_n)$ and $c_{f_2}(\mu_n,\nu_n)$ requires at most f_1+1 and f_2+1 multiplications, respectively, in $\mathbf{A}$. Moreover, note that $f_1, f_2 \le |\ell|^2+|\ell|$; the maximum value $|\ell|^2+|\ell|$ is reached when $i_m = |\ell|^2+|\ell|$ and $(\mu_n,\nu_n) = (|\ell|,|\ell|)$. Recall that the required coefficients of $j(z)^e$ and $j(\ell z)^e$, for $e = 1,2,\ldots,|\ell|+1$, have degrees bounded by $q(|\ell|^2+|\ell|)$. So Step 3 requires a total of at most

$$\#W\left(\#W+1\right)\left(|\ell|^2+|\ell|+1\right)M(q(|\ell|^2+|\ell|))$$

multiplications in $\mathbb{F}_q$. Storing the entries of D requires a space of

$$\#W\left(\#W+1\right)\left(q(|\ell|^2+|\ell|)+1\right)$$

elements in $\mathbb{F}_q$.

As for Step 5, since D is a lower triangular matrix, we can use forward substitution to solve the equation $DX = B$ to obtain the solutions

$$\begin{aligned} w_{|\ell|,|\ell|} &= \frac{b_{1,1}}{d_{1,1}}, \\ w_{|\ell|,|\ell|-1} &= \frac{b_{2,1} - d_{2,1}w_{|\ell|,|\ell|}}{d_{2,2}}, \\ &\vdots \\ w_{0,0} &= \frac{b_{\#W,1} - \left(d_{\#W,1}w_{|\ell|,|\ell|} + d_{\#W,2}w_{|\ell|,|\ell|-1} + \cdots + d_{\#W,\#W-1}w_{1,0}\right)}{d_{\#W,\#W}}. \end{aligned}$$

Note that the denominators $d_{m,m}$ above are just ± 1 so there is no actual division here. Moreover, $\deg_T(d_{m,n}) \leq q(|\ell|^2 + |\ell|)$ and by [BL97, Corollary 3.8], we have

$$\deg_T(w_{\mu,\nu}) \leq \frac{q|\ell|(|\ell|+1)^2}{2}.$$

Hence, we need a total of

$$\frac{(\#W-1)\#W}{2}\ M\left(q(|\ell|^2+|\ell|), \frac{q|\ell|(|\ell|+1)^2}{2}\right)$$

multiplications in $\mathbb{F}_q$ to obtain the $w_{\mu,\nu}$, where $\frac{(\#W-1)\#W}{2}$ is the complexity of doing forward substitution.

By comparing all the requirements for this algorithm, we see that Step 4 dominates the other steps. Table 8.2 gives a summary of the asymptotic complexity of each step of Algorithm 8.3.2. We replace N and $\#W$ in the analysis above using the equalities $N = |\ell|^2 + |\ell| - 1$ and $\#W = (|\ell|+1)(|\ell|+2)/2$. Note that by definition of N, we have

$$q^{2\deg_T(\ell)} < N < 2q^{2\deg_T(\ell)}.$$

Theorem 8.3.3. *Algorithm 8.3.2 correctly computes the coefficients $w_{\mu,\nu}$ of the modular polynomial*

$$\Phi_\ell(X,Y) = X^{|\ell|+1} + Y^{|\ell|+1} + \sum_{\mu=0}^{|\ell|}\sum_{\nu=0}^{|\ell|} w_{\mu,\nu}X^\mu Y^\nu,$$

in $O\left(|\ell|^6 M(q|\ell|^2)\right)$ $\mathbb{F}_q$-multiplications, and requires space of $O(q|\ell|^6)$ $\mathbb{F}_q$-elements as $|\ell| \longrightarrow \infty$.

Steps	**Complexity**	
	Operations	Space
1	negligible	negligible
2	$O\left(\lvert\ell\rvert M(\lvert\ell\rvert^2)M(q\lvert\ell\rvert^2)\right)$	$O\left(q\lvert\ell\rvert^5\right)$
3	negligible	negligible
4	$O\left(\lvert\ell\rvert^6 M(q\lvert\ell\rvert^2)\right)$	$O(q\lvert\ell\rvert^6)$
5	$O(\lvert\ell\rvert^4 M(q\lvert\ell\rvert^2, q\lvert\ell\rvert^3))$	–
6	–	–

Table 8.2: Time and space complexity for Algorithm 8.3.2

Proof. The correctness follows from the discussion preceding the algorithm, wherein a system of equations involving the unknowns $w_{\mu,\nu}$ was obtained and solved. The operation and space requirements come from the analysis above. □

Example 8.3.4. As input, let $q = 3$ and $\ell = T + 1 \in \mathbf{A} = \mathbb{F}_3[T]$ with

$$j(z) = \sum_{i=0}^{\infty} a_i s^{i-1}$$

and

$$\begin{aligned} j(\ell z) &= -\frac{((T+1)s+1)^2}{s^3} + \sum_{i=1}^{\infty} a_i \left(\frac{s^3}{((T+1)s+1)^2}\right)^{i-1} \\ &= \frac{2}{s^3} + \frac{T+1}{s^2} + \frac{2T^2+T+2}{s} + \sum_{i=1}^{\infty} a_i \left(\frac{s^3}{((T+1)s+1)^2}\right)^{i-1}, \end{aligned}$$

where the a_i are the coefficients obtained from Example 5.4.9 for $q = 3$. Note that $|\ell| = 3$. We determine the coefficients $w_{\mu,\nu} = w_{\nu,\mu}$ of the polynomial

$$\Phi_\ell(X, Y) = X^4 + Y^4 + \sum_{\mu=0}^{3}\sum_{\nu=0}^{3} w_{\mu,\nu} X^\mu Y^\nu.$$

By (8.21) and (8.22), we get the sets

$$W = \{(\mu, \nu) \mid 0 \le \mu \le 3,\ 0 \le \nu \le \mu\} \quad \text{and} \quad V = \{(k, h) \mid 0 \le k \le 3,\ k \le h \le 3\}.$$

Hence, $\#W = \#V = 10$. Let $i = k|\ell| + h$ for $(k, h) \in V$, which gives

$$I = \{0, 1, 2, 3, 4, 5, 6, 8, 9, 12\}.$$

Calculate the powers $j(z)^e$ and $j(\ell z)^e$ for $e = 2, 3, 4$ to determine the coefficients $a_i(e)$ and $b_i(e)$, respectively. From these coefficients, one obtains

$$B = -\begin{pmatrix} 1 \\ 2T+2 \\ T^2+2T+1 \\ T^3+T+2 \\ T^4+T^3+T+1 \\ 2T^5+T^4+2T^3+2T^2+T+2 \\ 2T^6+2T^4+2T+2 \\ T^8+2T^7+T^6+2T^5+T^4+2T^3+T^2+2T+2 \\ T^7+T^6+2T^4+2T^3+T+1 \\ T^{12}+2T^{10}+T^6+2T^2+2 \end{pmatrix}$$

and

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & d_{3,2} & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ d_{4,1} & d_{4,2} & d_{4,3} & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & d_{5,2} & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & d_{6,2} & d_{6,3} & 0 & d_{6,5} & 2 & 0 & 0 & 0 & 0 \\ d_{7,1} & d_{7,2} & d_{7,3} & d_{7,4} & d_{7,5} & d_{7,6} & 1 & 0 & 0 & 0 \\ 0 & d_{8,2} & d_{8,3} & 0 & d_{8,5} & d_{8,6} & 0 & 1 & 0 & 0 \\ d_{9,1} & d_{9,2} & d_{9,3} & d_{9,4} & d_{9,5} & d_{9,6} & d_{9,7} & d_{9,8} & 2 & 0 \\ d_{10,1} & d_{10,2} & d_{10,3} & d_{10,4} & d_{10,5} & d_{10,6} & d_{10,7} & d_{10,8} & d_{10,9} & 1 \end{pmatrix},$$

with

$$d_{3,2} = 2T^3 + T,$$

$$d_{4,1} = 2T^9 + 2,$$

$$
\begin{aligned}
d_{4,2} &= 2T^6 + 2T^4 + 2T^2, \\
d_{4,3} &= 2T^3 + T \\
&\vdots \\
d_{10,6} &= T^{15} + 2T^{13} + T^{12} + 2T^{10} + T^9 + T^6 + 2T^4 + T + 2, \\
d_{10,7} &= 2T^6 + 2T^4 + 2T^2 + 1, \\
d_{10,8} &= T^{12} + T^9 + T^6 + T^4 + T^3 + T^2 + 2, \\
d_{10,9} &= 2T^3 + T.
\end{aligned}
$$

Finally, the coefficients $w_{\mu,\nu}$ of $\Phi_\ell(X, Y)$ are obtained from the matrix equation $DX = B$ using forward substitution. The required coefficients are as follows:

$$
\begin{aligned}
w_{3,3} &= 2 \\
w_{3,2} &= 2T + 2 \\
w_{3,1} &= 2T^4 + 2T^3 + 2T + 2 \\
w_{3,0} &= T^9 + 2T^7 + 2T^6 + T^4 \\
w_{2,2} &= 2T^{10} + 2T^9 + 2T^4 + 2T^3 + 2T^2 + 2T \\
w_{2,1} &= T^{13} + T^{12} + 2T^{11} + 2T^{10} + 2T^7 + 2T^6 + T^5 + T^4 \\
w_{2,0} &= 0 \\
w_{1,1} &= 2T^{22} + 2T^{21} + 2T^{20} + T^{18} + 2T^{16} + 2T^{15} + 2T^{14} + 2T^{10} + T^9 + 2T^8 \\
w_{1,0} &= T^{27} + 2T^{21} + 2T^{18} + T^{12} \\
w_{0,0} &= T^{36} + 2T^{34} + 2T^{33} + T^{31} + 2T^{30} + T^{28} + T^{24} + 2T^{22} + T^{21} + 2T^{19} + 2T^{18} + T^{16}
\end{aligned}
$$

Let

$$
H = \max_{(\mu,\nu)\in W} \{\deg_T(w_{\mu,\nu})\} = \log_q \max_{0\le\mu,\nu\le|\ell|} \{|w_{\mu,\nu}|\}.
$$

Bae and Lee [BL97, Corollary 3.8] showed that H is bounded as follows:

$$
\frac{|\ell|}{q} \quad \le \quad H \quad \le \quad \frac{q|\ell|(|\ell|+1)^2}{2}. \tag{8.34}
$$

In Example 8.3.4 we get $H = \log_3 |w_{0,0}| = 36$, whereas $q^{\deg(\ell)-1} = 1$ and $(q/2)|\ell|(|\ell|+1)^2 = 72$.

Definition 8.3.5. The value H in the preceding paragraph is called the *(logarithmic) height* of $\Phi_\ell(X, Y)$.

Remark 8.3.6.

1. Based on (8.34) and $\#W$, we see that storing $\Phi_\ell(X, Y)$ requires $O(q|\ell|^5)$ space of $\mathbb{F}_q$ elements.
2. We can also apply Theorem 5.5.9 to Drinfeld modules over $\mathbb{F}_\mathfrak{p} = \mathbf{A}/\mathfrak{p}$, with $\mathfrak{p} = (P)$ and $\gcd(\ell, P) = 1$, by reducing $\Phi_\ell(X, Y)$ modulo P. The roots of these polynomial in $\mathbb{F}_\mathfrak{p}$ are the j-invariants of Drinfeld modules over $\mathbb{F}_\mathfrak{p}$.

Example 8.3.7. Recall from Example 6.1.8 that we obtained some explicit isogenies between Drinfeld modules φ and ψ defined over $\mathbb{L} = \mathbb{F}_\mathfrak{p} = \mathbf{A}/\mathfrak{p}$, where $\mathbf{A} = \mathbb{F}_3[T]$ and $\mathfrak{p}$ is generated by $P(T) = T^5 + 2T + 1$. Here we show that $j(\psi)$ is a root of $\Phi_\ell(X, j(\varphi))$, which verifies that $\varphi/\mathbb{F}_\mathfrak{p}$ and $\psi/\mathbb{F}_\mathfrak{p}$ are ℓ-isogenous. This example is evidence of the correctness of our implementation.

(a) T-isogeny: Let $\varphi = (T^2, T^3)$ and $\psi = (2T^4 + T^2, 2T^4 + T + 2)$, with j-invariants $j(\varphi) = T + 2$ and $j(\psi) = 2T^4 + T^3 + 2T^2 + T + 2$, respectively. In $\mathbb{F}_\mathfrak{p}$, we have

$$\begin{aligned}\Phi_T(X, j(\varphi)) = X^4 &+ (2T^3 + 1)X^3 + (T^3 + 2T^2 + 1)X^2 + (T^3 + 2T^2 + T + 1)X \\ &+ 2T^3 + T^2 + 2T + 1.\end{aligned}$$

This polynomial has four roots in $\mathbb{F}_\mathfrak{p}$:

$$\begin{aligned} &2T^4 + 2T^3 + T^2 + T + 1, && 2T^4 + T^3 + 2T^2 + T + 2 = j(\psi), \\ &T^4 + T^2 + T + 2, && T^4 + T^3 + 2T^2. \end{aligned}$$

So $j(\psi)$ is a root of $\Phi_\ell(X, j(\varphi))$.

(b) $(T+1)$-isogeny: Let $\varphi = (T^2, T^2+2T)$ and $\psi = (2T^4+2T+2, 2T^3+T^2+2T)$ with j-invariants $j(\varphi) = T^2$ and $j(\psi) = T^4+2T^3+T^2$. Now

$$\Phi_{T+1}(X, j(\varphi)) = X^4 + (2T^4+T^3+2T+1)X^3 + (2T^4+2T^3+2T^2)X^2 + (2T^3+2T^2+2T+1)X + T^2$$

has two roots in $\mathbb{F}_{\mathfrak{p}}$, namely $2T^3+T$ and $j(\psi) = T^4+2T^3+T^2$. So

$$\Phi_{T+1}(j(\psi), j(\varphi)) = 0.$$

(c) $(T+2)$-isogeny: Let $\varphi = (T^3, T^4+1)$ and $\psi = (2T^4+1, T^4+T^3+T^2+1)$ with $j(\varphi) = T^4+T^3+T^2+2T+2$ and $j(\psi) = 2T^4+2T^3+2T+2$, respectively. The four roots of

$$\Phi_{T+2}(X, j(\varphi)) = X^4 + (T^4+2T^3+2T^2+1)X^3 + (2T^4+T+2)X^2 + (2T^4+T^3+2T^2+T)X + T^4+T^2+2T$$

in $\mathbb{F}_{\mathfrak{p}}$ are

$$2T^2+2, \qquad 2T^4+2T^3+2T+2 = j(\psi),$$
$$2T^4+2T^3+T^2+2T+2, \qquad T^4+T^2+2T+2.$$

So $j(\psi)$ satisfies

$$\Phi_{T+2}(j(\psi), j(\varphi)) = 0.$$

We present a few more examples of modular polynomials $\Phi_\ell(X, Y)$ in Section A.1. These were obtained by implementing Algorithm 8.3.2 in SAGE [S+17]. So far, we have computed the Drinfeld modular polynomials for

1. $\ell = T$ for primes powers $2 \le q \le 25$,
2. $\ell = T+\varepsilon$, $\varepsilon \in \mathbb{F}_q^*$ for primes $2 \le q \le 23$, and

3. all primes $\ell \in \mathbf{A}$ of degree 2 for $q = 2, 3, 5$.

We noticed in our computations that for $\deg_T(\ell) = 1$, the logarithmic height H of $\Phi_\ell(X, Y)$ is exactly equal to $q(|\ell|^2 + |\ell|)$. It is also worth mentioning that we have conducted several tests on the results we obtained.

(a) We compared the modular polynomials we computed with those given in [BL97] (for $\ell = T$ and $T + 1$ with $q = 3$ and for $\ell = T$ with $q = 3$) and [Sch95] (for $\ell = T$ with $q = 2, 3, 4, 5$). The modular polynomials we computed agree with those given in the two papers.

(b) We verified that the j-invariants $j(\varphi)$ and $j(\psi)$ of ℓ-isogenous Drinfeld modules φ and ψ, respectively, obtained using Proposition 6.1.6 are roots of $\Phi_\ell(X, Y)$. This verification was done using $q = 3, 5, 7$, $\ell = T + \varepsilon$ with $\varepsilon \in \mathbb{F}_q$, and $[\mathbb{F}_\mathfrak{p} : \mathbb{F}_q] = 2, 3, 4, 5$.

(c) All the Drinfeld modular polynomials we computed satisfied the Kronecker congruence relation given in Theorem 5.5.7.

The main issue in computing (classical) modular polynomials, as pointed out for example, in [Elk98] and [Coh84] in the elliptic curve case is the rapid growth in the size and number of the coefficients. The height $h(\Phi_n)$ (the logarithm of the maximum absolute value of the coefficients) of the modular polynomial $\Phi_n(X, Y)$ in the elliptic curve case is estimated to be $6(n + 1) \log n$, for a prime $n \in \mathbb{Z}$ (see [Coh84]). We also have the same main obstacle in the Drinfeld module case. The size (in terms of degrees) and number of coefficients of $\Phi_\ell(X, Y)$ also grow rapidly, especially when $\deg(\ell) > 1$. For high degrees of ℓ, it is likely that the number of coefficients would make it impossible to store the resulting modular polynomials. Moreover, the degrees of the coefficients $a_i(e)$, $b_i(e)$, and $c_i(\mu, \nu)$ also increase as $|\ell|$ (or $\deg(\ell)$) increases. Recall that the largest degree bound on these coefficients is equal to $q(|\ell|^2 + |\ell|)$. If $\deg(\ell) = 1$, then we get a degree bound of $q^3 + q^2$. But as soon as $\deg(\ell)$ becomes greater than 1, the degree bound $q(|\ell|^2 + |\ell|)$ also grows. Further, as the height of

$\Phi_\ell(X, Y)$ is dependent on ℓ, it also increases as $\deg(\ell)$ gets larger. Roughly, we need $O(q|\ell|^5)$ space to store the resulting modular polynomial. So again, this demands a considerable amount of storage. Finally, we mention that a substantial number of precomputations is also required in the computation of Drinfeld modular polynomials, which starts from the calculation of s-expansions of the j-invariants involved in the algorithm above, see Section 8.2.

8.4 Computation of ℓ-Isogeny Volcanoes of Drinfeld Modules

Throughout this section we assume that q is a power of an odd prime $p \in \mathbb{Z}$ and $\mathbb{F}_\mathfrak{p}$ is an $\mathbf{A}$-field with q^d elements and $\mathbf{A}$-characteristic $\mathfrak{p} = (P(T))$, where $\deg_T(P) = d$. Assume that $\ell \in \mathbf{A}^+$ is prime with $\ell \neq P$. Our objective here is to give an algorithm for computing ℓ-isogeny volcanoes for ordinary rank two Drinfeld modules defined over $\mathbb{F}_\mathfrak{p}$ whose j-invariants are not equal to 0. Our main tool for constructing this algorithm is the modular polynomial $\Phi_\ell(X, Y)$.

We require some precomputations for the algorithm. Recall that a Drinfeld module $\varphi/\mathbb{F}_\mathfrak{p}$ is uniquely determined by

$$\varphi_T = \gamma(T) + g\tau + \Delta\tau^2, \quad g \in \mathbb{F}_\mathfrak{p},\ \Delta \in \mathbb{F}_\mathfrak{p}^*.$$

We use Proposition 6.3.8 and apply (5.37) to the pair (g, Δ) to compute the Hasse invariant $H(\varphi)$ beforehand to check whether or not $\varphi/\mathbb{F}_\mathfrak{p}$ is ordinary. Note that this precomputation requires application of the Frobenius of $\mathbb{F}_q$, i.e., the q-th power map. If $\varphi/\mathbb{F}_\mathfrak{p}$ is ordinary, we then compute its j-invariant $j = g^{q+1}/\Delta$. We also need to determine $\Phi_\ell(X, Y) \pmod{\mathfrak{p}}$.

Now suppose $H(\varphi) \not\equiv 0 \pmod{\mathfrak{p}}$. We say that a j-invariant is *visited* if we have determined all the roots of $\Phi_\ell(X, j)$, otherwise, we say that it is *unvisited*. Accordingly, we construct the sets V and U for the visited and unvisited j-invariants, respectively. Let E be the multiset of undirected edges (j_1, j_2), where j_1 and j_2 satisfy $\Phi_\ell(j_1, j_2) = 0$. Note that due to dual isogenies, we consider the edge (j_1, j_2) the same as (j_2, j_1).

In the following description of our algorithm, we have to check whether or not 0 is among the roots of $\Phi_\ell(X, j)$ to avoid components containing this j-invariant. Recall from Section 7.2.3 that a Drinfeld module with j-invariant 0 could be ordinary or supersingular and it has extra automorphisms.

We start at $j = j(\varphi)$ and determine the set of roots R in $\mathbb{F}_\mathfrak{p}$ of $\Phi_\ell(X, j)$. Add j to V. If $R \neq \emptyset$, say $R = \{r_1, r_2, \ldots, r_k\}$, and $0 \notin R$, then add the roots $r_1, r_2, \ldots, r_k$ to U. Add the pairs (r_i, j), for $1 \leq i \leq k$, to E (counting root multiplicities). Now if j is one of the roots r_i, we remove it from U to guarantee that we will not visit it again. If $U \neq \emptyset$, then we take an element $u \in U$, and apply the same process to u. Find the set of roots $R' = \{r'_1, r'_2, \ldots, r'_m\}$ of $\Phi_\ell(X, u)$. Note that R' contains j, so it is not empty. If $0 \notin R'$, then add u to V and add the roots $r'_1, r'_2, \ldots, r'_m$ to U. Add the pair (r'_i, u), for $1 \leq\ i \leq m$, to E (counting root multiplicities) if $(u, r'_i) \notin E$. Remove from U any root r'_i that coincides with j or u. We continue this process until we finally exhausted all the elements of U. Then we construct the graph G with vertex set V and edge set E.

This process leads to the following algorithm.

Algorithm 8.4.1. Computing an ℓ-Volcano for a Drinfeld module

Input: An odd prime power $q \in \mathbb{Z}$, a finite field $\mathbb{F}_\mathfrak{p}$ with q^d elements, a nonzero vertex $j \in \mathbb{F}_\mathfrak{p}$, where $j \neq 0$ is the j-invariant of an ordinary Drinfeld module $\varphi/\mathbb{F}_\mathfrak{p}$, and the modular polynomial $\Phi_\ell(X, Y)$.

Output: The ℓ-isogeny volcano $G \subset G_\ell(\mathbb{F}_\mathfrak{p})$ containing $j(\varphi)$.

1. $E \longleftarrow \{\}$ and $V \longleftarrow \{j\}$.
2. Compute $\Phi_\ell(X, j)$.
3. $U \longleftarrow \{\text{roots of } \Phi_\ell(X, j) \text{ in } \mathbb{F}_\mathfrak{p}\} - V$.
4. If $0 \in U$, then exit the algorithm.
5. $E \longleftarrow E \cup \{(u, j)\}$ for $u \in U$ (counting root multiplicities).

6. For u in U:

   (a) Compute $\Phi_\ell(X, u)$.

   (b) $R' \longleftarrow \{\text{roots of } \Phi_\ell(X, u) \text{ in } \mathbb{F}_\mathfrak{p}\} - V$.

   (c) If $0 \in R'$, then exit the algorithm.

   Else,

   i. $V \longleftarrow V \cup \{u\}$ and $U \longleftarrow U \cup R'$.

   ii. $E \longleftarrow E \cup \{(r', u)\}$ for $r' \in R'$ (counting root multiplicities), if $(u, r') \notin E$.

   iii. $U \longleftarrow U - V$.

7. Construct the graph G with vertex set V and edge set E.

8. Output G.

Before we analyze the complexity of this algorithm, we first determine the size of G and then obtain a bound on this size. Recall that ordinary Drinfeld modules in an ℓ-isogeny volcano belong to the same isogeny class, and this class is determined by the characteristic polynomial $P_{a,b}$ of the Frobenius F as we have seen in Section 7.2. Let $\mathcal{K} = \mathbf{K}\left(\sqrt{a^2 - 4b}\right)$, where $b = \varepsilon P$ for some $\varepsilon \in \mathbb{F}_q^*$ and $P = P(T)$ is the monic generator of $\mathfrak{p}$. As in the previous chapter, let $\mathbf{A}[F]$ be the Frobenius order in $\mathcal{K}$. Again, we use f_F to denote the Frobenius conductor and f_φ to represent the endomorphism conductor. Then we have the following result.

Lemma 8.4.2. *Let G be an ℓ-isogeny volcano of an ordinary Drinfeld module $\varphi/\mathbb{F}_\mathfrak{p}$ such that $0 \notin G$. Let s be the size of its crater, n its height, and m be its number of vertices. Then m is one of the following:*

(a) $1 + (|\ell| + 1)\left(\frac{|\ell|^n - 1}{|\ell| - 1}\right)$,

(b) $2\left(\frac{|\ell|^{n+1} - 1}{|\ell| - 1}\right)$,

(c) $s|\ell|^n$.

Proof. Note that the height of G is $\nu_\ell(f_F) = n \geq 0$. We partition G into sets G_k, $k = 0, 1, \ldots, n$, where G_k is the set of all vertices at level k of G. We determine m by considering the cases in Table 7.2.

