UNIVERSITY OF SOUTHAMPTON

Faculty of Social and Human Sciences
Mathematical Sciences

Group actions on differentials of curves and cohomology bases of hyperelliptic curves

by

Joseph J. Tait

A thesis submitted in partial fulfillment for the
degree of Doctor of Philosophy

November 2014

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF SOCIAL AND HUMAN SCIENCES
MATHEMATICAL SCIENCES

Doctor of Philosophy

Group actions on differentials of curves and cohomology bases of hyperelliptic curves

by Joseph J. Tait

In this thesis we consider the natural action of a subgroup G of the automorphism group of an algebraic curve on spaces of differentials and similar algebraic structures. We focus on curves over an algebraically closed field k of characteristic $p > 0$, and in particular on cases where p divides the order of the group G. There is also an emphasis on explicit examples and concrete computations throughout the thesis.

After covering background material about smooth projective curves we remind the reader of the details of hyperelliptic curves. Given a hyperelliptic curve X, we present an explicit basis for $H^0(X, \Omega_X^{\otimes m})$, the space of global polydifferentials of degree m.

We apply our study of hyperelliptic curves by computing bases of $H^1(X, \mathcal{O}_X)$ and the first de Rham cohomology group of X, $H^1_{\mathrm{dR}}(X/k)$. We make these computations via Čech cohomology, and use them to determine the action of a specific automorphism τ of order p on $H^1_{\mathrm{dR}}(X/k)$. We then show that the natural short exact sequence of $k[\langle\tau\rangle]$-modules

$$0 \to H^0(X, \Omega_X) \to H^1_{\mathrm{dR}}(X) \to H^1(X, \mathcal{O}_X) \to 0$$

does not split if X is ramified above ∞. We also give a Mittag-Leffler style theorem for hyperelliptic curves.

We finally consider the question of when G acts faithfully on the space $H^0(X, \Omega_X^{\otimes m})$, for any smooth projective curve X. We give a complete and concise answer to this question, as well as extending the result to general Riemann-Roch spaces $H^0(X, \mathcal{O}_X(D))$ where D is a G-invariant divisor of degree at least $2g_X - 2$. Lastly, we use our earlier work for hyperelliptic curves to elucidate the main theorem.

Contents

Academic Thesis: Declaration of Authorship

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

Title of thesis: Group actions on differentials of curves and cohomology bases of hyperelliptic curves.

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 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 works of others, this has always been 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 or jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
7. The majority of the work in Chapter 5, and parts of Chapter 2, have been published in *Faithfulness of actions on Riemann-Roch spaces*, to appear in the Canadian Journal of Mathematics. None of the other work has been published before submission.

Signed:

Date:

Acknowledgements

I would first and foremost like to thank my supervisor, Bernhard Köck, for his great guidance and patience, both in matters of mathematics and style. He has always afforded the greatest amount of time and care in reading and annotating work, and especially in considering how mathematics may be extended and presentation improved. Lastly, I would like to thank Bernhard for never letting anyone else know that his understanding of my native language is clearly greater than mine. I would further like to thank both Gareth Jones and David Singerman for mathematical discussions.

My office mates have been a great source of inspiration, and have made the last four years incredibly interesting, enjoyable and in no way predictable. In particular, I would like to mention Alex Bailey, Matt Burfitt, Chris Cave, Charles Cox, Tyrone Cutler, Max Fennelly, Michal Ferov, Martin Finn-Sell, Martin Fluch, Robin Frankhuizen, Giovanni Gandini, Tom Harris, Pip Hiscock, Ana Khukhro, David Matthews, Ingrid Membrillo-Solis, Raffaele Rainone, Amin Saied, Yafet Sanchez-Sanchez, Rob Snocken, Simon St. John-Green, Ed Tye, Mike West and Michaele Zordan. I would also like to thank Vesna Perisic for many an enjoyable teaching session, and Alex Stasinski for many enlightening chats about both ale and maths.

I would like to thank my sister and mother for their support, being available to discuss anything and for many good laughs. I would like to thank Laur for her encouragement, for believing in me and for many kind words. And, of course, thank you to Abby, Dotty and JP for their concern and interest, no matter how hard it may be to detect.

Finally, I would like to thank EPSRC for providing funding for my PhD.

