The canonical representation of the Drinfeld curve

LUCAS LAURENT and BERNHARD KÖCK

Abstract

If $C$ is a smooth projective curve over an algebraically closed field $F$ and $G$ is a group of automorphisms of $C$, the canonical representation of $C$ is given by the induced $F$-linear action of $G$ on the vector space $H^0(C, \Omega_C)$ of holomorphic differentials on $C$. Computing it is still an open problem in general when the cover $C \to C/G$ is wildly ramified. In this paper, we fix a prime power $q$, we consider the Drinfeld curve, i.e., the curve $C$ given by the equation $XY^q - X^qY - Z^q + 1 = 0$ over $\mathbb{F} = \mathbb{F}_q$ together with its standard action by $G = \text{SL}_2(\mathbb{F}_q)$, and decompose $H^0(C, \Omega_C)$ as a direct sum of indecomposable representations of $G$, thus solving the aforementioned problem in this case.

1 Introduction

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

This problem has been introduced by Hecke in 1928 [Hec28], and it has been solved in 1934 by Chevalley and Weil [CWH34] in the case the characteristic of $F$ does not divide the order of $G$. If in contrast the characteristic $p$ of $F$ does divide the order of $G$, then $H^0(C, \Omega_C)$ is a modular representation, and this problem becomes notoriously hard, one reason being that already for fairly small groups listing the indecomposable representations is a formidable problem.
However, some progress has been made. In 1986, Nakajima [Nak86] and Kani [Kan86] independently computed this representation for an arbitrary finite group of automorphisms $G$ of $C$, in the case where the cover $C \to C/G$ is at most tamely ramified. Moreover, most of the theorems leading to Kani’s and Nakajima’s result have been generalised in [Kö04] to the so-called weakly ramified case, the simplest but, in a sense, most frequent form of wild ramification.

On the other hand, restricting the type of the group $G$ rather than the ramification of $C \to C/G$ has lead to some progress as well. Indeed, Valentinì and Madan [VM81] solved the problem for $G$ a cyclic $p$-group. Karanikolopoulos and Kontogeorgis [KK13] extended this result to an arbitrary cyclic group $G$. Moreover, Bleher, Chinburg, and Kontogeorgis [BCK20] gave an algorithm to solve the problem in the case when $G$ 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]. Further results in this context have been obtained by Rzedowski-Calderón, Villa-Salvador and Madan in [RCVSM96] and [RCVSM00], by Marques and Ward in [MW18], by Garnek in [Gar23] and by Bleher and Camacho in [BC23].

The object of this paper is to find the decomposition of $H^0(C, \Omega_C)$ as a direct sum of indecomposable $F[G]$-modules when $G = SL_2(F_q)$, $q = p^r$ for some $r \geq 1$, $F = F_q$, and $C$ is the Drinfeld curve together with the action of $G$ as presented in Section 2. The precise result is stated in Theorem 2.1. Note that because the Sylow $p$-subgroups of $G$ are isomorphic to the additive group of $F_q$, we can apply the algorithm from [BCK20] if, and only if, $r = 1$. In that paper, the authors give a formula for the decomposition of $\text{Res}^G_H H^0(C, \Omega_C)$ 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. Conlon’s induction theorem [CR87, Corollary 80.51] implies that the $F[G]$-module structure of $H^0(C, \Omega_C)$ is completely determined by this. This procedure has led to a first proof of Theorem 2.1 in the case $r = 1$, see [Lau21, Chapter 2].

In order to prove Theorem 2.1 for an arbitrary $r \geq 1$, we however use the following very different approach. In Section 3 we first compute an explicit basis of the vector space $H^0(C, \Omega_C)$ over $F$. Then from the action of $G$ on this basis, we find a decomposition of the $F[G]$-module $H^0(C, \Omega_C)$ in Section 4 which has been inspired by the case $r = 1$. From [Bon11, Corollary 10.1.5] we obtain that each summand in this decomposition is indecomposable.