1. $\ell \nmid f_\varphi$ and $\ell \nmid f_F/f_\varphi$: In this case $n = 0$, i.e., $\mathbf{A}[F]$ is ℓ-maximal. So $G = G_0$ and $m = s = \#G_0$. We see from Table 7.2 that there are three possible cases: (a) $\varphi/\mathbb{F}_\mathfrak{p}$ has one horizontal ℓ-isogeny, so G could be a vertex with a loop or a simple edge which implies that $s = 1$ or $s = 2$; (b) $\varphi/\mathbb{F}_\mathfrak{p}$ has two horizontal ℓ-isogenies, so G could be a simple cycle or a double edge or a vertex with two loops which implies that $s \geq 1$; or (c) $\varphi/\mathbb{F}_\mathfrak{p}$ has no ℓ-isogenies, so $s = 1$ and G is an isolated vertex with no loops. In all cases, m takes on one of the values in the lemma with $n = 0$.

2. $\ell \nmid f_\varphi$ and $\ell \mid f_F/f_\varphi$: Here $\ell \mid f_F$, i.e., $\mathbf{A}[F]$ is not ℓ-maximal. Therefore $n \geq 1$. In this case $j(\varphi)$ is in the crater G_0. Then we have the three cases shown in Figure 7.2. In Figure 7.2(a), we see that $s = \#G_0 = 1$. Table 7.2 shows that ℓ is inert in $\mathcal{O}_\mathcal{K}$, so there are $|\ell| + 1$ descending ℓ-isogenies from $j(\varphi)$, and hence, $\#G_1 = |\ell| + 1$. Due to the $(|\ell|+1)$-regularity condition on internal vertices of the sides of a volcano (see Theorem 7.2.22), each vertex in G_1 has $|\ell|$ descending ℓ-isogenies and one ascending isogeny. So $\#G_2 = (|\ell| + 1)|\ell|$. Following the same argument, we see that $\#G_n = (|\ell| + 1)|\ell|^{n-1}$. So
$$m = 1 + (|\ell| + 1)\sum_{i=0}^{n-1} |\ell|^i = 1 + (|\ell| + 1)\left(\frac{|\ell|^n - 1}{|\ell| - 1}\right).$$
Now in Figure 7.2(b), $s = \#G_0 = 2$. We see from Table 7.2 that ℓ is ramified in $\mathcal{O}_\mathcal{K}$ and $j(\varphi)$ has one horizontal ℓ-isogeny and $|\ell|$ descending ℓ-isogenies. Thus, $\#G_1 = 2|\ell|$. Now, due to the $(|\ell|+1)$-regularity condition, each vertex in G_1 has one ascending and $|\ell|$ descending ℓ-isogenies. Thus, $\#G_2 = 2|\ell|^2$. By continuing this argument, we see that the floor G_n has $2|\ell|^n$ vertices. Therefore,
$$m = 2\sum_{i=0}^{n} |\ell|^i = 2\left(\frac{|\ell|^{n+1} - 1}{|\ell| - 1}\right).$$

As for Figure 7.2(c), $s = \#G_0$. Table 7.2 shows that $j(\varphi)$ has two horizontal and $|\ell| - 1$ descending ℓ-isogenies. Thus, $\#G_1 = s(|\ell| - 1)$. Now each vertex in G_1 has one ascending and $|\ell|$ descending ℓ-isogenies by Theorem 7.2.22 so $\#G_2 = s(|\ell| - 1)|\ell|$. So down to the floor, we see that $\#G_n = s(|\ell| - 1)|\ell|^{n-1}$. It follows that

$$m = s + s(|\ell| - 1)\sum_{i=0}^{n-1} |\ell|^i = s|\ell|^n.$$

3. $\ell \mid f_\varphi$ and $\ell \nmid f_F/f_\varphi$: In this case $\ell \mid f_F$, i.e., $\mathbf{A}[F]$ is not ℓ-maximal and $n \geq 1$. We see from Table 7.2 that $\varphi/\mathbb{F}_\mathfrak{p}$ has only one ascending ℓ-isogeny, in which case, $\varphi/\mathbb{F}_\mathfrak{p}$ is on the floor G_n. Since $n \geq 1$, G must be one of the volcanoes in Figure 7.2. So we already have determined m from the second case above.

4. $\ell \mid f_\varphi$ and $\ell \mid f_F/f_\varphi$: Clearly, $\ell \mid f_F$ in this case so that $n \geq 1$.As shown in Table 7.2, $\varphi/\mathbb{F}_\mathfrak{p}$ has one ascending and $|\ell|$ descending ℓ-isogenies. So $\varphi/\mathbb{F}_\mathfrak{p}$ must be on the side of G. It also follows that G must be one of the volcanoes in Figure 7.2, in which case, we already have m from the second case above.

□

As we noted earlier, Drinfeld modules over $\mathbb{F}_\mathfrak{p}$ which are contained in an isogeny volcano belong to the same isogeny class. It follows that $m = \#G$ in the preceding lemma is bounded. In particular,

$$m \leq \#j_{a,b}(\mathbb{F}_\mathfrak{p}),$$

where $j_{a,b}(\mathbb{F}_\mathfrak{p})$ is as defined in (7.4). Note that $\#j_{a,b}(\mathbb{F}_\mathfrak{p})$ is equal to the Hurwitz class number (see (3.6)), $\mathbf{H}(\mathbf{A}[F])$, of $\mathbf{A}[F]$ as stated in [Gek08, Proposition 6.8] (see also [Yu95b, Corollary to Proposition 7]).[1]. Recall that $\mathbf{A}[F]$ has discriminant D_F as given in (7.1). We determine a bound on $\mathbf{H}(\mathbf{A}[F])$. Let f' be the conductor of $\mathcal{O}'$ for every $\mathcal{O}'$ containing $\mathbf{A}[F]$, and note

[1]The term *Gauss class number* is used in [Gek08] instead of the term Hurwitz class number in [Yu95b].

that $f' \mid f_F$. Additionally, $[\mathcal{O}_{\mathcal{K}}^* : \mathcal{O}'^*] = 1$ in our case. Using (3.6) and (3.5) gives us

$$\mathbf{H}(\mathbf{A}[F]) = \sum_{f'|f_F} h'(\mathcal{O}') = \sum_{f'|f_F} h(\mathcal{O}') \leq \sum_{f'|f_F} |f'| h(\mathcal{O}_{\mathcal{K}}) \prod_{Q|f'} \left(1 - \frac{\chi_{\mathcal{K}}(Q)}{|Q|}\right), \tag{8.35}$$

where Q runs through all the monic irreducible divisors of f'. Note that $\chi_{\mathcal{K}}(Q) \in \{-1, 0, 1\}$ and $q \leq |Q|$ for every Q dividing f', so $(1 - \chi_{\mathcal{K}}(Q)/|Q|) \leq (1 + 1/q)$. Let $\omega(f')$ be the number of distinct irreducible factors of f'. Then $\omega(f') \leq \deg_T(f')$. This bound is sharp and is attained if f_F splits into linear polynomials that are inert. Also, note that $|f'| = q^{\deg_T(f')}$. So

$$\mathbf{H}(\mathbf{A}[F]) \leq h(\mathcal{O}_{\mathcal{K}}) \sum_{f'|f_F} |f'| \left(1 + \frac{1}{q}\right)^{\deg_T(f')} = h(\mathcal{O}_{\mathcal{K}}) \sum_{f'|f_F} (q+1)^{\deg_T(f')}.$$

Let $\tau(f_F)$ be the number of divisors of f_F. Then

$$\tau(f_F) \leq \sum_{i=1}^{\deg_T(f_F)} \binom{\deg_T(f_F)}{i} \leq 2^{\deg_T(f_F)} - 1,$$

where equality is attained when f_F splits into $\deg_T(f_F)$ distinct linear factors over $\mathbb{F}_q$. Note that $\deg_T(f') \leq \deg_T(f_F)$. So we have

$$\mathbf{H}(\mathbf{A}[F]) \leq h(\mathcal{O}_{\mathcal{K}})(2^{\deg_T(f_F)} - 1)\,(q+1)^{\deg_T(f_F)}$$

Now, $h(\mathcal{O}_{\mathcal{K}}) = \eta h(\mathcal{K})$ by Theorem 3.5.3 with $\eta \in \{1, 2\}$. So

$$h(\mathcal{O}_{\mathcal{K}}) \leq 2h(\mathcal{K}) \leq 2(\sqrt{q} + 1)^{2g}$$

by Lemma 3.5.4, where $\deg_T(D_{\mathcal{K}}) \in \{2g+1, 2g+2\}$. So $\deg_T(D_{\mathcal{K}}) = 2g + 1 + \epsilon$ where

$$\epsilon = \begin{cases} 0, & \text{if } d \text{ is odd} \\ 1, & \text{if } d \text{ is even.} \end{cases}$$

Recall that $D_F = f_F^2 D_{\mathcal{K}} = a^2 - 4\varepsilon P(T)$ with $\varepsilon \in \mathbb{F}_q^*$ (see (7.1)). Note that

$$d = \deg_T(D_F) = 2\deg_T(f_F) + 2g + 1 + \epsilon,$$

so $2g + 2\deg_T(f_F) = d - 1 - \epsilon$ and $2\deg_T(f_F) = d - 2g - 1 - \epsilon \leq d - 1 - \epsilon$. Also,

$$d - 1 - \epsilon = \begin{cases} d-2, & \text{if } d \text{ is even} \\ d-1, & \text{if } d \text{ is odd} \end{cases}.$$

So

$$d - 1 - \epsilon = 2\left\lfloor \frac{d-1}{2} \right\rfloor.$$

Then

$$\begin{aligned} \mathbf{H}(\mathbf{A}[F]) &\leq 2(\sqrt{q}+1)^{2g}(2^{\deg_T(f_F)} - 1)\,(q+1)^{\deg_T(f_F)} \\ &< 2(\sqrt{q}+1)^{2g+2\deg_T(f_F)}2^{\deg_T(f_F)}, \end{aligned}$$

as $q + 1 < (\sqrt{q}+1)^2$ and $2^x - 1 < 2^x$. It follows that

$$\mathbf{H}(\mathbf{A}[F]) < 2\left(\sqrt{2}(\sqrt{q}+1)\right)^{d-1-\epsilon}.$$

So

$$m = O\left((\sqrt{2}(\sqrt{q}+1))^{d-1-\epsilon}\right). \tag{8.36}$$

One of the required inputs for Algorithm 8.4.1 is the j-invariant of a Drinfeld module $\varphi/\mathbb{F}_\mathfrak{p}$ determined by $\varphi_T = (g, \Delta)$ with $g \in \mathbb{F}_\mathfrak{p}$ and $\Delta \in \mathbb{F}_\mathfrak{p}^*$. In particular, j depends on g and Δ since $j = g^{q+1}/\Delta$. The size of $\varphi/\mathbb{F}_\mathfrak{p}$ is approximately

$$2d\log q = 2\log q^d = 2\log|P|.$$

So to measure complexity and storage requirements of an algorithm in terms of the size of $\varphi/\mathbb{F}_\mathfrak{p}$, we need to let $q^d = |P| \longrightarrow \infty$. Another input in the algorithm is the modular polynomial which is measured in terms of its degree $|\ell|+1$. So we also need to determine the complexity as $|\ell| \longrightarrow \infty$. So in this case, three quantities can tend to ∞, namely $\deg_T(\ell)$, $\deg_T(P)$, and q.

Recall from Section 8.1 that $R(n)$ is the number of $\mathbb{F}_\mathfrak{p}$-operations required to find a root of a polynomial of degree n over $\mathbb{F}_\mathfrak{p}$.

Theorem 8.4.3. *Let $\varphi/\mathbb{F}_{\mathfrak{p}}$ be an ordinary Drinfeld module with j-invariant $j(\varphi) \neq 0$. Algorithm 8.4.1 correctly computes the ℓ-isogeny volcano $G \subset G_\ell(\mathbb{F}_{\mathfrak{p}})$ containing $j(\varphi)$ using*

$$O\left((\sqrt{2}(\sqrt{q}+1))^{2\left\lfloor\frac{d-1}{2}\right\rfloor}R(|\ell|)M(d)\right) \tag{8.37}$$

$\mathbb{F}_q$-multiplications, as $|P|, |\ell| \longrightarrow \infty$, where $d = \deg_T(P)$.

Proof. All the vertices in the volcano are visited and each pair of Drinfeld modules $\varphi/\mathbb{F}_{\mathfrak{p}}$ and $\psi/\mathbb{F}_{\mathfrak{p}}$ with j-invariants $j(\varphi)$ and $j(\psi)$, respectively, satisfying $\Phi_\ell(j(\varphi), j(\psi)) = 0$ are ℓ-isogenous via Theorem 5.5.9. Moreover, $G \subset G_\ell(\mathbb{F}_{\mathfrak{p}})$ is an ordinary connected component with j-invariants of ℓ-isogenous ordinary Drinfeld modules as vertices and with edges determined by isogenies between Drinfeld modules. So it follows from Corollary 7.2.11 that G is an isogeny volcano. The correctness of Algorithm 8.4.1 now follows.

Assume that $\Phi_\ell(X, Y)$ is already known. We have to compute $\Phi_\ell(X, v)$ in $\mathbb{F}_{\mathfrak{p}}$, for each $v \in G$. Polynomial evaluation costs $O(|\ell|)$ $\mathbb{F}_{\mathfrak{p}}$-multiplications in this case since $\Phi_\ell(X, v)$ is of degree $|\ell| + 1$ (see Section 8.1), and one multiplication in $\mathbb{F}_{\mathfrak{p}}$ costs $O(M(d))$ $\mathbb{F}_q$-operations by Lemma 8.1.2. So polynomial evaluation costs $O(|\ell|M(d))$ $\mathbb{F}_q$-operations.

Next, we need to determine the roots of $\Phi_\ell(X, v)$ in $\mathbb{F}_{\mathfrak{p}}$, for each $v \in G$. Since $\Phi_\ell(X, v)$ is of degree $|\ell| + 1$ in X, this requires $R(|\ell| + 1)$ $\mathbb{F}_{\mathfrak{p}}$-operations. So the total cost of finding the roots of $\Phi_\ell(X, v)$ is $O(R(|\ell|)M(d))$ which dominates the cost of computing $\Phi_\ell(X, v)$. Thus, the total number of $\mathbb{F}_q$-operations required to compute an ℓ-isogeny volcano via Algorithm 8.4.1 is

$$O(mR(|\ell|)M(d)),$$

where m is bounded as in (8.36). So the complexity (8.37) follows. □

Remark 8.4.4. Note that in Algorithm 8.4.1, we have simplified things by assuming that $\Phi_\ell(X, Y)$ is already known. Unlike in the elliptic curve case, however, there is no readily available database of modular polynomials for Drinfeld modules. Only a few examples of

these polynomials have been computed, see [BL97] and [Sch95]. So we had to compute modular polynomials for this research.

Example 8.4.5. Let $\mathbf{A} = \mathbb{F}_3[T]$, $\ell = T$ and $\mathbb{F}_\mathfrak{p} = \mathbf{A}/\mathfrak{p}$, where $\mathfrak{p} = (P(T))$ with $P(T) = T^8 + 2T^5 + T^4 + 2T^2 + 2T + 2$. Recall that Lemma 7.2.13 predicts what form the crater of a volcano takes on depending on how ℓ decomposes in $\mathcal{O}_\mathcal{K}$. We verify that our results conform with this prediction by computing ℓ-isogeny volcanoes over $\mathbb{F}_\mathfrak{p}$ and checking that the crater of each isogeny volcano is one of those indicated in Lemma 7.2.13. Here $\mathcal{K} = \mathbf{K}(\sqrt{a^2 - 4b})$ is obtained by using the Frobenius polynomial $P_{a,b}$ for Drinfeld modules with the following j-invariants:

$$j_1 = 2T^6 + 2T^4 + 2T^3 + 2T + 2 \qquad j_4 = 2T^6 + T^5 + T^3 + T + 1$$

$$j_2 = 2T^5 + 2T^3 + 2T^2 + T + 2 \qquad j_5 = T^5 + 2T^4 + 2T^2 + T + 1$$

$$j_3 = 2T^7 + 2T^5 + T^4 + 2T + 1 \qquad j_6 = T^6 + 2T^4 + 2T^3 + 2T^2 + 2$$

We summarize the values of a, b, and the discriminants $D_F = a^2 - 4b$ in Table 8.3 and the craters of the the isogeny volcanoes and splitting behaviour of ℓ in $\mathcal{O}_\mathcal{K}$ in Table 8.4. All class numbers of maximal orders in this example were computed using MAGMA [BCP97], while the volcanoes were computed using SAGE [S$^+$17]. The class numbers of non-maximal orders were calculated using (3.5).

j	(a, b)	$D_F = a^2 - 4b$
j_1	$(T^4 + T^2, P(T))$	$2(T + 2)(T^5 + 2T + 1)$
j_2	$(T^4 + 2T^3 + T^2 + T + 1, 2P(T))$	$2T(T^3 + T^2 + T + 2)(T^4 + T^3 + T^2 + 1)$
j_3	$(2T^3 + 2T + 1, P(T))$	$2(T + 2)(T^3 + T^2 + 2T + 1)(T^4 + T^2 + 2)$
j_4	$(2T^4 + 2T^3 + 2T^2 + T + 2, 2P(T))$	$2T^2(T^6 + T^5 + T^3 + T^2 + 1)$
j_5	$(2T^4 + 2T^3 + T^2 + T + 2, 2P(T))$	$2T^2(T + 1)(T^5 + T^3 + T^2 + 2)$
j_6	$(2T^4 + 2T^3 + T^2 + T + 2, 2P(T))$	$2T^3(T + 1)^2(T^3 + 2T^2 + 1)$

Table 8.3: Parameters for $\mathcal{K}$ for some volcanoes in $G_T(\mathbb{F}_\mathfrak{p})$

We implemented code in SAGE [S$^+$17] to check that the volcanoes we obtained using Algorithm 8.4.1 satisfy the properties given in Section 7.2; particularly, the type of crater

j	**Crater of the Volcano containing** j	**Behaviour of** T **in** $\mathcal{K}$
j_1	simple cycle	split
j_2	simple edge	ramified
j_3	single vertex	inert
j_4	single vertex	inert
j_5	simple cycle	split
j_6	simple edge	ramified

Table 8.4: Some T-isogeny volcanoes in $G_T(\mathbb{F}_\mathfrak{p})$

and the fact that $G - C$ is a disjoint union of trees, where C is the crater of G. We used the following parameters for our verification:

1. $q = 3$, $d = 2, 3, \ldots, 12$ for $\ell = T$,
2. $q = 3$, $d = 2, 3, \ldots, 8$ for $\ell = T^2 + 1$,
3. $q = 5$, $d = 2, 3, 4, 5$ for $\ell = T$,
4. $q = 9$, $d = 2, 3, 4, 5$ for $\ell = T$.

8.5 Computation of Endomorphism Rings and Explicit Isogenies

Throughout this section we assume that $\ell \in \mathbf{A}^+$ is prime and $\mathbb{F}_\mathfrak{p}$ is an $\mathbf{A}$-field via the structure morphism $\gamma : \mathbf{A} \longrightarrow \mathbb{F}_\mathfrak{p}$ with finite characteristic $\mathfrak{p}$. Here, $\mathfrak{p}$ is generated by a monic irreducible polynomial $P(T) \in \mathbf{A}$ of degree d. So $\#\mathbb{F}_\mathfrak{p} = q^d$, where we assume q to be a power of an odd prime in $\mathbb{Z}$. All Drinfeld modules considered here are not isogenous to a Drinfeld module with j-invariant 0. We also assume that they are ordinary and of rank two. We present some examples involving computations of (1) the endomorphism ring $\mathcal{O}_\varphi = \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\varphi)$ of a Drinfeld module $\varphi/\mathbb{F}_\mathfrak{p}$ and (2) explicit ℓ-isogenies between Drinfeld modules over $\mathbb{F}_\mathfrak{p}$. Again, we use $R(n)$ and $M(n)$ as defined in Section 8.1.

8.5.1 Computation of the Endomorphism Ring

In the elliptic curve case, an important application of isogeny volcanoes is in finding the endomorphism ring of an ordinary elliptic curve over a finite field. See, for instance, [Fou01], [Koh96] and [Sut13]. We show that this is also the case for Drinfeld modules.

The endomorphism ring $\mathcal{O}_\varphi$ of an ordinary Drinfeld module $\varphi/\mathbb{F}_\mathfrak{p}$ is an order in an imaginary quadratic function field $\mathcal{K} = \mathbf{K}(\sqrt{a^2 - 4b})$, where a and b are the coefficients of the Frobenius polynomial $P_{a,b}$ of $\varphi/\mathbb{F}_\mathfrak{p}$ (see Section 7.1). It is uniquely determined by its conductor f_φ in the maximal order $\mathcal{O}_\mathcal{K}$ of $\mathcal{K}$. This conductor can be determined by locating the level of $j(\varphi)$ in its component $G \subset G_\ell(\mathbb{F}_\mathfrak{p})$, for each prime ℓ dividing the conductor f_F of $\mathbf{A}[F]$ in $\mathcal{O}_\mathcal{K}$. Note that the conductor of $\mathbf{A}[F]$ in $\mathcal{O}_\varphi$ is f_F/f_φ, see Lemma 3.2.7. Now let $\nu_\ell(f_F) = n$, which is the height of G. Let $D_\mathcal{K}$ be the discriminant of $\mathcal{O}_\mathcal{K}$. Note that

$$D_F = f_F^2 D_\mathcal{K} = a^2 - 4b = a^2 - 4\varepsilon P \quad \text{and so} \quad f_F^2 = \frac{a^2 - 4\varepsilon P}{D_\mathcal{K}},$$

where $\deg_T(P) = d$ and $2\deg_T(a) \leq d$ by Theorem 6.3.4(ii). We have

$$n = \frac{\nu_\ell\left(\frac{a^2-4\varepsilon P}{D_\mathcal{K}}\right)}{2} = \frac{\deg_T(D_F) - \deg_T(D_\mathcal{K})}{2} \leq \frac{\deg_T(D_F)}{2} \leq \frac{d}{2}. \tag{8.38}$$

If we know $\nu_\ell(f_F/f_\varphi)$, say it is m, then we can determine $\nu_\ell(f_\varphi)$ from m and n. We use Lemma 7.2.24 to find m. So we have to find a descending path from $j(\varphi)$ to the floor of the volcano. The length of this path is m, so $j(\varphi)$ is at level $n - m$ which is the ℓ-adic valuation of f_φ. Note that $j(\varphi)$ admits at most two horizontal ℓ-isogenies. So if we construct three paths from $j(\varphi)$, then at least one of these paths is a descending path. Since the isogenies in a descending path are all descending, it follows that this is the shortest path to the floor of G. We now have proved the correctness of the next algorithm. Here, we assume that the Frobenius polynomial $P_{a,b}$ has been precomputed.

Algorithm 8.5.1. Computing the ℓ-adic valuation of f_φ

Input: A prime $\ell \in \mathbf{A}^+$ dividing f_F, the j-invariant $j = j(\varphi) \neq 0$ of an ordinary Drin-

feld module $\varphi/\mathbb{F}_{\mathfrak{p}}$, the ℓ-adic valuation n of the Frobenius conductor f_F, and the modular polynomial $\Phi_\ell(X, Y)$.

Output: The ℓ-adic valuation f_φ where f_φ is the endomorphism conductor.

1. Compute $\Phi_\ell(X, j)$.
2. Compute the set of roots R of $\Phi_\ell(X, j)$ in $\mathbb{F}_{\mathfrak{p}}$.
3. If $\#R \leq 1$, then output 0.
4. Create three distinct paths starting from j of length at most n. Stop growing any of these paths until either it has exceeded the length n or it reaches the floor of the isogeny volcano, i.e., the degree of the last visited vertex is 1.
5. Output n minus the length of the shortest path.

Algorithm 8.5.1 is a combination of techniques from Kohel's algorithm for computing endomorphism rings of ordinary elliptic curves using isogeny volcanoes (see [Koh96], p.46) and Fouquet's algorithm for finding a descending path to the floor of an isogeny volcano (see [Fou01], pp.57-58, or [FM02]). Given an ordinary elliptic curve E, Kohel's algorithm finds the level of E in an ℓ-isogeny volcano (with a prime $\ell \in \mathbb{Z}$ in this case) by comparing lengths of two paths from $j(E)$ to the floor of the isogeny volcano. Fouquet's algorithm, on the other hand, compares three paths from $j(E)$ to find a descending path to the floor of the isogeny volcano.

Note that the required inputs for this algorithm are the j-invariant of $\varphi/\mathbb{F}_{\mathfrak{p}}$, a prime $\ell \in \mathbf{A}^+$ dividing the Frobenius conductor, the Drinfeld modular polynomial for ℓ, and the height of the volcano. Similar to Algorithm 8.4.1, we also have to measure complexity in terms of $|P|$ and $|\ell|$.

