UNIVERSITY OF Southampton

Faculty of Social Sciences
School of Mathematical Sciences

The canonical representation of the Drinfeld curve

Author:
Lucas Laurent
Student ID: 31955908

Supervisor:
Dr Bernhard Köck

Thesis for the degree of
Master of Philosophy

September 2021

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF SOCIAL SCIENCES

SCHOOL OF MATHEMATICAL SCIENCES

Master of Philosophy

The canonical representation of the Drinfeld curve

by Lucas Laurent

We compute the decomposition of the canonical representation arising from the action of the group $SL_2(\mathbb{F}_q)$ on the Drinfeld curve over the algebraic closure of the finite field $\mathbb{F}_q$ for q a prime power. We first solve the problem for $q = p$ a prime number, where methods from a recent paper by Bleher, Chinburg, and Kontogeorgis apply because $SL_2(\mathbb{F}_p)$ has cyclic Sylow p-subgroups. The computations simplify drastically compared to the general case treated in the paper because in addition of being cyclic, the Sylow p-subgroups have order p and their normaliser is p-hypo-elementary. This allows us to use the Green correspondence in the case of trivial intersection. Secondly, we solve the problem for q a general prime power, by computing a concrete basis for the space of global holomorphic differentials and studying the action of $SL_2(\mathbb{F}_q)$ on it.

Contents

Declaration of authorship

I declare that this thesis and the work presented in it is my own and has been generated by me as the result of my own original research.

Title of thesis: The canonical representation of the Drinfeld curve

I confirm that:

1. This work was done wholly or mainly while in candidature for a research degree at this University;
2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
3. Where I have consulted the published work of others, this is always clearly attributed;
4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
5. I have acknowledged all main sources of help;
6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
7. Parts of Chapter 1 and Chapter 3 have been published as [LK21].

Signature:

Date:

Acknowledgements

I would like to first thank my supervisor Bernhard Köck for suggesting this problem, which arose from a discussion with Adriano Marmora. His patience, support, and guidance have always been extremely helpful, as well as the great care with which he reviewed my work. I would also like to thank Peter Kropholler for his continued interest in our research.

Introduction

The action of a finite group of automorphisms G of a smooth projective curve C over an algebraically closed field $\mathbb{F}$ induces a linear action of G on the $\mathbb{F}$-vector space of holomorphic differentials of C, denoted by $H^0\big(C, \Omega_C\big)$. This space hence becomes an $\mathbb{F}[G]$-module, which is known to have dimension $g(C)$ the genus of the curve C, a well-known and fundamental invariant of smooth projective curves. Thus, it is natural to try and find the decomposition of $H^0\big(C, \Omega_C\big)$ as a direct sum of indecomposable $\mathbb{F}[G]$-modules.

This problem has first been introduced by Hecke in 1928 [Hec28], and it has been solved in 1934 by Chevalley and Weil [CWH34], assuming that the characteristic of $\mathbb{F}$ does not divide the order of G. If we assume that $\mathbb{F}$ has characteristic p dividing the order of G, then we are in the case of modular representation theory, and this problem becomes notoriously hard because the tools of classical representation theory do not apply anymore. For example, Maschke's theorem does not hold, i.e. there exist some indecomposable $\mathbb{F}[G]$-modules which are not simple. However, some progress has been made. In 1986, Nakajima [Nak86] and Kani [Kan86] independently found the decomposition for an arbitrary finite group of automorphisms G of C, in the case where the cover $C \longrightarrow C/G$ has only tame ramification. Most of the theorems leading to Kani's and Nakajima's result have been generalised by Köck [Kö04] to the so-called weakly ramified case, the simplest but most frequent form of wild ramification.
However, the study of the decomposition in the case of arbitrary ramification had seen some progress earlier than the solution for tame ramification. Indeed, Valentini and Madan [VM81] solved the problem for G a cyclic p-group in 1981. In 2013, Karanikolopoulos alongside with Kontogeorgis then extended Valentini's and Madan's result to a general cyclic group G [KK13]. Finally, Bleher, Chinburg, and Kontogeorgis [BCK20] gave an algorithm to solve the problem in 2020 in the case where G admits a non-trivial cyclic Sylow p-subgroup, which is a necessary and sufficient condition for G to admit finitely many isomorphism classes of indecomposable representations [Hig54].

In this thesis, we will find the decomposition of $H^0\big(C,\Omega_C\big)$ as an $\mathbb{F}[G]$-module for $G = SL_2\big(\mathbb{F}_q\big)$, $q = p^r$ for some $r \in \mathbb{N}_{\geq 1}$, $\mathbb{F} = \overline{\mathbb{F}_q}$ a fixed algebraic closure of $\mathbb{F}_q$, and C the Drinfeld curve together with the action of G as presented in Subsection 1.2.2. The decomposition in the general case is stated in the following theorem.

Theorem 0.1. *For $0 \leq j \leq q-2$, let V^j be the $(j+1)$-dimensional vector space over $\mathbb{F}$*

$$V^j := \mathbb{F}x^j \oplus \mathbb{F}x^{j-1}y \oplus \cdots \oplus \mathbb{F}xy^{j-1} \oplus \mathbb{F}y^j,$$

equipped with the $\mathbb{F}$-linear action of G where $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G$ acts on $x^{j-i}y^i$ by

$$g \cdot x^{j-i}y^i = (\alpha x + \gamma y)^{j-i}(\beta x + \delta y)^i.$$

Then V^j is an indecomposable $\mathbb{F}[G]$-module, and the following isomorphism of $\mathbb{F}[G]$-modules holds.

$$H^0\big(C,\Omega_C\big) \cong \bigoplus_{j=0}^{q-2} V^j$$

Note that because the Sylow p-subgroups of G are isomorphic to the direct product of r copies of C_p, we can apply the results from [BCK20] if and only if $r = 1$. In that paper, the three authors give a formula for the decomposition of $H^0\big(C,\Omega_C\big)_H$ where $H = P \rtimes C'$ is a p-hypo-elementary subgroup of G, i.e. P is a cyclic p-subgroup and C' is a cyclic p'-subgroup. Then they use the fact that the $\mathbb{F}[G]$-module structure of $H^0\big(C,\Omega_C\big)$ is completely determined by its $\mathbb{F}[H]$-module structure when restricted to the p-hypo-elementary subgroups of G. This follows for example from Conlon's induction theorem [CR81, Corollary 80.51]. In conclusion, this leads to a proof of Theorem 0.1 in the case $r = 1$. We will detail this proof in Chapter 2.
In order to prove Theorem 0.1 for an arbitrary $r \geq 1$, we use the following very different approach, which is presented in Chapter 3. First, we compute a concrete basis for the $\mathbb{F}$-vector space $H^0\big(C,\Omega_C\big)$ in Section 3.1. Then from the action of G on this basis, we find a decomposition of the $\mathbb{F}[G]$-module $H^0\big(C,\Omega_C\big)$ in Section 3.2, which is inspired from the case $r = 1$. In the same section, we finally prove that each summand is indecomposable as $\mathbb{F}[G]$-module.

Chapter 1

Background on curves and setup of the problem

1.1 Background on curves

In this section, we will present some of the background needed to understand what the canonical representation of a curve is, and see what challenges arise in computing its decomposition.

1.1.1 Algebraic curves

There are two traditional ways to define algebraic curves: one is using the classical viewpoint, and the other one is using scheme theory. While being extremely powerful, we will not adopt the scheme-theoretic viewpoint in this thesis, because it is too general for our purpose. For the rest of this section, we will let k denote an algebraically closed field. In particular, by an affine or projective variety, we mean a subset of $\mathbb{A}^n(k)$ or $\mathbb{P}^n(k)$ defined by polynomials, which are homogeneous in the projective case. When we refer to a topology, we mean the Zariski topology.

We assume that the reader has some basic knowledge about the theory of algebraic curves, however we recall some basic definitions and results. The following is an adaptation from [Ful69], [Har97], and [Tai14, Chapter 2].

Definition 1.1. A smooth projective curve C is a smooth projective variety of dimension 1 over k.

Remark 1.2. Because all the curves in this thesis are smooth, and nearly all curves are projective, we will refer to a smooth projective curve simply by *a curve*. If the curve is affine, we will clearly state it. It is well-known that a projective curve can

be covered by a union of open subsets which are affine curves [Ful69, Proposition 6.3.3].

Definition 1.3. A morphism $f : C \longrightarrow C'$ of affine curves is the restriction to C of a map of the following form, where f_1 and f_2 are elements of $k[x, y]$.

$$\begin{aligned} \mathbb{A}^2(k) &\longrightarrow \mathbb{A}^2(k) \\ (x, y) &\longmapsto \big(f_1(x, y), f_2(x, y)\big) \end{aligned}$$

If C and C' are projective curves, then a map $f : C \longrightarrow C'$ is a morphism if and only if $C = \cup_{i\in I} C_i$ and $C' = \cup_{j\in J} C'_j$ for finite sets I and J and open subsets $C_i, {C'}_j$ which are affine curves, such that for all $i \in I$, $f(C_i) \subseteq {C'}_j$ for some $j \in J$ and $f|_{C_i}$ is a morphism of affine curves.

Definition 1.4. A rational function on a curve C is any morphism $C \longrightarrow \mathbb{P}^1(k)$ other than the constant morphism mapping all points of C to the point at infinity $[1 : 0]$. Such functions form a field, called the *function field of* C and denoted by $k(C)$. Suppose that $f : C \longrightarrow C'$ is a morphism of curves. We define the degree of f to be

$$\deg f = \Big[k(C) : f^\circ\big(k(C')\big)\Big],$$

where f° denotes precomposition by the morphism f.

Next, we define regularity and the local ring at a point.

Definition/Proposition 1.5. Let C be a curve, P be a point of C, and $f \in k(C)$. We say that f is *regular at* P if and only if $f(P) \neq [1 : 0]$. The set of regular functions at P is denoted by $\mathcal{O}_{C,P}$ or $\mathcal{O}_P$, and is a local ring with maximal ideal $\mathfrak{m}_P = \{f \in \mathcal{O}_P \mid f(P) = 0\}$. It is called the *local ring of* C *at* P, and in addition to being a local ring, it is a discrete valuation ring [Har97, Theorems I.5.1, I.6.2A] whose valuation is denoted by ord_P. A generator of $\mathfrak{m}_P$ is called a *local parameter of* C *at* P. For an open subset $\emptyset \neq U \subseteq C$, f is *regular on* U if and only if f is regular at all points of U. A *regular function on* C is an element of $k(C)$ which is regular on C.

Let us now state the definition of a finite group action on a curve.

Definition 1.6. Let C be a curve, and Γ be a finite group. We say that Γ acts on C if and only if each element of Γ induces an automorphism of the curve C such that the composition of resulting automorphisms is compatible with the multiplication law in Γ. From this perspective, a group action of Γ on C is simply a group homomorphism $\Gamma \longrightarrow \mathrm{Aut}(C)$.

Remark 1.7. In this thesis, actions on curves will be left actions.

An action of a finite group Γ on a curve C gives rise to an action of the stabiliser Γ_P on the local ring $\mathcal{O}_{C,P}$ for any point P of C, given by

$$\gamma \cdot f(Q) = f\big(\gamma^{-1} \cdot Q\big),$$

for all $\gamma \in \Gamma_P$ and all $Q \in C$.

We can now define the lower ramification subgroups as adapted from [BCK20, Section 4].

Definition 1.8. Let $i \geq -1$ and P be a point of C. The *i-th lower ramification group at P* $\Gamma_{i,P}$ is defined to be the subgroup of the stabiliser of P, Γ_P, which acts trivially on $\mathcal{O}_{C,P}/\mathfrak{m}_P^{i+1}$. We call $\Gamma_{0,P}$ *the inertia subgroup at P*, and it is equal to Γ_P.

1.1.2 Differentials on a curve

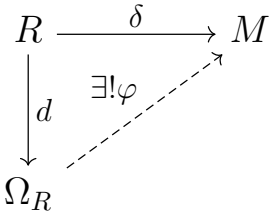
We will now define the concept of differentials on a curve C. We will start with an abstract definition involving a universal property, to then construct a concrete example satisfying the property. This is an adaptation of [Ful69, Section 8.4].

We first define derivations.

Definition 1.9. Let R be a commutative ring containing k and M be an R-module. A derivation of R into M over k is a k-linear map $d : R \longrightarrow M$ such that for all $x, y \in R$ the Leibniz formula is satisfied, i.e. $d(xy) = xd(y) + yd(x)$.

Let us now define the module of differentials using a universal property.

Definition 1.10. Let R be a commutative ring containing k. The module of differentials Ω_R of R over k is any R-module alongside with a derivation $d : R \longrightarrow \Omega_R$ of R into Ω_R over k such that the following universal property is satisfied.
For all R-modules M with a derivation $\delta : R \longrightarrow M$ of R into M over k, there exists a unique R-module homomorphism $\varphi : \Omega_R \longrightarrow M$ such that $\delta = \varphi \circ d$.



Remark 1.11. Because such an R-module homomorphism is unique, any two modules of differentials of R over k are uniquely isomorphic as R-modules. Hence, the notion of module of differentials of R over k is well-defined up to unique isomorphism.

Because this definition is quite abstract, we will now gain insight by constructing a module and a derivation which satisfy the universal property.