Acknowledgements. The second author thanks Adriano Marmora for early, extensive and insightful discussions about the general theme of this
paper where the specific problem underlying this paper has arisen. The authors also thank Peter Kropholler for his continued interest in our research. Finally, the authors thank the referees for carefully reading the paper and for their constructive comments, particularly for pointing out that the just mentioned indecomposability can be easily derived from the literature.

2 Preliminaries about the Drinfeld curve and statement of main result

In this section, we introduce some notations and facts about the Drinfeld curve and state our main result.

Throughout, we fix an algebraically closed field \( \mathbb{F} \) of characteristic \( p > 0 \) and a power \( q = p^r \) of \( p \). The Drinfeld curve \( C \) is then defined as the zero locus in \( \mathbb{P}^2(\mathbb{F}) \) of the homogeneous polynomial

\[
XY^q - X^qY - Z^{q+1},
\]

which is the compactification of the affine curve \( C_Z \) defined by \( xy^q - x^qy - 1 \). This curve has \( q + 1 \) points at infinity defined by \( XY^q - X^qY = 0 \), which are the points \([x : y : 0]\) where \( x, y \in \mathbb{F}_q \). As seen in [Bon11, Propositions 2.1.1 and 2.4.1], the projective curve \( C \) is smooth and irreducible. Usually, we will simply write

\[
M := H^0(C; \Omega_C)
\]

for the vector space over \( \mathbb{F} \) of holomorphic differentials on \( C \). By definition, \( M \) has dimension \( g(C) \), the genus of \( C \), which by the genus-degree formula is \( g(C) = \frac{q(q-1)}{2} \) [Bon11, Subsection 2.5.1]. We denote the function field of \( C \) by \( \mathbb{F}(C) \).

We view \( \mathbb{F}_q \) as the unique subfield of \( \mathbb{F} \) containing \( q \) elements. For \( g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G := SL_2(\mathbb{F}_q) \) and \([x : y : z] \in C \), we then define

\[
g \cdot [x : y : z] := [\alpha x + \beta y : \gamma x + \delta y : z].
\]

It is straightforward to verify that the map

\[
G \times C \longrightarrow C, \quad (g, [x : y : z]) \longmapsto g \cdot [x : y : z]
\]

defines a left action of \( G \) on the algebraic curve \( C \). Pulling back differentials finally defines a right action of \( G \) on \( M \) which is called the canonical representation of \( C \) and which is the object of study of this paper. Our main result, see [Theorem 2.1] below, computes this modular representation.
We view the elements of $\mathbb{F}^2$ as row vectors and consider the standard right action of $G = SL_2(\mathbb{F}_q)$ on $\mathbb{F}^2$. For $k \geq 0$, let $V^k$ denote the $k^{th}$ symmetric power $\text{Sym}^k(\mathbb{F}^2)$ of $\mathbb{F}^2$ together with its induced action of $G$.

**Theorem 2.1.** We have the following decomposition of $H^0(C, \Omega_C)$ into indecomposable $\mathbb{F}[G]$-modules:

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

In particular, the $\mathbb{F}[G]$-module $H^0(C, \Omega_C)$ is semi-simple if and only if $q = p$.

**Proof.** Establishing this isomorphism of $\mathbb{F}[G]$-modules, see Corollary 4.2, is the object of the remaining two sections of this paper.

If $0 \leq k \leq q-1$, then, by Remark 4.3 below and [Bon11, Corollary 10.1.5], the intersection of all non-zero $\mathbb{F}[G]$-submodules of $V^k$ is non-zero; in particular, $V^k$ is indecomposable.

Furthermore, if $q = p$, the $\mathbb{F}[G]$-modules $V^0, \ldots, V^{p-1}$ are simple by [Alp86, p. 15–16]. (In fact, they form a full set of non-isomorphic simple $\mathbb{F}[G]$-modules). On the other hand, if $q > p$, then $V^p$ is not simple; this follows for example from [Bon11, Theorem 10.1.8].

### 3 A basis of the space of global holomorphic differentials

The goal of this section is to exhibit an explicit basis of the vector space $M$. First, we identify a local parameter at each point of $C$. These will be used to verify that certain differentials on $C$ are holomorphic.