Theorem 8.5.2. *Algorithm 8.5.1 correctly computes the ℓ-adic valuation of f_F/f_φ in*

$$O(dR(|\ell|)M(d))$$

$\mathbb{F}_q$*-operations, as* $|P|, |\ell| \longrightarrow \infty$*, where* $d = \deg_T(P)$*. Consequently, this algorithm gives the* ℓ*-adic valuation of the endomorphism conductor* f_φ*.*

Proof. What remains to establish is the complexity of Algorithm 8.5.1. We know that the ℓ-adic valuation of f_F/f_φ is bounded by n. If we obtained a path of length greater than n, then this means that the path passed through some vertices along the crater. For each vertex in a path we need to compute $\Phi_\ell(X, v)$ in $O(|\ell|)$ $\mathbb{F}_\mathfrak{p}$-multiplications since $\Phi_\ell(X, v)$ is of degree $|\ell| + 1$ and then find a root of this polynomial in $R(|\ell| + 1)$ $\mathbb{F}_\mathfrak{p}$-multiplications. So the cost of finding roots dominates the cost of polynomial evaluation. As pointed out in Lemma 8.1.2, we must multiply each of the $R(|\ell| + 1)$ $\mathbb{F}_\mathfrak{p}$-multiplication by $M(d)$ to obtain the number of multiplications in $\mathbb{F}_q$. Thus, Algorithm 8.5.1 costs

$$O(nR(|\ell|)M(d))$$

$\mathbb{F}_q$-multiplications and since n is bounded by $d/2$ (see (8.38)), this complexity becomes

$$O(dR(|\ell|)M(d))$$

$\mathbb{F}_q$-multiplications as $|P|, |\ell| \longrightarrow \infty$. □

Example 8.5.3. Let $q = 3$, $\ell = T \in \mathbf{A} = \mathbb{F}_3[T]$, and $\mathbb{F}_\mathfrak{p} = \mathbf{A}/\mathfrak{p}$, where $\mathfrak{p} = (P(T))$ with $P(T) = T^{12} + T^6 + T^5 + T^4 + T^2 + 2 \in \mathbf{A}$. Consider the Drinfeld module

$$\varphi/\mathbb{F}_\mathfrak{p} = (g, \Delta) = (T, 2T^{11} + 2T^{10} + T^9 + T^8 + T^7 + T^6 + 2T^3 + T^2 + 2T)$$

with j-invariant $j_0 = j(\varphi) = T^6 + T^5 + 2T^4 + T^3 + T^2 + T + 2$. The Frobenius polynomial here is

$$P_{a,b}(X) = X^2 - aX + b = X^2 - (T^6 + T^5 + 2T^4 + T^2 + 1)X + 2P(T),$$

so the discriminant of $\mathbf{A}[F]$ is

$$D_F = a^2 - 4b = (T^3)^2(2T^6 + 2T^5 + 2T^4 + T^3 + 2T + 1),$$

where $F = 2(T^6 + T^5 + 2T^4 + T^2 + 1) + 2T^3\sqrt{2T^6 + 2T^5 + 2T^4 + T^3 + 2T + 1}$. So $\mathbf{A}[F]$ is not T-maximal and the T-adic valuation of the Frobenius conductor $f_F = T^3$ is 3. By using Algorithm 8.5.1, we get the following three paths P_1, P_2, and P_3 to the floor of the isogeny volcano containing j_0.

1. P_1:

$$j_0 = T^{10} + T^9 + T^3 + T^2 + T + 2$$

$$j_1 = T^{10} + 2T^8 + T^7 + T^6 + 2T^5 + 2T^4 + 2T^3 + 1$$

$$j_2 = 2T^{11} + T^8 + T^7 + 2T^4 + T^3 + 2T + 1$$

2. P_2:

$$j_0 = T^{10} + T^9 + T^3 + T^2 + T + 2$$

$$j_1 = T^{11} + 2T^{10} + T^9 + T^8 + T^7 + 2T^6 + 2T^4 + T^3 + T^2 + T$$

$$j_2 = T^6 + T^5 + 2T^4 + T^3 + T^2 + T + 2$$

$$j_3 = 2T^{11} + T^{10} + 2T^9 + T^7 + T^4 + 2T^3 + 2T^2 + 2T$$

$$j_4 = 2T^{11} + T^{10} + 2T^9 + T^4 + T^3 + 2T$$

$$j_5 = 2T^{10} + T^5 + T^3 + 2T^2 + 2T + 2$$

3. P_3:

$$j_0 = T^{10} + T^9 + T^3 + T^2 + T + 2$$

$$j_1 = 2T^9 + T^4 + T^2 + T$$

$$j_2 = T^{10} + 2T^7 + T^6 + T^2$$

Thus, both P_1 and P_3 are of length 2. So $\nu_\ell(f_F/f_\varphi) = 2$, and $\nu_\ell(f_\varphi) = 1$. Since f_F has only one irreducible factor, we conclude that $f_\varphi = T$, and hence $\mathcal{O}_\varphi = \mathbf{A} + T\mathcal{O}_\mathcal{K}$.

8.5.2 Explicit ℓ-isogenies

In this subsection we present algorithms for computing ℓ-isogenies between ordinary Drinfeld modules over $\mathbb{F}_{\mathfrak{p}}$. Let φ and ψ be rank two ordinary Drinfeld modules over $\mathbb{F}_{\mathfrak{p}}$, which are uniquely determined by

$$\varphi_T = c_0 + c_1\tau + c_2\tau^2 \qquad \text{and} \qquad \psi_T = d_0 + d_1\tau + d_2\tau^2,$$

respectively, where $c_0, c_1, d_0, d_1 \in \mathbb{F}_{\mathfrak{p}}$, $c_2, d_2 \in \mathbb{F}_{\mathfrak{p}}^*$, and $c_0 = d_0 = \gamma(T)$. (see (6.1)). Let $j(\varphi)$ and $j(\psi)$ be the j-invariants of φ and ψ, respectively. Suppose $\varphi/\mathbb{F}_{\mathfrak{p}}$ and $\psi/\mathbb{F}_{\mathfrak{p}}$ are ℓ-isogenous. Then $\Phi_\ell(j(\psi), j(\varphi)) = 0$ in $\mathbb{F}_{\mathfrak{p}}$. Since $\varphi/\mathbb{F}_{\mathfrak{p}}$ and $\psi/\mathbb{F}_{\mathfrak{p}}$ are ℓ-isogenous, there exists an isogeny $u : \varphi \longrightarrow \psi$ of degree ℓ over $\mathbb{F}_{\mathfrak{p}}$, where $u \in \mathbb{F}_{\mathfrak{p}}\{\tau\}$. Our task here is to give an algorithm that determines u. We also present a method for computing the dual isogeny $\widehat{u} : \psi \longrightarrow \varphi$ of u.

Let $\deg_T(\ell) = k \geq 1$. By Remark 6.1.5, it follows that $\deg_T(\ell) = \deg_\tau(u) = \deg_\tau(\widehat{u}) = k$. Write

$$u = \sum_{i=0}^{k} u_i\tau^i \qquad \text{and} \qquad \widehat{u} = \sum_{i=0}^{k} \widehat{u}_i\tau^i.$$

First we determine the coefficients $u_i \in \mathbb{F}_{\mathfrak{p}}$ of u, for $i = 0, 1, \ldots, k$. By Definition 4.3.1, we have

$$u \cdot \varphi_a = \psi_a \cdot u, \qquad \text{for all } a \in \mathbf{A}.$$

In particular,

$$u \cdot \varphi_T = \psi_T \cdot u.$$

So

$$\left(\sum_{i=0}^{k} u_i\tau^i\right) \cdot \left(\sum_{i=0}^{2} c_i\tau^i\right) = \left(\sum_{i=0}^{2} d_i\tau^i\right) \cdot \left(\sum_{i=0}^{k} u_i\tau^i\right).$$

By comparing coefficients, we get a system of $k + 3$ equations for the unknowns u_i for $i = 0, 1, \ldots, k$. This system of equations is of the form

$$
\begin{aligned}
u_0c_0 &= d_0u_0 \\
u_0c_1 + u_1c_0^q &= d_0u_1 + d_1u_0^q \\
u_0c_2 + u_1c_1^q + u_2c_0^{q^2} &= d_2u_0^{q^2} + d_1u_1^q + d_0u_2 \\
&\vdots \\
u_{k-2}c_2^{q^{k-2}} + u_{k-1}c_1^{q^{k-1}} + u_kc_0^{q^k} &= d_2u_{k-2}^{q^2} + d_1u_{k-1}^q + d_0u_k \\
u_{k-1}c_2^{q^{k-1}} + u_kc_1^{q^k} &= d_2u_{k-1}^{q^2} + d_1u_k^q \\
u_kc_2^{q^k} &= d_2u_k^{q^2}.
\end{aligned}
\tag{8.39}
$$

So we use the last $k+1$ equations of this system to determine u. We obtain

$$u_k^{q^2-1} = y$$

from the last equation in (8.39), where $y = c_2^{q^k}d_2^{-1} \in \mathbb{F}_\mathfrak{p}^*$. The existence of u guarantees that y has a (q^2-1)st root in $\mathbb{F}_\mathfrak{p}$. We can also verify the existence of (q^2-1)-st root(s) of y by confirming that

$$y^{\frac{q^d-1}{e}} = 1$$

in $\mathbb{F}_\mathfrak{p}$, where

$$e = \gcd(q^d-1, q^2-1) = \begin{cases} q-1, & \text{if } d \text{ is odd} \\ q^2-1, & \text{if } d \text{ is even.} \end{cases}$$

Furthermore, if y has a (q^2-1)st root in $\mathbb{F}_\mathfrak{p}$, then it has exactly e such roots in $\mathbb{F}_\mathfrak{p}$.

By using (8.39), we can determine the coefficients of u by finding the roots of the following polynomials in $\mathbb{F}_\mathfrak{p}$:

$$
\begin{aligned}
&\text{For } u_k: \quad d_2X^{q^2-1} - c_2^{q^k} = 0 \\
&\text{For } u_{k-1}: \quad d_2X^{q^2} - c_2^{q^{k-1}}X + d_1u_k^q - u_kc_1^{q^k} = 0 \\
&\text{For } u_{k-i}\ (i = 2, 3, \ldots, k): \\
&\quad d_2X^{q^2} - c_2^{q^{k-i}}X + d_0u_{k+2-i} + d_1u_{k+1-i}^q - u_{k+1-i}c_1^{q^{k+1-i}} - u_{k+2-i}c_0^{q^{k+2-i}} = 0.
\end{aligned}
\tag{8.40}
$$

We obtain several $(k+1)$-tuples $(u_0, u_1, \ldots, u_k)$ from (8.40) as possible coefficients of u. Then we choose one of those tuples that satisfy the system (8.39) as the coefficients of u. The validity of the following algorithm now follows.

Algorithm 8.5.4. Computing ℓ-isogenies

Input: A prime $\ell \in \mathbf{A}^+$ of degree $k \geq 1$, the field $\mathbb{F}_\mathfrak{p}$, and two ℓ-isogenous ordinary Drinfeld modules φ and ψ over $\mathbb{F}_\mathfrak{p}$.

Output: The ℓ-isogeny $u : \varphi \longrightarrow \psi$.

1. Compute the coefficients of the equations in (8.39) using

$$u \cdot \varphi_T = \psi_T \cdot u.$$

2. Compute the unknowns $u_0, \ldots, u_k$ using (8.40).
3. $u \longleftarrow \sum_{i=0}^{k} u_i \tau^i$.
4. Output u.

Note that in this algorithm, we assumed that $\varphi/\mathbb{F}_\mathfrak{p}$ and $\psi/\mathbb{F}_\mathfrak{p}$ are ℓ-isogenous. So we know that u exists and its degree (as a polynomial in τ) is $\deg_T(\ell)$. If we input two Drinfeld modules which are not known to be ℓ-isogenous, then the existence of such u is not guaranteed. In this case, we might still find an isogeny from $\varphi/\mathbb{F}_\mathfrak{p}$ to $\psi/\mathbb{F}_\mathfrak{p}$ by exhaustively searching for a polynomial in $\mathbb{F}_\mathfrak{p}\{\tau\}$ of degree $\deg_T(\ell)$ in τ that would satisfy the prerequisites of being an isogeny from $\varphi/\mathbb{F}_\mathfrak{p}$ to $\psi/\mathbb{F}_\mathfrak{p}$.

Remark 8.5.5. Algorithm 8.5.4 does more:

1. It finds all the isogenies φ to ψ, including the ones defined over any extension of $\mathbb{F}_q$, namely all the roots of (8.40) that satisfy (8.39) and belong to the extension.
2. It detects when φ and ψ are not isogenous, by failing to find solutions of (8.40) and (8.39).

As for the computation of $\widehat{u}$, we use u and one of φ_ℓ or ψ_ℓ to compute the coefficients of $\widehat{u}$ (see Proposition 4.3.6 and Definition 4.3.9). We use φ_ℓ in this case. By (4.8), we can write

$$\varphi_\ell = \sum_{i=0}^{2k} a_i \tau^i,$$

where $a_i \in \mathbb{F}_\mathfrak{p}$ for $i = 0, 1, \ldots, 2k$, $a_0 = \gamma(\ell)$, and $a_{2k} \neq 0$. The exact values of the coefficients a_i, for $i = 0, 1, \ldots, 2k$, can be determined by using the following result.

Lemma 8.5.6. *Let $\varphi/\mathbb{F}_\mathfrak{p}$ be a rank two Drinfeld module determined by*

$$\varphi_T = \gamma(T) + g\tau + \Delta\tau^2$$

and $a \in \mathbf{A}$ be a polynomial of degree k. Then $\varphi_a = \sum_{i=0}^{2k} a_i \tau^i$, where the coefficients a_i, for $i = 0, 1, \ldots, 2k$, are determined via the following recursive formula:

$$\begin{aligned} a_0 &= \gamma(a) \\ a_1 &= \left(a_0^q g - a_0 g\right) \gamma(T^q - T)^{-1} \\ a_i &= \left(a_{i-1}^q g - a_{i-1} g^{q^{i-1}} + a_{i-2}^{q^2} \Delta - a_{i-2} \Delta^{q^{i-2}}\right) \gamma(T^{q^i} - T)^{-1}, \text{ for } i = 2, 3, \ldots, 2k. \end{aligned} \tag{8.41}$$

Proof. See [Jun00, Lemma 3.2.2]. □

By Proposition 4.3.6, we have

$$\varphi_\ell = \widehat{u} \cdot u.$$

So

$$\sum_{i=0}^{2k} a_i \tau^i = \left(\sum_{i=0}^{k} \widehat{u}_i \tau^i\right) \cdot \left(\sum_{i=0}^{k} u_i \tau^i\right),$$

from which we obtain the following system of $2k + 1$ equations for the unknowns $\widehat{u}_i$, $i =$

$0, 1, \ldots, k$:

$$\begin{aligned} a_0 &= \widehat{u}_0 u_0 \\ a_1 &= \widehat{u}_0 u_1 + \widehat{u}_1 u_0^q \\ a_2 &= \widehat{u}_0 u_2 + \widehat{u}_1 u_1^q + \widehat{u}_2 u_0^{q^2} \\ &\vdots \\ a_k &= \widehat{u}_0 u_k + \widehat{u}_1 u_{k-1}^q + \cdots + \widehat{u}_k u_0^{q^k} \\ a_{k+1} &= \widehat{u}_1 u_k^q + \widehat{u}_2 u_{k-1}^{q^2} + \cdots + \widehat{u}_k u_1^{q^k} \\ &\vdots \\ a_{2k} &= \widehat{u}_k u_k^{q^k}. \end{aligned} \tag{8.42}$$

This system gives the following recursive formula for the coefficients of $\widehat{u}$:

$$\begin{aligned} \widehat{u}_0 &= a_0 u_0^{-1}, \\ \widehat{u}_m &= \left(a_m - \left(\sum_{i=0}^{m-1} \widehat{u}_i u_{m-i}^{q^i} \right) \right) u_0^{-q^m}, \quad \text{for } 1 \leq m \leq k. \end{aligned} \tag{8.43}$$

Note that this formula gives a unique value of $\widehat{u}$. We summarize the procedure for computing the dual isogeny $\widehat{u} : \psi \longrightarrow \varphi$ as follows:

Algorithm 8.5.7. Computing the dual ℓ-isogeny $\widehat{u} : \psi \longrightarrow \varphi$

Input: A prime $\ell \in \mathbf{A}^+$ of degree k and an ℓ-isogeny $u : \varphi \longrightarrow \psi$ of two ordinary Drinfeld modules φ and ψ over $\mathbb{F}_{\mathfrak{p}}$.

Output: The dual ℓ-isogeny $\widehat{u} : \psi \longrightarrow \varphi$.

1. Compute φ_ℓ using (8.41).
2. Compute the coefficients of the equations in (8.42) using
$$\widehat{u} \cdot u = \varphi_\ell.$$
3. Compute the unknowns $\widehat{u}_0, \ldots, \widehat{u}_k$ using (8.43).
4. $\widehat{u} \longleftarrow \sum_{i=0}^{k} \widehat{u}_i \tau^i$.

5. Output $\widehat{u}$.

For Algorithms 8.5.4 and 8.5.7, we need ℓ-isogenies. Recall that an ℓ-isogeny is a polynomial of degree $k = \deg_T(\ell)$ in τ (see Remark 6.1.5) with coefficients in $\mathbb{F}_{\mathfrak{p}}$. So its size is approximately

$$\log |P|^{\deg_T(\ell)} = k \log |P| = kd \log q.$$

So we measure complexities and size requirements in terms of $|P|^{\deg_T(\ell)} = q^{kd}$ wherein up to three quantities can tend to ∞: $k = \deg_T(\ell)$, $d = \deg_T(P)$, and q.

Theorem 8.5.8. *Let $\ell \in \mathbf{A}^+$ be a prime such that $\gcd(\ell, P(T)) = 1$. Let $\deg_T(P) = d$. If φ and ψ are ℓ-isogenous rank two Drinfeld modules over $\mathbb{F}_{\mathfrak{p}}$, then*

(a) Algorithm 8.5.4 correctly computes $u : \varphi \longrightarrow \psi$ in

$$O(\deg_T(\ell) R(q^2) M(d))$$

$\mathbb{F}_q$-operations, as $|P|^{\deg_T(\ell)} \longrightarrow \infty$.

(b) Algorithm 8.5.7 correctly computes $\widehat{u} : \psi \longrightarrow \varphi$ in

$$O(\deg_T(\ell)^2 M(d))$$

$\mathbb{F}_q$-operations, as $|P|^{\deg_T(\ell)} \longrightarrow \infty$.

Proof. We have already proved the validity of each algorithm. So what remains to be done is to establish the complexity of each. Again, let $\deg_T(\ell) = k$.

(a) We see from (8.39) that computing each coefficient of τ^i in $u \cdot \varphi_T$ (or $\psi_T \cdot u$), for $i = 0, 1, \ldots, k+2$, requires at most three multiplications and three q^i-th powers in $\mathbb{F}_{\mathfrak{p}}$. By Lemma 8.1.1, computing q^i-th power costs $O(M(d))$ $\mathbb{F}_q$-operations. Thus, computing the corresponding coefficient of τ^i in $u \cdot \varphi_T$ costs at most $O(M(d))$ multiplications in $\mathbb{F}_q$. The same number of operations is also required for finding the coefficient of τ^i in

$\psi_T \cdot u$ giving a total of no more than $O(M(d))$ multiplications in $\mathbb{F}_q$. So Step 1 can be completed using at most $O(kM(d))$ multiplications in $\mathbb{F}_q$.

As for Step 2, we need to find roots of the $k+1$ polynomials in (8.40). Note that these polynomials are of degree at most q^2. So finding a root in $\mathbb{F}_{\mathfrak{p}}$ costs $R(q^2)M(d)$ multiplications in $\mathbb{F}_q$. Therefore, this step requires at most

$$(k+1)R(q^2)M(d)$$

$\mathbb{F}_q$-multiplications. So this step dominates the entire algorithm. Therefore, by using Algorithm 8.5.4, we can compute $u : \varphi \longrightarrow \psi$, $u \in \mathbb{F}_{\mathfrak{p}}\{\tau\}$, in

$$O(kR(q^2)M(d))$$

$\mathbb{F}_q$-operations, as $k, d, q \longrightarrow \infty$.

(b) To compute φ_ℓ in Step 1 of Algorithm 8.5.7, we use (8.41). Each coefficient a_i, for $i = 0, 1, \ldots, 2k$, requires at most five multiplications, five q^i-th powers, and one inversion. Again, the powers required in this step are of the form α^{q^i}, for $\alpha \in \mathbb{F}_{\mathfrak{p}}$ and positive integer i. By Lemma 8.1.1, raising to the q^ith power requires $O(M(d))$ $\mathbb{F}_q$-multiplications. The inversion also requires $O(M(d))$ multiplications in $\mathbb{F}_q$ by Lemma 8.1.3. Thus, Step 1 requires at most $O(M(d))$ multiplications in $\mathbb{F}_q$.

For Step 2, we need to compute the number of operations required to compute the coefficients in (8.42). Each coefficient requires at most $k+1$ multiplications and k powers involving the exponents q^i, for $i = 1, 2, \ldots, k$. Again, raising to the q^i-th power requires $O(M(d))$ $\mathbb{F}_q$-multiplications. Note that there are $2k+1$ such coefficients. So Step 2 costs at most

$$O(k^2 M(d))$$

operations in $\mathbb{F}_q$.

For Step 3, note that the values $u_{m-i}^{q^i}$ for $m = 1, 2, \ldots, k$ and $i = 0, 1, \ldots, m-1$ are already accounted for in Step 3. So we do not have to reconsider the number of

operations to obtain these values here. The computation of

$$\widehat{u}_k = \left(a_k - \left(\sum_{i=0}^{k-1} \widehat{u}_i u_{k-i}^{q^i} \right) \right) u_0^{-q^k},$$

is obtained using $k+1$ multiplications and one inversion in $\mathbb{F}_{\mathfrak{p}}$. Again, one inversion in $\mathbb{F}_{\mathfrak{p}}$ requires $O(M(d))$ $\mathbb{F}_q$-operations by Lemma 8.1.3. The total number of multiplications in this step is $((k+1)(k+2)/2)M(d)$. Asymptotically, this gives a complexity of

$$O(k^2 M(d))$$

$\mathbb{F}_q$-multiplications for Step 3. Note that we get the same asymptotic complexity in Step 2. So Algorithm 8.5.7 computes $\widehat{u}$ using $O(k^2 M(d))$ operations in $\mathbb{F}_q$.

□

Example 8.5.9. Let $q = 3$, $\ell = T^2 + 1 \in \mathbf{A} = \mathbb{F}_q[T]$, and $\mathbb{F}_{\mathfrak{p}} = \mathbf{A}/\mathfrak{p}$ with $\mathfrak{p} = (P(T))$ and $P(T) = T^9 + 2T^3 + 2T^2 + T + 1$. The Drinfeld modules $\varphi = (T, T)$ and $\psi = (T, 2T^7 + T^6 + 2T^5 + 2T^4 + 2T^3 + T)$ have j-invariants

$$j(\varphi) = T^3 \qquad \text{and} \qquad j(\psi) = T^8 + 2T^6 + T^2 + T + 1,$$

respectively. These j-invariants satisfy $\Phi_\ell(j(\varphi), j(\psi)) = 0$, so φ and ψ are ℓ-isogenous. We determine an ℓ-isogeny $u : \varphi \longrightarrow \psi$ and its dual $\widehat{u} : \psi \longrightarrow \varphi$, where $u, \widehat{u} \in \mathbb{F}_{\mathfrak{p}}\{\tau\}$.

Note that $\deg_\tau(u) = \deg_T(\ell) = 2$ by Remark 6.1.5, so let $u = u_0 + u_1\tau + u_2\tau^2$. Moreover, u should satisfy the equation

$$u \cdot \varphi_T = \psi_T \cdot u,$$

where

$$\varphi_T = c_0 + c_1\tau + c_2\tau^2 = T + T\tau + T\tau^2$$

and

$$\psi_T = d_0 + d_1\tau + d_2\tau^2 = T + T\tau + (2T^7 + T^6 + 2T^5 + 2T^4 + 2T^3 + T)\tau^2.$$

From (8.39), we obtain

$$\begin{aligned} u_0c_0 &= d_0u_0 \\ u_0c_1 + u_1c_0^3 &= d_0u_1 + d_1u_0^3 \\ u_0c_2 + u_1c_1^3 + u_2c_0^9 &= d_0u_2 + d_1u_1^3 + d_2u_0^9 \\ u_1c_2^3 + u_2c_1^9 &= d_1u_2^3 + d_2u_1^9 \\ u_2c_2^9 &= d_2u_2^9. \end{aligned} \tag{8.44}$$

By using (8.40), we get

$$\begin{aligned} &\text{For } u_2: \quad d_2X^8 - c_2^9 = 0 \\ &\text{For } u_1: \quad d_2X^9 - c_2^3X + d_1u_2^3 - u_2c_1^9 = 0 \\ &\text{For } u_0: \quad d_2X^9 - c_2X + d_0u_2 + d_1u_1^3 - u_1c_1^3 - u_2c_0^9 = 0. \end{aligned} \tag{8.45}$$

Eighteen possible 3-tuples (u_0, u_1, u_2) are obtained from (8.45), only two of which satisfy (8.44). These are

$$(T^7 + 2T^6 + 2T^5 + T^4 + 2T, T^6 + 2T^5 + 2T^4 + T^3 + T + 1, T^7 + T^6 + 2T^5 + 2T^4 + 2T^2)$$

and

$$(2T^7 + T^6 + T^5 + 2T^4 + T, 2T^6 + T^5 + T^4 + 2T^3 + 2T + 2, 2T^7 + 2T^6 + T^5 + T^4 + T^2).$$

Let the coefficients of u be the first of the two solutions above.