Proposition 1.12. *For any commutative ring R containing k, the module of differentials Ω_R of R over k exists.*

Proof. Let R be a commutative ring containing k, and for each $x \in R$, let $[x]$ be a symbol. Let F be the free R-module on these symbols. Define N to be the R-submodule of F generated by elements of the form $[x+y]-[x]-[y]$, $[\alpha x]-\alpha[x]$, and $[xy]-x[y]-y[x]$ for all $x, y \in R$ and all $\alpha \in k$. Then, let $\Lambda := F/N$ and $d : R \longrightarrow \Lambda$ mapping $x \in R$ to $[x]+N \in \Lambda$. By definition of N, d is a derivation of R into Λ over k. Suppose that M is another module of differentials of R over k with a derivation $\delta : R \longrightarrow M$ of R into M over k. Then there exists a unique R-module homomorphism $\varphi : \Lambda \longrightarrow M$ such that $\delta = \varphi \circ d$, which is given by $\varphi\big([x]+N\big) = \delta(x)$, and which is well-defined by definition of N and because δ is a derivation of R into M over k.
This allows us to define $\Omega_R := \Lambda$, with $d : R \longrightarrow \Omega_R$ mapping $x \in R$ to $[x]+N$ as the module of differentials of R over k. □

In this thesis, we are interested in the module of differentials obtained from setting $R = k(C)$.

Now that we have defined the module of differentials $\Omega_{k(C)}$ of $k(C)$ over k, the next proposition [Sti09, Proposition 1.5.9] will help us defining the notion of regularity and pullback of a differential.

Proposition 1.13. *The module of differentials $\Omega_{k(C)}$ is a 1-dimensional $k(C)$-vector space. If t is a local parameter at any point of C, then $\Omega_{k(C)} = k(C)dt$, i.e. dt is a basis element of $\Omega_{k(C)}$.*

Let us now define the notion of regularity of a differential.

Definition 1.14. Let $\omega \in \Omega_{k(C)}$, P be a point of C, and t be a local parameter at P. Then by Proposition 1.13, there exists a unique $f \in k(C)$ such that $\omega = f dt$. We say that ω *is regular at* P if and only if f is a regular function at P. For an open subset $\emptyset \neq U \subseteq C$, we say that ω *is regular on* U if and only if f is regular at all points of U. A *regular (or holomorphic) differential on* C is an element of $\Omega_{k(C)}$ which is regular on C, and we denote them by $H^0\big(C, \Omega_C\big)$.

Let us define the pullback of a differential.

Definition 1.15. Let $\varphi : C \longrightarrow C'$ be a morphism of curves, and let $\omega = f dt$ be an element of $\Omega_{k(C')}$. We define the *pullback of* ω *along the morphism* φ to be $\varphi^*\omega := (f \circ \varphi) d(f \circ \varphi) \in \Omega_{k(C)}$.

We observe that $H^0\big(C, \Omega_C\big)$ is a k-vector space, and it carries a consequent amount of geometric information about the curve C. In particular, a fundamental invariant of the curve C, its genus, is defined in the following way [Ful69, Proposition 8.2.3].

Definition/Proposition 1.16. The $k(C)$-vector space $H^0\big(C, \Omega_C\big)$ has finite dimension as a k-vector space, and this dimension is called *the genus of* C. We denote it by $g(C)$.

Remark 1.17. In the case where $k = \mathbb{C}$, a curve is also a compact Riemann surface, which already has a notion of topological genus, i.e. half the dimension of the first homology group over $\mathbb{Z}$. It can be shown that the two notions of genus agree, see for example [Hal15, Sections 5 and 6].

1.1.3 Divisors on a curve and ramification

Let us now introduce the concept of ramification of a morphism between curves. In order to make the notion of ramification simpler, we will use divisors, as found in [Har97, Section II.6]. From this, we will derive a much simpler equation for the ramification index at a point when the morphism is the quotient by a finite group action.

Definition 1.18. A divisor on a curve C is a formal sum $\sum_{P \in C} n_P P$ for integers n_P such that only finitely many of them are non-zero. In other words, it is an element of the free abelian group on the set C, which we denote by $\operatorname{Div} C$. We get a group homomorphism $\deg : \operatorname{Div} C \longrightarrow \mathbb{Z}$ by mapping $\sum_{P \in C} n_P P$ to $\sum_{P \in C} n_P$.

Let us define the ramification index at a point for a morphism of curves $f : C \longrightarrow C'$. Recall that $\mathcal{O}_{C,P}$ and $\mathcal{O}_{C',Q}$ are discrete valuation rings by Definition/Proposition 1.5.

Definition 1.19. Let $P \in C$ and $Q \in C'$ such that $f(P) = Q$. Furthermore, let $t \in \mathcal{O}_{C',Q}$ be a generator of $\mathfrak{m}_{C',Q}$ (a local parameter at Q), and ord_P be the discrete valuation on the ring $\mathcal{O}_{C,P}$. Then precomposing with the morphism f gives a ring homomorphism $f^{\#} : \mathcal{O}_{C',Q} \longrightarrow \mathcal{O}_{C,P}$. The ramification index of f at P is defined to be $\operatorname{ord}_P\big(f^{\#}(t)\big)$.

Remark 1.20. The ramification index does not depend on the choice of t because any two local parameters at Q differ by a unit.

Let us now define the different types of ramification of the morphism f at a point $P \in C$.

Definition 1.21. Let $P \in C$. If $e_P = 1$, we say that f is unramified at P, and if $e_P > 1$, we say that f is ramified at P. In the latter case, if $\operatorname{char} k$ is 0 or p and p does not divide e_P, we say that the ramification of f at P is *tame*. If $\operatorname{char} k = p$ and p divides e_P, we say that the ramification of f at P is *wild*.

Now, we define the pullback of a divisor by a morphism, which will help us finding a simpler way to compute ramification indices in the case of a quotient by a finite group action.

Definition 1.22. Let Q be a point of C' seen as an element of $\operatorname{Div} C'$, and $t \in \mathcal{O}_{C',Q}$ be a local parameter of C' at Q. We define

$$f^*Q := \sum_{P \in C, f(P)=Q} \operatorname{ord}_P\big(f^\#(t)\big) P.$$

Extending by $\mathbb{Z}$-linearity, we obtain a group homomorphism $f^* : \operatorname{Div} C' \longrightarrow \operatorname{Div} C$.

Let us now state a useful proposition, which is a reformulation of [Har97, Propositions II.6.8, II.6.9].

Proposition 1.23. *For all $D' \in \operatorname{Div} C'$, the following formula holds.*

$$\deg f^*D' = \deg f \deg D'$$

Now, let Γ be a finite group acting on the curve C as in Definition 1.6. Because C is smooth and projective and because Γ is finite, we can consider the quotient of C/Γ, which is also a smooth projective curve [Sho94, Example 2.1.7.8]. We obtain a morphism of curves

$$\pi : C \longrightarrow C/\Gamma,$$

for which the computation of the ramification index at a point of C is much simpler, as presented in the next proposition. In particular, π is a *Galois cover of curves*, which means that $k(C)/\pi^\circ\big(k(C/\Gamma)\big)$ is a Galois extension of Galois group Γ.

Proposition 1.24. *Let P be a point of C. Then $e_P = |\Gamma_P|$, where Γ_P is the stabiliser of P in Γ.*

Proof. Let $Q = \pi(P)$. By Proposition 1.23, $\deg \pi^*Q = \deg \pi \deg Q$. By definition, we know that $\deg \pi = |\Gamma|$, and also $\deg Q = 1$. Therefore, $\deg \pi^*Q = |\Gamma|$. We compute that $\pi^*Q = \sum_{R \in C, \pi(R)=Q} e_R R$, and $\{R \in C \mid \pi(R) = Q\} = \Gamma \cdot P$. Now, for any $R \in \Gamma \cdot P$, $e_R = e_P$ because $\mathcal{O}_{C,R} \cong \mathcal{O}_{C,P}$ as discrete valuation rings. We obtain that $\pi^*Q = e_P \sum_{R \in \Gamma \cdot P} R$, so by taking degrees we get $e_P |\Gamma \cdot P| = |\Gamma|$ or equivalently $e_P = \frac{|\Gamma|}{|\Gamma \cdot P|} = |\Gamma_P|$, where the last step comes from the orbit-stabiliser theorem. □

This proposition allows us to compute ramification indices easily in the case of a quotient by a finite group action. We will use this in Subsection 1.2.3.

1.2 Setup of the problem

In this section, we will present the problem in detail. Let us recall that p is a prime number, $q = p^r$ for some $r \in \mathbb{N}_{\geq 1}$, $G = SL_2(\mathbb{F}_q)$, and $\mathbb{F} = \overline{\mathbb{F}_q}$ a fixed algebraic closure of $\mathbb{F}_q$. First, we will introduce a few important facts about the group G, continue with the Drinfeld curves, and finally compute their quotients under the action of G and some of its subgroups.

1.2.1 Some facts about the group $SL_2(\mathbb{F}_q)$

Before introducing the Drinfeld curves, we will gather a few important facts about the group G here. This will allow us to detail the action of G on the curves in the next subsection. All facts can be found in [Bon12, Section 1.1].

Recall that G is the group of 2×2 matrices with entries in the finite field $\mathbb{F}_q$ of determinant 1, so it is a subgroup of $GL_2(\mathbb{F}_q)$. First, by counting the number of ordered pairs of linearly independent 2×1 columns in $\mathbb{F}_q$, we know that the order of $GL_2(\mathbb{F}_q)$ is $(q^2-1)(q^2-q)$. Then G is the kernel of the surjective determinant homomorphism $GL_2(\mathbb{F}_q) \to \mathbb{F}_q^\times$, so by the first isomorphism theorem we get

$$|G| = q(q-1)(q+1).$$

From the order of G, we know that any of its Sylow p-subgroup has order q. One of these subgroups is the subgroup of upper unitriangular matrices

$$U = \left\{ \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \middle| r \in \mathbb{F}_q \right\} \cong \mathbb{F}_q^+ \cong C_p^r$$

which, with

$$T = \left\{ \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix} \middle| \varepsilon \in \mathbb{F}_q^\times \right\} \cong \mathbb{F}_q^\times \cong C_{q-1}$$

form the subgroup

$$H = U \rtimes T = \left\{ \begin{pmatrix} \varepsilon & r \\ 0 & \varepsilon^{-1} \end{pmatrix} \middle| \varepsilon, r \in \mathbb{F}_q, \varepsilon \neq 0 \right\}$$

of upper triangular matrices. Also, we notice that U is cyclic if and only if $q = p$ is prime. In this case, the subgroup H will be of high relevance in Chapter 2, because it is p-hypo-elementary.

1.2.2 The Drinfeld curves

The Drinfeld curve C is defined as the zero locus in $\mathbb{P}^2\big(\mathbb{F}\big)$ of the homogeneous polynomial

$$XY^q - X^qY - Z^{q+1},$$

which is the compactification of the affine curve C_Z defined by $XY^q - X^qY - 1$. In this process, we add $q+1$ points at infinity defined by $XY^q - X^qY = 0$. In other words, we add the points $[x : y : 0]$ where $x, y \in \mathbb{F}_q$. As seen in [Bon12, Proposition 2.4.1], C is a smooth projective curve of degree $q+1$. This allows us to consider the $\mathbb{F}$-vector space of holomorphic differentials on C, which we will denote by $M = H^0\big(C, \Omega_C\big)$. Because C is a smooth projective curve, M has dimension $g(C)$ the genus of C by definition, which by the genus-degree formula is $g(C) = \frac{q(q-1)}{2}$ [Bon12, Subsection 2.5.1].

As explained in [Bon12], G acts on the left of the Drinfeld curve C. For an element $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G$, the corresponding curve automorphism is given by φ_g, defined as follows.

$$\begin{aligned} \varphi_g : C &\longrightarrow C \\ [x : y : z] &\longmapsto [\alpha x + \beta y : \gamma x + \delta y : z] \end{aligned}$$

For readability, let us identify each $g \in G$ with the corresponding φ_g, and write $g \cdot [x : y : z]$ for $\varphi_g\big([x : y : z]\big)$.

The following lemma gathers two useful facts about the action of G on C.

Lemma 1.25. *The action of G on the affine chart C_Z is free, and G acts transitively on the points at infinity $C \setminus C_Z \cong \mathbb{P}^1\big(\mathbb{F}_q\big)$.*

Proof. The first statement is [Bon12, Proposition 2.1.2].
For the second statement, we observe that an element of G maps a point at infinity of C to a point at infinity of C, because the action of G leaves the z-coordinate of any point invariant. In order to show that the action of G restricted to the points at infinity is transitive, we use the orbit-stabiliser theorem. The number of points at infinity is $|C \setminus C_Z| = |\mathbb{P}^1\big(\mathbb{F}_q\big)| = q+1$, and the subgroup of upper triangular matrices H, which has order $q(q-1)$, is the stabiliser of the point $[1 : 0 : 0]$. Therefore, the cardinality of the orbit of the point at infinity $[1 : 0 : 0]$ is

$$\frac{|G|}{|H|} = \frac{q(q-1)(q+1)}{q(q-1)} = q + 1 = |C \setminus C_Z|.$$

Hence, every point at infinity lies in the orbit of $[1 : 0 : 0]$ under the action of G, i.e. G acts transitively on the points at infinity. □

In Chapter 2 and 3, we will need to use some concrete local parameters on the curve C. Therefore, we compute such a parameter at each point in the next lemma.