Nomenclature

$\lfloor D \rfloor$	The divisor D after applying the floor function applied to each coefficient
$\langle a \rangle$	Fractional part of $a \in \mathbb{R}$
$\langle -,- \rangle$	Serre duality pairing
$\mathbb{A}^1_k$	Affine line over k
$\mathrm{Aut}(X)$	Automorphism group of X
$\check{d}$	Čech cohomology differential
D	Divisor
$\mathrm{div}(f)$; $\mathrm{div}(\omega)$	The divisor of a function or differential
$\mathrm{Div}(X)$	Space of divisors on X
$\deg(D)$	Degree of the divisor D
δ_P	Different exponent at the point P
e_P	Ramification index at the point P
g_X	Genus of the curve X
G	Subgroup of the automorphism group of a curve
$G_i(P)$	The i^{th} ramification group at the point P
$H^0(X,\Omega_X)$	Space of global holomorphic differentials on X
$H^0(X,\Omega_X(D))$	Space of differentials associated to the divisor D on X
$H^0(X,\mathcal{O}_X(D))$	Space of meromorphic functions associated to the divisor D on X
$H^0(X,\Omega_X^{\otimes m})$	Space of global holomorphic polydifferentials of degree m on X
$H^1(X,\mathcal{O}_X)$	First cohomology group of $\mathcal{O}_X$
$\check{H}^n(\mathcal{U})$	The n^{th} Čech cohomology group corresponding to the cover $\mathcal{U}$
$H^1_{\mathrm{dR}}(X/k)$	The first algebraic de Rham cohomology group of X
k	Algebraically closed field of characteristic $p \geq 0$
K_X	Canonical divisor on X
$K(X)$	Function field of X
$\underline{K}(X)$	Constant sheaf of $K(X)$
M^G	Subspace of M fixed by G
$\mathcal{M}_{X,P}$	Maximal ideal of $\mathcal{O}_{X,P}$
$\mathrm{ord}_P(f)$; $\mathrm{ord}_P(\omega)$	Order at the point P of a function or differential
$\mathcal{O}_X$	Sheaf of rational functions on X

$\mathcal{O}_{X,P}$	Ring of functions that are regular at the point P
Ω_X	Sheaf of differentials on X
$\Omega_X^{\otimes m}$	Sheaf of polydifferentials of degree m
$\Omega_{K(X)}$	Module of differentials of $K(X)$
$\underline{\Omega}_{K(X)}$	Constant sheaf of $\Omega_{K(X)}$
ω	Differential
P, P', P_a	Points on X
$\mathbb{P}_k^1$	Projective line over k
π	Projection map from X to the quotient curve X/G
π^*	Associated map between function fields $K(Y)$ and $K(X)$
π_*	Push forward map from $\mathrm{Div}(X)$ to $\mathrm{Div}(Y)$
Q, Q', Q_a	Points on Y
R	Ramification divisor
X	Projective smooth curve over k

To no-one…

Chapter 1

Introduction

Geometry and topology provide perhaps the greatest source of both intuition and vision in mathematics, whilst algebra balances the scales, being the exemplar of precision and abstraction. A most compelling example of the interplay between these two areas is the triple equivalence of Riemann surfaces, complex function fields and complex curves. On the one hand, compact Riemann surfaces constitute all spaces that occur in the topological classification of connected, compact, orientable surfaces. On the other hand, complex function fields lie strongly in the algebraic end of the spectrum, with strong relations to number theory and Galois theory. Finally, it is algebraic curves that most clearly unites algebra and geometry.

The genus is arguably the most important invariant of topological surfaces. It is possible to use it to define the Euler characteristic, and it also benefits from being very easy to describe — the genus of a connected, compact, orientable surface is just the number of "holes" or "handles" it has. Given this, any theory that claims to be equivalent to the study of Riemann surfaces would do well to explain how it gives rise to the concept of genus.

In the case of algebraic curves, it is Riemann-Roch theory that allows us to extend the definition of genus. Originally only for Riemann surfaces, the theory focusses on meromorphic functions and differentials. It is this focus which allows the definition to be generalised, first just to complex algebraic curves, then to curves over any algebraically closed field k. The genus appears as a constant in Riemann-Roch theory, most notably as the dimension of the vector space of holomorphic differentials and in the Riemann-Roch theorem itself. The fact that the genus can be defined in terms of differentials demonstrates why differentials, and in particular holomorphic differentials, play such an important role in the theory of algebraic curves.