Now let us find the dual isogeny $\widehat{u}$ such that $\widehat{u} \cdot u = \varphi_{T^2+1}$. By using (8.41), we obtain

$$\begin{aligned} \varphi_{T^2+1} &= a_0 + a_1\tau + a_2\tau^2 + a_3\tau^3 + a_4\tau^4 \\ &= T^2 + 1 + (T^4 + T^2)\tau + (2T^4 + T^3 + 2T)\tau^2 + (2T^4 + T^3 + 2T^2 + 2T)\tau^3 \\ &\quad + (T^4 + T^3 + 2T^2 + 2T)\tau^4. \end{aligned}$$

Let $\widehat{u} = \widehat{u}_0 + \widehat{u}_1\tau + \widehat{u}_2\tau^2$. Then, by using (8.42), we obtain the following system of equations

$$\begin{aligned}
a_0 &= \widehat{u}_0 u_0 \\
a_1 &= \widehat{u}_0 u_1 + \widehat{u}_1 u_0^3 \\
a_2 &= \widehat{u}_0 u_2 + \widehat{u}_1 u_1^3 + \widehat{u}_2 u_0^9 \\
a_3 &= \widehat{u}_1 u_2^3 + \widehat{u}_2 u_1^9 \\
a_4 &= \widehat{u}_2 u_2^9.
\end{aligned}$$

Finally, we get $\widehat{u} = \widehat{u}_0 + \widehat{u}_1\tau + \widehat{u}_2\tau^2$ by using (8.43), where

$$\begin{aligned}
\widehat{u}_0 &= 2T^7 + 2T^5 \\
\widehat{u}_1 &= 2T^7 + 2T^5 + 2T^4 + T^3 + 2T + 2 \\
\widehat{u}_2 &= 2T^8 + 2T^6 + 2T^5 + 2T^4 + T^3 + T^2 + 2T.
\end{aligned}$$

Remark 8.5.10. We verified that the isogenies u and $\widehat{u}$ from Example 8.5.9 satisfy the equations

(a) $u \cdot \varphi_{T^2+1} = \psi_{T^2+1} \cdot u$,

(b) $\widehat{u} \cdot \psi_{T^2+1} = \varphi_{T^2+1} \cdot \widehat{u}$,

(c) $\widehat{u} \cdot u = \varphi_{T^2+1}$, and

(d) $u \cdot \widehat{u} = \psi_{T^2+1}$,

as expected.

Chapter 9

Conclusion

Our main goal in this research is to study theoretical and computational aspects of rank two Drinfeld modules over $\mathbb{F}_{\mathfrak{p}}$, particularly their ℓ-isogeny volcanoes. We break down this goal into four objectives: establish properties of isogeny volcanoes, compute Drinfeld modular polynomials, compute isogeny volcanoes, and compute endomorphism rings and explicit isogenies of Drinfeld modules.

We derived a classification theorem for ℓ-isogenies of Drinfeld modules. This is analogous to Kohel's theorem for elliptic curves. We use relations of orders in the imaginary quadratic function field $\mathcal{K}$, the parametrization of the Drinfeld modular polynomial $\Phi_\ell(X, Y)$ for pairs of ℓ-isogenous curves, the quadratic reciprocity law, and the Drinfeld module analogue of Deuring lifting theorem to obtain this result. This classification theorem, together with the (number of) roots of Drinfeld modular polynomials, dictate the shape and properties of the isogeny volcanoes that we obtained. The features of these isogeny volcanoes are similar to those in the elliptic curve case.

In order to compute Drinfeld modular polynomials, we need to compute a sufficiently precise approximation of the modular j-function in terms of its Laurent series expansion. So we devised an algorithm for this purpose. It computes the j-invariant up to a certain precision using the power series expansions of the modular forms g and Δ. We gave a detailed complexity analysis for this algorithm and implemented it in SAGE. The algorithm for Drinfeld modular polynomials we presented here was based on the method given in [BL97]. Our main contribution here is a detailed complexity analysis treating both time and space requirements. We implemented this algorithm in SAGE.

As for computing isogeny volcanoes of Drinfeld modules, we devised an algorithm that

leverages our computation of Drinfeld modular polynomials $\Phi_\ell(X, Y)$. This algorithm was also implemented in SAGE. Additionally, we determined a bound on the number of vertices in an ℓ-isogeny volcano using the Hurwitz class number formula.

The last algorithms we devised in this thesis are for computing endomorphism rings and explicit ℓ-isogenies of Drinfeld modules. We find the prime factors of the Frobenius conductor and then determine their valuations in the endomorphism conductor by travelling through the isogeny volcano corresponding to each prime factor. For finding the exact power of any prime dividing the conductor f_φ of the endomorphism ring of a Drinfeld module φ, we use three paths from φ descending to the floor of the isogeny volcano. A shortest among of these paths is then used to obtain the exact power of that factor of f_φ. We performed a detailed runtime analysis for each of these algorithms and also implemented them in SAGE.

Among the first three algorithms that we presented, the algorithm for computing Drinfeld modular polynomials is the most costly. This is due to the size of the polynomials involved in the computation. We also noticed in our computations that for $\deg_T(\ell) = 1$, the logarithmic height H of $\Phi_\ell(X, Y)$ is exactly equal to $q(|\ell|^2 + |\ell|)$. For $\deg_T(\ell) = 2$, we obtained $H < q(|\ell|^2 + |\ell|)$. It would be interesting to know if these observations are true in general.

With the conclusion of this dissertation, we identify some possible future research directions that are related to what we have done. One thing that is of interest is to consider isogenies of rank two ordinary Drinfeld modules defined over finite fields of characteristic 2. In this study we only focused on the odd characteristic case because the endomorphism rings of rank two Drinfeld modules are orders in imaginary quadratic function fields. In particular, we needed the Frobenius endomorphism $\mathbf{A}[F]$ in examining isogeny volcanoes of Drinfeld modules. From its discriminant $D_F = a^2 - 4b$ we built the imaginary quadratic function field $\mathcal{K} = \mathbf{K}(\sqrt{D_F})$. In characteristic 2, $\mathcal{K}$ will not be of the form $\mathcal{K} = \mathbf{K}(\sqrt{D_F})$, i.e., it won't be obtained by adjoining the square root of the Frobenius discriminant. So it may be necessary to build $\mathcal{K}$ using a different method so that it becomes an imaginary

quadratic function field so that we may be able to apply our findings for ordinary Drinfeld modules over fields of characteristic 2.

Kohel treated the case of supersingular elliptic curves in his thesis, [Koh96, Chapter 7]. He showed that the ℓ-isogeny graph containing a supersingular elliptic curve is a connected graph. He also gave an algorithm that computes four (linearly independent over $\mathbb{Z}$) endomorphisms in $\mathrm{End}(E)$ for an ellliptic curve E over a finite field. We excluded supersingular Drinfeld modules and those Drinfeld modules with j-invariants equal to 0 in this thesis. It is interesting to know the properties of the isogeny graphs corresponding to these kinds of Drinfeld modules. Are they similar to Kohel's results? We suspect that there will also be some kind of regularity in the shape of these graphs but they will not resemble a volcano. Moreover, as far as we know, the explicit computation of the endomorphism rings of supersingular Drinfeld modules has not been explored yet.

For elliptic curves, Velu's formulas (see [Gal12, Section 25.1.1]) can be used to compute isogenies. We are not aware of any analogue of these formulas in the Drinfeld module case. Perhaps, a good starting point in this direction is Proposition 4.1.22 or [Yu95b, Section 2].

We are also curious to know if there are other ways to compute isogeny volcanoes of a given Drinfeld module. Recall that Proposition 6.1.6 gives a way to determine an ℓ-isogeny from $\varphi = (g, \Delta)$ to another Drinfeld module, with $\deg_T(\ell) = 1$, by using roots of a polynomial of degree $q + 1$ whose coefficients are $\gamma(\ell)$, g, and Δ. Is it possible to use this method to generate the entire ℓ-isogeny volcano containing φ? And if this is possible, can we determine the Drinfeld modular polynomial $\Phi_\ell(X, Y) \pmod{\mathfrak{p}}$ based on the vertices of this volcano?

One may also explore other possible applications of isogeny volcanoes. In the elliptic curve case, these isogeny volcanoes can be used to detect supersingularity of elliptic curves, see [Sut13]. Due to the similarities between isogeny volcanoes of Drinfeld modules and elliptic curves, detecting supersingularity in the Drinfeld module case may also be possible. Fouquet [Fou01] also used isogeny volcanoes for point counting on elliptic curves. It is interesting to

know if there is an analogue of this problem (and its solution using isogeny volcanoes) in the Drinfeld module case.

Finally, as for computing Drinfeld modular polynomials, we presented another approach for this in Section A.3. It is interesting to study the feasibility and runtime complexity of this approach to determine how it compares with Algorithm 8.3.2.

Bibliography

[Art24] E. Artin. Quadratische Körper im Gebiete der höheren Kongruenzen I and II. *Math. Zeitschr.*, 19(1):153–246, 1924.

[Bae92] S. Bae. On the modular equations for Drinfeld modules of rank 2. *J. Number Theory*, 42:123–133, 1992.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BCRS99] I. F. Blake, J. A. Csirik, M. Rubinstein, and G. Seroussi. On the Computation of Modular Polynomials for Elliptic Curves. Technical report, Hewlett-Packard Laboratories, 1999. Available at `http://www.csirik.net/modpoly-calc.pdf`.

[BK92] S. Bae and J. K. Koo. On the singular Drinfeld modules of rank 2. *Math. Z.*, 210:267–276, 1992.

[BL97] S. Bae and S. Lee. On the coefficients of the Drinfeld modular equation. *J. Number Theory*, 66:85–101, 1997.

[BLS12] R. Bröker, K. Lauter, and A. V. Sutherland. Modular polynomials via isogeny volcanoes. *Math. Comp.*, 81:1201–1231, 2012.

[BR09] F. Breuer and H.-G. Rück. Drinfeld modular polynomials in higher rank. *J. Number Theory*, 129:59–83, 2009.

[CF06] H. Cohen and G. Frey, editors. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Discrete Mathematics and Its Applications. Chapman & Hall/CRC, Boca Raton, USA, 2006.

[CL04] D. Charles and K. Lauter. Computing Modular Polynomials. Technical report, Microsoft Research, 2004. Available at `http://research.microsoft.com/en-us/um/people/klauter/modular_poly_final.pdf`.

[Coh84] P. Cohen. On the coefficients of the transformation polynomials for the elliptic modular function. *Math. Proc. Cambridge Philos. Soc.*, 95:389–402, 1984.

[Cox89] D. A. Cox. *Primes of the Form $x^2 + ny^2$*. Pure and Applied Mathematics. Wiley & Sons, Inc., NJ, USA, 1989.

[DH87] P. Deligne and D. Hussemöller. Survey of Drinfeld modules. *Contemp. Math.*, 67:25–91, 1987.

[Dri74] V. G. Drinfel'd. Elliptic modules. *Math. USSR Sbornik*, 23(4):561–592, 1974.

[DS05] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Number 228 in Graduate Texts in Mathematics. Springer Science + Business Media, LLC, New York, USA, 2005.

[Elk98] N. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin*, pages 21–76. AMS/International Press, 1998.

[Eng09] A. Enge. Computing modular polynomials in quasi-linear time. *Math. Comp.*, 78(267):1809–1824, 2009.

[FM02] M. Fouquet and F. Morain. Isogeny volcanoes and the SEA algorithm. In *Algorithmic Number Theory: 5th International Symposium, ANTS-V Sydney, Australia, July 712, 2002 Proceedings*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 276–291. Springer, Berlin, Germany, 2002.

[Fou01] M. Fouquet. *Anneau d'endomorphismes et cardinalité des courbes elliptiques: aspects algorithmiques*. PhD thesis, École Polytechnique, Palaiseau, France, 2001.

[Gal99] S. D. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS J. Comput. Math.*, 2:118–138, 1999.

[Gal12] S. D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, Cambridge, UK, 2012.

[Gek83] E.-U. Gekeler. Zur Arithmetik von Drinfeld-Moduln. *Math. Ann.*, 262:167–182, 1983.

[Gek85] E.-U. Gekeler. A product expansion for the discriminant function of Drinfeld modules of rank two. *J. Number Theory*, 21:135–140, 1985.

[Gek86] E.-U. Gekeler. *Drinfeld Modular Curves*. Number 1231 in Lecture Notes in Mathematics. Springer-Verlag, Berlin, Germany, 1986.

[Gek88] E.-U. Gekeler. On the coefficients of Drinfeld modular forms. *Invent. Math.*, 93:667–700, 1988.

[Gek91] E.-U. Gekeler. On finite Drinfeld modules. *J. Algebra*, 141:187–203, 1991.

[Gek99] E.-U. Gekeler. A survey of Drinfeld modular forms. *Turk. J. Math.*, 23:485–518, 1999.

[Gek08] E.-U. Gekeler. Frobenius distributions of Drinfeld modules over finite fields. *Trans. Amer. Math. Soc.*, 360(4):1695–1721, 2008.

[Gos78] D. Goss. Von Staudt for $\mathbb{F}_q[T]$. *Duke Math. J.*, 45(4):885–910, 1978.

[Gos80a] D. Goss. The algebraist's upper half-plane. *Bull. Amer. Math. Soc.*, 2(3):391–415, 1980.

[Gos80b] D. Goss. Modular forms for $\mathbb{F}_r[T]$. *J. Reine Angew. Math.*, 317:16–39, 1980.

[Gos98] D. Goss. *Basic Structures of Function Field Arithmetic*. Springer-Verlag, Berlin, Germany, 1998.

[GP02] J. Guajardo and C. Paar. Itoh-Tsujii inversion in standard basis and its application in cryptography and codes. *Des. Codes Cryptogr.*, 25(2):207–216, 2002.

[GS97] E.-U. Gekeler and B. A. Synder. Drinfeld modules over finite fields. In *Drinfeld Modules, Modular Schemes and Applications*, pages 66–87. World Scientific Publishing Co., 1997.

[GvdP80] L. Gerritzen and M. van der Put. *Schottky Groups and Mumford Curves*, volume 817 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, Germany, 1980.

[Hay79] D. R. Hayes. Explicit class field theory in global function fields. In *Studies in Algebra and Number Theory*, Advances in Mathematics Supplementary Studies, pages 173–217, New York, USA, 1979. Academic Press, Inc.

[Hay92] D. Hayes. A brief introduction to Drinfeld modules. In *The Arithmetic of Function Fields*, pages 1–32. de Gruyter & Co., 1992.

[HMV04] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag New York, Inc., New York, USA, 2004.

[Hus04] D. Husemöller. *Elliptic Curves*. Number 111 in Graduate Texts in Mathematics. Springer Science+Business Media, Inc., New York, USA, second edition, 2004.

[HY00] L.-C. Hsia and J. Yu. On characteristic polynomials of geometric Frobenius associated to Drinfeld modules. *Comp. Math.*, 122:261–280, 2000.

[Igu59] J. Igusa. Kroneckerian model of fields of elliptic modular functions. *Amer. J. Math.*, 81:561–577, 1959.

[Jun00] F. Jung. Characteristische Polynome von Drinfeld-Moduln, 2000. Diplomarbeit Saarbrüchen.

[Knu81] D. E. Knuth. *The Art of Computer Programming: Seminumerical Algorithms*, volume 2. Addison-Wesley Publishing Company, Massachusetts, USA, second edition, 1981.

[Koh96] D. Kohel. *Endomorphism Rings of Elliptic Curves Over Finite Fields*. PhD thesis, University of California at Berkeley, California, USA, 1996.

[Lan87] S. Lang. *Elliptic Functions*. Number 112 in Graduate Texts in Mathematics. Springer-Verlag, New York, USA, 2nd edition, 1987.

[Mat97] B. H. Matzat. Introduction to Drinfeld modules. In *Drinfeld Modules, Modular Schemes and Applications*, pages 3–16. World Scientific Publishing Co., 1997.

[Ore33a] O. Ore. On a special class of polynomials. *Trans. Amer. Math. Soc.*, 35(3):559–584, 1933.

[Ore33b] O. Ore. Theory of non-commutative polynomials. *Ann. Math., Second Series*, 34(3):480–508, 1933.

[Rab80] M. Rabin. Probabilistic algorithms in finite fields. *SIAM J. Comput.*, 9:273–280, 1980.

[Rei03] I. Reiner. *Maximal Orders*, volume 28 of *London Mathematical Society Monographs*. Oxford University Press, New York, USA, 2003.

[Ros02] M. Rosen. *Number Theory in Function Fields*. Number 210 in Graduate Texts in Mathematics. Springer-Verlag, New York, USA, 2002.

[S$^+$17] W. A. Stein et al. *Sage Mathematics Software (Version 7.6)*. The Sage Development Team, 2017. `http://www.sagemath.org`.

[Sal06] G. D. Villa Salvador. *Topics in the Theory of Algebraic Function Fields*. Mathematics: Theory and Applications. Birkhäuser, Boston, USA, 2006.

[Sch95] A. Schweizer. On the Drinfeld modular polynomial $\phi_T(X, Y)$. *J. Number Theory*, 52:53–68, 1995.

[Sch01] R. Scheidler. Cryptography in quadratic function fields. *Des. Codes Cryptogr.*, 22:239–264, 2001.

[Sil94] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Number 151 in Graduate Texts in Mathematics. Springer-Verlag, New York, USA, 1994.

[Sil09] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Number 106 in Graduate Texts in Mathematics. Springer Science+Business Media, LLC, New York, USA, 2nd edition, 2009.

[SS07] R. Scheidler and A. Stein. Class number approximation in cubic function fields. *Contrib. Discrete Math*, 2(2):107–132, 2007.

[Ste97] G. Van Steen. Some rigid geometry. In *Drinfeld Modules, Modular Schemes and Applications*, pages 88–102. World Scientific Publishing Co., 1997.

[Sut13] A. V. Sutherland. Isogeny volcanoes. *The Open Book Series*, 1:507–530, 2013. Available at `http://msp.org/obs/2013/1-1/p25.xhtml`.

[Tra03] M. Traulsen. *Galois Representations Associated to Drinfeld Modules in Special Characteristic and the Isogeny Conjecture for t-Motives*. PhD thesis, Swiss Federal Institute of Technology Zurich, Zurich, Switzerland, 2003.

[vdH04] G.-J. van der Heiden. Weil pairing for Drinfeld modules. *Monatsh. Math.*, 143:115–143, 2004.

[vdP97] M. van der Put. The structure of Ω and its quotients Λ/Ω. In *Drinfeld Modules, Modular Schemes and Applications*, pages 103–112. World Scientific Publishing Co., 1997.

[vdPT97] M. van der Put and J. Top. Analytic compactification and modular forms. In *Drinfeld Modules, Modular Schemes and Applications*, pages 113–140. World Scientific Publishing Co., 1997.

[vzGG03] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, Cambridge, United Kingdom, second edition, 2003.

[Yu95a] J.-K. Yu. A class number relation over function fields. *J. Number Theory*, 54:318–340, 1995.

[Yu95b] J.-K. Yu. Isogenies of Drinfeld modules over finite fields. *J. Number Theory*, 54:161–171, 1995.

[Zip93] R. Zippel. *Effective Polynomial Computation*. Kluwer Academic Publishers, Massachusetts, USA, 1993.

Appendix A

More on Drinfeld Modular Polynomials

A.1 Examples of Drinfeld Modular Polynomials

The modular polynomial $\Phi_\ell(X,Y)$ for Drinfeld modules, with monic irreducible polynomial $\ell \in \mathbf{A} = \mathbb{F}_q[T]$, takes the form

$$\Phi_\ell(X,Y) = X^{|\ell|+1} + Y^{|\ell|+1} + \sum_{\mu=0}^{|\ell|}\sum_{\nu=0}^{|\ell|} w_{\mu,\nu} X^\mu Y^\nu,$$

where $|\ell| = q^{\deg_T(\ell)}$ and $w_{\mu,\nu} = w_{\nu,\mu}$. Some of these polynomials are given below, where $\deg_T(\ell) \leq 2$ and $q = 2, 3$.

$q = 2$:

$$\begin{aligned}
\Phi_T(X,Y) &= X^3 + Y^3 + X^2Y^2 + T(X^2Y + XY^2) + (T^4 + T^3 + T^2 + T)(X^2 + Y^2) \\
&\quad + (T^5 + T^3 + T^2 + 1)XY + (T^8 + T^6 + T^4 + T^2)(X + Y) \\
&\quad + T^{12} + T^{11} + T^4 + T^3 \\
\Phi_{T+1}(X,Y) &= X^3 + Y^3 + X^2Y^2 + (T+1)(X^2Y + XY^2) + (T^4 + T^3)(X^2 + Y^2) \\
&\quad + (T^5 + T^4 + T^3)XY + (T^8 + T^6)(X + Y) + T^{12} + T^{11} + T^{10} + T^9 \\
\Phi_{T^2+T+1}(X,Y) &= X^5 + Y^5 + X^4Y^4 + (T^2 + T + 1)(X^4Y^2 + X^2Y^4) + (T^2 + T + 1)(X^4Y \\
&\quad + XY^4) + (T^8 + T^6 + T^5 + T^3)(X^4 + Y^4) + (T^6 + T^5 + T^3 + T^2)X^3Y^3 \\
&\quad + (T^{10} + T^9 + T^8 + T^3 + T^2 + T)(X^3Y^2 + X^2Y^3) + (T^8 + T^6 + T^5 \\
&\quad + T^3)(X^3Y + XY^3) + (T^{16} + T^{12} + T^{10} + T^6)(X^3 + Y^3) + (T^{16} + T^{10} \\
&\quad + T^9 + T^8 + T^6 + T^5)X^2Y^2 + (T^{18} + T^{17} + T^{12} + T^9 + T^8 + T^6)(X^2Y \\
&\quad + XY^2) + (T^{24} + T^{22} + T^{21} + T^{20} + T^{19} + T^{17} + T^{16} + T^{14} + T^{13} + T^{12}
\end{aligned}$$

$$+ T^{11} + T^9)(X^2 + Y^2) + (T^{22} + T^{21} + T^{20} + T^{19} + T^{14} + T^{13} + T^{12}$$
$$+ T^{11})XY$$

$q = 3$:

$$\Phi_T(X,Y) = X^4 + Y^4 + 2X^3Y^3 + 2T(X^3Y^2 + X^2Y^3) + 2T^4(X^3Y + XY^3) + (T^9$$
$$+ 2T^7 + 2T^3 + T)(X^3 + Y^3) + (2T^{10} + 2T^4 + 2T^2)X^2Y^2 + (T^{13} + 2T^{11}$$
$$+ 2T^7 + T^5)(X^2Y + XY^2) + (2T^{22} + 2T^{20} + 2T^{16} + 2T^{14} + 2T^{12} + 2T^{10}$$
$$+ 2T^8 + 2T^6 + 2)XY + (T^{27} + 2T^{21} + 2T^9 + T^3)(X + Y) + T^{36} + 2T^{34}$$
$$+ T^{30} + 2T^{28} + T^{24} + 2T^{22} + 2T^{18} + T^{16} + 2T^{12} + T^{10} + 2T^6 + T^4$$

$$\Phi_{T+1}(X,Y) = X^4 + Y^4 + 2X^3Y^3 + (2T + 2)(X^3Y^2 + X^2Y^3) + (2T^4 + 2T^3 + 2T$$
$$+ 2)(X^3Y + XY^3) + (T^9 + 2T^7 + 2T^6 + T^4)(X^3 + Y^3) + (2T^{10} + 2T^9$$
$$+ 2T^4 + 2T^3 + 2T^2 + 2T)X^2Y^2 + (T^{13} + T^{12} + 2T^{11} + 2T^{10} + 2T^7$$
$$+ 2T^6 + T^5 + T^4)(X^2Y + XY^2) + (2T^{22} + 2T^{21} + 2T^{20} + T^{18} + 2T^{16}$$
$$+ 2T^{15} + 2T^{14} + 2T^{10} + T^9 + 2T^8)XY + (T^{27} + 2T^{21} + 2T^{18} + T^{12})(X$$
$$+ Y) + T^{36} + 2T^{34} + 2T^{33} + T^{31} + 2T^{30} + T^{28} + T^{24} + 2T^{22} + T^{21}$$
$$+ 2T^{19} + 2T^{18} + T^{16}$$

$$\Phi_{T+2}(X,Y) = X^4 + Y^4 + 2X^3Y^3 + (2T + 1)(X^3Y^2 + X^2Y^3) + (2T^4 + T^3 + T$$
$$+ 2)(X^3Y + XY^3) + (T^9 + 2T^7 + T^6 + 2T^4)(X^3 + Y^3) + (2T^{10} + T^9$$
$$+ 2T^4 + T^3 + 2T^2 + T)X^2Y^2 + (T^{13} + 2T^{12} + 2T^{11} + T^{10} + 2T^7 + T^6$$
$$+ T^5 + 2T^4)(X^2Y + XY^2) + (2T^{22} + T^{21} + 2T^{20} + T^{18} + 2T^{16} + T^{15}$$
$$+ 2T^{14} + 2T^{10} + 2T^9 + 2T^8)XY + (T^{27} + 2T^{21} + T^{18} + 2T^{12})(X + Y)$$
$$+ T^{36} + 2T^{34} + T^{33} + 2T^{31} + 2T^{30} + T^{28} + T^{24} + 2T^{22} + 2T^{21} + T^{19}$$
$$+ 2T^{18} + T^{16}$$