**Lemma 3.1.** 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 $[x_0 : y_0 : z_0] \in C_Z$. Let $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ denote the two standard coordinates on the affine chart $C_Z$. Then $P$ becomes
Proposition 3.2. For example with basis \( dx \), let the coordinates \( s \). Finally, if \( y_0 \neq 0 \), we choose \( x - x_0 = \frac{x}{x_0} - \frac{y}{y_0} \).

Now, suppose that \( z_0 = 0 \). Then either \( x_0 \neq 0 \) or \( y_0 \neq 0 \). If \( x_0 \neq 0 \), we use the coordinates \( s = \frac{x}{x_0} \) and \( t = \frac{y}{y_0} \) and write \( P \) as \( (s_0, t_0) := \left( \frac{m_i}{m_j}, 0 \right) \). Since \( s^q - s - t^{q+1} = 0 \) and \( s_0 \in \mathbb{F}_q \), we obtain

\[
\begin{align*}
\omega_{i,j} &:= \frac{x^i y^j}{x^q dx} \\
\text{Then each } \omega_{i,j} \text{ is holomorphic on the whole of } C, \text{ i.e., } \omega_{i,j} \in M, \text{ and the set } \\
\{ \omega_{i,j} \mid 0 \leq i, j \leq q - 2, \ i + j \leq q - 2 \} \text{ is a basis of } M \text{ over } \mathbb{F}.
\end{align*}
\]

**Proof.** We will first show that each \( \omega_{i,j} \) is in \( M \). It then suffices to show that they are linearly independent over \( \mathbb{F} \) because the dimension of \( M \) is \( g(C) = \frac{(q-1)q}{2} \) which is easily seen to be equal to the number of \( \omega_{i,j} \).
We know, if \( t \) is a local parameter at any \( P \in C \), then the meromorphic differential \( fdt \) is regular at \( P \) if, and only if, the rational function \( f \) is regular at \( P \) [Har77, Section IV.2]. Let now \( 0 \leq i, j \leq q - 2 \) such that \( i + j \leq q - 2 \), and let \( P = [x_0 : y_0 : z_0] \in C \). Suppose first that \( z_0 \neq 0 \). Then, because \( x - \frac{x_0}{z_0} \) is a local parameter at \( P \) by Lemma 3.1 and because \( dx = d(x - \frac{x_0}{z_0}) \), we simply need to verify that \( \frac{x^q}{x^q} \) is a regular function at \( P \). This is the case because the value \( \frac{x_0}{z_0} \) of \( x \) at \( P \) is non-zero because \( \frac{x_0}{z_0} \left( \frac{w}{z_0} \right)^q - \left( \frac{x_0}{z_0} \right)^q \frac{w}{z_0} = 1 \). Therefore, \( \omega_{i,j} \) is holomorphic on \( C_Z \). Now, suppose that \( z_0 = 0 \) and \( x_0 \neq 0 \), and let \( s = \frac{x}{y}, t = \frac{z}{y} \) as in the proof of Lemma 3.1. Then \( x = \frac{s}{t} \) and \( y = \frac{s}{t} \), so the following holds in \( \Omega_{F(C)/\mathbb{F}} \).

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

As above, because \( w \) is a local parameter at \( P \) by Lemma 3.1 and because \( -w^{q-(i+j)} v^q \) 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 \( \mathbb{F} \). Let \( \lambda_{i,j} \in \mathbb{F} \) such that \( \sum_{i,j} \lambda_{i,j} \omega_{i,j} = 0 \) in \( M \). Then

\[
\left( \sum_{i,j} \lambda_{i,j} x^i y^j \right) \frac{1}{x^q} dx = \sum_{i,j} \lambda_{i,j} x^i y^j \frac{1}{x^q} dx = 0 \quad \text{in} \quad \Omega_{F(C)/\mathbb{F}}
\]

and hence \( f(x, y) := \sum_{i,j} \lambda_{i,j} x^i y^j = 0 \) in \( \mathbb{F}(C) \). Therefore, the affine variety \( C_Z \) is a subset of the zero locus of \( f(x, y) \) in \( \mathbb{A}^2(\mathbb{F}) \), which implies by Hilbert’s Nullstellensatz that