On the other hand, we recall the famous quote

> "Whenever you have to do with a structure endowed entity Σ try to determine its group of automorphism" — Hermann Weyl [Wey52, pg. 144]

Indeed, the automorphism groups of algebraic curves, and in particular Riemann surfaces, have given rise to many interesting theories. For example, it is known that every finite group is the full automorphism group of some Riemann surface [Gre74, Thm. 6']. Of course, any group that acts on a curve X also acts on functions and differentials of X, such as $H^0(X, \Omega_X)$, the space of global holomorphic differentials.

The main focus of the thesis will be in studying such actions on Riemann-Roch spaces. In particular, we will consider the $k[G]$-module structure of various spaces of differentials on X, and related spaces, for a subgroup G of the automorphism group $\mathrm{Aut}(X)$, paying special attention to what happens in positive characteristic. Of course, if the characteristic divides the order of G the theory is often a lot more complex — for example, we no longer have Maschke's theorem, a fundamental result in classic representation theory.

The thesis is broken in to four main chapters (excluding this one). The first gives background and fixes notation. We now proceed to describe and motivate the other three chapters.

1.1 Bases of spaces of (poly)differentials on hyperelliptic curves

Hyperelliptic curves are a classically studied class of algebraic curves, characterised by being double covers of the projective line. In particular, any hyperelliptic curve X comes equipped with a projection map $\pi\colon X \to \mathbb{P}^1_k$, unique up to an automorphism of $\mathbb{P}^1_k$. They can be viewed as a natural extension of elliptic curves to higher genera, sharing a similar defining equation of $y^2 = f(x)$ (if $\mathrm{char}(k) \neq 2$). It is this concrete and relatively simple defining equation that allows explicit calculations to be made for them. Added to this, there exist hyperelliptic curves with every possible genus (except one and zero), so in this sense they are not a very restrictive class to consider. Moreover, hyperelliptic curves also have a number of nice geometric properties — for example, they can be characterised entirely in terms of Weierstrass points [Mir95, Chap. VII, §4, ex. R], and also every genus 2 curve is hyperelliptic [Liu02, Prop. 7.4.9].

We study hyperelliptic curves throughout this thesis. However, despite being commonplace in algebraic geometry, it is not always easy to find precise statements in the literature. This is especially true when working over a field of characteristic two, where hyperelliptic curves behave very differently. Because of this we split Chapter 3 in to two sections, according to the characteristic of k, and start each section by collecting results that will be needed either later in the chapter or the rest of thesis.

The highlights of Chapter 3 are Proposition 3.2.5 and Proposition 3.1.2, which give bases of the space of holomorphic differentials and polydifferentials of a hyperelliptic curve X of genus $g \geq 2$ when the characteristic of k is two and is not two, respectively. We first state the basis when the characteristic of k is not 2, recalling that in this case the function field $K(X)$ is equal to $k(x, y)$, where y satisfies $y^2 = f(x)$ for some polynomial $f(x) \in k[x]$.

Proposition. *Let $m \geq 1$ and let $\omega := \frac{dx^{\otimes m}}{y^m}$. Then a basis of $H^0(X, \Omega_X^{\otimes m})$ is given by:*

$$\begin{array}{ll} \omega, x\omega, \ldots, x^{g-1}\omega & \textit{if } m = 1, \\ \omega, x\omega, x^2\omega & \textit{if } m = g = 2, \\ \omega, x\omega, \ldots, x^{m(g-1)}\omega;\ y\omega, xy\omega, \ldots, x^{(m-1)(g-1)-2}y\omega & \textit{otherwise.} \end{array}$$

Note that the case where $m = 1$ is already in the literature, see [Liu02, Prop. 7.4.26] or [Gri89, Ch. IV, §4, Prop. 4.3].

On the other hand, if $\mathrm{char}(k) = 2$ then $K(X)$ is still equal to an extension of $k(x)$ of the form $k(x, y)$, but this time we require y to satisfy $y^2 + H(x)y = F(x)$, where $F(x)$ and $H(x)$ are polynomials in $k[x]$, whose degrees will determine the genus.