$$\Phi_{T^2+1}(X,Y) = X^{10} + Y^{10} + 2X^9Y^9 + (2T^3 + 2T)(X^9Y^6 + X^6Y^9) + (T^2 + 1)(X^9Y^5 + X^5Y^9) + (T^5 + 2T)(X^9Y^4 + X^4Y^9) + (2T^{12} + 2T^{10} + T^8 + 2T^6 + T^4 + T^2 + 1)(X^9Y^3 + X^3Y^9) + (T^5 + T^3)(X^9Y^2 + X^2Y^9) + (T^{14} + 2T^{10} + T^8 + 2T^6 + T^4 + 2T^2 + 2)(X^9Y + XY^9) + (T^{27} + 2T^{21} + 2T^{19} + 2T^{17} + T^{15} + 2T^{13} + 2T^9 + 2T^7 + T^5)(X^9 + Y^9) + (T^{14} + T^{12} + T^2 + 1)X^8Y^8 + (T^{23} + 2T^{19} + 2T^{17} + T^{15} + 2T^{13} + T^{11} + 2T^7 + 2T^5 + 2T^3)(X^8Y^7 + X^7Y^8) + (2T^{30} + 2T^{28} + 2T^4 + 1)(X^8Y^6 + X^6Y^8) + (T^{29} + T^{27} + T^{23} + T^{21} + T^{17} + 2T^{15} + T^{13} + T^3 + T)(X^8Y^5 + X^5Y^8) + (2T^{32} + T^{28} + T^{26} + T^{24} + 2T^{22} + T^{20} + 2T^{16} + 2T^{14} + T^{10} + 2T^8 + T^6 + T^2 + 2)(X^8Y^4 + X^4Y^8) + (T^{39} + T^{37} + 2T^{35} + T^{29} + 2T^{27} + 2T^{25} + 2T^{23} + T^{21} + T^{19} + T^{13} + T^{11} + 2T^9 + 2T^7 + T^5 + 2T^3 + T)(X^8Y^3 + X^3Y^8) + (2T^{32} + T^{30} + T^{28} + 2T^{26} + 2T^{22} + T^{20} + T^{16} + 2T^{12} + T^{10} + 2T^8 + T^6 + 2T^2)(X^8Y^2 + X^2Y^8) + (T^{35} + T^{33} + 2T^{27} + T^{25} + T^{21} + 2T^{19} + 2T^{17} + 2T^{15} + 2T^{13} + T^{11} + T^7 + 2T^5)(X^8Y + XY^8) + (2T^{26} + T^{24} + T^{22} + T^{20} + T^{18} + T^{16} + T^{14} + T^{12} + T^{10} + 2T^8)(X^8 + Y^8) + (T^{32} + T^{24} + 2T^{22} + T^{20} + T^{16} + T^{14} + 2T^{12} + T^4 + 2T^2 + 1)X^7Y^7 + (T^{41} + 2T^{39} + 2T^{35} + 2T^{31} + T^{29} + 2T^{25} + T^{23} + 2T^{21} + T^{19} + 2T^{17} + T^{15} + T^{13} + T^{11} + 2T^9 + T^7 + 2T^3 + 2T)(X^7Y^6 + X^6Y^7) + (2T^{50} + 2T^{46} + T^{38} + 2T^{36} + 2T^{34} + T^{32} + T^{24} + T^{22} + T^{20} + 2T^{18} + T^{14} + 2T^{12} + 2T^{10} + 2T^8 + 2T^6)(X^7Y^5 + X^5Y^7) + (T^{59} + 2T^{55} + T^{53} + T^{51} + 2T^{49} + T^{47} + 2T^{43} + 2T^{37} + T^{35} + T^{33} + T^{29} + T^{27} + T^{25} + T^{23} + T^{15} + T^{13} + T^{11})(X^7Y^4 + X^4Y^7) + (2T^{66} + 2T^{64} + T^{62} + T^{60} + 2T^{58} + T^{54} + 2T^{52} + T^{50} + 2T^{48} + T^{46} + T^{42} + 2T^{40} + T^{34} + T^{32} + 2T^{28} + T^{26} + T^{22} + 2T^{20}$$

$$+ T^{16} + 2T^{12} + 2T^{10} + 2T^8 + 2T^6 + 2T^4 + 2T^2)(X^7Y^3 + X^3Y^7) + (T^{59}$$
$$+ 2T^{57} + 2T^{55} + 2T^{53} + 2T^{49} + T^{47} + T^{43} + T^{39} + 2T^{37} + T^{35} + T^{29}$$
$$+ 2T^{27} + T^{25} + 2T^{21} + 2T^{15} + T^7)(X^7Y^2 + X^2Y^7) + (2T^{62} + 2T^{60} + T^{56}$$
$$+ T^{52} + T^{50} + 2T^{48} + 2T^{46} + T^{44} + 2T^{40} + T^{38} + 2T^{36} + 2T^{34} + T^{32}$$
$$+ 2T^{30} + 2T^{24} + 2T^{22} + 2T^{20} + 2T^{18} + T^{16} + 2T^{14} + 2T^{10} + T^8)(X^7Y$$
$$+ XY^7) + (T^{81} + 2T^{63} + 2T^{57} + 2T^{51} + T^{45} + 2T^{39} + 2T^{27} + 2T^{21}$$
$$+ T^{15})(X^7 + Y^7) + (T^{46} + T^{40} + T^{38} + T^{34} + T^{32} + 2T^{28} + 2T^{26} + 2T^{18}$$
$$+ T^{16} + T^{14} + 2T^{10} + 2T^8 + 2T^6 + T^2)X^6Y^6 + (T^{57} + 2T^{55} + T^{53} + 2T^{51}$$
$$+ 2T^{49} + T^{47} + 2T^{45} + 2T^{43} + 2T^{41} + 2T^{37} + 2T^{35} + 2T^{33} + 2T^{31} + T^{29}$$
$$+ T^{27} + 2T^{25} + T^{23} + T^{21} + 2T^{19} + T^{17} + T^{15} + T^{11} + T^9 + 2T^7 + 2T^5$$
$$+ 2T)(X^6Y^5 + X^5Y^6) + (2T^{68} + 2T^{66} + 2T^{60} + 2T^{56} + 2T^{54} + T^{52}$$
$$+ 2T^{48} + T^{46} + 2T^{44} + 2T^{42} + 2T^{40} + T^{36} + 2T^{30} + 2T^{22} + T^{20} + 2T^{18}$$
$$+ T^{10} + T^8 + 2T^6 + 2T^4 + 2T^2)(X^6Y^4 + X^4Y^6) + (T^{81} + T^{69} + 2T^{65}$$
$$+ 2T^{61} + T^{53} + 2T^{51} + T^{47} + 2T^{45} + T^{43} + 2T^{39} + 2T^{37} + 2T^{35} + T^{33}$$
$$+ 2T^{27} + T^{25} + T^{23} + 2T^{21} + 2T^{19} + 2T^{17} + T^{15} + T^{13} + T^{11} + T^9$$
$$+ 2T^5)(X^6Y^3 + X^3Y^6) + (2T^{84} + T^{82} + 2T^{68} + T^{66} + 2T^{64} + 2T^{60} + T^{56}$$
$$+ 2T^{52} + T^{50} + 2T^{48} + 2T^{46} + 2T^{44} + 2T^{40} + 2T^{38} + T^{36} + T^{34} + 2T^{32}$$
$$+ 2T^{28} + T^{26} + T^{24} + T^{22} + 2T^{18} + T^{14} + T^{12} + 2T^{10})(X^6Y^2 + X^2Y^6)$$
$$+ (T^{95} + 2T^{91} + 2T^{89} + T^{85} + 2T^{77} + T^{75} + 2T^{73} + 2T^{71} + T^{69} + T^{67}$$
$$+ T^{65} + T^{57} + 2T^{55} + 2T^{53} + 2T^{51} + 2T^{49} + T^{47} + T^{43} + 2T^{39} + 2T^{37}$$
$$+ 2T^{35} + T^{33} + T^{31} + T^{29} + 2T^{25} + 2T^{21} + T^{19} + T^{17} + 2T^{15}$$
$$+ T^{13})(X^6Y + XY^6) + (T^{108} + 2T^{102} + 2T^{100} + 2T^{98} + T^{96} + 2T^{94} + T^{90}$$
$$+ 2T^{88} + T^{86} + T^{82} + T^{80} + 2T^{78} + 2T^{76} + T^{74} + 2T^{72} + T^{66} + T^{64}$$

$$+ T^{62} + T^{58} + T^{50} + T^{48} + 2T^{46} + T^{42} + 2T^{40} + T^{38} + 2T^{36} + T^{34} + T^{32}$$
$$+ 2T^{30} + 2T^{26} + 2T^{24} + 2T^{22} + T^{20})(X^6 + Y^6) + (2T^{64} + 2T^{62} + T^{58}$$
$$+ T^{52} + T^{46} + T^{44} + T^{38} + T^{36} + T^{34} + T^{32} + 2T^{30} + 2T^{28} + T^{26} + T^{20}$$
$$+ T^{18} + 2T^{14} + T^{10} + T^8 + 2T^4 + 2T^2)X^5Y^5 + (T^{77} + 2T^{73} + 2T^{71}$$
$$+ T^{69} + 2T^{63} + T^{61} + 2T^{57} + 2T^{55} + 2T^{53} + 2T^{51} + 2T^{49} + T^{47} + T^{45}$$
$$+ 2T^{43} + 2T^{41} + 2T^{39} + T^{37} + 2T^{35} + 2T^{31} + 2T^{23} + 2T^{19} + 2T^{15} + 2T^{13}$$
$$+ 2T^{11} + 2T^7 + T^5)(X^5Y^4 + X^4Y^5) + (2T^{82} + T^{76} + T^{74} + T^{72} + 2T^{70}$$
$$+ 2T^{68} + T^{66} + 2T^{64} + 2T^{62} + 2T^{54} + T^{52} + 2T^{44} + T^{42} + 2T^{40} + 2T^{38}$$
$$+ T^{36} + 2T^{34} + T^{28} + 2T^{26} + 2T^{24} + 2T^{18} + T^{16} + T^{14} + 2T^{12}$$
$$+ T^{10})(X^5Y^3 + X^3Y^5) + (2T^{95} + 2T^{93} + T^{91} + T^{89} + T^{85} + 2T^{83} + T^{79}$$
$$+ 2T^{77} + 2T^{73} + T^{71} + 2T^{69} + 2T^{67} + 2T^{65} + 2T^{63} + 2T^{59} + 2T^{57} + T^{55}$$
$$+ 2T^{53} + 2T^{47} + T^{43} + T^{35} + 2T^{33} + T^{31} + T^{27} + T^{25} + 2T^{21} + 2T^{19}$$
$$+ T^{17} + 2T^{15} + 2T^{13})(X^5Y^2 + X^2Y^5) + (T^{104} + 2T^{100} + 2T^{98} + T^{92}$$
$$+ T^{90} + 2T^{88} + T^{86} + T^{78} + 2T^{76} + T^{74} + T^{70} + T^{68} + 2T^{66} + 2T^{64}$$
$$+ T^{62} + T^{60} + T^{56} + 2T^{54} + T^{52} + 2T^{48} + 2T^{44} + T^{42} + T^{36} + 2T^{34}$$
$$+ 2T^{30} + 2T^{28} + T^{26} + T^{22} + 2T^{18})(X^5Y + XY^5) + (2T^{107} + T^{105} + T^{103}$$
$$+ T^{101} + T^{99} + T^{97} + T^{95} + T^{93} + T^{91} + 2T^{87} + 2T^{85} + T^{81} + T^{79} + 2T^{77}$$
$$+ T^{71} + 2T^{69} + 2T^{67} + 2T^{65} + 2T^{63} + 2T^{61} + T^{59} + 2T^{53} + T^{51} + T^{49}$$
$$+ T^{47} + T^{45} + T^{43} + 2T^{39} + 2T^{37} + T^{35} + 2T^{29} + T^{27} + T^{25} + 2T^{23})(X^5$$
$$+ Y^5) + (T^{86} + T^{82} + T^{80} + T^{78} + 2T^{70} + 2T^{66} + T^{64} + 2T^{60} + 2T^{58}$$
$$+ T^{56} + 2T^{52} + T^{48} + 2T^{46} + T^{44} + 2T^{42} + 2T^{40} + T^{36} + T^{34} + 2T^{32}$$
$$+ T^{30} + 2T^{28} + T^{22} + T^{20} + T^{18} + 2T^{14} + T^{12} + 2T^{10})X^4Y^4 + (2T^{93}$$
$$+ T^{83} + T^{81} + 2T^{79} + 2T^{75} + 2T^{71} + 2T^{69} + T^{65} + T^{61} + 2T^{59} + 2T^{57}$$

$$+ T^{53} + T^{47} + T^{45} + 2T^{43} + 2T^{41} + T^{39} + 2T^{37} + T^{35} + T^{33} + T^{27} + T^{25}$$
$$+ 2T^{23} + 2T^{21} + T^{19} + 2T^{17})(X^4Y^3 + X^3Y^4) + (2T^{104} + 2T^{98} + 2T^{96}$$
$$+ T^{94} + T^{90} + T^{88} + 2T^{86} + 2T^{84} + 2T^{80} + T^{78} + T^{76} + T^{74} + T^{68} + T^{64}$$
$$+ 2T^{62} + 2T^{58} + T^{56} + T^{54} + T^{50} + T^{48} + T^{46} + 2T^{44} + 2T^{42} + T^{40} + T^{36}$$
$$+ 2T^{34} + T^{28} + T^{26} + T^{24} + T^{22} + T^{20})(X^4Y^2 + X^2Y^4) + (T^{107} + T^{103}$$
$$+ 2T^{101} + T^{99} + T^{97} + 2T^{95} + T^{93} + 2T^{85} + 2T^{81} + T^{79} + T^{77} + 2T^{75}$$
$$+ 2T^{73} + T^{71} + 2T^{69} + T^{67} + 2T^{65} + T^{63} + T^{61} + T^{59} + T^{57} + 2T^{55}$$
$$+ 2T^{51} + 2T^{41} + 2T^{37} + T^{35} + 2T^{33} + 2T^{31} + 2T^{29} + 2T^{27} + 2T^{21})(X^4Y$$
$$+ XY^4) + (2T^{78} + T^{72} + T^{66} + T^{60} + T^{54} + T^{48} + T^{42} + T^{36} + T^{30}$$
$$+ 2T^{24})(X^4 + Y^4) + (T^{108} + 2T^{102} + T^{100} + 2T^{98} + 2T^{92} + T^{90} + T^{88}$$
$$+ T^{84} + T^{82} + 2T^{80} + T^{78} + 2T^{76} + T^{70} + 2T^{68} + T^{66} + 2T^{64} + 2T^{62}$$
$$+ 2T^{60} + T^{58} + T^{56} + T^{54} + T^{52} + 2T^{50} + 2T^{48} + T^{46} + 2T^{42} + T^{40}$$
$$+ 2T^{38} + T^{36} + 2T^{32} + T^{28} + T^{24} + 2T^{22} + T^{20} + 2T^{18})X^3Y^3 + (2T^{103}$$
$$+ 2T^{101} + 2T^{97} + T^{93} + 2T^{91} + T^{89} + 2T^{83} + 2T^{81} + 2T^{79} + 2T^{77} + T^{71}$$
$$+ T^{69} + T^{65} + 2T^{63} + T^{61} + 2T^{59} + T^{57} + T^{53} + T^{51} + T^{49} + 2T^{47} + 2T^{45}$$
$$+ 2T^{43} + 2T^{41} + T^{37} + T^{33} + 2T^{29} + 2T^{25} + T^{21})(X^3Y^2 + X^2Y^3)$$
$$+ (2T^{106} + T^{86} + T^{82} + 2T^{76} + T^{74} + T^{72} + 2T^{70} + T^{68} + T^{66} + 2T^{64}$$
$$+ T^{62} + T^{60} + 2T^{58} + T^{56} + T^{54} + T^{50} + T^{48} + 2T^{46} + T^{44} + T^{42}$$
$$+ 2T^{40} + T^{38} + T^{36} + 2T^{34} + T^{30} + T^{28} + T^{26} + T^{24})(X^3Y + XY^3)$$
$$+ (2T^{105} + 2T^{99} + T^{97} + T^{95} + 2T^{93} + 2T^{89} + 2T^{87} + 2T^{85} + T^{83} + T^{51}$$
$$+ T^{45} + 2T^{43} + 2T^{41} + T^{39} + T^{35} + T^{33} + T^{31} + 2T^{29})(X^3 + Y^3)$$
$$+ (2T^{106} + 2T^{104} + 2T^{98} + T^{94} + 2T^{92} + 2T^{90} + 2T^{88} + 2T^{86} + 2T^{84}$$
$$+ T^{82} + 2T^{80} + T^{78} + T^{76} + T^{72} + T^{70} + T^{66} + T^{64} + T^{60} + T^{58} + T^{54}$$

$$
\begin{aligned}
&+ 2T^{52} + T^{50} + T^{48} + T^{46} + T^{44} + T^{42} + T^{38} + 2T^{36} + 2T^{34} + T^{32} \\
&+ 2T^{30} + T^{26})X^2Y^2 + (T^{105} + 2T^{103} + 2T^{99} + 2T^{95} + 2T^{93} + 2T^{91} + T^{89} \\
&+ 2T^{87} + 2T^{85} + 2T^{83} + 2T^{51} + T^{49} + T^{45} + T^{41} + T^{39} + T^{37} + 2T^{35} \\
&+ T^{33} + T^{31} + T^{29})(X^2Y + XY^2) + (T^{104} + 2T^{102} + 2T^{100} + T^{98} + 2T^{92} \\
&+ T^{90} + T^{88} + 2T^{86} + 2T^{50} + T^{48} + T^{46} + 2T^{44} + T^{38} + 2T^{36} + 2T^{34} \\
&+ T^{32})(X^2 + Y^2) + (T^{104} + T^{100} + T^{98} + T^{96} + 2T^{94} + 2T^{92} + 2T^{90} \\
&+ 2T^{86} + 2T^{50} + 2T^{46} + 2T^{44} + 2T^{42} + T^{40} + T^{38} + T^{36} + T^{32})XY \\
\Phi_{T^2+T+2}(X,Y) = {} & X^{10} + Y^{10} + X^9Y^9 + (2T^3 + 2T + 2)(X^9Y^6 + X^6Y^9) + (T^2 + T \\
&+ 2)(X^9Y^5 + X^5Y^9) + (T^5 + T^4 + T^3 + 2T^2 + T)(X^9Y^4 + X^4Y^9) \\
&+ (2T^{12} + 2T^{10} + 2T^9 + T^8 + T^7 + T^5 + 2T^4 + 2T^2 + 2T + 1)(X^9Y^3 \\
&+ X^3Y^9) + (T^5 + T^4 + 2T^3 + 2T^2 + 2T + 1)(X^9Y^2 + X^2Y^9) + (T^{14} \\
&+ T^{13} + T^{12} + 2T^{11} + T^{10} + T^8 + T^7 + T^4 + T^3 + T^2 + T + 2)(X^9Y \\
&+ XY^9) + (T^{27} + 2T^{21} + 2T^{19} + 2T^{18} + 2T^{17} + 2T^{16} + 2T^{14} + T^{13} \\
&+ 2T^{11} + 2T^{10} + T^8 + T^6 + 2T^5 + 2T^4)(X^9 + Y^9) + (T^{14} + T^{13} + 2T^{12} \\
&+ 2T^{11} + 2T^{10} + T^9 + 2T^5 + 2T^4 + T^3 + 2T^2 + 2T + 1)X^8Y^8 + (T^{23} \\
&+ T^{22} + T^{21} + 2T^{20} + T^{19} + 2T^{17} + 2T^{16} + 2T^{13} + 2T^{12} + 2T^{11} + 2T^{10} \\
&+ T^8 + T^6 + T^5 + T^4 + 2T^3)(X^8Y^7 + X^7Y^8) + (2T^{30} + 2T^{28} + 2T^{27} \\
&+ 2T^4 + 2T^3 + 2T + 1)(X^8Y^6 + X^6Y^8) + (T^{29} + T^{28} + 2T^{27} + T^{23} + T^{22} \\
&+ 2T^{21} + 2T^{20} + 2T^{19} + T^{18} + T^{17} + T^{16} + 2T^{14} + T^{12} + 2T^{10} + 2T^9 \\
&+ 2T^8 + 2T^7 + 2T^4 + T^3 + 2T + 2)(X^8Y^5 + X^5Y^8) + (2T^{32} + 2T^{31} \\
&+ 2T^{30} + T^{29} + 2T^{28} + T^{26} + T^{25} + 2T^{24} + T^{23} + 2T^{20} + 2T^{18} + T^{17} \\
&+ T^{13} + T^{10} + T^7 + T^6 + 2T^5 + 2T^4 + T^3 + 1)(X^8Y^4 + X^4Y^8) + (T^{39} \\
&+ T^{37} + T^{36} + 2T^{35} + 2T^{34} + 2T^{33} + 2T^{32} + 2T^{31} + T^{30} + 2T^{28} + T^{27}
\end{aligned}
$$

$$+ 2T^{25} + T^{24} + 2T^{23} + T^{22} + T^{21} + T^{20} + T^{19} + 2T^{16} + T^{15} + 2T^{14}$$
$$+ 2T^{13} + 2T^{12} + 2T^{11} + T^{8} + 2T^{7} + T^{5} + T^{4} + 2T^{3} + 2T^{2} + T$$
$$+ 1)(X^8Y^3 + X^3Y^8) + (2T^{32} + 2T^{31} + T^{29} + 2T^{28} + 2T^{27} + 2T^{26} + 2T^{25}$$
$$+ 2T^{24} + 2T^{23} + T^{22} + T^{19} + 2T^{18} + 2T^{17} + T^{15} + 2T^{14} + 2T^{13} + T^{12}$$
$$+ T^9 + T^8 + 2T^5 + 2T^3 + T)(X^8Y^2 + X^2Y^8) + (T^{35} + T^{34} + 2T^{33} + T^{32}$$
$$+ T^{31} + 2T^{30} + T^{29} + T^{28} + T^{27} + T^{25} + 2T^{24} + T^{22} + 2T^{18} + 2T^{17}$$
$$+ 2T^{14} + 2T^{13} + 2T^{12} + T^{10} + 2T^7 + T^6 + 2T^5 + 2T^4)(X^8Y + XY^8)$$
$$+ (2T^{26} + 2T^{25} + 2T^{23} + 2T^{21} + 2T^{19} + 2T^{17} + 2T^{15} + 2T^{13} + 2T^{11}$$
$$+ 2T^9 + T^8)(X^8 + Y^8) + (T^{32} + T^{31} + T^{30} + 2T^{29} + 2T^{28} + 2T^{27} + T^{24}$$
$$+ 2T^{22} + 2T^{21} + T^{20} + 2T^{19} + T^{18} + T^{16} + T^{14} + T^{13} + T^{12} + 2T^{10}$$
$$+ 2T^7 + 2T^6 + T^5 + T^3 + 2T^2 + T + 1)X^7Y^7 + (T^{41} + T^{40} + 2T^{38}$$
$$+ 2T^{37} + 2T^{35} + 2T^{34} + 2T^{33} + T^{32} + T^{29} + 2T^{28} + 2T^{27} + 2T^{25} + T^{24}$$
$$+ T^{23} + T^{21} + 2T^{20} + 2T^{19} + 2T^{17} + T^{16} + T^{15} + 2T^{14} + 2T^{13} + 2T^{10}$$
$$+ T^9 + 2T^8 + 2T^7 + T^6 + T^5 + T^4 + T^2 + T + 1)(X^7Y^6 + X^6Y^7)$$
$$+ (2T^{50} + 2T^{49} + 2T^{48} + T^{47} + 2T^{45} + 2T^{41} + 2T^{40} + 2T^{39} + 2T^{38}$$
$$+ T^{37} + 2T^{36} + 2T^{34} + T^{33} + 2T^{31} + T^{30} + 2T^{29} + 2T^{27} + T^{24} + T^{23}$$
$$+ 2T^{22} + T^{21} + T^{15} + 2T^{14} + T^{12} + T^{11} + T^9 + 2T^8 + T^6 + T^5 + 2T^2$$
$$+ T)(X^7Y^5 + X^5Y^7) + (T^{59} + T^{58} + T^{57} + 2T^{56} + T^{55} + T^{53} + T^{52}$$
$$+ 2T^{51} + T^{50} + 2T^{47} + 2T^{45} + T^{44} + T^{41} + 2T^{40} + T^{39} + 2T^{38} + T^{37}$$
$$+ T^{36} + 2T^{35} + 2T^{30} + 2T^{28} + T^{27} + 2T^{26} + 2T^{22} + 2T^{18} + 2T^{17} + T^{16}$$
$$+ T^{13} + 2T^{12} + T^{11} + 2T^{10} + T^8 + T^7 + T^6 + 2T^2)(X^7Y^4 + X^4Y^7)$$
$$+ (2T^{66} + 2T^{64} + 2T^{63} + T^{62} + T^{61} + 2T^{60} + T^{59} + T^{57} + T^{56} + 2T^{52}$$
$$+ T^{51} + T^{50} + T^{48} + 2T^{47} + 2T^{46} + 2T^{43} + 2T^{42} + T^{41} + 2T^{40} + 2T^{39}$$