Lemma 1.26. *Let $P = [x_0 : y_0 : z_0]$ be a point of C.*

- *If $z_0 \neq 0$, then a local parameter at P is $\frac{X}{Z} - \frac{x_0}{z_0}$.*
- *If $z_0 = 0$ and $x_0 \neq 0$, then a local parameter at P is $\frac{Z}{X}$.*
- *If $z_0 = 0$ and $y_0 \neq 0$, then a local parameter at P is $\frac{Z}{Y}$.*

Proof. Let us begin with a point $[x_0 : y_0 : z_0] \in C_Z$. Recall that C is the projective plane curve given by the equation $XY^q - X^qY - Z^{q+1}$. Then, dehomogenising with respect to Z, we introduce the variables $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ to obtain that C_Z is the affine plane curve given by the equation $xy^q - x^qy - 1$, and P becomes $(\tilde{x_0}, \tilde{y_0}) := \left(\frac{x_0}{z_0}, \frac{y_0}{z_0}\right)$. Now, from the injective regular map $C_Z \hookrightarrow \mathbb{A}^2(\mathbb{F})$, we get a surjective ring homomorphism $\mathcal{O}_{\mathbb{A}^2(\mathbb{F}),(\tilde{x_0},\tilde{y_0})} \twoheadrightarrow \mathcal{O}_{C_Z,(\tilde{x_0},\tilde{y_0})}$. Therefore, the maximal ideal $\mathfrak{m}$ of $\mathcal{O}_{C_Z,(\tilde{x_0},\tilde{y_0})}$ is generated by the image of $x - \tilde{x_0}$ and $y - \tilde{y_0}$ under this surjective map. By Nakayama's lemma, because $\mathcal{O}_{C_Z,(\tilde{x_0},\tilde{y_0})}$ is a discrete valuation ring, only one of these generators suffices, and this generator will be a local parameter for C_Z at $(\tilde{x_0}, \tilde{y_0})$. Using the equations $\tilde{x_0}\tilde{y_0}^q - \tilde{x_0}^q\tilde{y_0} = 1 = xy^q - x^qy$, we obtain that

$$\begin{aligned}(x - \tilde{x_0})\tilde{y_0}^q - \tilde{x_0}^q(y - \tilde{y_0}) &= -(\tilde{x_0}\tilde{y_0}^q - \tilde{x_0}^q\tilde{y_0}) + x\tilde{y_0}^q - \tilde{x_0}^qy \\ &= -(xy^q - x^qy) + x\tilde{y_0}^q - \tilde{x_0}^qy \\ &= y(x - \tilde{x_0})^q - x(y - \tilde{y_0})^q \in \mathfrak{m}^2\end{aligned}$$

therefore because both $\tilde{x_0}$ and $\tilde{y_0}$ are non-zero, $x - \tilde{x_0}$ and $y - \tilde{y_0}$ differ by a unit, hence both generate $\mathfrak{m}$. Without loss of generality, we choose $x - \tilde{x_0} = \frac{X}{Z} - \frac{x_0}{z_0}$.
Now, suppose that $z_0 = 0$. Then either $x_0 \neq 0$ or $y_0 \neq 0$. If $x_0 \neq 0$, we dehomogenise the equation for C with respect to X using $s = \frac{Y}{X}$ and $t = \frac{Z}{X}$, to obtain that C_X is the affine plane curve given by the equation $s^q - s - t^{q+1} = 0$, and P becomes $(s_0, t_0) := \left(\frac{y_0}{x_0}, 0\right)$. As above, we know that the maximal ideal $\mathfrak{m}$ of $\mathcal{O}_{C_X,(s_0,t_0)}$ is generated by the images of $s - s_0$ and $t - t_0$. This time, since $s_0 \in \mathbb{F}_q$ we get

$$s - s_0 = s^q - t^{q+1} - s_0 = s^q - t^{q+1} - s_0^q = (s - s_0)^q - (t - t_0)^{q+1},$$

hence $s - s_0 \in \mathfrak{m}^q \subseteq \mathfrak{m}^2$, which cannot be true for a local parameter. Thus, $t = \frac{Z}{X}$ is a local parameter at P.
Finally, if $y_0 \neq 0$ we dehomogenise the equation for C with respect to Y using $v = \frac{X}{Y}$ and $w = \frac{Z}{Y}$, to obtain that C_Y is the affine plane curve given by the

equation $v - v^q - w^{q+1} = 0$, and P becomes $(v_0, w_0) := \left(\frac{x_0}{y_0}, 0\right)$. Then, again because $v_0 \in \mathbb{F}_q$, we obtain that $v - v_0 \in \mathfrak{m}^q \subseteq \mathfrak{m}^2$, which cannot be true for a local parameter. Therefore, $w = \frac{Z}{Y}$ is a local parameter at P. □

Now, the action of G on C induces a linear action on the $\mathbb{F}$-vector space M, defined using the pullback of a holomorphic differential by an element $g \in \mathrm{Aut}(C)$. We obtain a linear representation of G over $\mathbb{F}$, or an $\mathbb{F}[G]$-module, of high importance in this thesis.

Definition 1.27. The $\mathbb{F}[G]$-module M obtained by letting G act on the $\mathbb{F}$-vector space as above is called *the canonical representation* of the curve C under the action of G.

We are interested in the way that M decomposes as the direct sum of indecomposable $\mathbb{F}[G]$-modules.

1.2.3 Some quotients by subgroups of $SL_2(\mathbb{F}_q)$

Because the Drinfeld curve C is smooth and projective and because G is finite, we can consider the quotient C/L for any subgroup $L \leq G$, which is also a smooth projective curve [Sho94, Example 2.1.7.8]. Moreover, for each $L \leq G$, we obtain a quotient morphism

$$\pi_L : C \longrightarrow C/L$$

which is a Galois cover of curves. Some quotients will be crucial in the computation of the canonical representation in the case where $q = p$ is a prime in Chapter 2. However, because these computations are interesting for their own sake, we present them here.

Lemma 1.28. *The isomorphism $C/G \cong \mathbb{P}^1(\mathbb{F})$ holds, and the ramification points of π_G are the points at infinity $C \setminus C_Z$, each of them having ramification index $q(q-1)$.*

Proof. By [Bon12, Theorem 2.2.2], we know that $C_Z/G \cong \mathbb{A}^1(\mathbb{F})$, so because G acts transitively on the points at infinity $C \setminus C_Z$ by Lemma 1.25, we get that $C/G \cong \mathbb{P}^1(\mathbb{F})$ and all the points at infinity map to the same point $\infty = [1:0]$ in $\mathbb{P}^1(\mathbb{F})$. By Proposition 1.24, a point of C is ramified if and only if it has non-trivial stabiliser, in which case the ramification index is the order of the stabiliser. Because the action of G is free on C_Z by Lemma 1.25, the only points which can be ramified are the points at infinity. It follows from the second part of Lemma 1.25 that they all have stabiliser conjugate to H, hence each point at infinity is ramified, of ramification index $|H| = q(q-1)$. □

We are interested in the quotients of C by the subgroups U and $H = U \rtimes T$, because they play a particularly important role in the next chapter when $q = p$ is a prime, where we compute the restriction of the canonical representation to H in this case.

Lemma 1.29. *The isomorphism $C/H \cong \mathbb{P}^1(\mathbb{F})$ holds, and the ramification points of π_H are the points at infinity $C \setminus C_Z$. The ramification index of $[1:0:0]$ is $q(q-1)$, and the ramification indices of all other points at infinity are $q-1$.*

Proof. We use [Bon12, Theorem 2.2.1], and we get that the morphism

$$\begin{aligned} C_Z &\longrightarrow \mathbb{A}^1(\mathbb{F}) \setminus \{0\} \\ (x,y) &\longmapsto y^{q-1} \end{aligned}$$

induces an isomorphism $C_Z/H \cong \mathbb{A}^1(\mathbb{F}) \setminus \{0\}$. Indeed, it is surjective because $\mathbb{F}$ is algebraically closed, it is constant on orbits of H because every element of $\mathbb{F}_q^\times$ is a $(q-1)$-th root of unity, and the differential is non-zero at all points of C_Z. The only remaining task is to show that if $(x_0,y_0),(x_1,y_1) \in C_Z$ such that $y_0^{q-1} = y_1^{q-1}$, then $(x_1,y_1) = h \cdot (x_0,y_0)$ for some $h \in H$, i.e. the two points lie in the same orbit under the action of H. Now, because both y_0 and y_1 are roots of the polynomial $Y^{q-1} - y_1^{q-1}$, we know that there exists some $\varepsilon \in \mathbb{F}_q^\times$ such that $y_0 = \varepsilon y_1$. Using the equation for C_Z, we know that $y_0 \neq 0$, so we can let $r = \frac{x_1 - \varepsilon x_0}{y_0}$. In order to conclude, we first need to show that $r \in \mathbb{F}_q$, i.e. $r^q = r$.

$$\begin{aligned} r^q - r &= \frac{x_1^q - \varepsilon x_0^q}{y_0^q} - \frac{x_1 - \varepsilon x_0}{y_0} \\ &= \left(\frac{x_1^q}{y_0^q} - \frac{x_1}{y_0}\right) - \varepsilon\left(\frac{x_0^q}{y_0^q} - \frac{x_0}{y_0}\right) \\ &= \frac{1}{\varepsilon}\left(\frac{x_1^q}{y_1^q} - \frac{x_1}{y_1}\right) - \varepsilon\left(\frac{x_0^q}{y_0^q} - \frac{x_0}{y_0}\right) \\ &= \frac{1}{\varepsilon y_1^{q+1}}\left(x_1^q y_1 - x_1 y_1^q\right) - \frac{\varepsilon}{y_0^{q+1}}\left(x_0^q y_0 - x_0 y_0^q\right) \\ &= \frac{\varepsilon}{y_0^{q+1}} - \frac{1}{\varepsilon y_1^{q+1}} \\ &= 0 \end{aligned}$$

The last equation holds because $y_0^{q+1} = \varepsilon^2 y_1^{q+1}$. We obtain that $h = \begin{pmatrix} \varepsilon & r \\ 0 & \varepsilon^{-1} \end{pmatrix} \in H$ and $h \cdot (x_0,y_0) = (x_1,y_1)$, which is what we wanted.
Now, H is the stabiliser of the point at infinity $[1:0:0]$, and $T \leq H$ is the stabiliser of $[0:1:0]$ inside H so because $|T| = q-1$, $[0:1:0]$ has an orbit of size

q by the orbit-stabiliser theorem. Thus, H has two orbits on the points at infinity, and $C/H \cong \mathbb{P}^1(\mathbb{F})$ where π_H maps $[1:0:0]$ to $[0:1]$ and every other point at infinity to $\infty = [1:0]$. By Proposition 1.24, we get directly that all the points at infinity are ramified, with $[1:0:0]$ still having ramification index $|H| = q(q-1)$, and all other points at infinity having ramification index $|T| = q-1$. The points at infinity are the only ones which are ramified because $H \leq G$, and G acts freely on C_Z by Lemma 1.25. □

Lemma 1.30. *The isomorphism $C/U \cong \mathbb{P}^1(\mathbb{F})$ holds, and the only ramification point of π_U is $[1:0:0]$, of ramification index q.*

Proof. We already know by [Bon12, Theorem 2.2.3] that $C_Z/U \cong \mathbb{A}^1(\mathbb{F}) \setminus \{0\}$ via the isomorphism induced by the following morphism.

$$\begin{aligned} C_Z &\longrightarrow \mathbb{A}^1(\mathbb{F}) \setminus \{0\} \\ (x,y) &\longmapsto y \end{aligned}$$

It is easy to see that U stabilises the point at infinity $[1:0:0]$. Also, because $\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \cdot [0:1:0] = [r:1:0]$, the point $[0:1:0]$ has trivial stabiliser in U, and hence by the orbit-stabiliser theorem, $[0:1:0]$ has an orbit of size $q = |U|$ under the action of U. Therefore, $C/U \cong \mathbb{P}^1(\mathbb{F})$, where π_U maps $[1:0:0]$ to $[0:1]$ and all other points at infinity to $[1:0]$. We also get by Lemma 1.25 and Proposition 1.24 that the only point of C which is ramified is $[1:0:0]$, and it has ramification index q. □

Remark 1.31. The three quotient maps π_G, π_H and π_U are wildly ramified.

Chapter 2

Solution when $q = p$ is a prime

In this chapter, we will compute the decomposition as $\mathbb{F}[G]$-module of the canonical representation M of the Drinfeld curve C when $q = p$ is a prime. In this case, $G = SL_2(\mathbb{F}_p)$, which has cyclic Sylow p-subgroups of order p. We will first compute the decomposition of M when restricted to the subgroup H of upper triangular matrices using [BCK20], and then we will use the Green correspondence to deduce the decomposition of M as a representation of G.

Remark 2.1. The paper [BCK20] requires a right action of G on the $\mathbb{F}$-vector space of holomorphic differentials. The action of G on the curve C defined in Subsection 1.2.2 is a left action, so defining the linear action of G on the space of holomorphic differentials by pulling back yields a right action. However, in order to be consistent with the notation from Theorem 0.1, we define from now on the linear action of G on the space of holomorphic differentials M by pulling back by inverses, i.e. for all $g \in G$ and all $\omega \in M$, $g \cdot \omega := \left(g^{-1}\right)^* \omega$.
For a left $\mathbb{F}[G]$-module A, we define the corresponding right $\mathbb{F}[G]$-module $\tilde{A}$ by letting G act by inverses. It is easy to see that $A = \tilde{\tilde{A}}$, and that A is indecomposable if, and only if, $\tilde{A}$ is indecomposable. Indeed, this follows from the fact that for all $g \in G$, $\left(g^{-1}\right)^{-1} = g$. Therefore, we obtain that $A \cong \oplus_{i=1}^{\ell} A_i$ is a decomposition of A as left $\mathbb{F}[G]$-module if and only if $\tilde{A} \cong \oplus_{i=1}^{\ell} \tilde{A}_i$ is a decomposition of $\tilde{A}$ as a right $\mathbb{F}[G]$-module. Thus, we can use [BCK20] with the left $\mathbb{F}[G]$-module M. From now on, $\mathbb{F}[G]$-modules are understood to be *left* $\mathbb{F}[G]$-modules.

2.1 The restriction of the canonical representation to H

In this section, we will apply the three steps of [BCK20, Remark 4.4] to compute the decomposition of the $\mathbb{F}[G]$-module obtained from the canonical representation

arising from the action of the subgroup of upper triangular matrices $H = U \rtimes T$ on the Drinfeld curve C. In other words, we will compute the decomposition of M_H as the direct sum of indecomposable $\mathbb{F}[H]$-modules. From Step 2 onwards, we will need the exact semidirect product structure for H. For this, we just need to compute

$$\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix} \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \varepsilon^2 r \\ 0 & 1 \end{pmatrix},$$

to conclude that $H = U \rtimes_\chi T$ where χ maps $\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$ to $\chi_\varepsilon \in \mathrm{Aut}(U)$, sending $\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$ to $\begin{pmatrix} 1 & \varepsilon^2 r \\ 0 & 1 \end{pmatrix}$. We denoted this map by χ because we can see it as a character $\chi : T \to \mathbb{F}$ mapping $\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$ to ε^2.