Proposition. *Let $m \geq 1$ and let $\omega := \frac{dx^{\otimes m}}{H(x)^m}$. Then a basis of $H^0(X, \Omega_X^{\otimes m})$ is given by:*

$$\begin{array}{ll} \omega, x\omega, \ldots, x^{g-1}\omega & \textit{if } m = 1, \\ \omega, x\omega, x^2\omega & \textit{if } m = g = 2, \\ \omega, x\omega, \ldots, x^{m(g-1)}\omega;\ y\omega, xy\omega, \ldots, x^{(m-1)(g-1)-2}y\omega & \textit{otherwise.} \end{array}$$

Note that the case where $m = 1$ can again be found in [Liu02, Prop. 7.4.26].

Equipped with the knowledge of these explicit bases we can examine group actions on $H^0(X, \Omega_X^{\otimes m})$ much more readily. For example, in Chapter 5 we compute the action of the hyperelliptic involution σ on the above basis. Using this we can see when the group generated by σ acts faithfully on $H^0(X, \Omega_X^{\otimes m})$, explicating the main theorem of Chapter 5 in this case.

1.2 Group actions on algebraic de Rham cohomology

In the study of smooth manifolds de Rham cohomology is a well-established tool, which determines to what extent closed differential forms on a smooth manifold M fail to be exact. To further demonstrate its significance, we note that in 1931 Georges de Rham proved that the de Rham cohomology of any smooth real or complex manifold M is isomorphic to the singular cohomology of M in [deR31].

Given that de Rham cohomology is defined on complex manifolds, and hence Riemann Surfaces, an obvious question to ask is whether one can define an analog of de Rham cohomology for algebraic curves. Grothendieck answered this in a letter to Atiyah [Gro66], where he in fact defined the algebraic de Rham cohomology of a scheme. The Hodge-de Rham spectral sequence arose from this definition, and has been much studied. In particular, Deligne and Illusie proved that if, for example, X is a complex, smooth, projective variety then

$$H^n_{\mathrm{dR}}(X) \cong \bigoplus_{i=0}^{n} H^i(X, \Omega_X^{n-i}),$$

see [DeIl87]. When X is a curve this is more or less equivalent to saying that we have a canonical short exact sequence

$$0 \to H^0(X, \Omega_X) \to H^1_{\mathrm{dR}}(X/k) \to H^1(X, \mathcal{O}_X) \to 0. \tag{1.1}$$

Moreover, most of the time (for example, whenever $\mathrm{char}(k) = 0$), this sequence splits not only as k vector spaces, but also as $k[G]$-modules, where G is a subgroup of $\mathrm{Aut}(X)$. However, this is not always the case — in particular, if $\mathrm{char}(k) = p > 0$ divides the order G, the sequence may not split. In [Hor12] Hortsch demonstrated that if X is a hyperelliptic curve over k, an algebraically closed field of characteristic p, and has $y^2 = x^p - x$ as a defining equation, then (1.1) does not split.

Theorem 4.4.3, given below, generalises this result. Before stating this, we recall that any automorphism τ of X commutes with the hyperelliptic involution σ, and since $\mathbb{P}^1_k \cong X/\langle\sigma\rangle$ then τ induces an automorphism of $\mathbb{P}^1_k$.

Theorem. *Let X be a hyperelliptic curve over an algebraically closed field k of characteristic $p \geq 3$. Suppose there exists $\tau \in \mathrm{Aut}(X)$ such that the induced automorphism $\bar{\tau}\colon \mathbb{P}^1_k \to \mathbb{P}^1_k$ is given by $x \mapsto x + a$ for some $0 \neq a \in k$. We let $G = \langle\tau\rangle$ be the subgroup of $\mathrm{Aut}(X)$ generated by τ, and further suppose that X is ramified above $\infty \in \mathbb{P}^1_k$. Then the sequence (1.1) does not split as a sequence of $k[G]$-modules.*

Such curves exist in every genus and every characteristic (greater than 2), and we give examples of such curves in Chapter 4. We also give an example from [KY10] of a curve that is as described in Theorem 4.4.3, except that it is not ramified above $\infty \in \mathbb{P}^1_k$, and show that for this curve the short exact sequence (1.1) does split.