$$+ 2T^{38} + 2T^{37} + 2T^{36} + T^{35} + T^{34} + T^{33} + 2T^{29} + 2T^{27} + T^{26} + 2T^{25}$$
$$+ 2T^{22} + 2T^{21} + T^{20} + T^{18} + T^{17} + T^{15} + T^{13} + T^{11} + T^{10} + T^{9} + T^{8}$$
$$+ 2T^{5} + 2T^{4} + T^{2} + T)(X^{7}Y^{3} + X^{3}Y^{7}) + (T^{59} + T^{58} + 2T^{56} + T^{55}$$
$$+ T^{54} + 2T^{53} + 2T^{52} + 2T^{51} + 2T^{50} + T^{49} + T^{46} + 2T^{45} + 2T^{44} + T^{42}$$
$$+ 2T^{41} + 2T^{40} + T^{37} + T^{36} + 2T^{34} + T^{33} + T^{32} + 2T^{31} + T^{30} + T^{29}$$
$$+ T^{28} + 2T^{27} + T^{26} + 2T^{25} + T^{23} + T^{21} + T^{18} + T^{17} + T^{16} + T^{14}$$
$$+ 2T^{13} + T^{9} + T^{6} + T^{5} + 2T^{4})(X^{7}Y^{2} + X^{2}Y^{7}) + (2T^{62} + 2T^{61} + T^{60}$$
$$+ 2T^{59} + 2T^{58} + T^{57} + 2T^{54} + T^{52} + 2T^{51} + T^{50} + 2T^{49} + 2T^{48} + 2T^{47}$$
$$+ 2T^{46} + T^{44} + 2T^{43} + 2T^{41} + 2T^{40} + T^{39} + T^{38} + 2T^{37} + T^{35} + T^{34}$$
$$+ T^{31} + 2T^{30} + 2T^{29} + 2T^{25} + 2T^{23} + T^{21} + T^{19} + 2T^{18} + 2T^{17} + 2T^{16}$$
$$+ T^{15} + 2T^{11} + 2T^{10} + T^{8})(X^{7}Y + XY^{7}) + (T^{81} + 2T^{63} + 2T^{57} + 2T^{54}$$
$$+ 2T^{51} + 2T^{48} + 2T^{42} + T^{39} + 2T^{33} + 2T^{30} + T^{24} + T^{18} + 2T^{15}$$
$$+ 2T^{12})(X^{7} + Y^{7}) + (T^{46} + 2T^{45} + T^{40} + 2T^{39} + T^{38} + T^{37} + T^{36} + T^{34}$$
$$+ 2T^{33} + T^{32} + T^{31} + T^{30} + T^{29} + 2T^{27} + 2T^{26} + 2T^{25} + 2T^{24} + 2T^{23}$$
$$+ 2T^{22} + 2T^{21} + 2T^{20} + T^{19} + 2T^{18} + 2T^{17} + T^{15} + 2T^{9} + T^{8} + 2T^{7}$$
$$+ 2T^{6} + 2T^{5} + T^{4} + 2T^{3} + 2T^{2} + 2)X^{6}Y^{6} + (T^{57} + 2T^{55} + T^{53} + T^{52}$$
$$+ T^{50} + T^{48} + 2T^{47} + 2T^{45} + T^{44} + T^{42} + T^{40} + T^{39} + 2T^{37} + 2T^{36}$$
$$+ T^{34} + T^{32} + T^{30} + T^{29} + T^{28} + T^{27} + 2T^{26} + T^{25} + T^{24} + 2T^{21}$$
$$+ T^{18} + 2T^{15} + 2T^{14} + T^{12} + T^{11} + 2T^{9} + 2T^{8} + 2T^{7} + T^{5} + 2T^{3}$$
$$+ 1)(X^{6}Y^{5} + X^{5}Y^{6}) + (2T^{68} + 2T^{67} + T^{66} + T^{65} + T^{64} + 2T^{63} + 2T^{60}$$
$$+ T^{59} + T^{58} + T^{57} + T^{56} + T^{55} + T^{54} + T^{52} + 2T^{51} + T^{49} + T^{48} + 2T^{46}$$
$$+ 2T^{45} + 2T^{44} + T^{41} + T^{40} + T^{39} + 2T^{36} + T^{35} + 2T^{34} + 2T^{32} + T^{31}$$
$$+ 2T^{30} + 2T^{29} + 2T^{25} + T^{24} + T^{22} + T^{20} + T^{17} + 2T^{13} + 2T^{12} + 2T^{10}$$

$$+ 2T^7 + T^6 + T^5 + 2T^3 + T^2 + T)(X^6Y^4 + X^4Y^6) + (T^{81} + T^{69} + T^{66}$$
$$+ 2T^{65} + 2T^{64} + 2T^{61} + 2T^{58} + T^{56} + T^{54} + T^{53} + T^{52} + T^{50} + T^{49}$$
$$+ 2T^{47} + 2T^{46} + T^{44} + 2T^{43} + T^{41} + 2T^{40} + 2T^{39} + T^{38} + T^{37} + T^{36}$$
$$+ T^{34} + T^{33} + T^{31} + 2T^{30} + 2T^{29} + T^{28} + 2T^{27} + 2T^{26} + 2T^{24} + T^{22}$$
$$+ 2T^{21} + T^{17} + T^{16} + T^{15} + 2T^{14} + T^{12} + 2T^{11} + T^{10} + 2T^9 + T^8 + 2T^7$$
$$+ T^6 + T^5 + T^4)(X^6Y^3 + X^3Y^6) + (2T^{84} + T^{82} + 2T^{68} + 2T^{67} + T^{65}$$
$$+ T^{63} + 2T^{60} + T^{59} + T^{58} + 2T^{57} + T^{55} + 2T^{54} + 2T^{52} + T^{51} + T^{50}$$
$$+ T^{48} + 2T^{47} + 2T^{45} + 2T^{44} + T^{43} + 2T^{41} + T^{39} + T^{38} + 2T^{37} + T^{36}$$
$$+ T^{35} + T^{34} + 2T^{32} + T^{30} + 2T^{29} + T^{27} + T^{26} + 2T^{25} + T^{24} + 2T^{22}$$
$$+ 2T^{20} + 2T^{17} + 2T^{15} + T^{14} + T^{13} + 2T^{12} + T^{11} + 2T^{10} + 2T^9)(X^6Y^2$$
$$+ X^2Y^6) + (T^{95} + T^{94} + T^{93} + 2T^{92} + T^{91} + 2T^{89} + 2T^{88} + 2T^{87} + T^{86}$$
$$+ 2T^{85} + 2T^{77} + 2T^{76} + T^{74} + T^{72} + 2T^{71} + 2T^{70} + T^{68} + 2T^{67} + 2T^{66}$$
$$+ T^{65} + 2T^{64} + T^{62} + T^{61} + 2T^{58} + 2T^{57} + T^{56} + 2T^{54} + 2T^{53} + 2T^{52}$$
$$+ T^{51} + T^{50} + 2T^{48} + T^{47} + T^{46} + 2T^{45} + T^{44} + 2T^{43} + T^{40} + 2T^{39}$$
$$+ T^{38} + 2T^{36} + 2T^{35} + T^{34} + 2T^{33} + T^{32} + 2T^{31} + 2T^{30} + T^{29} + T^{27}$$
$$+ T^{26} + T^{21} + T^{20} + 2T^{19} + T^{18} + T^{17} + 2T^{16} + T^{15} + 2T^{14})(X^6Y$$
$$+ XY^6) + (T^{108} + 2T^{102} + 2T^{100} + 2T^{99} + 2T^{98} + 2T^{97} + 2T^{95} + T^{94}$$
$$+ 2T^{92} + 2T^{91} + 2T^{90} + T^{89} + T^{87} + 2T^{86} + 2T^{85} + T^{82} + T^{80} + T^{79}$$
$$+ T^{77} + T^{75} + 2T^{74} + 2T^{72} + T^{71} + T^{70} + T^{68} + 2T^{66} + 2T^{65} + T^{64}$$
$$+ 2T^{62} + 2T^{61} + T^{60} + 2T^{59} + 2T^{58} + 2T^{55} + T^{53} + T^{52} + 2T^{50} + T^{49}$$
$$+ T^{47} + T^{46} + T^{45} + T^{44} + T^{43} + T^{42} + 2T^{41} + 2T^{38} + T^{37} + 2T^{36}$$
$$+ 2T^{35} + 2T^{33} + T^{32} + 2T^{30} + T^{28} + T^{24} + 2T^{23} + 2T^{21} + T^{19} + 2T^{18}$$
$$+ T^{17} + T^{16})(X^6 + Y^6) + (2T^{64} + T^{63} + 2T^{62} + 2T^{61} + 2T^{60} + 2T^{59}$$

$$+ T^{57} + 2T^{56} + 2T^{55} + 2T^{54} + T^{52} + 2T^{51} + T^{49} + 2T^{48} + 2T^{46} + T^{45}$$
$$+ T^{44} + 2T^{43} + T^{41} + 2T^{40} + 2T^{38} + 2T^{36} + T^{35} + 2T^{33} + 2T^{32} + 2T^{31}$$
$$+ T^{30} + 2T^{29} + T^{28} + T^{26} + 2T^{24} + T^{23} + 2T^{21} + 2T^{20} + 2T^{18} + 2T^{16}$$
$$+ T^{15} + 2T^{14} + T^{13} + T^{11} + 2T^{10} + 2T^{8} + T^{6} + 2T^{5} + 2T^{3} + T)X^5Y^5$$
$$+ (T^{77} + T^{76} + T^{75} + 2T^{74} + T^{73} + 2T^{71} + 2T^{70} + T^{66} + T^{65} + 2T^{63}$$
$$+ T^{62} + 2T^{61} + 2T^{60} + 2T^{59} + 2T^{57} + 2T^{55} + 2T^{54} + 2T^{53} + 2T^{52} + T^{51}$$
$$+ 2T^{49} + 2T^{47} + 2T^{46} + 2T^{45} + T^{44} + 2T^{42} + T^{41} + 2T^{40} + 2T^{39} + 2T^{38}$$
$$+ 2T^{37} + 2T^{35} + T^{34} + T^{33} + T^{32} + T^{31} + 2T^{30} + T^{29} + 2T^{28} + T^{26}$$
$$+ T^{25} + 2T^{24} + T^{23} + 2T^{22} + T^{21} + T^{16} + T^{14} + 2T^{13} + 2T^{12} + T^{10}$$
$$+ 2T^{7} + 2T^{6} + 2T^{4})(X^5Y^4 + X^4Y^5) + (2T^{82} + T^{81} + T^{76} + 2T^{75} + T^{74}$$
$$+ 2T^{70} + T^{69} + 2T^{68} + 2T^{67} + 2T^{65} + 2T^{64} + 2T^{63} + 2T^{62} + T^{60} + 2T^{58}$$
$$+ 2T^{56} + 2T^{54} + T^{52} + 2T^{51} + 2T^{49} + T^{48} + T^{47} + T^{46} + 2T^{45} + 2T^{44}$$
$$+ 2T^{43} + T^{41} + T^{40} + 2T^{37} + T^{34} + T^{33} + T^{32} + T^{31} + 2T^{30} + T^{29}$$
$$+ 2T^{28} + 2T^{27} + 2T^{26} + T^{25} + 2T^{24} + 2T^{23} + 2T^{22} + T^{21} + T^{19} + T^{18}$$
$$+ 2T^{16} + 2T^{15} + T^{13} + 2T^{11} + 2T^{10} + 2T^{9})(X^5Y^3 + X^3Y^5) + (2T^{95}$$
$$+ 2T^{94} + T^{93} + T^{92} + 2T^{91} + T^{90} + T^{89} + T^{88} + T^{87} + 2T^{86} + 2T^{84}$$
$$+ 2T^{83} + T^{79} + 2T^{78} + 2T^{77} + T^{75} + T^{74} + T^{73} + T^{72} + T^{71} + 2T^{70}$$
$$+ 2T^{69} + 2T^{66} + T^{65} + 2T^{64} + T^{63} + 2T^{62} + 2T^{60} + 2T^{58} + T^{57} + 2T^{56}$$
$$+ 2T^{55} + 2T^{54} + 2T^{53} + T^{51} + T^{50} + 2T^{49} + 2T^{47} + 2T^{46} + 2T^{45} + 2T^{43}$$
$$+ 2T^{41} + 2T^{38} + T^{37} + T^{36} + 2T^{35} + 2T^{34} + 2T^{33} + 2T^{31} + T^{29} + 2T^{28}$$
$$+ T^{26} + 2T^{24} + 2T^{22} + T^{18} + T^{16} + 2T^{13} + 2T^{12})(X^5Y^2 + X^2Y^5)$$
$$+ (T^{104} + T^{103} + T^{102} + 2T^{101} + T^{100} + 2T^{98} + 2T^{97} + 2T^{96} + 2T^{92} + T^{91}$$
$$+ T^{90} + T^{89} + 2T^{87} + 2T^{85} + T^{84} + T^{83} + 2T^{82} + 2T^{81} + T^{78} + 2T^{76}$$

$$+ 2T^{75} + T^{74} + 2T^{73} + T^{72} + T^{70} + T^{68} + T^{67} + T^{66} + T^{64} + T^{63} + T^{62}$$
$$+ T^{60} + T^{58} + 2T^{57} + T^{56} + 2T^{55} + T^{52} + T^{47} + T^{45} + 2T^{44} + T^{43}$$
$$+ 2T^{42} + T^{40} + 2T^{39} + 2T^{38} + T^{37} + 2T^{36} + 2T^{35} + T^{34} + T^{33} + T^{32}$$
$$+ 2T^{31} + 2T^{29} + 2T^{28} + 2T^{27} + T^{26} + 2T^{22} + 2T^{18})(X^5Y + XY^5)$$
$$+ (2T^{107} + 2T^{106} + 2T^{104} + 2T^{102} + 2T^{100} + 2T^{98} + 2T^{96} + 2T^{94} + 2T^{92}$$
$$+ 2T^{90} + 2T^{89} + T^{88} + T^{86} + T^{84} + T^{83} + 2T^{82} + T^{79} + 2T^{78} + 2T^{77}$$
$$+ T^{75} + T^{74} + 2T^{73} + T^{71} + 2T^{70} + 2T^{69} + 2T^{66} + T^{65} + 2T^{62} + 2T^{61}$$
$$+ 2T^{59} + 2T^{57} + 2T^{55} + 2T^{53} + 2T^{51} + T^{50} + T^{47} + T^{46} + 2T^{43} + T^{42}$$
$$+ 2T^{41} + T^{40} + 2T^{39} + T^{38} + 2T^{37} + T^{36} + 2T^{35} + T^{34} + 2T^{33} + 2T^{32}$$
$$+ T^{30} + T^{28} + 2T^{26} + T^{25} + T^{24} + T^{21} + 2T^{20})(X^5 + Y^5) + (T^{86} + T^{85}$$
$$+ T^{84} + 2T^{83} + T^{81} + T^{80} + T^{79} + 2T^{78} + T^{77} + T^{76} + 2T^{75} + T^{74} + T^{73}$$
$$+ 2T^{72} + T^{71} + T^{68} + 2T^{66} + T^{65} + T^{64} + T^{62} + 2T^{61} + T^{59} + T^{58} + 2T^{57}$$
$$+ 2T^{56} + T^{53} + T^{50} + T^{48} + T^{47} + 2T^{46} + 2T^{44} + T^{42} + 2T^{41} + 2T^{40}$$
$$+ 2T^{39} + 2T^{38} + T^{37} + T^{36} + T^{34} + 2T^{32} + 2T^{30} + 2T^{29} + T^{27} + T^{26}$$
$$+ 2T^{25} + T^{24} + T^{23} + 2T^{21} + 2T^{20} + T^{18} + 2T^{15} + 2T^{14} + T^{13} + T^{12}$$
$$+ 2T^{11} + T^{10} + 2T^8)X^4Y^4 + (2T^{93} + T^{90} + T^{84} + T^{83} + T^{82} + T^{81}$$
$$+ 2T^{79} + T^{78} + 2T^{76} + 2T^{73} + 2T^{72} + 2T^{71} + T^{70} + 2T^{69} + 2T^{68} + T^{67}$$
$$+ T^{66} + 2T^{64} + T^{63} + T^{62} + T^{61} + 2T^{60} + 2T^{57} + T^{56} + T^{55} + T^{54} + T^{53}$$
$$+ 2T^{51} + T^{50} + T^{48} + 2T^{47} + T^{46} + 2T^{45} + T^{43} + T^{42} + 2T^{41} + T^{34} + T^{33}$$
$$+ T^{31} + T^{30} + 2T^{28} + 2T^{27} + 2T^{26} + 2T^{25} + 2T^{24} + T^{23} + T^{22} + 2T^{21}$$
$$+ 2T^{20} + 2T^{18} + T^{16} + T^{15} + T^{13} + 2T^{12})(X^4Y^3 + X^3Y^4) + (2T^{104}$$
$$+ 2T^{103} + 2T^{102} + T^{101} + T^{100} + T^{99} + 2T^{98} + 2T^{97} + T^{96} + T^{95} + 2T^{94}$$
$$+ 2T^{93} + 2T^{91} + T^{90} + T^{89} + 2T^{88} + T^{87} + 2T^{86} + 2T^{85} + 2T^{84} + 2T^{82}$$

$$+ 2T^{81} + 2T^{80} + 2T^{79} + 2T^{77} + 2T^{75} + 2T^{73} + 2T^{72} + 2T^{71} + 2T^{70} + T^{67}$$
$$+ 2T^{65} + 2T^{64} + T^{62} + T^{61} + 2T^{60} + T^{57} + T^{56} + T^{54} + 2T^{53} + 2T^{52}$$
$$+ T^{49} + T^{48} + 2T^{47} + 2T^{46} + 2T^{45} + T^{44} + T^{43} + T^{42} + 2T^{40} + 2T^{39}$$
$$+ 2T^{35} + T^{34} + 2T^{33} + 2T^{32} + T^{30} + T^{29} + 2T^{28} + T^{27} + 2T^{24} + 2T^{22}$$
$$+ 2T^{21} + 2T^{20} + 2T^{19} + 2T^{18} + 2T^{17} + 2T^{16})(X^4Y^2 + X^2Y^4) + (T^{107}$$
$$+ T^{106} + T^{105} + T^{104} + 2T^{103} + 2T^{100} + 2T^{99} + T^{98} + 2T^{97} + 2T^{94}$$
$$+ 2T^{93} + T^{92} + T^{91} + T^{90} + T^{89} + 2T^{87} + 2T^{86} + T^{85} + 2T^{84} + 2T^{83}$$
$$+ T^{82} + T^{81} + T^{79} + 2T^{78} + T^{77} + 2T^{76} + 2T^{75} + 2T^{74} + 2T^{73} + T^{71}$$
$$+ 2T^{70} + 2T^{69} + 2T^{68} + T^{67} + T^{66} + 2T^{65} + T^{64} + T^{63} + 2T^{62} + T^{61}$$
$$+ T^{60} + T^{59} + 2T^{58} + T^{57} + T^{56} + 2T^{55} + T^{52} + T^{51} + T^{50} + 2T^{49} + T^{48}$$
$$+ 2T^{47} + 2T^{46} + 2T^{45} + T^{44} + 2T^{43} + T^{42} + T^{41} + 2T^{39} + T^{37} + 2T^{36}$$
$$+ 2T^{34} + 2T^{30} + 2T^{26} + 2T^{24} + 2T^{21} + 2T^{20})(X^4Y + XY^4) + (2T^{78}$$
$$+ 2T^{75} + 2T^{69} + 2T^{63} + 2T^{57} + 2T^{51} + 2T^{45} + 2T^{39} + 2T^{33} + 2T^{27}$$
$$+ T^{24})(X^4 + Y^4) + (T^{108} + 2T^{102} + T^{100} + 2T^{98} + 2T^{97} + 2T^{96} + 2T^{95}$$
$$+ 2T^{94} + T^{93} + T^{92} + 2T^{91} + 2T^{90} + T^{89} + 2T^{88} + T^{86} + 2T^{85} + 2T^{83}$$
$$+ 2T^{82} + 2T^{80} + 2T^{79} + 2T^{77} + T^{76} + T^{75} + 2T^{74} + 2T^{72} + 2T^{71} + 2T^{69}$$
$$+ T^{68} + T^{67} + T^{64} + 2T^{63} + T^{62} + 2T^{60} + 2T^{59} + T^{58} + 2T^{57} + T^{56} + T^{55}$$
$$+ 2T^{53} + 2T^{51} + T^{50} + T^{49} + T^{48} + 2T^{45} + 2T^{44} + T^{43} + 2T^{40} + T^{39}$$
$$+ 2T^{37} + 2T^{36} + T^{35} + T^{34} + 2T^{33} + 2T^{31} + T^{29} + 2T^{28} + 2T^{27} + 2T^{26}$$
$$+ T^{25} + 2T^{24} + T^{21} + 2T^{20} + T^{19} + 2T^{18})X^3Y^3 + (2T^{103} + T^{102} + 2T^{101}$$
$$+ T^{99} + 2T^{97} + T^{96} + T^{94} + 2T^{92} + T^{91} + 2T^{90} + T^{89} + 2T^{88} + T^{86}$$
$$+ T^{85} + 2T^{83} + 2T^{82} + 2T^{81} + 2T^{79} + T^{78} + 2T^{77} + T^{76} + T^{74} + 2T^{72}$$
$$+ T^{71} + 2T^{67} + 2T^{66} + 2T^{64} + T^{63} + 2T^{62} + 2T^{61} + T^{60} + 2T^{54} + T^{53}$$

$$+ T^{48} + T^{47} + 2T^{46} + 2T^{44} + 2T^{40} + T^{38} + 2T^{37} + T^{34} + 2T^{32} + T^{31}$$
$$+ 2T^{30} + T^{29} + 2T^{27} + 2T^{26} + T^{23} + 2T^{22} + 2T^{20})(X^3Y^2 + X^2Y^3)$$
$$+ (2T^{106} + T^{105} + 2T^{103} + T^{102} + 2T^{100} + T^{99} + 2T^{97} + T^{96} + 2T^{94} + T^{93}$$
$$+ 2T^{91} + T^{90} + 2T^{88} + T^{87} + T^{86} + 2T^{84} + 2T^{83} + 2T^{82} + 2T^{81} + 2T^{76}$$
$$+ T^{75} + T^{74} + 2T^{73} + T^{72} + 2T^{70} + T^{69} + T^{68} + 2T^{67} + T^{66} + 2T^{64} + T^{63}$$
$$+ T^{62} + 2T^{61} + T^{60} + 2T^{58} + T^{57} + T^{56} + 2T^{55} + T^{54} + T^{50} + T^{44} + T^{38}$$
$$+ 2T^{31} + 2T^{30} + T^{29} + 2T^{27} + T^{26} + 2T^{25} + T^{24})(X^3Y + XY^3) + (2T^{105}$$
$$+ 2T^{102} + T^{99} + T^{97} + T^{96} + T^{95} + 2T^{94} + T^{93} + 2T^{92} + 2T^{89} + T^{88}$$
$$+ T^{87} + T^{86} + 2T^{85} + 2T^{84} + T^{83} + T^{82} + T^{51} + T^{48} + 2T^{45} + 2T^{43}$$
$$+ 2T^{42} + 2T^{41} + T^{40} + 2T^{39} + T^{38} + T^{35} + 2T^{34} + 2T^{33} + 2T^{32} + T^{31}$$
$$+ T^{30} + 2T^{29} + 2T^{28})(X^3 + Y^3) + (2T^{106} + T^{105} + 2T^{104} + T^{103} + T^{101}$$
$$+ 2T^{99} + 2T^{98} + T^{97} + T^{95} + T^{94} + T^{93} + 2T^{92} + T^{89} + 2T^{88} + 2T^{86}$$
$$+ 2T^{85} + T^{84} + T^{83} + T^{82} + 2T^{80} + 2T^{79} + 2T^{77} + 2T^{75} + 2T^{74} + T^{73}$$
$$+ 2T^{72} + 2T^{71} + 2T^{69} + 2T^{68} + T^{67} + 2T^{66} + 2T^{65} + 2T^{63} + 2T^{62} + T^{61}$$
$$+ 2T^{60} + 2T^{59} + 2T^{57} + 2T^{56} + T^{55} + 2T^{54} + 2T^{53} + T^{52} + T^{51} + 2T^{48}$$
$$+ T^{47} + 2T^{42} + T^{41} + 2T^{40} + T^{39} + T^{37} + 2T^{36} + T^{35} + T^{34} + 2T^{33}$$
$$+ 2T^{31} + T^{30} + T^{29} + 2T^{28} + 2T^{27} + 2T^{25} + 2T^{24})X^2Y^2 + (T^{105} + 2T^{103}$$
$$+ 2T^{102} + T^{100} + 2T^{99} + T^{96} + 2T^{95} + T^{94} + T^{92} + T^{91} + 2T^{90} + T^{89}$$
$$+ T^{88} + T^{87} + 2T^{86} + 2T^{84} + 2T^{83} + 2T^{82} + 2T^{51} + T^{49} + T^{48} + 2T^{46}$$
$$+ T^{45} + 2T^{42} + T^{41} + 2T^{40} + 2T^{38} + 2T^{37} + T^{36} + 2T^{35} + 2T^{34} + 2T^{33}$$
$$+ T^{32} + T^{30} + T^{29} + T^{28})(X^2Y + XY^2) + (T^{104} + T^{103} + 2T^{101} + T^{100}$$
$$+ T^{99} + T^{98} + T^{97} + T^{96} + 2T^{95} + 2T^{94} + T^{93} + 2T^{92} + T^{91} + 2T^{90}$$
$$+ 2T^{89} + T^{87} + 2T^{86} + 2T^{50} + 2T^{49} + T^{47} + 2T^{46} + 2T^{45} + 2T^{44} + 2T^{43}$$