Before starting to apply [BCK20, Remark 4.4], let us first present its different steps in a simpler version adapted to our needs.
We begin by describing the isomorphism classes of indecomposable $\mathbb{F}[H]$-modules, using [BCK20, Remark 3.4].

Proposition 2.2. *Let $\zeta \in \mathbb{F}$ be a fixed primitive $(p-1)$-th root of unity, so that $\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$ generates T. For each $0 \leq a \leq p-2$, let S_a be the simple 1-dimensional $\mathbb{F}[C]$-module on which $\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$ acts as multiplication by ζ^a. We view S_a as an $\mathbb{F}[H]$-module by letting U act trivially. Moreover, for $i \in \mathbb{Z}$, let $\nu^i(a)$ be the unique representative of $2i + a \mod (p-1)$ in $\{0, 1, \ldots, p-2\}$. There are $|H| = p(p-1)$ isomorphism classes of indecomposable $\mathbb{F}[H]$-modules, and they are all uniserial. They are completely determined by their socle S_a for $0 \leq a \leq p-2$ and their $\mathbb{F}$-dimension $1 \leq b \leq p$. The corresponding $\mathbb{F}[H]$-module is denoted by $U_{a,b}$, and its ascending composition factors are the first b factors in the following list.*

$$S_a, S_{\nu^{-1}(a)}, S_{\nu^{-2}(a)}, \ldots, S_{\nu^{-(p-2)}(a)}, S_a$$

Remark 2.3. For readability, we will denote $\nu^i(0)$ by ν^i.

Let us now present [BCK20, Remark 4.4], which gives the steps in order to compute the decomposition of M_H. The first step amounts to the following definition. It defines a divisor D_j, which is completely determined by the ramification subgroups for the Galois cover of curves $\pi_U : C \longrightarrow C/U \cong \mathbb{P}^1(\mathbb{F})$ from Lemma 1.30. Recall that the only branch point is the point at infinity $[1 : 0 : 0]$, which is mapped to $[0 : 1]$.

Definition 2.4. Let $0 \leq j \leq p-1$, and recall that U is cyclic of order p. Let h be the unique jumping number in the ramification subgroups at $[1:0:0]$, i.e. h is the minimal element of $\mathbb{Z}_{\geq -1}$ such that the lower ramification subgroup U_{h+1} from Definition 1.8 is trivial. We let $D_j = s_j[0:1]$ for the integer $s_j = \left\lfloor \frac{p-1+(p-1-j)h}{p} \right\rfloor$.

We will now state a theorem explaining how to compute the decomposition of M_H from the divisors D_j. The first part and the second part of the theorem correspond respectively to Step 2 and Step 3 of [BCK20, Remark 4.4].

Theorem 2.5. *1. Let $E = C/U$ and $F = C/H$, and let F_{ram} be the points of F which ramify in the Galois cover of curves $E \longrightarrow F$, of Galois group $H/U \cong T$. For each $Q \in F_{ram}$, choose $E(Q) \in E$ lying above Q, and $C(Q) \in C$ lying above $E(Q)$. Let $T_{E(Q)}$ be the stabiliser of $E(Q)$ in E, and identify it with the maximal p'-quotient of $H_{C(Q)}$. Define the character $\theta_{C(Q)}$ as follows, where $t_{C(Q)}$ denotes a local parameter of C at $C(Q)$.*

$$\begin{aligned} \theta_{C(Q)} : H_{C(Q)} &\longrightarrow \mathcal{O}_{C,C(Q)}/\mathfrak{m}_{C(Q)} \cong \mathbb{F}^\times \\ h &\longmapsto \frac{h \cdot t_{C(Q)}}{t_{C(Q)}} \mod \left(t_{C(Q)}\right) \end{aligned}$$

Then $\theta_{C(Q)}$ factors through $T_{E(Q)}$, and let us define $\theta_{E(Q)} = \theta_{C(Q)}^p$. Again, let $0 \leq j \leq p-1$, and we define the element $\ell_{E(Q),j}$ to be the unique representative of $-\mathrm{ord}_{E(Q)}(D_j) \mod (p-1)$ in $\{0,1,\ldots,p-2\}$. Finally, for any $0 \leq j \leq p$ we let $M^{(j)}$ be the kernel of the action of $(\sigma-1)^j$ on M, where $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ generates U. Then the Brauer character of the dual of the $\mathbb{F}[H]$-module $S_{\nu^j} \otimes_{\mathbb{F}} \left(M^{(j+1)}/M^{(j)}\right)$, is equal to

$$\delta_{j,p-1}\beta_0 + \sum_{Q \in F_{ram}} \sum_{t=1}^{p-2} \frac{t}{p-1} \theta_{E(Q)}^t - \sum_{Q \in F_{ram}} \sum_{t=1}^{\ell_{E(Q),j}} \theta_{E(Q)}^{-t} + n_j \beta\big(\mathbb{F}[T]\big),$$

where

$$n_j = \frac{\deg(D_j)-1}{p-1} + \frac{1}{p-1} \sum_{Q \in F_{ram}} \left(\ell_{E(Q),j} - \frac{p-2}{2} \right),$$

δ is the usual Kronecker delta, β_0 is the trivial Brauer character, and $\beta\big(\mathbb{F}[T]\big)$ is the Brauer character of $\mathbb{F}[T]$.

2. Let $0 \leq a \leq p-2$ and $1 \leq b \leq p$. Using the notation $U_{a,b}$ from Proposition 2.2, the number $n(a,b)$ of copies of $U_{a,b}$ in the decomposition of M as a direct sum of indecomposable $\mathbb{F}[H]$-modules is as follows. We define $n_1(a,b)$

to be the number of copies of the $\mathbb{F}[T]$-module $S_{\nu^{-(b-1)}(a)}$ in the decomposition of $M^{(b)}/M^{(b-1)}$ as a direct sum of simple $\mathbb{F}[T]$-modules. Also, we define $n_2(a,b)$ to be the number of copies of the $\mathbb{F}[T]$-module $S_{\nu^{-b}(a)}$ in the decomposition of $M^{(b+1)}/M^{(b)}$ in a direct sum of simple $\mathbb{F}[T]$-modules. Then $n(a,b)$ is given by

$$n(a,b) = n_1(a,b) - n_2(a,b).$$

Proof. This is [BCK20, Remark 4.4], using the fact that the preimages of the branch points in F_{ram} have stabiliser equal to T. We also use the classification from Proposition 2.2 to define the numbers $n(a,b)$.
Note that the definition of D_j from Definition 2.4 agrees with the description of D_j from Step 1 of [BCK20, Remark 4.4]. Indeed, as π_U is ramified at only point, namely at $[1:0:0]$ over $[0:1]$ with inertia group U, the subgroup $I_{[1:0:0]}$ there corresponds to our subgroup U which is cyclic of order p. In particular, the numbers n_I and $n\big([1:0:0]\big)$ there are equal to 1, hence $i\big([1:0:0]\big)$ there is equal to 0, the index j runs through $\{0,\dots,p-1\}$ and the number t there is equal to j. Moreover, t is already written in base p and the number $a_{1,t}$ there is equal to j. Therefore, the sum defining D_j there reduces to one summand of the form $s_j[0:1]$ with s_j as in Definition 2.4.
In the definition of n_j, we also use the fact that $g\big(C/U\big) = 0$ because $C/U \cong \mathbb{P}^1\big(\mathbb{F}\big)$ by Lemma 1.30.
Finally, $\overline{H}$ corresponds to T therefore $\#\overline{H} = p-1$, and $\overline{H}_{E(Q)}$ is the whole of T for each $Q \in F_{\text{ram}}$. □

2.1.1 The jumping number

Lemma 2.6. *The jumping number h from Definition 2.4 is $p+1$.*

Proof. The inertia group of $[1:0:0]$ inside U is $U_{[1:0:0]} = U$ of order p. Therefore, computing the lower ramification subgroups at $[1:0:0]$ reduces to computing the jump in the numbering of these subgroups of U. In order to do this, let us find an appropriate open set of C around $[1:0:0]$. First, let us look at the affine chart C_X of C, which is the affine curve defined by $s^p - s - t^{p+1}$ where $s = \frac{Y}{X}$ and $t = \frac{Z}{X}$ following the notation from the proof of Lemma 1.26. Then an element $\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$ of U acts on a point (s,t) in C_X in the following way.

$$\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \cdot (s,t) = \left(\frac{s}{1+rs}, \frac{t}{1+rs} \right)$$

We notice that the action is not defined on the whole of C_X, but taking away the points $(s,0)$ for $s \neq 0$ suffices to obtain an open subset of C_X containing

$(0,0)$ on which U acts as described above. The subset of C_X is obviously open in C, since C_X is open in C and we removed only $p-1$ points, that is, a finite number of points. Let us denote the open subset of C_X by V. Then we get a ring isomorphism $\mathcal{O}_{C,[1:0:0]} \cong \mathcal{O}_{V,(0,0)}$, which allows us to work with affine coordinates. From Lemma 1.26, we already know that t is a local parameter at $[1:0:0]$ under this isomorphism. Now, let us look at $t+\mathfrak{m}^r \in \mathcal{O}_{V,(0,0)}/\mathfrak{m}^r$ for some $r \geq 0$, and its behavior under the action of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \left(t+\mathfrak{m}^r\right) = \frac{t}{1-s} + \mathfrak{m}^r$$

Therefore U acts trivially on $t+\mathfrak{m}^r$ if and only if $\frac{t}{1-s} - t = \frac{st}{1-s} \in \mathfrak{m}^r$, which is equivalent to $st \in \mathfrak{m}^r$ since $1-s$ is a unit. Because t is a local parameter at $(0,0)$, we can use valuations. First, we notice that by s not being a unit and vanishing at $(0,0)$, we get that $\mathrm{ord}_{(0,0)}(s) > 0$. Therefore, $\mathrm{ord}_{(0,0)}\left(s^p\right) > \mathrm{ord}_{(0,0)}(s)$ and we obtain that

$$\mathrm{ord}_{(0,0)}(s) = \min\left\{\mathrm{ord}_{(0,0)}\left(s^p\right), \mathrm{ord}_{(0,0)}(s)\right\} = \mathrm{ord}_{(0,0)}\left(s^p - s\right).$$

Now, recalling that $s^p - s = t^{p+1}$, we get that $\mathrm{ord}_{(0,0)}(s) = p+1$, and thus that $\mathrm{ord}_{(0,0)}(st) = p+2$. From this fact, we know that U acts non-trivially on $t+\mathfrak{m}^r$ if and only if $r \geq p+3$. Thus, U_i is trivial for all $i \geq p+2$ and $U_i = U$ for all $0 \leq i \leq p+1$, i.e. the jump in the lower ramification groups happens at index $h = p+1$. □

2.1.2 The Brauer characters

We will now use the order of the divisor D_j at the points P of C/U to find the elements $\ell_{P,j} := -\mathrm{ord}_P(D_j) \mod (p-1) \in \{0,1,\ldots,p-2\}$ for all $0 \leq j \leq p-1$, which will help us find the Brauer characters from Theorem 2.5.

Lemma 2.7. *For all $0 \leq j \leq p-1$, the divisor D_j is the following.*

$$D_j = \begin{cases} (p-j)[0:1] & \text{if } 0 \leq j \leq p-2 \\ 0 & \text{if } j = p-1 \end{cases}$$

Also, the only point P of C/U for which $\ell_{P,j} \neq 0$ is $P = [0:1]$, and it is equal to the following, depending on $0 \leq j \leq p-1$.

$$\ell_{[0:1],j} = \begin{cases} p-2 & \text{if } j = 0 \\ j-1 & \text{if } 1 \leq j \leq p-2 \\ 0 & \text{if } j = p-1 \end{cases}$$

Proof. From Lemma 2.6, we get that for $0 \leq j \leq p-1$,

$$s_j = \left\lfloor \frac{p-1+(p-1-j)(p+1)}{p} \right\rfloor = \left\lfloor p+1-j-\frac{2+j}{p} \right\rfloor,$$

and hence $s_j = p-j$ for all $0 \leq j \leq p-2$, and $s_{p-1} = 0$. Thus, D_j is of the form above. Now because $\mathrm{ord}_P(D_j) = 0$ for all $P \neq [0:1] \in C/U$, we know that $\ell_{P,j}$ might be non-zero only for $P = [0:1]$. Also, D_{p-1} being the zero divisor, we know that $\ell_{[0:1],p-1} = 0$. For $j = 0$, we get

$$\ell_{[0:1],0} \equiv -p \mod (p-1) \equiv p-2 \mod (p-1),$$

and finally, for $1 \leq j \leq p-2$, we get

$$\begin{aligned} \ell_{[0:1],j} &\equiv -(p-j) \mod (p-1) \\ &\equiv j-1 \mod (p-1), \end{aligned}$$

which is what we wanted. □

Now, let us apply the results from Lemma 2.7 to find the Brauer characters from Theorem 2.5. Thus, because T has order coprime to p and because $\mathbb{F}$ is algebraically closed, Brauer characters of $\mathbb{F}[T]$-modules correspond to classical characters once we pick a correspondence between roots of unity of $\mathbb{F}$ and $\mathbb{C}$, hence we will identify the two notions of characters. In what follows, we will denote by τ the character sending a fixed generator of T to $\omega = e^{\frac{2\pi i}{p-1}} \in \mathbb{C}$. It is a well-known fact from classical representation theory that $\tau^0, \tau, \tau^2, \ldots, \tau^{p-2}$ are the irreducible characters of T.