We prove the above theorem by first computing explicit bases of each of the spaces in (1.1). Given the projection $\pi\colon X \to \mathbb{P}^1_k$, by Čech cohomology we have

$$H^1(X, \mathcal{O}_X) \cong \frac{\mathcal{O}_X(U_0 \cap U_\infty)}{\{f_0 - f_\infty | f_i \in \mathcal{O}_X(U_i)\}}, \tag{1.2}$$

where $U_0 = X\backslash\pi^{-1}(0)$ and $U_\infty = X\backslash\pi^{-1}(\infty)$. In the preceding chapter we already computed a basis of $H^0(X,\Omega_X)$, and we use this along with Serre duality and the above identity to compute a basis of $H^1(X,\mathcal{O}_X)$, see Theorem 4.2.1.

Theorem. *The elements* $\frac{y}{x},\ldots,\frac{y}{x^g} \in K(X)$ *are regular on* $U_0 \cap U_\infty$*, and their residue classes* $\left[\frac{y}{x}\right],\ldots,\left[\frac{y}{x^g}\right]$ *in* (1.2) *form a basis of* $H^1(X,\mathcal{O}_X)$.

It should be noted that this basis is the same regardless of characteristic — since this is not the case for the dual space $H^0(X,\Omega_X)$, this may be surprising. We also apply this theorem to provide a Mittag-Leffler style theorem for hyperelliptic curves, see Corollary 4.2.2.

To describe an explicit basis of $H^1_{\mathrm{dR}}(X/k)$ we use Čech cohomology, similarly to (1.2). In this case $H^1_{\mathrm{dR}}(X/k)$ is a quotient of the space

$$\left\{(\omega_0,\omega_\infty,f_{0,\infty})|\omega_i \in \Omega_X(U_i), f_{0,\infty} \in \mathcal{O}_X(U_0 \cap U_\infty), df_{0,\infty} = \omega_0|_{U_0\cap U_\infty} - \omega_\infty|_{U_0\cap U_\infty}\right\}.$$

At the start of Section 4.3 we define polynomials $\phi_i(x)$ and $\psi_i(x)$ in terms of $f(x)$, and polynomials $\Phi_i(x,y)$ and $\Psi_i(x,y)$ in terms of $F(x)$ and $H(x)$, for $1 \le i \le g$, when the characteristic of k is $p \neq 2$ and $p = 2$ respectively. We then use these in Theorem 4.3.1 to present a basis of $H^1_{\mathrm{dR}}(X/k)$.

Theorem. *A basis of* $H^1_{dR}(X/k)$ *is formed by*

$$\left[\left(\left(\frac{\psi_i(x)}{2yx^{i+1}}\right)dx,\left(\frac{-\phi_i(x)}{2yx^{i+1}}\right)dx,x^{-i}y\right)\right] \quad \textit{and} \quad \left[\left(\frac{x^{i-1}}{y}dx,\frac{x^{i-1}}{y}dx,0\right)\right],\ i = 1,\ldots,g,$$

if $\mathrm{char}(k) \neq 2$, *and by*

$$\left[\left(\left(\frac{\Psi_i(x,y)}{x^{i+1}H(x)}\right)dx,\left(\frac{\Phi_i(x,y)}{x^{i+1}H(x)}\right)dx,x^{-i}y\right)\right] \quad \textit{and} \quad \left[\left(\frac{x^{i-1}}{H(x)}dx,\frac{x^{i-1}}{H(x)}dx,0\right)\right],\ i = 1,\ldots,g,$$

otherwise.

We use the above bases along with the canonical projection $p\colon H^1_{\mathrm{dR}}(X/k) \to H^1(X,\mathcal{O}_X)$ to prove Theorem 4.4.3. In particular, we suppose that the short exact sequence 1.1 has a splitting map $s\colon H^1(X,\mathcal{O}_X) \to H^1_{\mathrm{dR}}(X/k)$, and then by studying the action of τ on the basis element $\left[\left(\left(\frac{\psi_g(x)}{2yx^{g+1}}\right)dx,\left(\frac{-\phi_g(x)}{2yx^{g+1}}\right)dx,x^{-g}y\right)\right]$, and its image $\left[\frac{y}{x^g}\right]$ in $H^1(X,\mathcal{O}_X)$, we arrive at a contradiction.