$$+ 2T^{42} + T^{41} + T^{40} + 2T^{39} + T^{38} + 2T^{37} + T^{36} + T^{35} + 2T^{33} + T^{32})(X^2$$
$$+ Y^2) + (T^{104} + T^{103} + T^{102} + 2T^{101} + T^{99} + T^{98} + T^{97} + 2T^{96} + 2T^{95}$$
$$+ T^{94} + T^{93} + 2T^{92} + T^{91} + 2T^{89} + 2T^{88} + T^{87} + 2T^{86} + 2T^{50} + 2T^{49}$$
$$+ 2T^{48} + T^{47} + 2T^{45} + 2T^{44} + 2T^{43} + T^{42} + T^{41} + 2T^{40} + 2T^{39} + T^{38}$$
$$+ 2T^{37} + T^{35} + T^{34} + 2T^{33} + T^{32})XY$$

$$\Phi_{T^2+2T+2}(X,Y) = X^{10} + Y^{10} + 2X^9Y^9 + (2T^3 + 2T + 1)(X^9Y^6 + X^6Y^9) + (T^2 + 2T$$
$$+ 2)(X^9Y^5 + X^5Y^9) + (T^5 + 2T^4 + T^3 + T^2 + T)(X^9Y^4 + X^4Y^9)$$
$$+ (2T^{12} + 2T^{10} + T^9 + T^8 + 2T^7 + 2T^5 + 2T^4 + 2T^2 + T + 1)(X^9Y^3$$
$$+ X^3Y^9) + (T^5 + 2T^4 + 2T^3 + T^2 + 2T + 2)(X^9Y^2 + X^2Y^9) + (T^{14}$$
$$+ 2T^{13} + T^{12} + T^{11} + T^{10} + T^8 + 2T^7 + T^4 + 2T^3 + T^2 + 2T + 2)(X^9Y$$
$$+ XY^9) + (T^{27} + 2T^{21} + 2T^{19} + T^{18} + 2T^{17} + T^{16} + T^{14} + T^{13} + 2T^{11}$$
$$+ T^{10} + 2T^8 + 2T^6 + 2T^5 + T^4)(X^9 + Y^9) + (T^{14} + 2T^{13} + 2T^{12} + T^{11}$$
$$+ 2T^{10} + 2T^9 + T^5 + 2T^4 + 2T^3 + 2T^2 + T + 1)X^8Y^8 + (T^{23} + 2T^{22}$$
$$+ T^{21} + T^{20} + T^{19} + 2T^{17} + T^{16} + 2T^{13} + T^{12} + 2T^{11} + T^{10} + 2T^8 + 2T^6$$
$$+ T^5 + 2T^4 + 2T^3)(X^8Y^7 + X^7Y^8) + (2T^{30} + 2T^{28} + T^{27} + 2T^4 + T^3$$
$$+ T + 1)(X^8Y^6 + X^6Y^8) + (T^{29} + 2T^{28} + 2T^{27} + T^{23} + 2T^{22} + 2T^{21}$$
$$+ T^{20} + 2T^{19} + 2T^{18} + T^{17} + 2T^{16} + T^{14} + 2T^{12} + T^{10} + 2T^9 + T^8 + 2T^7$$
$$+ T^4 + T^3 + 2T + 1)(X^8Y^5 + X^5Y^8) + (2T^{32} + T^{31} + 2T^{30} + 2T^{29}$$
$$+ 2T^{28} + T^{26} + 2T^{25} + 2T^{24} + 2T^{23} + 2T^{20} + 2T^{18} + 2T^{17} + 2T^{13} + T^{10}$$
$$+ 2T^7 + T^6 + T^5 + 2T^4 + 2T^3 + 1)(X^8Y^4 + X^4Y^8) + (T^{39} + T^{37} + 2T^{36}$$
$$+ 2T^{35} + T^{34} + 2T^{33} + T^{32} + 2T^{31} + 2T^{30} + T^{28} + T^{27} + 2T^{25} + 2T^{24}$$
$$+ 2T^{23} + 2T^{22} + T^{21} + 2T^{20} + T^{19} + T^{16} + T^{15} + T^{14} + 2T^{13} + T^{12}$$
$$+ 2T^{11} + 2T^8 + 2T^7 + T^5 + 2T^4 + 2T^3 + T^2 + T + 2)(X^8Y^3 + X^3Y^8)$$

$$+ (2T^{32} + T^{31} + 2T^{29} + 2T^{28} + T^{27} + 2T^{26} + T^{25} + 2T^{24} + T^{23} + T^{22}$$
$$+ 2T^{19} + 2T^{18} + T^{17} + 2T^{15} + 2T^{14} + T^{13} + T^{12} + 2T^{9} + T^{8} + T^{5} + T^{3}$$
$$+ 2T)(X^8Y^2 + X^2Y^8) + (T^{35} + 2T^{34} + 2T^{33} + 2T^{32} + T^{31} + T^{30} + T^{29}$$
$$+ 2T^{28} + T^{27} + T^{25} + T^{24} + 2T^{22} + T^{18} + 2T^{17} + T^{14} + 2T^{13} + T^{12}$$
$$+ 2T^{10} + 2T^{7} + 2T^{6} + 2T^{5} + T^{4})(X^8Y + XY^8) + (2T^{26} + T^{25} + T^{23}$$
$$+ T^{21} + T^{19} + T^{17} + T^{15} + T^{13} + T^{11} + T^{9} + T^{8})(X^8 + Y^8) + (T^{32}$$
$$+ 2T^{31} + T^{30} + T^{29} + 2T^{28} + T^{27} + T^{24} + 2T^{22} + T^{21} + T^{20} + T^{19} + T^{18}$$
$$+ T^{16} + T^{14} + 2T^{13} + T^{12} + 2T^{10} + T^{7} + 2T^{6} + 2T^{5} + 2T^{3} + 2T^{2} + 2T$$
$$+ 1)X^7Y^7 + (T^{41} + 2T^{40} + T^{38} + 2T^{37} + 2T^{35} + T^{34} + 2T^{33} + 2T^{32}$$
$$+ T^{29} + T^{28} + 2T^{27} + 2T^{25} + 2T^{24} + T^{23} + T^{21} + T^{20} + 2T^{19} + 2T^{17}$$
$$+ 2T^{16} + T^{15} + T^{14} + 2T^{13} + T^{10} + T^{9} + T^{8} + 2T^{7} + 2T^{6} + T^{5} + 2T^{4}$$
$$+ 2T^{2} + T + 2)(X^7Y^6 + X^6Y^7) + (2T^{50} + T^{49} + 2T^{48} + 2T^{47} + T^{45}$$
$$+ T^{41} + 2T^{40} + T^{39} + 2T^{38} + 2T^{37} + 2T^{36} + 2T^{34} + 2T^{33} + T^{31} + T^{30}$$
$$+ T^{29} + T^{27} + T^{24} + 2T^{23} + 2T^{22} + 2T^{21} + 2T^{15} + 2T^{14} + T^{12} + 2T^{11}$$
$$+ 2T^{9} + 2T^{8} + T^{6} + 2T^{5} + 2T^{2} + 2T)(X^7Y^5 + X^5Y^7) + (T^{59} + 2T^{58}$$
$$+ T^{57} + T^{56} + T^{55} + T^{53} + 2T^{52} + 2T^{51} + 2T^{50} + 2T^{47} + 2T^{45} + 2T^{44}$$
$$+ T^{41} + T^{40} + T^{39} + T^{38} + T^{37} + 2T^{36} + 2T^{35} + T^{30} + T^{28} + T^{27} + T^{26}$$
$$+ T^{22} + T^{18} + 2T^{17} + 2T^{16} + T^{13} + T^{12} + T^{11} + T^{10} + 2T^{8} + T^{7} + 2T^{6}$$
$$+ T^{2})(X^7Y^4 + X^4Y^7) + (2T^{66} + 2T^{64} + T^{63} + T^{62} + 2T^{61} + 2T^{60} + 2T^{59}$$
$$+ 2T^{57} + T^{56} + 2T^{52} + 2T^{51} + T^{50} + T^{48} + T^{47} + 2T^{46} + T^{43} + 2T^{42}$$
$$+ 2T^{41} + 2T^{40} + T^{39} + 2T^{38} + T^{37} + 2T^{36} + 2T^{35} + T^{34} + 2T^{33} + T^{29}$$
$$+ T^{27} + T^{26} + T^{25} + 2T^{22} + T^{21} + T^{20} + T^{18} + 2T^{17} + 2T^{15} + 2T^{13}$$
$$+ 2T^{11} + T^{10} + 2T^{9} + T^{8} + T^{5} + 2T^{4} + T^{2} + 2T)(X^7Y^3 + X^3Y^7) + (T^{59}$$

$$+ 2T^{58} + T^{56} + T^{55} + 2T^{54} + 2T^{53} + T^{52} + 2T^{51} + T^{50} + T^{49} + 2T^{46}$$
$$+ 2T^{45} + T^{44} + 2T^{42} + 2T^{41} + T^{40} + T^{37} + 2T^{36} + T^{34} + T^{33} + 2T^{32}$$
$$+ 2T^{31} + 2T^{30} + T^{29} + 2T^{28} + 2T^{27} + 2T^{26} + 2T^{25} + T^{23} + T^{21} + 2T^{18}$$
$$+ T^{17} + 2T^{16} + 2T^{14} + 2T^{13} + T^{9} + 2T^{6} + T^{5} + T^{4})(X^7Y^2 + X^2Y^7)$$
$$+ (2T^{62} + T^{61} + T^{60} + T^{59} + 2T^{58} + 2T^{57} + 2T^{54} + T^{52} + T^{51} + T^{50}$$
$$+ T^{49} + 2T^{48} + T^{47} + 2T^{46} + T^{44} + T^{43} + T^{41} + 2T^{40} + 2T^{39} + T^{38} + T^{37}$$
$$+ 2T^{35} + T^{34} + 2T^{31} + 2T^{30} + T^{29} + T^{25} + T^{23} + 2T^{21} + 2T^{19} + 2T^{18}$$
$$+ T^{17} + 2T^{16} + 2T^{15} + T^{11} + 2T^{10} + T^{8})(X^7Y + XY^7) + (T^{81} + 2T^{63}$$
$$+ 2T^{57} + T^{54} + 2T^{51} + T^{48} + T^{42} + T^{39} + 2T^{33} + T^{30} + 2T^{24} + 2T^{18}$$
$$+ 2T^{15} + T^{12})(X^7 + Y^7) + (T^{46} + T^{45} + T^{40} + T^{39} + T^{38} + 2T^{37} + T^{36}$$
$$+ T^{34} + T^{33} + T^{32} + 2T^{31} + T^{30} + 2T^{29} + T^{27} + 2T^{26} + T^{25} + 2T^{24}$$
$$+ T^{23} + 2T^{22} + T^{21} + 2T^{20} + 2T^{19} + 2T^{18} + T^{17} + 2T^{15} + T^{9} + T^{8} + T^{7}$$
$$+ 2T^{6} + T^{5} + T^{4} + T^{3} + 2T^{2} + 2)X^6Y^6 + (T^{57} + 2T^{55} + T^{53} + 2T^{52}$$
$$+ 2T^{50} + 2T^{48} + 2T^{47} + 2T^{45} + 2T^{44} + 2T^{42} + 2T^{40} + T^{39} + 2T^{37} + T^{36}$$
$$+ 2T^{34} + 2T^{32} + 2T^{30} + T^{29} + 2T^{28} + T^{27} + T^{26} + T^{25} + 2T^{24} + 2T^{21}$$
$$+ 2T^{18} + 2T^{15} + T^{14} + 2T^{12} + T^{11} + 2T^{9} + T^{8} + 2T^{7} + T^{5} + 2T^{3}$$
$$+ 2)(X^6Y^5 + X^5Y^6) + (2T^{68} + T^{67} + T^{66} + 2T^{65} + T^{64} + T^{63} + 2T^{60}$$
$$+ 2T^{59} + T^{58} + 2T^{57} + T^{56} + 2T^{55} + T^{54} + T^{52} + T^{51} + 2T^{49} + T^{48}$$
$$+ 2T^{46} + T^{45} + 2T^{44} + 2T^{41} + T^{40} + 2T^{39} + 2T^{36} + 2T^{35} + 2T^{34} + 2T^{32}$$
$$+ 2T^{31} + 2T^{30} + T^{29} + T^{25} + T^{24} + T^{22} + T^{20} + 2T^{17} + T^{13} + 2T^{12}$$
$$+ 2T^{10} + T^{7} + T^{6} + 2T^{5} + T^{3} + T^{2} + 2T)(X^6Y^4 + X^4Y^6) + (T^{81} + T^{69}$$
$$+ 2T^{66} + 2T^{65} + T^{64} + 2T^{61} + T^{58} + 2T^{56} + 2T^{54} + T^{53} + 2T^{52} + 2T^{50}$$
$$+ T^{49} + 2T^{47} + T^{46} + 2T^{44} + 2T^{43} + T^{41} + T^{40} + 2T^{39} + 2T^{38} + T^{37}$$

$$+ 2T^{36} + 2T^{34} + T^{33} + T^{31} + T^{30} + 2T^{29} + 2T^{28} + 2T^{27} + T^{26} + T^{24}$$

$$+ 2T^{22} + 2T^{21} + T^{17} + 2T^{16} + T^{15} + T^{14} + 2T^{12} + 2T^{11} + 2T^{10} + 2T^{9}$$

$$+ 2T^{8} + 2T^{7} + 2T^{6} + T^{5} + 2T^{4})(X^6Y^3 + X^3Y^6) + (2T^{84} + T^{82} + 2T^{68}$$

$$+ T^{67} + 2T^{65} + 2T^{63} + 2T^{60} + 2T^{59} + T^{58} + T^{57} + 2T^{55} + 2T^{54} + 2T^{52}$$

$$+ 2T^{51} + T^{5}0 + T^{48} + T^{47} + T^{45} + 2T^{44} + 2T^{43} + T^{41} + 2T^{39} + T^{38}$$

$$+ T^{37} + T^{36} + 2T^{35} + T^{34} + 2T^{32} + T^{30} + T^{29} + 2T^{27} + T^{26} + T^{25} + T^{24}$$

$$+ 2T^{22} + 2T^{20} + T^{17} + T^{15} + T^{14} + 2T^{13} + 2T^{12} + 2T^{11} + 2T^{10}$$

$$+ T^{9})(X^6Y^2 + X^2Y^6) + (T^{95} + 2T^{94} + T^{93} + T^{92} + T^{91} + 2T^{89} + T^{88}$$

$$+ 2T^{87} + 2T^{86} + 2T^{85} + 2T^{77} + T^{76} + 2T^{74} + 2T^{72} + 2T^{71} + T^{70} + 2T^{68}$$

$$+ 2T^{67} + T^{66} + T^{65} + T^{64} + 2T^{62} + T^{61} + T^{58} + 2T^{57} + 2T^{56} + T^{54}$$

$$+ 2T^{53} + T^{52} + T^{51} + 2T^{50} + T^{48} + T^{47} + 2T^{46} + 2T^{45} + 2T^{44} + 2T^{43}$$

$$+ 2T^{40} + 2T^{39} + 2T^{38} + T^{36} + 2T^{35} + 2T^{34} + 2T^{33} + 2T^{32} + 2T^{31} + T^{30}$$

$$+ T^{29} + T^{27} + 2T^{26} + T^{21} + 2T^{20} + 2T^{19} + 2T^{18} + T^{17} + T^{16} + T^{15}$$

$$+ T^{14})(X^6Y + XY^6) + (T^{108} + 2T^{102} + 2T^{100} + T^{99} + 2T^{98} + T^{97} + T^{95}$$

$$+ T^{94} + 2T^{92} + T^{91} + 2T^{90} + 2T^{89} + 2T^{87} + 2T^{86} + T^{85} + T^{82} + T^{80}$$

$$+ 2T^{79} + 2T^{77} + 2T^{75} + 2T^{74} + 2T^{72} + 2T^{71} + T^{70} + T^{68} + 2T^{66} + T^{65}$$

$$+ T^{64} + 2T^{62} + T^{61} + T^{60} + T^{59} + 2T^{58} + T^{55} + 2T^{53} + T^{52} + 2T^{50}$$

$$+ 2T^{49} + 2T^{47} + T^{46} + 2T^{45} + T^{44} + 2T^{43} + T^{42} + T^{41} + 2T^{38} + 2T^{37}$$

$$+ 2T^{36} + T^{35} + T^{33} + T^{32} + 2T^{30} + T^{28} + T^{24} + T^{23} + T^{21} + 2T^{19}$$

$$+ 2T^{18} + 2T^{17} + T^{16})(X^6 + Y^6) + (2T^{64} + 2T^{63} + 2T^{62} + T^{61} + 2T^{60}$$

$$+ T^{59} + 2T^{57} + 2T^{56} + T^{55} + 2T^{54} + T^{52} + T^{51} + 2T^{49} + 2T^{48} + 2T^{46}$$

$$+ 2T^{45} + T^{44} + T^{43} + 2T^{41} + 2T^{40} + 2T^{38} + 2T^{36} + 2T^{35} + T^{33} + 2T^{32}$$

$$+ T^{31} + T^{30} + T^{29} + T^{28} + T^{26} + 2T^{24} + 2T^{23} + T^{21} + 2T^{20} + 2T^{18}$$

$$+ 2T^{16} + 2T^{15} + 2T^{14} + 2T^{13} + 2T^{11} + 2T^{10} + 2T^{8} + T^{6} + T^{5} + T^{3}$$

$$+ 2T)X^5Y^5 + (T^{77} + 2T^{76} + T^{75} + T^{74} + T^{73} + 2T^{71} + T^{70} + 2T^{66} + T^{65}$$

$$+ 2T^{63} + 2T^{62} + 2T^{61} + T^{60} + 2T^{59} + 2T^{57} + 2T^{55} + T^{54} + 2T^{53} + T^{52}$$

$$+ T^{51} + 2T^{49} + 2T^{47} + T^{46} + 2T^{45} + 2T^{44} + T^{42} + T^{41} + T^{40} + 2T^{39}$$

$$+ T^{38} + 2T^{37} + 2T^{35} + 2T^{34} + T^{33} + 2T^{32} + T^{31} + T^{30} + T^{29} + T^{28}$$

$$+ 2T^{26} + T^{25} + T^{24} + T^{23} + T^{22} + T^{21} + 2T^{16} + 2T^{14} + 2T^{13} + T^{12}$$

$$+ 2T^{10} + 2T^{7} + T^{6} + T^{4})(X^5Y^4 + X^4Y^5) + (2T^{82} + 2T^{81} + T^{76} + T^{75}$$

$$+ T^{74} + 2T^{70} + 2T^{69} + 2T^{68} + T^{67} + T^{65} + 2T^{64} + T^{63} + 2T^{62} + T^{60}$$

$$+ 2T^{58} + 2T^{56} + 2T^{54} + T^{52} + T^{51} + T^{49} + T^{48} + 2T^{47} + T^{46} + T^{45}$$

$$+ 2T^{44} + T^{43} + 2T^{41} + T^{40} + T^{37} + T^{34} + 2T^{33} + T^{32} + 2T^{31} + 2T^{30}$$

$$+ 2T^{29} + 2T^{28} + T^{27} + 2T^{26} + 2T^{25} + 2T^{24} + T^{23} + 2T^{22} + 2T^{21} + 2T^{19}$$

$$+ T^{18} + 2T^{16} + T^{15} + 2T^{13} + T^{11} + 2T^{10} + T^{9})(X^5Y^3 + X^3Y^5) + (2T^{95}$$

$$+ T^{94} + T^{93} + 2T^{92} + 2T^{91} + 2T^{90} + T^{89} + 2T^{88} + T^{87} + T^{86} + T^{84}$$

$$+ 2T^{83} + T^{79} + T^{78} + 2T^{77} + T^{75} + 2T^{74} + T^{73} + 2T^{72} + T^{71} + T^{70}$$

$$+ 2T^{69} + T^{66} + T^{65} + T^{64} + T^{63} + T^{62} + T^{60} + T^{58} + T^{57} + T^{56} + 2T^{55}$$

$$+ T^{54} + 2T^{53} + T^{51} + 2T^{50} + 2T^{49} + 2T^{47} + T^{46} + 2T^{45} + 2T^{43} + 2T^{41}$$

$$+ T^{38} + T^{37} + 2T^{36} + 2T^{35} + T^{34} + 2T^{33} + 2T^{31} + T^{29} + T^{28} + 2T^{26}$$

$$+ T^{24} + T^{22} + 2T^{18} + 2T^{16} + 2T^{13} + T^{12})(X^5Y^2 + X^2Y^5) + (T^{104}$$

$$+ 2T^{103} + T^{102} + T^{101} + T^{100} + 2T^{98} + T^{97} + 2T^{96} + 2T^{92} + 2T^{91} + T^{90}$$

$$+ 2T^{89} + T^{87} + T^{85} + T^{84} + 2T^{83} + 2T^{82} + T^{81} + T^{78} + 2T^{76} + T^{75}$$

$$+ T^{74} + T^{73} + T^{72} + T^{70} + T^{68} + 2T^{67} + T^{66} + T^{64} + 2T^{63} + T^{62} + T^{60}$$

$$+ T^{58} + T^{57} + T^{56} + T^{55} + T^{52} + 2T^{47} + 2T^{45} + 2T^{44} + 2T^{43} + 2T^{42}$$

$$+ T^{40} + T^{39} + 2T^{38} + 2T^{37} + 2T^{36} + T^{35} + T^{34} + 2T^{33} + T^{32} + T^{31}$$

$$+ T^{29} + 2T^{28} + T^{27} + T^{26} + 2T^{22} + 2T^{18})(X^5Y + XY^5) + (2T^{107} + T^{106}$$
$$+ T^{104} + T^{102} + T^{100} + T^{98} + T^{96} + T^{94} + T^{92} + T^{90} + 2T^{89} + 2T^{88}$$
$$+ 2T^{86} + 2T^{84} + T^{83} + T^{82} + T^{79} + T^{78} + 2T^{77} + T^{75} + 2T^{74} + 2T^{73}$$
$$+ T^{71} + T^{70} + 2T^{69} + T^{66} + T^{65} + T^{62} + 2T^{61} + 2T^{59} + 2T^{57} + 2T^{55}$$
$$+ 2T^{53} + 2T^{51} + 2T^{50} + T^{47} + 2T^{46} + 2T^{43} + 2T^{42} + 2T^{41} + 2T^{40} + 2T^{39}$$
$$+ 2T^{38} + 2T^{37} + 2T^{36} + 2T^{35} + 2T^{34} + 2T^{33} + T^{32} + 2T^{30} + 2T^{28} + T^{26}$$
$$+ T^{25} + 2T^{24} + T^{21} + T^{20})(X^5 + Y^5) + (T^{86} + 2T^{85} + T^{84} + T^{83} + 2T^{81}$$
$$+ T^{80} + 2T^{79} + 2T^{78} + 2T^{77} + T^{76} + T^{75} + T^{74} + 2T^{73} + 2T^{72} + 2T^{71}$$
$$+ T^{68} + 2T^{66} + 2T^{65} + T^{64} + T^{62} + T^{61} + 2T^{59} + T^{58} + T^{57} + 2T^{56}$$
$$+ 2T^{53} + T^{50} + T^{48} + 2T^{47} + 2T^{46} + 2T^{44} + T^{42} + T^{41} + 2T^{40} + T^{39}$$
$$+ 2T^{38} + 2T^{37} + T^{36} + T^{34} + 2T^{32} + 2T^{30} + T^{29} + 2T^{27} + T^{26} + T^{25}$$
$$+ T^{24} + 2T^{23} + T^{21} + 2T^{20} + T^{18} + T^{15} + 2T^{14} + 2T^{13} + T^{12} + T^{11}$$
$$+ T^{10} + 2T^{8})X^4Y^4 + (2T^{93} + 2T^{90} + 2T^{84} + T^{83} + 2T^{82} + T^{81} + 2T^{79}$$
$$+ 2T^{78} + T^{76} + 2T^{73} + T^{72} + 2T^{71} + 2T^{70} + 2T^{69} + T^{68} + T^{67} + 2T^{66}$$
$$+ T^{64} + T^{63} + 2T^{62} + T^{61} + T^{60} + 2T^{57} + 2T^{56} + T^{55} + 2T^{54} + T^{53}$$
$$+ 2T^{51} + 2T^{50} + 2T^{48} + 2T^{47} + 2T^{46} + 2T^{45} + T^{43} + 2T^{42} + 2T^{41} + 2T^{34}$$
$$+ T^{33} + T^{31} + 2T^{30} + T^{28} + 2T^{27} + T^{26} + 2T^{25} + T^{24} + T^{23} + 2T^{22}$$
$$+ 2T^{21} + T^{20} + T^{18} + 2T^{16} + T^{15} + T^{13} + T^{12})(X^4Y^3 + X^3Y^4) + (2T^{104}$$
$$+ T^{103} + 2T^{102} + 2T^{101} + T^{100} + 2T^{99} + 2T^{98} + T^{97} + T^{96} + 2T^{95} + 2T^{94}$$
$$+ T^{93} + T^{91} + T^{90} + 2T^{89} + 2T^{88} + 2T^{87} + 2T^{86} + T^{85} + 2T^{84} + 2T^{82}$$
$$+ T^{81} + 2T^{80} + T^{79} + T^{77} + T^{75} + T^{73} + 2T^{72} + T^{71} + 2T^{70} + 2T^{67}$$
$$+ T^{65} + 2T^{64} + T^{62} + 2T^{61} + 2T^{60} + 2T^{57} + T^{56} + T^{54} + T^{53} + 2T^{52}$$
$$+ 2T^{49} + T^{48} + T^{47} + 2T^{46} + T^{45} + T^{44} + 2T^{43} + T^{42} + 2T^{40} + T^{39}$$