Proposition 2.8. *For all $0 \leq j \leq p-1$, the character of the dual of the $\mathbb{F}[T]$-module $S_{\nu^j} \otimes_{\mathbb{F}} \left(M^{(j+1)}/M^{(j)}\right)$ is the following.*

$$\begin{cases} \sum_{t=0}^{p-2} \tau^t & \text{if } j = 0 \\ \sum_{t=1}^{p-1-j} \tau^t & \text{if } 1 \leq j \leq p-2 \\ 0 & \text{if } j = p-1 \end{cases}$$

Proof. Now, we want to look at the curve $C/H \cong \mathbb{P}^1(\mathbb{F})$ studied in Lemma 1.29, and its relation with C/U. The only two points which ramify in the Galois cover of curves $\mathbb{P}^1(\mathbb{F}) \cong C/U \longrightarrow C/H \cong \mathbb{P}^1(\mathbb{F})$ of Galois group $H/U \cong T$ (which we identify from now on) are $[0:1]$ and $[1:0]$, each of ramification index $p-1 = |T|$. Therefore, in the sequence of covers

$$C \longrightarrow C/U \cong \mathbb{P}^1(\mathbb{F}) \longrightarrow C/H \cong \mathbb{P}^1(\mathbb{F}),$$

we have that $[1:0:0]$ lies above $[0:1]$ which lies above $[0:1]$. Similarly, $[0:1:0]$ lies above $[1:0]$ which lies above $[1:0]$. In the middle term, we obtain that $T_{[0:1]} = T$, and $T_{[1:0]} = T$ too, because $H_{[0:1:0]} = T$.
Next, we determine the characters θ as defined in Theorem 2.5.
Because $t = \frac{Z}{X}$ is a local parameter of C at $[1:0:0]$ by Lemma 1.26, the character $\theta_{[1:0:0]} : H_{[1:0:0]} = H \longrightarrow \mathbb{F}^\times$ is defined by

$$\begin{aligned}\theta_{[1:0:0]}\left(\begin{pmatrix}\varepsilon & r\\ 0 & \varepsilon^{-1}\end{pmatrix}\right) &= \frac{\begin{pmatrix}\varepsilon & r\\ 0 & \varepsilon^{-1}\end{pmatrix}\cdot t}{t} \mod (t)\\ &= \frac{1}{\varepsilon^{-1} - rs} \mod (t)\\ &= \varepsilon \mod (t)\end{aligned}$$

and hence, because $\varepsilon \in \mathbb{F}_p$, we get that $\theta_{[0:1]} = (\theta_{[1:0:0]} \mid_T)^p = \theta_{[1:0:0]} \mid_T$.
We also need to look at $\theta_{[0:1:0]}$. Hence, we need a local parameter of C at $[0:1:0]$, which we have already computed to be $w = \frac{Z}{Y}$ in Lemma 1.26. Therefore, $\theta_{[0:1:0]} : H_{[0:1:0]} = T \longrightarrow \mathbb{F}^\times$ is defined by

$$\begin{aligned}\theta_{[0:1:0]}\left(\begin{pmatrix}\varepsilon & 0\\ 0 & \varepsilon^{-1}\end{pmatrix}\right) &= \frac{\begin{pmatrix}\varepsilon & 0\\ 0 & \varepsilon^{-1}\end{pmatrix}\cdot w}{w} \mod (w)\\ &= \frac{\varepsilon^{-1}w}{w} \mod (w)\\ &= \varepsilon^{-1} \mod (w),\end{aligned}$$

hence we obtain that $\theta_{[1:0]} = \theta_{[0:1:0]}$.
Now, notice that the characters $\theta_{[0:1]}$ and $\theta_{[1:0]}$ defined above correspond to the complex characters τ and τ^{-1} respectively, so the $\mathbb{F}[T]$-module $S_{\nu^j} \otimes_{\mathbb{F}} \left(M^{(j+1)}/M^{(j)}\right)$ has character

$$\delta_{j,p-1}\tau^0 + \sum_{t=1}^{p-2}\frac{t}{p-1}\tau^t + \sum_{t=1}^{p-2}\frac{t}{p-1}\tau^{-t} - \sum_{t=1}^{\ell_{[0:1],j}}\tau^{-t} + n_j\sum_{t=0}^{p-2}\tau^t,$$

for

$$n_j = \frac{\deg(D_j)-1}{p-1} + \frac{1}{p-1}\left(\ell_{[0:1],j} - \frac{p-2}{2}\right) + \frac{1}{p-1}\left(0 - \frac{p-2}{2}\right),$$

where δ denotes the usual Kronecker delta. Here, we used the fact that F_{ram} is $\big\{[0:1],[1:0]\big\}$, and that $\ell_{[1:0],j} = 0$ by Lemma 2.7. Using a convenient change of index in the second sum, the first two sums merge to obtain

$$\delta_{j,p-1}\tau^0 + \sum_{t=1}^{p-2}\tau^t - \sum_{t=1}^{\ell_{[0:1],j}}\tau^{-t} + n_j\sum_{t=0}^{p-2}\tau^t,$$

which is the form we will use to compute the characters.
Suppose that $j = 0$. Then the Brauer character is

$$\sum_{t=1}^{p-2} \tau^t - \sum_{t=1}^{p-2} \tau^{-t} + \sum_{t=0}^{p-2} \tau^t = \sum_{t=0}^{p-2} \tau^t$$

because $n_0 = \frac{p-1}{p-1} + \frac{1}{p-1}\left(p-2-\frac{p-2}{2}\right) - \frac{p-2}{2(p-1)} = 1$ and $\ell_{[0:1],0} = p-2$.
Now, suppose that $j = p-1$. Then $n_{p-1} = \frac{0-1}{p-1} + \frac{1}{p-1}\left(0-\frac{p-2}{2}\right) - \frac{p-2}{2(p-1)} = \frac{1-p}{p-1} = -1$ and $\ell_{[0:1],p-1} = 0$, so the character is

$$\tau^0 + \sum_{t=1}^{p-2} \tau^t - \sum_{t=0}^{p-2} \tau^t,$$

which simplifies to give the zero character.
Finally, if $1 \leq j \leq p-2$, then

$$n_j = \frac{p-j-1}{p-1} + \frac{1}{p-1}\left(j-1-\frac{p-2}{2}\right) + \frac{1}{p-1}\left(0-\frac{p-2}{2}\right) = 0.$$

Thus if $j = 1$, then because $\ell_{[0:1],1} = 0$, the character is simply

$$\sum_{t=1}^{p-2} \tau^t,$$

and if $2 \leq j \leq p-2$, then because $\ell_{[0:1],j} = j-1$ the character is the following.

$$\sum_{t=1}^{p-2} \tau^t - \sum_{t=1}^{j-1} \tau^{-t} = \sum_{t=1}^{p-1-j} \tau^t$$

□

From the characters presented in Lemma 2.8, we compute the characters of the $\mathbb{F}[T]$-module $M^{(j+1)}/M^{(j)}$ for each $0 \leq j \leq p-1$. This is crucial in order to compute the numbers $n(a,b)$ from Theorem 2.5.

Corollary 2.9. *The characters of the $\mathbb{F}[T]$-modules $M^{(j+1)}/M^{(j)}$ are as follows.*

$$\begin{cases} \tau^0 + \tau^1 + \cdots + \tau^{p-2} & \text{if } j = 0 \\ \tau^{-j} + \tau^{-j+1} + \cdots + \tau^{p-3-2j} + \tau^{p-2-2j} & \text{if } 1 \leq j \leq p-2 \\ 0 & \text{if } j = p-1 \end{cases}$$

Proof. To compute the character of $M^{(j+1)}/M^{(j)}$ as an $\mathbb{F}[T]$-module, we take the dual of the dual of the character of $S_{\nu^j} \otimes_{\mathbb{F}} \left(M^{(j+1)}/M^{(j)}\right)$, which results in conjugating the characters of Proposition 2.8. Then we tensor on the left by $S_{\nu^{-j}}$ to obtain $M^{(j+1)}/M^{(j)}$, which amounts to multiplying by the character τ^{-2j}.
For the character of $M^{(1)}/M^{(0)}$, we conjugate $\sum_{t=0}^{p-2} \tau^t$ and multiply by τ^0, so we obtain $\sum_{t=0}^{p-2} \tau^t$ again. Now conjugating the zero character and multiplying it by $\tau^{-2(p-1)}$ obviously still yields the zero character, so the character of $M^{(p)}/M^{(p-1)}$ is the zero character. Now, for $1 \leq j \leq p-2$, we get that the character of $M^{(j+1)}/M^{(j)}$ is

$$\begin{aligned}
\tau^{-2j} \sum_{t=1}^{p-1-j} \overline{\tau^t} &= \tau^{-2j} \sum_{t=1}^{p-1-j} \tau^{-t} \\
&= \tau^{-2j} \sum_{t=1}^{p-1-j} \tau^{p-1-t} \\
&= \tau^{-2j} \left(\tau^j + \tau^{j+1} + \cdots + \tau^{p-2}\right) \\
&= \tau^{-j} + \tau^{-j+1} + \cdots + \tau^{p-3-2j} + \tau^{p-2-2j},
\end{aligned}$$

which is what we wanted. □

2.1.3 The numbers $n(a,b)$ and the decomposition of M_H

We use the previous information to find the decomposition of M as an $\mathbb{F}[H]$-module, provided by the numbers $n(a,b)$ of Theorem 2.5.

Proposition 2.10. *Let $0 \leq a \leq p-2$ and $1 \leq b \leq p$. Then $n_1(a,b)$ is given by the following.*

$$n_1(a,b) = \begin{cases} 1 \text{ if } a \in \{b-1, b, b+1, \ldots, p-2\} \\ 0 \text{ otherwise} \end{cases}$$

Proof. We use the characters computed in Corollary 2.9.
Recall that $\nu^{-(b-1)}(a) = a - 2b + 2 \mod (p-1)$ in $\{0, 1, \ldots, p-2\}$.
If $b = 1$, the module is $M^{(1)}/M^{(0)}$ which has character $\sum_{t=0}^{p-2} \tau^t$, so $n_1(a,b) = 1$ in this case.
If $b = p$, then the module is $M^{(p)}/M^{(p-1)}$, which we saw has character zero, so $n_1(a,b) = 0$.
Now, suppose that $2 \leq b \leq p-1$. Then the module of interest is $M^{(b)}/M^{(b-1)}$,

which has character

$$\sum_{t=1}^{p-b} \tau^{-b+t} = \tau^{-b+1} + \tau^{-b+2} + \cdots + \tau^{p-2b}.$$

Therefore, $n_1(a,b) = 1$ if $a-2b+2 \equiv -b+t \mod (p-1)$ for a $t \in \{1,2,\ldots,p-b\}$, and $n_1(a,b) = 0$ otherwise. Now, this equation is equivalent to $a = b+t-2$ as integers for a $t \in \{1,2,\ldots,p-b\}$, because $0 \leq a \leq p-2$ by definition, and combined with the fact that $t \in \{1,2,\ldots,p-b\}$, we get that $a+b-t \in \{b-1,b,b+1,\ldots,p-2\}$. Thus, we finally obtain that $n_1(a,b) = 1$ if $a \in \{b-1,b,b+1,\ldots,p-2\}$, and $n_1(a,b) = 0$ otherwise. □

Proposition 2.11. *Let $0 \leq a \leq p-2$ and $1 \leq b \leq p$. Then $n_2(a,b)$ is given by the following.*

$$n_2(a,b) = \begin{cases} 1 \text{ if } a \in \{b,b+1,\ldots,p-2\} \\ 0 \text{ otherwise} \end{cases}$$

Proof. We use the characters computed in Corollary 2.9.
Recall that $\nu^{-b}(a) = a-2b \mod (p-1)$ in $\{0,1,\ldots,p-2\}$.
If $b = p$, we have $n_2(a,b) = 0$ by definition, and for $b = p-1$, we are interested in the character of the module $M^{(p)}/M^{(p-1)}$ which we saw is the zero character, so $n_2(a,b) = 0$ in this case too.
Thus, suppose that $1 \leq b \leq p-2$. Then we are interested in the $\mathbb{F}[T]$-module $M^{(b+1)}/M^{(b)}$, which affords the following character.

$$\sum_{t=0}^{p-b-2} \tau^{-b+t} = \tau^{-b} + \tau^{-b+1} + \cdots + \tau^{p-3-2b} + \tau^{p-2-2b}$$

Therefore, $n_2(a,b) = 1$ if $a-2b \equiv -b+t \mod (p-1)$ for some $t \in \{0,1,\ldots,p-b-2\}$, and $n_2(a,b) = 0$ otherwise. The equation is equivalent to $a = b+t$ as integers because $0 \leq a \leq p-2$, and by definition of t, we also have $b+t \in \{b,b+1,\ldots,p-2\} \subseteq \{0,1,\ldots,p-2\}$. Hence, we get that $n_2(a,b) = 1$ if $a \in \{b,b+1,\ldots,p-2\}$, and $n_2(a,b) = 0$ otherwise. □

Corollary 2.12. *Let $0 \leq a \leq p-2$ and $1 \leq b \leq p$. Then $n(a,b)$ is given by the following.*

$$n(a,b) = \begin{cases} 1 \text{ if } a = b-1 \\ 0 \text{ otherwise} \end{cases}$$

Therefore, as an $\mathbb{F}[H]$-module, M admits the decomposition

$$M \cong U_{0,1} \oplus U_{1,2} \oplus \cdots \oplus U_{p-3,p-2} \oplus U_{p-2,p-1},$$

where the $U_{j-1,j}$ are the $\mathbb{F}[H]$-modules from Proposition 2.2.

Proof. Simply combine the formula $n(a,b) = n_1(a,b) - n_2(a,b)$, Proposition 2.10, and Proposition 2.11. □

2.2 The Green correspondence

Now that we know the decomposition of M_H into its indecomposable components, we can use the Green correspondence below [Alp86, Theorem 10.1] to find the structure of M as an $\mathbb{F}[G]$-module, which will prove Theorem 0.1 in the case where $q = p$ is a prime.