\[
f(x, y) \in \text{Rad}(f(x, y)) \subseteq \text{Rad}(xy^q - x^q y - 1) = (xy^q - x^q y - 1),
\]

where the last equality holds because \( xy^q - x^q y - 1 \) is an irreducible polynomial in \( \mathbb{F}[x, y] \) by [Bon11, Proposition 2.1.1]. Hence \( xy^q - x^q y - 1 \) divides
\( f(x, y) \) in \( \mathbb{F}[x, y] \), which can only happen if \( f(x, y) = 0 \) in \( \mathbb{F}[x, y] \) because otherwise \( f(x, y) \) is of finite total degree at most \( q - 2 \). Therefore, the \( \omega_{i,j} \) are linearly independent.

**Remark 3.3.** The differentials \( \omega_{i,j} \) defined in Proposition 3.2 have the following vanishing order at \( P = [x_0 : y_0 : z_0] \in C \).

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

This follows from the proof above and the fact that

\[
\text{ord}_P(s) = \min \{ \text{ord}_P(s^q), \text{ord}_P(s) \} = \text{ord}_P(s^q - s) = \text{ord}_P(t^{q+1}) = q + 1
\]

if \( P = [1 : 0 : 0] \) and similarly that \( \text{ord}_P(v) = q + 1 \) if \( P = [0 : 1 : 0] \).

4 The decomposition of \( M \) as an \( \mathbb{F}[G] \)-module

By the Krull-Schmidt theorem, \( M \) has a decomposition as a direct sum of indecomposable right \( \mathbb{F}[G] \)-modules which are unique up to isomorphism and permutation. The goal of this section is to find these indecomposable \( \mathbb{F}[G] \)-modules and their multiplicity.

First, we compute the action of an element of \( G \) on the basis of \( M \) given in Proposition 3.2.

**Lemma 4.1.** 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

\[
g^*(\omega_{i,j}) = \frac{(\alpha x + \beta y)^i(\gamma x + \delta y)^j}{x^q}dx.
\]

**Proof.** We have \( g^*(x) = \alpha x + \beta y \) and \( g^*(y) = \gamma x + \delta y \). Using the fact that \( \frac{1}{x}dx = \frac{1}{y}dy \) as in the proof of Proposition 3.2, this implies that

\[
g^*(dx) = d(\alpha x + \beta y) = \left( \alpha + \beta \left( \frac{y}{x} \right)^q \right) dx = \frac{\alpha x^q + \beta y^q}{x^q}dx.
\]
Putting these facts together, we obtain that
\[ g^* (\omega_{i,j}) = \frac{(\alpha x + \beta y)^i (\gamma x + \delta y)^j}{(\alpha x + \beta y)^q} \alpha x^q + \beta y^q x^q dx \]
\[ = \frac{(\alpha x + \beta y)^i (\gamma x + \delta y)^j}{x^q} dx, \]
as was to be shown.

The next result states that the \( \mathbb{F}[G] \)-module \( M \) can be expressed as a direct sum of the \( \mathbb{F}[G] \)-modules \( V^k = \text{Sym}^k(\mathbb{F}_q^2) \), \( k = 0, \ldots, q-2 \); these are obviously not isomorphic to each other and indecomposable as we’ve seen in the proof of Theorem 2.1.

**Corollary 4.2.** 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 4.1, each \( \omega_{i,j} \) is mapped to a sum of basis elements of degree \( i + j \) under the action of any element of \( G \). Therefore, if \( W^k \) is the subspace of \( M \) with basis \( \{ \omega_{i,j} \mid i + j = k \} \) then \( M \cong \bigoplus_{k=0}^{q-2} W^k \) as \( \mathbb{F}[G] \)-modules, because each \( W^k \) is stable under the action of \( G \) and the \( \omega_{i,j} \) form a basis of \( M \) by Proposition 3.2. Furthermore, by Lemma 4.1, mapping \( \omega_{i,j} \) to \((1,0)^i \cdot (0,1)^j \) in \( \text{Sym}^k(\mathbb{F}_q^2) = V^k \) evidently defines an isomorphism of right \( \mathbb{F}[G] \)-modules. Combining these two facts finishes the proof.