1.3 Faithful actions on Riemann-Roch spaces

Given a smooth, projective curve X of genus g over an algebraically closed field k, a significant open problem is to completely determine the $k[G]$-module structure of $H^0(X,\Omega_X)$, for any subgroup G of $\mathrm{Aut}(X)$. This was done for the case $k = \mathbb{C}$ by Chevalley and Weil in 1934, see [CWH34]. The result was later broadened to a curve over any algebraically closed field of characteristic zero by Lewittes [Lew63], and Broughton's paper [Bro87] gives another method of generalising to this case. The question has also been answered by Kani [Kan86] and Nakajima [Nak84], if the projection $\pi\colon X \to Y := X/G$ is tamely ramified. Valentini and Madan [VM81] determined the structure when π may be wildly ramified, but they assume that G is a cyclic group of order p^n, and this was recently generalised by Karanikolopoulos and Kontogeorgis to any cyclic group [KaKo13].

A weaker though naturally related question is: "When does G act faithfully on $H^0(X,\Omega_X)$?" We answer this in full generality in Theorem 5.3.1, and also extend the result to look at the space of holomorphic polydifferentials, denoted $H^0(X,\Omega_X^{\otimes m})$.

Theorem. *Suppose that $g \geq 2$ and let $m \geq 1$. Then G does not act faithfully on $H^0(X,\Omega_X^{\otimes m})$ if and only if G contains a hyperelliptic involution and one of the following two sets of conditions holds:*

- *$m = 1$ and $p = 2$;*
- *$m = 2$ and $g = 2$.*

Our main method of attack in proving this is comparing the dimension of $H^0(X,\Omega_X^{\otimes m})$ to its fixed space, $H^0(X,\Omega_X^{\otimes m})^G$. We compute the latter dimension precisely in Proposition 5.1.2, where we see that if n is the order of G and R is the ramification divisor of the projection $\pi\colon X \to Y$ then

$$\dim_k\left(H^0(X,\Omega_X^{\otimes m})^G\right) = (2m-1)(g_Y - 1) + \deg\left\lfloor \frac{m\pi_*(R)}{n} \right\rfloor,$$

apart from a few exceptional cases. We then use this to determine exactly when G acts trivially if $g_Y = 0$ and G is of prime order, since the $\deg\left\lfloor \frac{m\pi_*(R)}{n} \right\rfloor$ term is easier to handle in this instance. We are then able to reduce to this case in general, since any group that fails to act faithfully on $H^0(X,\Omega_X^{\otimes m})$ contains a subgroup which acts trivially on the space.

We use similar techniques to determine when G acts trivially on more general Riemann-Roch spaces, such as $H^0(X,\mathcal{O}_X(D))$ for a G-invariant divisor D of degree at least $2g-1$.

The results of this chapter appear in [KT14].

Chapter 2

Background on algebraic curves

In this chapter we give basic definitions and results that will be used throughout the thesis. The vast majority of these results apply to smooth, connected, projective curves over any algebraically closed fields, with no further assumptions, though occasionally we do specialise slightly more than this. All definitions and results should be available in textbooks on algebraic curves or algebraic geometry in general, such as [Ful89] or [Har77] . As such, we will rarely provide proofs for results given.

We start by defining precisely what we mean by a curve, and by functions and differentials on a curve. We then go on to give some basic results about these objects, and finally define the genus of a curve.

In the next section we define divisors, canonical divisors and the Riemann–Roch spaces associated to divisors. We then reach the highlight of the section with the statement of the Riemann–Roch theorem. We give corollaries to this, which show some of its applications.

In the penultimate section of this chapter we consider ramification. We define ramification and branch points, and subsequently the ramification divisor. We then use this to state a strong version of the Riemann–Hurwitz formula, at the level of divisors. The section concludes by looking at group actions on curves, and defining higher ramification to state Hilbert's formula.

The chapter finishes by discussing Serre duality, which will be used in the fourth chapter of the thesis. We do this using a particularly explicit, non-cohomological, description of $H^1(X, \mathcal{O}_X)$ and $H^1(X, \Omega_X)$.

2.1 Set up

Throughout this thesis k will denote an algebraically closed field of characteristic $p \geq 0$. It should be noted that while the majority of results in the thesis hold for all characteristics, including $p = 0$, our main focus will be on the case $p > 0$.