Theorem 2.13 (Green correspondence)**.** *Let S be a Sylow p-subgroup of G, and $L = N_G(S)$. Then there is a one-to-one correspondence between isomorphism classes of indecomposable non-projective $\mathbb{F}[L]$-modules and isomorphism classes of indecomposable non-projective $\mathbb{F}[G]$-modules. The correspondence is given by taking induction and restriction of modules, i.e. for an indecomposable non-projective $\mathbb{F}[G]$-module A, its restriction A_L has a unique indecomposable non-projective $\mathbb{F}[L]$-summand B up to isomorphism. Then there exist projective $\mathbb{F}[L]$ and $\mathbb{F}[G]$-modules Q and P respectively such that the following isomorphisms hold.*

$$A_L \cong B \oplus Q$$
$$B^G \cong A \oplus P$$

This correspondence is tailored to our needs, because the subgroup of upper unitriangular matrices U is a Sylow p-subgroup, $H = U \rtimes T = N_G(U)$, and we know the structure of M_H. Furthermore, by the description of the indecomposable $\mathbb{F}[H]$-modules in Proposition 2.2, the indecomposable projective $\mathbb{F}[H]$-modules all have dimension p, and for $1 \leq j \leq p-1$, the indecomposable $\mathbb{F}[H]$-module $U_{j-1,j}$ has dimension j. Hence we conclude that all the indecomposable $\mathbb{F}[H]$-modules appearing in the decomposition of M_H are non-projective, so we can apply the Green correspondence.

We will use an explicit description of some indecomposable $\mathbb{F}[G]$-modules, as found in [Alp86, pp. 14-16]. For $0 \leq j \leq p-1$, we define V^j to be the $\mathbb{F}$-vector space of homogeneous polynomials in $\mathbb{F}[x,y]$ of degree j, so that V^j has dimension $j+1$. We define

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot x = \alpha x + \gamma y, \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot y = \beta x + \delta y$$

which extends to an automorphism of the algebra $\mathbb{F}[x,y]$. Therefore, G acts linearly on V^j for all $0 \leq i \leq p-1$. We are interested in $V^0, V^2, \ldots, V^{p-2}$ and their restriction as $\mathbb{F}[H]$-modules. As detailed in [Alp86, pp. 77-79], the indecomposable

projective $\mathbb{F}[G]$-modules have dimension either p or $2p$, so $V^0, \dots, V^{p-2}$ are non-projective $\mathbb{F}[G]$-modules, and hence the Green correspondence applies too. Let us now state and prove a result about their structure when considered as $\mathbb{F}[H]$-modules.

Lemma 2.14. *Let $0 \leq j \leq p-2$, and for each $0 \leq i \leq j$ define the $\mathbb{F}$-vector space $W^i = \mathbb{F}x^j \oplus \mathbb{F}x^{j-1}y \oplus \cdots \oplus \mathbb{F}x^{j-i}y^i$. Then each W^i is an $\mathbb{F}[H]$-submodule of V_H^j, and they are the only non-trivial submodules of V_H^j. Thus because the following chain of inclusions holds, V_H^j is a uniserial $\mathbb{F}[H]$-module.*

$$0 \subsetneq W^0 \subsetneq W^1 \subsetneq \cdots \subsetneq W^j = V_H^j$$

Proof. Suppose that $W \subseteq V_H^j$ is a non-trivial $\mathbb{F}[H]$-submodule. Using the basis of V_H^j given by the elements $x^j, x^{j-1}y, \dots, xy^{j-1}, y^j$, any element of W can be seen as a polynomial in y with coefficients in $\mathbb{F}[x]$. Since W is non-trivial and because any non-empty subset of $\mathbb{N}$ admits a minimum, there exists an element $0 \neq w \in W$ of minimal degree in y. Let $0 \leq k \leq j$ be this minimal degree, and suppose that $k \geq 1$. Using the basis for V^j, there exist some $\lambda_0, \dots, \lambda_k \in \mathbb{F}$ such that $w = \sum_{i=0}^{k} \lambda_i x^{j-i}y^i$. Now, we easily compute that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in H$ acts on a basis element $x^{j-i}y^i$ as follows.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot x^{j-i}y^i = x^j + \binom{i}{i-1} x^{j-1}y + \cdots + \binom{i}{1} x^{j-i+1}y^{i-1} + x^{j-i}y^i$$

Therefore, we get that the action of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ on w yields

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot w = \sum_{i=0}^{k} \lambda_i \sum_{\ell=0}^{i} \binom{i}{i-\ell} x^{j-\ell}y^{\ell},$$

and we observe that the degree in y of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot w$ is still k and has leading coefficient $\lambda_k x^{j-k}$, which is the same as the leading coefficient of w. Now, because $w \in W$ and W is $\mathbb{F}[H]$-stable, we get that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot w - w \in W$. Also, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot w - w$ has coefficient in $x^{j-k+1}y^{k-1}$ equal to $k\lambda_k$ which is non-zero because $k \neq 0$ and $\lambda_k \neq 0$, thus $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot w - w \neq 0$ in W. However, this last element has degree in y strictly smaller than the degree in y of w, which is a contradiction with the supposed minimality. Therefore we obtain that $k = 0$, which gives $w = \lambda_0 x^j$. This allows us to conclude that $W^0 := \mathbb{F}x^j \subseteq W$ is an $\mathbb{F}[H]$-submodule of W.

Now, suppose that $W^0 \subsetneq W$. Then W/W^0 is a non-trivial $\mathbb{F}[H]$-module, and we repeat a similar argument. Indeed, let $0 \neq w^1 + W^0 \in W/W^0$ be an element of minimal degree k^1 in y. Note that we must have $k^1 \geq 1$ because $w^1 + W^0 \neq 0 + W^0$. Suppose that $k^1 \geq 2$. Then we use the basis for W/W^0 arising from the quotient of the basis of V^j to find coefficients $\lambda_1^1, \ldots, \lambda_{k^1}^1 \in \mathbb{F}$ such that

$$w^1 + W^0 = \sum_{i=1}^{k^1} \lambda_i^1 \left(x^{j-i} y^i + W^1 \right),$$

from which we get that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot (w^1 + W^0) = \sum_{i=1}^{k^1} \lambda_i^1 \sum_{\ell=1}^{i} \binom{i}{i-\ell} \left(x^{j-\ell} y^\ell + W^1 \right),$$

and we again conclude that $w^1 + W^0$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot (w^1 + W^0)$ have the same degree in y with the same leading coefficient. Therefore because the element

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot (w^1 + W^0) - (w^1 + W^0) \in W/W^0$$

is non-zero since it has coefficient in $\left(x^{j-k^1+1} y^{k^1-1} + W^1 \right)$ equal to $k^1 \lambda_{k^1}^1 \neq 0$, it has degree in y strictly smaller than k^1, which is again a contradiction. Thus $k^1 = 1$, from which we obtain that $w^1 + W^0 = \lambda_1^1 x^{j-1} y + W^1$, and hence $\left(\mathbb{F}x^j \oplus \mathbb{F}x^{j-1}y \right) / W^0 \subseteq W/W^0$ is an $\mathbb{F}[H]$-submodule. By the correspondence theorem applied to W/W^0, we get that $W^1 := \mathbb{F}x^j \oplus \mathbb{F}x^{j-1}y \subseteq W$ is an $\mathbb{F}[H]$-submodule. If $W^1 \subsetneq W$, considering W/W^1, we can repeat the same argument on the minimal degree k^2 of a non-zero element $w^2 + W^1 \in W/W^1$ to conclude that $k^2 = 2$, by exhibiting a contradiction if we suppose that $k^2 \geq 3$. From this, we conclude that $W^2 = \mathbb{F}x^j \oplus \mathbb{F}x^{j-1}y \oplus \mathbb{F}x^{j-2}y^2 \subseteq W$ is an $\mathbb{F}[H]$-submodule, by applying the correspondence theorem to W/W^2.
One can repeat the argument to obtain that $W^0, W^1, \ldots, W^j$ are the only non-trivial $\mathbb{F}[H]$-submodules of V_H^j. Furthermore, since the inclusions

$$0 \subsetneq W^0 \subsetneq W^1 \subsetneq \cdots \subsetneq W^j = V_H^j$$

hold, we get that all the $\mathbb{F}[H]$-submodules of V_H^j are ordered by inclusion. □

We will actually see that for each $1 \leq j \leq p-1$, the indecomposable non-projective $\mathbb{F}[H]$-module $U_{j-1,j}$ corresponds to the simple non-projective $\mathbb{F}[G]$-module V^{j-1}, in the sense of the Green correspondence. This fact is at the core of our first proof of Theorem 0.1 in the case $q = p$, which we specify below.

Theorem 2.15. *The $\mathbb{F}[G]$-module M admits the following decomposition into indecomposable summands.*

$$M \cong V^0 \oplus V^1 \oplus \cdots \oplus V^{p-2}$$

Proof. We already know from [Alp86, pp. 14-16] that $V^0, V^1, \ldots, V^{p-2}$ are indecomposable $\mathbb{F}[G]$-modules.
First, we obviously have that $V_H^0 = U_{0,1}$ is the trivial $\mathbb{F}[H]$-module.
By Lemma 2.14, V_H^j is uniserial, which implies that it is an indecomposable $\mathbb{F}[H]$-module of dimension $j+1$. The classification from Proposition 2.2 then directly gives the isomorphism of $\mathbb{F}[H]$-modules $V_H^{j-1} \cong U_{j-1,j}$. We conclude that in the context of the Green correspondence, for all $1 \leq j \leq p-1$ the modules $U_{j-1,j}$ and V^{j-1} correspond to one another.
Now, because the restriction of a projective $\mathbb{F}[G]$-module to H is a projective $\mathbb{F}[H]$-module [Alp86, Theorem II.5.6] and because the $U_{j-1,j}$ are non-projective, we know that in the decomposition of M as a direct sum of indecomposable $\mathbb{F}[G]$-modules, none of the direct summands are projective. Therefore, we can apply the Green correspondence to any indecomposable summand appearing in the decomposition of M as an $\mathbb{F}[G]$-module.
Suppose that $M \cong S^0 \oplus S^1 \oplus \cdots \oplus S^r$ for some $r \in \mathbb{Z}_{\geq 1}$ and some non-projective indecomposable $\mathbb{F}[G]$-modules S^j. Then restricting to H yields an isomorphism of $\mathbb{F}[H]$-modules

$$U_{0,1} \oplus U_{1,2} \oplus \cdots \oplus U_{p-2,p-1} \cong S_H^0 \oplus S_H^1 \oplus \cdots \oplus S_H^r$$

which directly gives by the Krull-Schmidt theorem that $r = p-2$ and that without loss of generality, $S_H^{j-1} \cong U_{j-1,j}$ for all $1 \leq j \leq p-1$. Since the isomorphisms $V_H^{j-1} \cong U_{j-1,j}$ for all $1 \leq j \leq p-1$ hold too, we get by the injectivity of restricting isomorphism classes of non-projective indecomposable $\mathbb{F}[G]$-modules to H that $V^j \cong S^j$ as $\mathbb{F}[G]$-modules for all $0 \leq j \leq p-2$. □

Remark 2.16. Because each V^j appearing in the decomposition of M is a simple $\mathbb{F}[G]$-module by [Alp86, pp. 14-16], we obtain that M is semi-simple. This is an interesting fact which does not hold if q is not a prime, as detailed in Corollary 3.11.

Chapter 3

Solution for q a general prime power

In this final chapter, we will present a solution to the problem of computing the decomposition of the canonical representation M of the Drinfeld curve C as an $\mathbb{F}[G]$-module in the general case of a prime power $q = p^r$ for some $r \in \mathbb{N}_{\geq 1}$. The methods we will use are radically different. We begin by computing a concrete basis for the $\mathbb{F}$-vector space M, and then we study the action of G directly on this basis, to deduce a decomposition for M as an $\mathbb{F}[G]$-module. We finish by proving that each summand is indecomposable, using some tools from modular representation theory.

3.1 A basis for the space of holomorphic differentials

In order to compute the decomposition of the $\mathbb{F}[G]$-module $M = H^0\big(C, \Omega_C\big)$, we will make use of a basis for the $\mathbb{F}$-vector space M. The goal of this section is to exhibit such a basis.

In order to show that a differential is holomorphic on C, we need a local parameter at each point of C, which we have already done in Lemma 1.26. We exhibit a basis for the $\mathbb{F}$-vector space M in the next proposition.

Proposition 3.1. *For $0 \leq i, j \leq q-2$ and $i + j \leq q-2$, define*

$$\omega_{i,j} = \frac{x^i y^j}{x^q} dx \in \Omega_{\mathbb{F}(C)/\mathbb{F}} = \mathbb{F}(C)dx,$$

where $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, and $\Omega_{\mathbb{F}(C)/\mathbb{F}}$ is the 1-dimensional $\mathbb{F}(C)$-vector space of meromorphic differentials. Then each $\omega_{i,j}$ is holomorphic on the whole of C, i.e. $\omega_{i,j} \in M$, and $\{\omega_{i,j} \mid 0 \leq i, j \leq q-2,\ i + j \leq q-2\}$ is a basis for the $\mathbb{F}$-vector space M.