$$+ T^{35} + T^{34} + T^{33} + 2T^{32} + T^{30} + 2T^{29} + 2T^{28} + 2T^{27} + 2T^{24} + 2T^{22}$$
$$+ T^{21} + 2T^{20} + T^{19} + 2T^{18} + T^{17} + 2T^{16})(X^4Y^2 + X^2Y^4) + (T^{107}$$
$$+ 2T^{106} + T^{105} + 2T^{104} + 2T^{103} + T^{100} + 2T^{99} + 2T^{98} + 2T^{97} + T^{94}$$
$$+ 2T^{93} + 2T^{92} + T^{91} + 2T^{90} + T^{89} + 2T^{87} + T^{86} + T^{85} + T^{84} + 2T^{83}$$
$$+ 2T^{82} + T^{81} + T^{79} + T^{78} + T^{77} + T^{76} + 2T^{75} + T^{74} + 2T^{73} + T^{71} + T^{70}$$
$$+ 2T^{69} + T^{68} + T^{67} + 2T^{66} + 2T^{65} + 2T^{64} + T^{63} + T^{62} + T^{61} + 2T^{60}$$
$$+ T^{59} + T^{58} + T^{57} + 2T^{56} + 2T^{55} + 2T^{52} + T^{51} + 2T^{50} + 2T^{49} + 2T^{48}$$
$$+ 2T^{47} + T^{46} + 2T^{45} + 2T^{44} + 2T^{43} + 2T^{42} + T^{41} + 2T^{39} + T^{37} + T^{36}$$
$$+ T^{34} + T^{30} + T^{26} + T^{24} + 2T^{21} + T^{20})(X^4Y + XY^4) + (2T^{78} + T^{75}$$
$$+ T^{69} + T^{63} + T^{57} + T^{51} + T^{45} + T^{39} + T^{33} + T^{27} + T^{24})(X^4 + Y^4)$$
$$+ (T^{108} + 2T^{102} + T^{100} + 2T^{98} + T^{97} + 2T^{96} + T^{95} + 2T^{94} + 2T^{93} + T^{92}$$
$$+ T^{91} + 2T^{90} + 2T^{89} + 2T^{88} + T^{86} + T^{85} + T^{83} + 2T^{82} + 2T^{80} + T^{79}$$
$$+ T^{77} + T^{76} + 2T^{75} + 2T^{74} + 2T^{72} + T^{71} + T^{69} + T^{68} + 2T^{67} + T^{64} + T^{63}$$
$$+ T^{62} + 2T^{60} + T^{59} + T^{58} + T^{57} + T^{56} + 2T^{55} + T^{53} + T^{51} + T^{50} + 2T^{49}$$
$$+ T^{48} + T^{45} + 2T^{44} + 2T^{43} + 2T^{40} + 2T^{39} + T^{37} + 2T^{36} + 2T^{35} + T^{34}$$
$$+ T^{33} + T^{31} + 2T^{29} + 2T^{28} + T^{27} + 2T^{26} + 2T^{25} + 2T^{24} + 2T^{21} + 2T^{20}$$
$$+ 2T^{19} + 2T^{18})X^3Y^3 + (2T^{103} + 2T^{102} + 2T^{101} + T^{99} + 2T^{97} + 2T^{96}$$
$$+ 2T^{94} + T^{92} + T^{91} + T^{90} + T^{89} + T^{88} + 2T^{86} + T^{85} + 2T^{83} + T^{82}$$
$$+ 2T^{81} + 2T^{79} + 2T^{78} + 2T^{77} + 2T^{76} + 2T^{74} + T^{72} + T^{71} + 2T^{67} + T^{66}$$
$$+ T^{64} + T^{63} + T^{62} + 2T^{61} + 2T^{60} + T^{54} + T^{53} + 2T^{48} + T^{47} + T^{46} + T^{44}$$
$$+ T^{40} + 2T^{38} + 2T^{37} + 2T^{34} + T^{32} + T^{31} + T^{30} + T^{29} + 2T^{27} + T^{26} + T^{23}$$
$$+ T^{22} + T^{20})(X^3Y^2 + X^2Y^3) + (2T^{106} + 2T^{105} + T^{103} + T^{102} + 2T^{100}$$
$$+ 2T^{99} + T^{97} + T^{96} + 2T^{94} + 2T^{93} + T^{91} + T^{90} + 2T^{88} + 2T^{87} + T^{86}$$

$$+ 2T^{84} + T^{83} + 2T^{82} + T^{81} + 2T^{76} + 2T^{75} + T^{74} + T^{73} + T^{72} + 2T^{70}$$
$$+ 2T^{69} + T^{68} + T^{67} + T^{66} + 2T^{64} + 2T^{63} + T^{62} + T^{61} + T^{60} + 2T^{58}$$
$$+ 2T^{57} + T^{56} + T^{55} + T^{54} + T^{50} + T^{44} + T^{38} + T^{31} + 2T^{30} + 2T^{29} + T^{27}$$
$$+ T^{26} + T^{25} + T^{24})(X^3Y + XY^3) + (2T^{105} + T^{102} + T^{99} + T^{97} + 2T^{96}$$
$$+ T^{95} + T^{94} + T^{93} + T^{92} + 2T^{89} + 2T^{88} + T^{87} + 2T^{86} + 2T^{85} + T^{84}$$
$$+ T^{83} + 2T^{82} + T^{51} + 2T^{48} + 2T^{45} + 2T^{43} + T^{42} + 2T^{41} + 2T^{40} + 2T^{39}$$
$$+ 2T^{38} + T^{35} + T^{34} + 2T^{33} + T^{32} + T^{31} + 2T^{30} + 2T^{29} + T^{28})(X^3 + Y^3)$$
$$+ (2T^{106} + 2T^{105} + 2T^{104} + 2T^{103} + 2T^{101} + T^{99} + 2T^{98} + 2T^{97} + 2T^{95}$$
$$+ T^{94} + 2T^{93} + 2T^{92} + 2T^{89} + 2T^{88} + 2T^{86} + T^{85} + T^{84} + 2T^{83} + T^{82}$$
$$+ 2T^{80} + T^{79} + T^{77} + T^{75} + 2T^{74} + 2T^{73} + 2T^{72} + T^{71} + T^{69} + 2T^{68}$$
$$+ 2T^{67} + 2T^{66} + T^{65} + T^{63} + 2T^{62} + 2T^{61} + 2T^{60} + T^{59} + T^{57} + 2T^{56}$$
$$+ 2T^{55} + 2T^{54} + T^{53} + T^{52} + 2T^{51} + 2T^{48} + 2T^{47} + 2T^{42} + 2T^{41} + 2T^{40}$$
$$+ 2T^{39} + 2T^{37} + 2T^{36} + 2T^{35} + T^{34} + T^{33} + T^{31} + T^{30} + 2T^{29} + 2T^{28}$$
$$+ T^{27} + T^{25} + 2T^{24})X^2Y^2 + (T^{105} + 2T^{103} + T^{102} + 2T^{100} + 2T^{99} + 2T^{96}$$
$$+ 2T^{95} + 2T^{94} + 2T^{92} + T^{91} + T^{90} + T^{89} + 2T^{88} + T^{87} + T^{86} + T^{84}$$
$$+ 2T^{83} + T^{82} + 2T^{51} + T^{49} + 2T^{48} + T^{46} + T^{45} + T^{42} + T^{41} + T^{40} + T^{38}$$
$$+ 2T^{37} + 2T^{36} + 2T^{35} + T^{34} + 2T^{33} + 2T^{32} + 2T^{30} + T^{29} + 2T^{28})(X^2Y$$
$$+ XY^2) + (T^{104} + 2T^{103} + T^{101} + T^{100} + 2T^{99} + T^{98} + 2T^{97} + T^{96} + T^{95}$$
$$+ 2T^{94} + 2T^{93} + 2T^{92} + 2T^{91} + 2T^{90} + T^{89} + 2T^{87} + 2T^{86} + 2T^{50} + T^{49}$$
$$+ 2T^{47} + 2T^{46} + T^{45} + 2T^{44} + T^{43} + 2T^{42} + 2T^{41} + T^{40} + T^{39} + T^{38}$$
$$+ T^{37} + T^{36} + 2T^{35} + T^{33} + T^{32})(X^2 + Y^2) + (T^{104} + 2T^{103} + T^{102}$$
$$+ T^{101} + 2T^{99} + T^{98} + 2T^{97} + 2T^{96} + T^{95} + T^{94} + 2T^{93} + 2T^{92} + 2T^{91}$$
$$+ T^{89} + 2T^{88} + 2T^{87} + 2T^{86} + 2T^{50} + T^{49} + 2T^{48} + 2T^{47} + T^{45} + 2T^{44}$$

$$+ T^{43} + T^{42} + 2T^{41} + 2T^{40} + T^{39} + T^{38} + T^{37} + 2T^{35} + T^{34}$$
$$+ T^{33} + T^{32})XY$$

A.2 Computation of the Coefficients of ρ_a

The coefficients of ρ_a, $a \in \mathbf{A}$, can be determined by using the recurrence relation (5.26). Note that this formula requires division in $\mathbf{A}$. Instead of directly using(5.26), we present an alternative recurrence relation that only requires additions and multiplications in $\mathbb{F}_q$. For an integer $k \geq 1$, define

$$\begin{aligned} f_{0,k} &= T^k, \\ f_{i,k} &= \frac{f_{i-1,k}^q - f_{i-1,k}}{T^{q^i} - T}, \qquad i = 1, 2, \ldots, k-1, \\ f_{k,k} &= 1. \end{aligned}$$

Lemma A.2.1. *Let $a \in \mathbf{A}^+$ and β_i be the coefficients of $\rho_a = \sum_{i=0}^m \beta_i(a)\tau^i$, as defined in* (5.26). *If $a = \sum_{k=0}^m a_k T^k$, then*

$$\beta_i = \sum_{k=i}^{m} a_k f_{i,k}, \qquad \text{for } i = 0, 1, \ldots, m, \tag{A.1}$$

with $\beta_0 = a$ and $\beta_m = 1$.

Proof. We use induction on i. For $i = 0$, we have

$$\beta_0 = a = \sum_{k=0}^{m} a_k T^k = \sum_{k=0}^{m} a_k f_{0,k}.$$

Suppose the lemma holds for i. Then

$$\beta_{i+1} = \frac{\beta_i^q - \beta_i}{T^{q^{i+1}} - T} = \sum_{k=i}^{m} a_k \frac{f_{i,k}^q - f_{i,k}}{T^{q^{i+1}} - T} = \sum_{k=i+1}^{m} a_k f_{i+1,k}.$$

The last equality follows since the i-th term is 0 as $f_{i,i} = 1$. This completes the proof. □

Lemma A.2.2. *For all integers i and k such that $2 \leq k \leq m$ and $0 \leq i \leq k-1$, we have*

$$f_{i+1,k} - T^{q^{i+1}} f_{i+1,k-1} = f_{i,k-1}.$$

Proof. (Induction on i.) For $i = 0$ and for all k with $2 \leq k \leq m$, we have

$$\begin{aligned} f_{1,k} - T^q f_{1,k-1} &= \frac{f_{0,k}^q - f_{0,k}}{T^q - T} - T^q \ \frac{f_{0,k-1}^q - f_{0,k-1}}{T^q - T} \\ &= \frac{(T^{qk} - T^k) - (T^{q+(k-1)q} - T^{q+k-1})}{T^q - T} \\ &= \frac{T^{qk} - T^k - T^{qk} + T^{q+k-1})}{T^q - T} \\ &= \frac{T^{q+k-1} - T^k}{T^q - T} = T^{k-1} \ \frac{T^q - T}{T^q - T} \\ &= T^{k-1} = f_{0,k-1}. \end{aligned}$$

Suppose the lemma holds for i. Then

$$f_{i+1,k} - T^{q^{i+1}} f_{i+1,k-1} = \frac{f_{i,k}^q - f_{i,k}}{T^{q^{i+1}} - T} - T^{q^{i+1}} \ \frac{f_{i,k-1}^q - f_{i,k-1}}{T^{q^{i+1}} - T}. \tag{A.2}$$

By induction hypothesis, $f_{i,k} = T^{q^i} f_{i,k-1} + f_{i-1,k-1}$ for all k with $2 \leq k \leq m$. So $f_{i,k}^q = T^{q^{i+1}} f_{i,k-1}^q + f_{i-1,k-1}^q$, and hence, (A.2) becomes

$$\begin{aligned} f_{i+1,k} - T^{q^{i+1}} f_{i+1,k-1} &= \frac{T^{q^{i+1}} f_{i,k-1}^q + f_{i-1,k-1}^q - (T^{q^i} f_{i,k-1} + f_{i-1,k-1}) - T^{q^{i+1}} \ (f_{i,k-1}^q - f_{i,k-1})}{T^{q^{i+1}} - T} \\ &= \frac{\overbrace{f_{i-1,k-1}^q - f_{i-1,k-1}}^{=(T^{q^i}-T)f_{i,k-1} \text{ by definition of } f_{i,k}} + (T^{q^{i+1}} - T^{q^i}) f_{i,k-1}}{T^{q^{i+1}} - T} \\ &= \frac{(T^{q^{i+1}} - T) f_{i,k-1}}{T^{q^{i+1}} - T} = f_{i,k-1}. \end{aligned}$$

This completes the inductive step, and the result follows. □

Lemma A.2.3. *For integers $1 \leq k \leq m$ and $0 \leq i \leq k-1$, the $f_{i,k}$ satisfy the recurrence relation*

$$f_{i+1,k+1} = f_{i,k} + T^{q^{i+1}} f_{i+1,k}$$

with $f_{0,k} = T^k$ and $f_{k,k} = 1$.

Proof. This follows immediately from the previous lemma. □

Lemma A.2.4. $\deg_T(f_{i,k}) = q^i(k-i)$.

Proof. We use induction on i. For $i = 0$,

$$\deg_T(f_{0,k}) = \deg_T(T^k) = k = q^0(k-0)$$

for all k with $1 \leq k \leq m$. From the definition of $f_{i,k}$, we have

$$\deg_T(f_{i,k}) = q \deg_T(f_{i-1,k}) - q^i.$$

By induction hypothesis,

$$\deg_T(f_{i,k}) = q(q^{i-1}(k-i+1)) - q^i = q^i(k-i).$$

The result follows. □

Remark A.2.5. It is clear that the $f_{i,k}$ are completely independent of any $a \in \mathbf{A}$, and these polynomials only depend on q. We can see from Lemma A.2.3 that the $f_{i,k}$ can be obtained by applying additions, the q-th power map, and shifts.

Suppose we require the β_i for a polynomial $a \in \mathbf{A}^+$, with $\deg_T(a) = m$. Then the number of additions needed to obtain $f_{i,k}$ is

$$\sum_{k=1}^{m}\sum_{i=0}^{k-1} q^i(k-i) \leq m\sum_{k=1}^{m}\sum_{i=0}^{k-1} q^i = m\sum_{k=1}^{m}\frac{q^k-1}{q-1} < \frac{m}{q-1}\sum_{k=1}^{m} q^k = \frac{m}{q-1}\,\frac{q^{m+1}-q}{q-1}. \quad \text{(A.3)}$$

Now, each $a_k f_{i,k}$ in (A.1) for $i \leq k \leq m-1$ requires at most $q^i(k-i)$ multiplications in $\mathbb{F}_q$. So the total number of $\mathbb{F}_q$-multiplications for each β_i is at most

$$\sum_{k=i}^{m} q^i(k-i) \leq \sum_{k=i}^{m} q^{m-1} = (m-i)q^{m-1} < mq^{m-1}$$

since $q^i(k-i) \leq q^{m-1}$ for $i \leq k \leq m-1$. Given that $\beta_0 = a$ and $\beta_m = 1$, we still need to determine the remaining β_i for $i = 1, 2, \ldots, m-1$. So for $a \in \mathbf{A}^+$ of degree m, we require fewer than m^2q^{m-1} multiplications in $\mathbb{F}_q$ to obtain the β_i. Note that m^2q^{m-1} grows faster than (A.3) as $m \longrightarrow \infty$.

A.3 Another Way of Computing Drinfeld Modular Polynomials

We propose another approach for computing Drinfeld modular polynomials. This method also uses s-expansions and is similar to the algorithm for classical modular polynomials briefly described in [Elk98, Section 3] (cf. [Eng09]).

Let Y in $\Phi_\ell(X,Y)$ be the invariant $j = j(z)$. Note that all $|\ell|+1$ roots of $\Phi_\ell(X,j) = 0$ are known. These are the invariants $j_i = j \circ \alpha_i$, where $\alpha_i \in S_\ell$, $1 \leq i \leq |\ell|+1$, and S_ℓ is the system of representatives of Δ_ℓ^* (see (5.41)). Equivalently, these invariants are

$$j\left(\frac{z+a}{\ell}\right) \quad \text{and} \quad j(\ell z)$$

for $a \in \mathbf{A}$ with $\deg_T(a) < \deg_T(\ell)$ and $\gcd(a,\ell) = 1$. Let all the $j\left(\frac{z+a}{\ell}\right)$ be the "first" $|\ell|$ roots of $\Phi_\ell(X,j)$ and let the remaining root be $j_{|\ell|+1} = j(\ell z)$. Recall that $\Phi_\ell(X,j)$ is a symmetric polynomial, so it can be written as a polynomial in terms of elementary symmetric functions of the roots j_i. Write

$$\Phi_\ell(X,j) = \Phi_\ell(X) = \prod_{i=1}^{|\ell|+1}(X - j_i) = X^{|\ell|+1} + \sum_{k=1}^{|\ell|+1} e_k X^{|\ell|+1-k},$$

where the coefficients of $\Phi_\ell(X,j)$ are

$$e_k := e_k(j_1,\ldots,j_{|\ell|+1}) = \begin{cases} 1, & \text{if } k = 0 \\ \sum_{1 \leq h_1 < \ldots < h_k \leq |\ell|+1} \prod_{m=1}^{k} j_{h_m}, & \text{if } 1 \leq k \leq |\ell|+1 \\ 0, & \text{if } k > |\ell|+1. \end{cases}$$

We know from Corollary 5.5.6 that these coefficients are elements of $\mathbf{A}[j]$. We have also seen in Section 5.5 that given the s-expansion of j (with some precision) we can determine the s-expansions of all the j_i, and hence the s-expansions of the power sums

$$p_k := p_k(j_1,\ldots,j_{|\ell|+1}) = \sum_{i=0}^{|\ell|+1} j_i^k.$$

By using the Newton identities (see [Zip93, Proposition 74])

$$p_k - e_1 p_{k-1} + e_2 p_{k-2} + \cdots + (-1)^k k e_k = 0, \text{ if } k \leq |\ell|+1$$

$$p_k - e_1 p_{k-1} + e_2 p_{k-2} + \cdots + (-1)^k e_{|\ell|+1} p_{k-(|\ell|+1)} = 0, \text{ if } k \geq |\ell|+1,$$

one can write the coefficients e_k, for $k \leq |\ell| + 1$, as polynomials in the power sums p_i as follows:

$$\begin{aligned} e_0 &= 1 \\ e_1 &= p_1 \\ e_2 &= \frac{1}{2}\left(e_1 p_1 - p_2\right) \\ &\vdots \\ e_{|\ell|+1} &= \frac{(-1)^{|\ell|+1}}{|\ell|+1}\left(e_1 p_{|\ell|} - e_2 p_{|\ell|-1} + \cdots - p_{|\ell|+1}\right). \end{aligned} \tag{A.4}$$

Note that we did not actually implement this algorithm. An exact complexity analysis goes beyond this thesis and is subject to future work.

A.4 Miscellaneous

Proof of Lemma 8.2.10:

By definition of λ, see (8.13), it follows that

$$\begin{aligned} \lambda &\leq \frac{\log_q((N+2)q + N + 1) - 1}{2} \\ 2\lambda + 1 &\leq \log_q((N+2)q + N + 1) \\ q^{2\lambda+1} &\leq (N+2)q + N + 1 \leq (N+2)(q+1) \leq (3N)(3q) = 9Nq \\ q^{2\lambda} &< 9N \\ q^{\lambda} &< 3\sqrt{N}. \end{aligned} \tag{A.5}$$

Appendix B

Some Drinfeld Isogeny Volcanoes

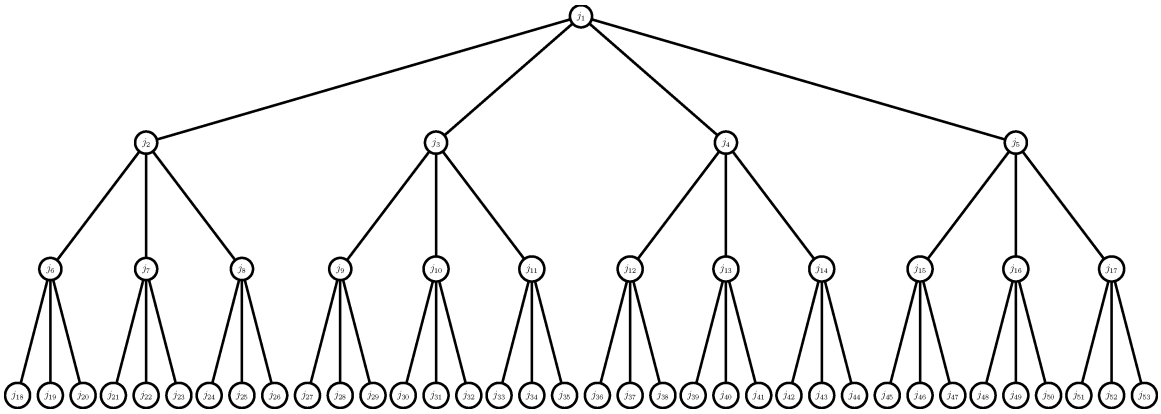


Figure B.1: T-isogeny volcano containing $j = 2T^7+T^6+2T^5+T^4+2T^3+2T$ over $\mathbb{F}_\mathfrak{p} = \mathbb{F}_3[T]/\mathfrak{p}$ with $\mathfrak{p} = (T^{11} + 2T^2 + 1)$

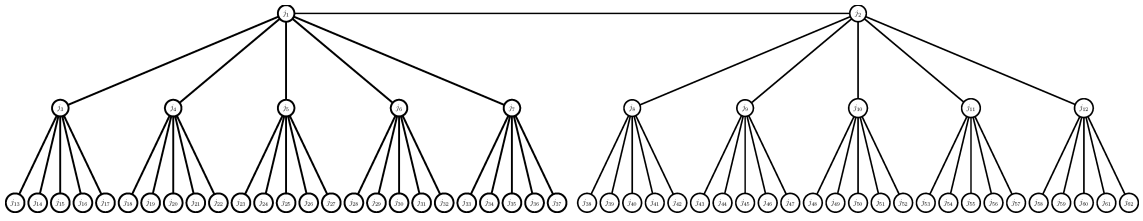


Figure B.2: T-isogeny volcano containing $j = 3T^5 + 4T^4 + T^2 + 2T$ over $\mathbb{F}_\mathfrak{p} = \mathbb{F}_5[T]/\mathfrak{p}$ with $\mathfrak{p} = (T^7 + 3T + 3)$

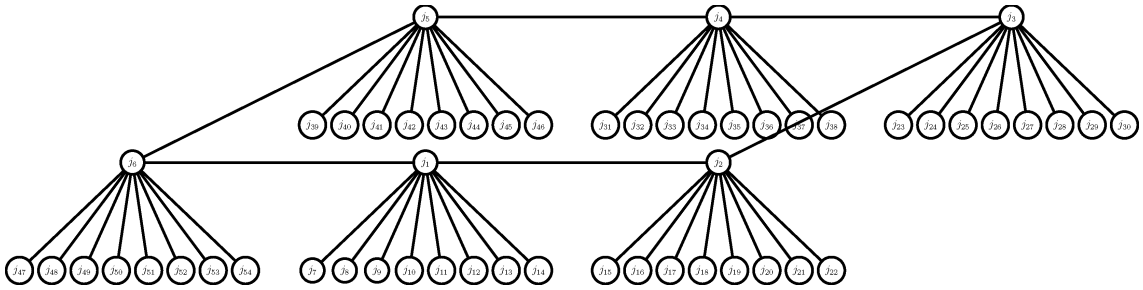


Figure B.3: (T^2+T+2)-isogeny volcano containing $j = T^9+2T^8+T^7+T^6+2T^5+T^4+2T^3$ over $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_3[T]/\mathfrak{p}$ with $\mathfrak{p} = (T^{10} + 2T^6 + +2T^5 + 2T^4 + T + 2)$