**Remark 4.3.** Let \( G = SL_2(\mathbb{F}) \) and consider the standard left action of \( G \) on \( \mathbb{F}^2 \). Then, the left \( \mathbb{F}[G] \)-modules \( \Delta(k) := \text{Sym}^k(\mathbb{F}^2) \), \( k \geq 0 \), play a crucial role in [Bon11, Section 10]. Furthermore, let the right \( \mathbb{F}[G] \)-module \( \hat{\Delta}(k) \) be obtained from the left \( \mathbb{F}[G] \)-module \( \Delta(k) \) via transposition on \( G \). We then have \( \text{Res}_G \Delta(k) \cong V^k \). In particular, Corollary 4.2 gives a geometric realisation of the modules \( \text{Res}_G \hat{\Delta}(k) \), thus extending the geometric viewpoint omnipresent in [Bon11].

**References**

[Alp86] J. L. Alperin. *Local representation theory*, volume 11 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986.

[BC23] Frauke M. Bleher and Nicholas Camacho. Holomorphic differentials of Klein four covers. *J. Pure Appl. Algebra*, 227(10):27pp, 2023.
[BCK20] Frauke M. Bleher, Ted Chinburg, and Aristides Kontogeorgis. Galois structure of the holomorphic differentials of curves. *J. Number Theory*, 216:1–68, 2020.

[Bon11] Cédric Bonnafé. *Representations of SL_2(F_q)*, volume 13 of *Algebra and Applications*. Springer-Verlag London, Ltd., London, 2011.

[CR87] Charles W. Curtis and Irving Reiner. *Methods of representation theory. Vol. II*. Pure and Applied Mathematics (New York). John Wiley & Sons, Inc., New York, 1987.

[CWH34] C. Chevalley, A. Weil, and E. Hecke. Über das Verhalten der Integrale 1. Gattung bei Automorphismen des Funktionenkörpers. *Abh. Math. Sem. Univ. Hamburg*, 10(1):358–361, 1934.

[Gar23] Jędrzej Garnek. p-group Galois covers of curves in characteristic p. *Trans. Amer. Math. Soc.*, 376(8):5857–5897, 2023.

[Har77] Robin Hartshorne. *Algebraic geometry*, volume No. 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1977.

[Hec28] E. Hecke. Über ein Fundamentalproblem aus der Theorie der elliptischen Modulfunktionen. *Abh. Math. Sem. Univ. Hamburg*, 6(1):235–257, 1928.

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

[Kö04] Bernhard Köck. Galois structure of Zariski cohomology for weakly ramified covers of curves. *Amer. J. Math.*, 126(5):1085–1107, 2004.

[Kan86] E. Kani. The Galois-module structure of the space of holomorphic differentials of a curve. *J. Reine Angew. Math.*, 1986(367):187–206, 1986.

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

[Lau21] Lucas P. Laurent. The canonical representation of the Drinfeld curve. *MPhil thesis, University of Southampton*, 2021.

[MW18] Sophie Marques and Kenneth Ward. Holomorphic differentials of certain solvable covers of the projective line over a perfect field. *Math. Nachr.*, 291(13):2057–2083, 2018.

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

[RCVSM96] Martha Rzedowski-Calderón, Gabriel Villa-Salvador, and Manohar L. Madan. Galois module structure of holomorphic differentials in characteristic p. *Arch. Math. (Basel)*, 66(2):150–156, 1996.

[RCVSM00] Martha Rzedowski-Calderón, Gabriel Villa-Salvador, and Manohar L. Madan. Galois module structure of holomorphic differentials. *Bull. Austral. Math. Soc.*, 62(3):493–509, 2000.

[VM81] Robert C. Valentini and Manohar L. Madan. Automorphisms and holomorphic differentials in characteristic p. *J. Number Theory*, 13(1):106–115, 1981.