Proof. We will show that the $\omega_{i,j}$ are holomorphic, i.e. $\omega_{i,j} \in M$, show that they are linearly independent over $\mathbb{F}$, which combined with the fact that we defined $g(C)$ elements gives that the $\omega_{i,j}$ form a basis.
Let us show that these differentials are holomorphic on C. We know, if t is a local parameter at a point, then the meromorphic differential fdt is regular at that point if and only if the rational function f is regular at that point. Let $0 \leq i, j \leq q-2$ such that $i+j \leq q-2$, and let $P = [x_0 : y_0 : z_0]$. Suppose first that $z_0 \neq 0$. Then, because $x - \frac{x_0}{z_0}$ is a local parameter at P by Lemma 1.26 and because $dx = d(x - \frac{x_0}{z_0})$, we simply need to verify that $\frac{x^i y^j}{x^q}$ is a regular function at P. This is the case because we supposed that $z_0 \neq 0$, and $\frac{x_0}{z_0} \neq 0$ because $\frac{x_0}{z_0}\left(\frac{y_0}{z_0}\right)^q - \left(\frac{x_0}{z_0}\right)^q \frac{y_0}{z_0} = 1$. Therefore, $\omega_{i,j}$ is holomorphic on C_Z.
Now, suppose that $z_0 = 0$ and $x_0 \neq 0$, and let $s = \frac{Y}{X}$, $t = \frac{Z}{X}$ as in the proof of Lemma 1.26. Then $x = \frac{1}{t}$ and $y = \frac{s}{t}$, so the following holds in $\Omega_{\mathbb{F}(C)/\mathbb{F}}$.

$$\omega_{i,j} = \frac{\left(\frac{1}{t}\right)^i \left(\frac{s}{t}\right)^j}{\left(\frac{1}{t}\right)^q} d\left(\frac{1}{t}\right) = t^{q-i-j} s^j \left(\frac{-1}{t^2}\right) dt = -t^{q-2-(i+j)} s^j dt$$

Because t is a local parameter at P by Lemma 1.26, we just need to check that $-t^{q-2-(i+j)}s^j$ is regular at P, which is the case because $x_0 \neq 0$ and $i+j \leq q-2$. Finally, suppose that $z_0 = 0$ and $y_0 \neq 0$, and let $v = \frac{X}{Y}$, $w = \frac{Z}{Y}$ as in Lemma 1.26. By observing that $x = \frac{v}{w}$ and $y = \frac{1}{w}$, combined with the fact that $\frac{1}{x^q}dx = \frac{1}{y^q}dy$ in $\Omega_{\mathbb{F}(C)/\mathbb{F}}$ (obtained by differentiating $xy^q - x^q y - 1 = 0$), the following holds.

$$\omega_{i,j} = \frac{\left(\frac{v}{w}\right)^i \left(\frac{1}{w}\right)^j}{\left(\frac{1}{w}\right)^q} d\left(\frac{1}{w}\right) = w^{q-i-j} v^i \left(\frac{-1}{w^2}\right) dw = -w^{q-2-(i+j)} v^i dw$$

As above, because w is a local parameter at P by Lemma 1.26 and because $-w^{q-2-(i+j)}v^i$ is regular at P, we have that $\omega_{i,j}$ is regular at P. We proved that each $\omega_{i,j}$ is an element of M.
Let us now show that these differentials are linearly independent over $\mathbb{F}$. Suppose that there are coefficients $\lambda_{i,j} \in \mathbb{F}$, not all zero, such that $\sum_{i,j} \lambda_{i,j}\omega_{i,j} = 0$ in M. Then certainly this sum is zero on the affine chart C_Z, where we can substitute the formula for each $\omega_{i,j}$ in the sum. We obtain

$$\sum_{i,j} \lambda_{i,j} x^i y^j \frac{1}{x^q} dx = \left(\sum_{i,j} \lambda_{i,j} x^i y^j\right) \frac{1}{x^q} dx = 0.$$

Now, because $\frac{1}{x^q}dx$ is nowhere vanishing in C_Z, and because $x - x_0$ is a local parameter at each point $(x_0, y_0) \in C_Z$ by Lemma 1.26, with $d(x - x_0) = dx$, we

conclude that $f(x,y) := \sum_{i,j} \lambda_{i,j} x^i y^j$ vanishes on the whole of C_Z. Therefore we get $\mathbb{V}\big(xy^q - x^q y - 1\big) \subseteq \mathbb{V}\big(f(x,y)\big)$, which gives by Hilbert's Nullstellensatz that

$$f(x,y) \in \mathrm{Rad}\big(f(x,y)\big) \subseteq \mathrm{Rad}\big(xy^q - x^q y - 1\big) = \big(xy^q - x^q y - 1\big),$$

where the last equality holds because $xy^q - x^q y - 1$ is an irreducible polynomial in $\mathbb{F}[x,y]$ by [Bon12, Proposition 2.1.1], so $\big(xy^q - x^q y - 1\big)$ is prime and hence radical. From this, we get that $xy^q - x^q y - 1$ divides $f(x,y)$ in $\mathbb{F}[x,y]$, which is a contradiction because $f(x,y)$ has degree less or equal than $q-2$, being a non-zero element. Therefore, the $\omega_{i,j}$ are linearly independent.
Now, for each choice of i, there are $q-1-i$ choices for j. Summing over i yields

$$\sum_{i=0}^{q-2}(q-1-i) = \sum_{k=1}^{q-1} k = \frac{q(q-1)}{2},$$

which is the number of differentials we defined, but also the genus of C, which is the dimension of M by Definition/Proposition 1.16.
Thus, we proved that the $\omega_{i,j}$ form a basis for the $\mathbb{F}$-vector space M. □

Remark 3.2. The differentials $\omega_{i,j}$ defined in Proposition 3.1 have the following vanishing order at $P = [x_0 : y_0 : z_0] \in C$.

$$\begin{cases} 0 & \text{if } z_0 \neq 0 \\ q-2-(i+j) & \text{if } z_0 = 0,\ x_0 \neq 0 \text{ and } y_0 \neq 0 \\ q-2-i+jq & \text{if } P = [1:0:0] \\ q-2-j+iq & \text{if } P = [0:1:0] \end{cases}$$

The arguments are the following.
First, $\omega_{i,j}$ does not vanish on C_Z because $\frac{x_0}{z_0} \neq 0 \neq \frac{y_0}{z_0}$ for any point $P = [x_0 : y_0 : z_0] \in C$ with $z_0 \neq 0$, since $\frac{x_0}{z_0}\left(\frac{y_0}{z_0}\right)^q - \left(\frac{x_0}{z_0}\right)^q \frac{y_0}{z_0} = 1$.
Now, if $P = [x_0 : y_0 : 0]$ with $x_0 \neq 0$, then using the notation from the proof of Proposition 3.1, $\omega_{i,j} = -t^{q-2-(i+j)} s^j dt$. Hence if $y_0 \neq 0$, then $\omega_{i,j}$ vanishes with order $q-2-(i+j)$ because s does not vanish at P.
Now, if $y_0 = 0$ then $P = [1:0:0]$. Using the fact that

$$\mathrm{ord}_P(s) = \min\{\mathrm{ord}_P(s^q), \mathrm{ord}_P(s)\} = \mathrm{ord}_P(s^q - s) = \mathrm{ord}_P(t^{q+1}) = q+1,$$

we get that $\omega_{i,j}$ vanishes with order $q-2-(i+j)+j(q+1) = q-2-i+jq$.
Finally, if $x_0 = 0$, then $P = [0:1:0]$ and we can use $\omega_{i,j} = -w^{q-2-(i+j)} v^i dw$, again using the same notation as in the proof of Proposition 3.1. A similar reasoning allows us to conclude that $\omega_{i,j}$ vanishes at $[0:1:0]$ with order $q-2-(i+j)+i(q+1) = q-2-j+iq$.

3.2 The decomposition of M as an $\mathbb{F}[G]$-module

3.2.1 A decomposition

First, we compute the action of an element of G on the basis from Proposition 3.1, namely $\{\omega_{i,j} \mid 0 \leq i, j \leq q-2,\ i+j \leq q-2\}$.

Lemma 3.3. *Let $0 \leq i, j \leq q-2$ such that $i+j \leq q-2$, and let $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G$. Then*

$$g \cdot \omega_{i,j} = \frac{(\delta x - \beta y)^i (-\gamma x + \alpha y)^j}{x^q} dx.$$

Proof. First, we note that $g^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$. Let us consider $\omega_{i,j}$ in the affine chart C_Z, so that $\omega_{i,j} = \frac{x^i y^j}{x^q} dx$. Then we obtain that $(g^{-1})^* x = \delta x - \beta y$ and $(g^{-1})^* y = -\gamma x + \alpha y$. Moreover, using the fact that $\frac{1}{x^q} dx = \frac{1}{y^q} dy$ as in the proof of Proposition 3.1,

$$\left(g^{-1}\right)^* dx = d\Big(\left(g^{-1}\right)^* x \Big) = d(\delta x - \beta y) = \left(\delta - \beta \left(\frac{y}{x}\right)^q\right) dx = \frac{\delta x^q - \beta y^q}{x^q} dx.$$

Putting these three facts together, we get that

$$\begin{aligned} \left(g^{-1}\right)^* \omega_{i,j} &= \frac{(\delta x - \beta y)^i (-\gamma x + \alpha y)^j}{(\delta x - \beta y)^q} \frac{\delta x^q - \beta y^q}{x^q} dx \\ &= \frac{(\delta x - \beta y)^i (-\gamma x + \alpha y)^j}{x^q} dx, \end{aligned}$$

because $(\delta x - \beta y)^q = \delta x^q - \beta y^q$ since $\mathbb{F}$ has characteristic p and $\delta, \beta \in \mathbb{F}_q$. □

Now, let us consider the $\mathbb{F}[G]$-modules V^j defined in the statement of Theorem 0.1, i.e. V^j has basis $\{x^{j-i} y^i \mid 0 \leq i \leq j\}$ for $0 \leq j \leq q-2$, and $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G$ acts linearly by mapping $x^{j-i} y^i$ to $(\alpha x + \gamma y)^{j-i} (\beta x + \delta y)^i$.
The next result states that the $\mathbb{F}[G]$-module M can be expressed as a direct sum of the $\mathbb{F}[G]$-modules V^j.

Lemma 3.4. *The following isomorphism of $\mathbb{F}[G]$-modules holds.*

$$M \cong \bigoplus_{k=0}^{q-2} V^k$$

Proof. Let us define the degree of each $\omega_{i,j}$ as $i+j$. Then by Lemma 3.3, each $\omega_{i,j}$ is mapped to a sum of basis elements of degree $i+j$ under the action of an element of G. Therefore, if W^k is the $\mathbb{F}$-vector space with basis $\{\omega_{i,j} \mid i+j=k\}$ then $M \cong \oplus_{k=0}^{q-2} W^k$ as $\mathbb{F}[G]$-modules, because each W^k is stable under the action of G and the $\omega_{i,j}$ form a basis for M by Proposition 3.1.
Now, by definition, the $\mathbb{F}[G]$-module W^k is isomorphic to the dual of the $\mathbb{F}[G]$-module V^k. However, the $\mathbb{F}[G]$-module V^k is actually self-dual. Indeed, it is straightforward to verify that mapping a basis element $x^{k-i}y^i$ in V^k to $(-1)^i \frac{x^i y^{k-i}}{x^q} dx = (-1)^i \omega_{i,k-i}$ in W^k defines an isomorphism of $\mathbb{F}[G]$-modules between V^k and W^k when extended by $\mathbb{F}$-linearity.
Combining both paragraphs finishes the proof. □

Remark 3.5. Because each V^k is self-dual, we obtain that M is a self-dual $\mathbb{F}[G]$-module.

Remark 3.6. In [Bon12, Subsection 10.1.1], the author defines some $\mathbb{F}[\mathbf{G}]$-modules $\Delta(k)$ for $\mathbf{G} = SL_2\big(\mathbb{F}\big)$. It turns out that by definition, $\mathrm{Res}_G^{\mathbf{G}} \Delta(k) \cong V^k$ as $\mathbb{F}[G]$-modules. Therefore, Lemma 3.4 gives a geometric interpretation of the modules $\Delta(k)$.

3.2.2 Indecomposability of each summand

Now that we have a decomposition of M as a direct sum of $\mathbb{F}[G]$-modules, we want to show that each summand is indecomposable. It suffices to show that for a subgroup $H \leq G$, the restriction of V^k as an $\mathbb{F}[H]$-module is indecomposable. We will use this with the subgroup L of lower unitriangular matrices, which is isomorphic to the additive group of $\mathbb{F}_q$, itself isomorphic to the direct product of r copies of the cyclic group of order p. In what follows, we let $R = \mathbb{F}[L]$.

Lemma 3.7. *The following isomorphism of $\mathbb{F}$-algebras holds, hence R is local, i.e. every element of R is either nilpotent or a unit.*

$$R \cong \mathbb{F}[Y_1, \ldots, Y_r] / \big(Y_1^p, \ldots, Y_r^p\big)$$

Proof. Because L is isomorphic to r copies of C_p, we get a surjective ring homomorphism $\mathbb{F}[X_1, \ldots, X_r] \longrightarrow R$, mapping X_i to a generator of the i-th copy of C_p in L. The kernel is the ideal $\big(X_1^p - 1, \ldots, X_r^p - 1\big)$, which is $\big((X_1-1)^p, \ldots, (X_r-1)^p\big)$ because $\mathbb{F}$ has characteristic p. Therefore, by the first isomorphism theorem, we get

$$\begin{aligned} R &\cong \mathbb{F}[X_1, \ldots, X_r] / \big((X_1-1)^p, \ldots, (X_r-1)^p\big) \\ &\cong \mathbb{F}[X_1 - 1, \ldots, X_r - 1] / \big((X_1-1)^p, \ldots, (X_r-1)^p\big) \\ &\cong \mathbb{F}[Y_1, \ldots, Y_r] / \big(Y_1^p, \ldots, Y_r^p\big), \end{aligned}$$

where we defined $Y_i := X_i - 1$. All the isomorphisms above are $\mathbb{F}$-algebras isomorphisms, so $R \cong \mathbb{F}[Y_1, \ldots, Y_r]/\big(Y_1^p, \ldots, Y_r^p\big)$ as $\mathbb{F}$-algebras. The RHS has only one prime ideal, which is the one generated by the residue classes of $Y_1, \ldots, Y_r$. Therefore, an element of the RHS is either in the unique maximal ideal, and hence has zero p-th power, or is not in the maximal ideal, in which case it is a unit. By the established isomorphism, this statement then also holds for R. □

Lemma 3.8. *Any cyclic R-module is indecomposable.*

Proof. Let $N = \langle x \rangle$ be a cyclic R-module. Then the map taking $r \in R$ to $r \cdot x$ is a surjective R-module homomorphism, so by the first isomorphism theorem we get that $N \cong R/I$ as R-modules, for an ideal $I \subseteq R$. Identifying the two modules, we have that $\mathrm{End}_R(N) \cong \big(R/I\big)^{op}$ as R-algebras, via the map $\Psi : \mathrm{End}_R(N) \to R/I$ sending $\varphi \in \mathrm{End}_R(N)$ to $\varphi(1 + I)$, which is an isomorphism because an element of $\mathrm{End}_R(N)$ is completely determined by the image of $1 + I$. By Lemma 3.7, we know that any element of R is either a unit or nilpotent, so it follows that any element of R/I is either a unit or nilpotent too. Thus, any element of $\big(R/I\big)^{op}$ is either a unit or a nilpotent, and we conclude that any element of $\mathrm{End}_R(N)$ is either a unit or nilpotent. By [Alp86, Theorem 2, p. 22], N is an indecomposable R-module. □

Lemma 3.9. *Any R-submodule of R (i.e. any ideal of R) is indecomposable.*

Proof. Suppose that $N \subseteq R$ is an R-submodule. Then we obtain the dual R-module homomorphism induced by the inclusion $R^* \to N^*$, which is the restriction map. Now, dualising is an exact contravariant functor because every short exact sequence of vector spaces splits, so the functor $\mathrm{Hom}\,\big(-, \mathbb{F}\big)$ is right-exact, in addition to being left-exact anyway. Here, the short exact sequence is

$$0 \longrightarrow N \longrightarrow R \longrightarrow R/N \longrightarrow 0,$$

which, after taking duals, becomes

$$0 \longrightarrow \big(R/N\big)^* \longrightarrow R^* \longrightarrow N^* \longrightarrow 0,$$

so N^* is isomorphic (as R-modules) to a quotient of R^*. Now, by [Alp86, Lemma 2, p. 40] we know that $R \cong R^*$ as R-modules, so N^* is isomorphic (as R-modules) to a quotient of R. Thus, N^* is a cyclic R-module, which implies by Lemma 3.8 that N^* is indecomposable, hence N is indecomposable too. □

We can now prove that the restriction of the $\mathbb{F}[G]$-modules V^k from Theorem 0.1 as R-modules are indecomposable.

Proposition 3.10. *For all $0 \leq j \leq q - 2$, the R-module V^j is indecomposable.*

Proof. First, we notice that an element $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$ of L acts on a basis element $x^i y^{j-i}$ by mapping it to $(x+ay)^i y^{j-i}$, so by setting $y = 1$, we get an isomorphic R-module with basis $\{1, x, \ldots, x^j\}$ such that an element $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$ of L, which we will identify with $a \in \mathbb{F}_q$, acts on x^i by mapping it to $(x+a)^i$. We identify V^j with this last R-module.
Let us introduce the R-algebra $V := \mathbb{F}[x]/(x^q - x)$, such that $a \in L$ maps x to $x + a$. Then, because $(x+a)^q - (x+a) = x^q + a^q - x - a = x^q - x$ since $a^q = a$, the action of R on V is well-defined. Let $0 \leq j \leq q-2$. First, we can notice that there is an R-module homomorphism $V^j \longrightarrow V$, mapping x^i to $x^i + (x^q - x)$. This is indeed compatible with the actions of L by their definition. Also, suppose that $f_1, f_2 \in V^j$ with $f_1 \neq f_2$, such that $f_1 + (x^q - x) = f_2 + (x^q - x)$. Then $x^q - x | f_2 - f_1$, but $f_2 - f_1$ is a non-zero element of V^j, so it has degree less or equal than j, itself being strictly less than q, which is a contradiction. Thus, the R-module homomorphism is injective, so V^j is isomorphic (as R-module) to an R-submodule of V.
Now, we want to show that $V \cong R$ as R-modules. Firstly, notice that $x^q - x$ splits over $\mathbb{F}_q$ by definition, and we get $x^q - x = \prod_{b \in \mathbb{F}_q} (x - b)$. Because two distinct factors are coprime, we get by the Chinese remainder theorem that the following map is an $\mathbb{F}$-algebra isomorphism.

$$\begin{aligned} V &\longrightarrow \prod_{b \in \mathbb{F}_q} \mathbb{F}[x]/(x-b) \\ f + (x^q - x) &\longmapsto \big(f + (x-b)\big)_{b \in \mathbb{F}_q} \end{aligned}$$

If $a \in L$, then an element $f + (x^q - x) \in V$ is mapped to $f(x+a) + (x^q - x)$, and an element $\big(f_b + (x-b)\big)_{b \in \mathbb{F}_q} \in \prod_{b \in \mathbb{F}_q} \mathbb{F}[x]/(x-b)$ is defined to be mapped to $\big(f_b(x+a) + (x-b)\big)_{b \in \mathbb{F}_q}$ under the action of a. Thus, the isomorphism becomes an R-module isomorphism.
Secondly, the following map is also an $\mathbb{F}$-vector space isomorphism, because the map is componentwise an isomorphism.

$$\begin{aligned} \prod_{b \in \mathbb{F}_q} \mathbb{F}[x]/(x-b) &\longrightarrow \prod_{b \in \mathbb{F}_q} \mathbb{F} \\ \big(f_b + (x-b)\big)_{b \in \mathbb{F}_q} &\longmapsto \big(f_b(b)\big)_{b \in \mathbb{F}_q} \end{aligned}$$

We can observe that $a \in L$ maps $\big(f_b + (x-b)\big)_{b \in \mathbb{F}_q}$ to $\big(f_b(x+a) + (x-b)\big)_{b \in \mathbb{F}_q}$, which is itself equal to $\big(f_b(b+a) + (x-b)\big)_{b \in \mathbb{F}_q}$. Therefore, defining the action of

$a \in L$ on the RHS as mapping an element $\big(\zeta_b\big)_{b\in\mathbb{F}_q} \in \prod_{b\in\mathbb{F}_q} \mathbb{F}$ to $\big(\zeta_{b+a}\big)_{b\in\mathbb{F}_q}$ turns the $\mathbb{F}$-vector space isomorphism into an R-module isomorphism.
Thirdly, we show that the following map is an R-module isomorphism, where $\tilde{R} = R$ as $\mathbb{F}$-vector spaces of basis $\{[b]|b \in \mathbb{F}_q\}$, but the action of an element $a \in L$ is defined to be $a \cdot \sum_{b\in\mathbb{F}_q} \zeta_b[b] = \sum_{b\in\mathbb{F}_q} \zeta_b[b-a]$.

$$\begin{aligned} \prod_{b\in\mathbb{F}_q} \mathbb{F} &\longrightarrow R \\ \big(\zeta_b\big)_{b\in\mathbb{F}_q} &\longmapsto \sum_{b\in\mathbb{F}_q} \zeta_b[b] \end{aligned}$$

Because $\{[b]|b \in \mathbb{F}_q\}$ is a basis for both $\mathbb{F}$-vector spaces, this map is an $\mathbb{F}$-vector space isomorphism. Therefore, we need to show that it is compatible with the action of L on both sides. For an element $a \in L$, $\big(\zeta_{b+a}\big)_{b\in\mathbb{F}_q}$ is mapped to $\sum_{b\in\mathbb{F}_q} \zeta_{b+a}[b]$ which, after a change of index, is equal to $\sum_{b\in\mathbb{F}_q} \zeta_b[b-a]$. Therefore, the map is an R-module isomorphism.
Fourthly and finally, the following map is an R-module isomorphism.

$$\begin{aligned} \tilde{R} &\longrightarrow R \\ \sum_{b\in\mathbb{F}_q} \zeta_b[b] &\longmapsto -\sum_{b\in\mathbb{F}_q} \zeta_b[b] \end{aligned}$$

By composing the four maps, we get that $V \cong R$ as R-modules.
We finally get that V^j is isomorphic (as R-modules) to an R-submodule of R. By Lemma 3.9, we obtain that V^j is indecomposable as R-module. □

Now, we have all the tools we need in order to prove Theorem 0.1.

Proof of Theorem 0.1. By Lemma 3.4 we know that $M \cong \oplus_{j=0}^{q-2} V^j$, and by Proposition 3.10 each one of the V^j is indecomposable as an $\mathbb{F}[L]$-module. This implies that each one of the V^j is indecomposable as an $\mathbb{F}[G]$-module, because the restriction of a direct sum of modules is the direct sum of the restrictions. □

Corollary 3.11. *The $\mathbb{F}[G]$-module M is semi-simple if and only if $q = p$.*

Proof. By Remark 3.6, $\mathrm{Res}_G^{\mathbf{G}} \Delta(k) \cong V^k$ as $\mathbb{F}[G]$-modules, for the $\mathbb{F}[\mathbf{G}]$-modules defined in [Bon12, Subsection 10.1.1] where $\mathbf{G} = SL_2\big(\mathbb{F}\big)$.
We use the classification of the simple $\mathbb{F}[G]$-modules from [Bon12, Theorem 10.1.8]. For $n \in \mathbb{N}$, define $I(n) = \{m \in \mathbb{N} \mid m_j \leq n_j \ \forall j \geq 0\}$ where $n = \sum_{j=0}^{\infty} n_j p^j$ and $m = \sum_{j=0}^{\infty} m_j p^j$ are the expansions in base p. Then for each $0 \leq j \leq q-2$, the

indecomposable $\mathbb{F}[G]$-module V^j is simple if and only if $I(j) = \{0, 1, 2, \ldots, j\}$. Now, $I(j) = \{0, 1, 2, \ldots, j\}$ for all $0 \leq j \leq p-2$, so M is semi-simple if $q = p$. However, if $q > p$ then V^p appears as a summand in the decomposition of M. It is easy to see that $1 \notin I(p)$, therefore V^p is not simple, and hence M is not semi-simple. $\square$

Conclusion

In this thesis, we managed to solve the following problem "*Given a curve and a finite group acting on it, compute the decomposition of the canonical representation as a direct sum of subrepresentations*" for the Drinfeld curves with an action of the finite group $SL_2(\mathbb{F}_q)$. The difficulty lied in the facts that we were in the presence of wild ramification, and $SL_2(\mathbb{F}_q)$ has cyclic Sylow p-subgroups if and only if $q = p$ is a prime. In order to solve the problem, we first focused on the case where $q = p$ is a prime, because we could use the recent paper [BCK20] which provides an algorithm to compute the decomposition in this case. Then, we solved the problem for a general prime power q by computing a concrete basis for the canonical representation as an $\mathbb{F}$-vector space, and by studying the action of $SL_2(\mathbb{F}_q)$ on it. From the latter, we could identify a decomposition and prove that each summand was indecomposable using techniques from modular representation theory.

Bibliography

[Alp86] J. L. Alperin. *Local representation theory.* Cambridge University Press, 1986.

[BCK20] F. M. Bleher, T. Chinburg, and A. Kontogeorgis. Galois structure of the holomorphic differentials of curves. *Journal of Number Theory*, 216:1–68, 2020.

[Bon12] C. Bonnafé. *Representations of $SL_2(\mathbb{F}_q)$.* Springer, 2012.

[CR81] C.W. Curtis and I. Reiner. *Methods of Representation Theory*, volume 2 of *A Wiley-Interscience publication.* Wiley, 1981.

[CWH34] C. Chevalley, A. Weil, and E. Hecke. Über das Verhalten der Integrale 1. Gattung bei Automorphismen des Funktionenkörpers. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 10(1):358–361, 1934.

[Ful69] W. Fulton. *Algebraic Curves. An introduction to Algebraic Geometry.* Addison-Wesley, 1969.

[Hal15] John Halliday. The Riemann-Roch theorem and Serre duality. `https://math.uchicago.edu/~may/REU2015/REUPapers/Halliday.pdf`, 2015.

[Har97] R. Hartshorne. *Algebraic geometry.* Springer, 1997.

[Hec28] E. Hecke. Über ein Fundamentalproblem aus der Theorie der elliptischen Modulfunktionen. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 6(1):235–257, 1928.

[Hig54] D. G. Higman. Indecomposable representations at characteristic p. *Duke Mathematical Journal*, 21(2):377–381, 1954.

[Kan86] E. Kani. The Galois-module structure of the space of holomorphic differentials of a curve. *Journal fur die Reine und Angewandte Mathematik*, 1986(367):187–206, 1986.

[KK13] S. Karanikolopoulos and A. Kontogeorgis. Representation of cyclic groups in positive characteristic and Weierstrass semigroups. *Journal of Number Theory*, 133(1):158–175, 2013.

[Kö04] B. Köck. Galois structure of Zariski cohomology for weakly ramified covers of curves. *American Journal of Mathematics*, 126(5):1085–1107, 2004.

[LK21] Lucas Laurent and Bernhard Köck. The canonical representation of the Drinfeld curve. `https://arxiv.org/abs/2108.05286`, 2021.

[Nak86] S. Nakajima. Galois module structure of cohomology groups for tamely ramified coverings of algebraic varieties. *Journal of Number Theory*, 22(1):115–123, 1986.

[Sho94] V. V. Shokurov. *Algebraic geometry I: algebraic curves, algebraic manifolds, and schemes*, volume 23 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, 1994.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*. Springer, 2009.

[Tai14] Joseph Tait. *Group actions on differentials of curves and cohomology bases of hyperelliptic curves*. PhD thesis, University of Southampton, November 2014.

[VM81] R. Valentini and M. Madan. Automorphisms and holomorphic differentials in characteristic p. *Journal of Number Theory*, 13(1):106–115, 1981.