When we refer to an *algebraic curve* (or often just a *curve*) we will mean a smooth, connected, projective variety of dimension one over k. In particular, we let $\mathbb{P}^1_k$ be the projective line. Similarly, when we refer to an *affine curve* we mean a smooth, connected, affine variety of dimension one over k. We recall that a morphism of affine curves X and Y is just a polynomial map $\phi\colon X \to Y$. Then if X and Y are algebraic curves, a map $\phi\colon X \to Y$ is a morphism if we can write $X = \cup X_i$ and $Y = \cup Y_i$ for open, affine X_i and Y_i, such that $\phi(X_i) \subseteq Y_i$ and $\phi|_{X_i}$ is a morphism for every i.

2.2 Functions and differentials

In this section we recall basic results pertaining to functions and differentials on a curve X.

A *meromorphic function* on X is any morphism $f\colon X \to \mathbb{P}^1_k$, other than the morphism mapping all points to infinity. The collection of meromorphic functions on X is denoted $K(X)$, and called the *function field* of X.

We recall that the category of algebraic curves and non-constant morphisms is actually equivalent to the category of function fields over k (which can be defined independently of curves as finitely generated fields of transcendence degree one over k). An overview of this correspondence is given in [Sti93, Appendix B]. Furthermore, when working over the complex numbers $\mathbb{C}$ we actually have a triple equivalence of categories. The category of function fields over $\mathbb{C}$ and the category of algebraic curves are both equivalent to the category of compact Riemann surfaces. A short explanation of the correspondence between complex curves and Riemann surfaces is given in [Gri89, Chap. 1, §2], whilst [Mir95] exhibits the connection between all three categories throughout.

Returning to our study of functions on X, we recall that a meromorphic function f on X is *regular* on an open set $U \subseteq X$ if the image $f(U)$ lies in $k = \mathbb{A}^1_k \subset \mathbb{P}^1_k$. We let $H^0(U, \mathcal{O}_X)$ denote the space of functions in $K(X)$ which are regular on U. Moreover, if $f \in K(X)$ is regular on X we say that f is *regular*, and then $H^0(X, \mathcal{O}_X)$ is the space of regular functions. Since X is projective $H^0(X, \mathcal{O}_X)$ is in fact isomorphic to k — i.e. the only regular functions are constant functions. The reader should note that we are using sheaf theoretic notation here. We will not give details of sheaves and sheaf cohomology (since it will rarely be needed), but we will still use the notation, in order to be with consistent with current work in the area.

Given $P \in X$ we say that a meromorphic function $f \in K(X)$ is ***regular at*** P if $f(P) \in k \subset \mathbb{P}^1_k$. The collection of functions regular at P form a ring, which we call $\mathcal{O}_{X,P}$.

Lemma 2.2.1. *For any* $P \in X$ *the ring* $\mathcal{O}_{X,P}$ *is a discrete valuation ring, with maximal ideal*

$$\mathcal{M}_{X,P} := \{f \in \mathcal{O}_{X,P} | f(P) = 0\}.$$

Proof. See [Ful89, Chap. 1, §4]. □

The valuation on $\mathcal{O}_{X,P}$ can be given as follows. Let $t \in \mathcal{O}_{X,P}$ be a generator of $\mathcal{M}_{X,P}$. Now any $0 \neq f \in \mathcal{O}_{X,P}$ can be written as $f = ut^n$ for some unique $n \in \mathbb{Z}_{\geq 0}$ and some unit $u \in \mathcal{O}_{X,P} \backslash \mathcal{M}_{X,P}$. We then define ***the order of*** f ***at*** P to be $\mathrm{ord}_P(f) := n$ (note that this is independent of the choice of t). For any $f \in K(X)^*$ and $P \in X$ at least one f or $1/f$ is an element of $\mathcal{O}_{X,P}$. Hence we may extend the definition of ord_P to the whole $K(X)^*$, by letting $\mathrm{ord}_P(f) := -\mathrm{ord}_P(1/f)$ whenever $f \notin \mathcal{O}_{X,P}$. If $\mathrm{ord}_P(f) = n > 0$ we say that f has a ***zero of order*** n at P, whilst if $\mathrm{ord}_P(f) = n < 0$ then we say that f has a ***pole of order*** n at P. Clearly, for any $f, g \in K(X)^*$ and $P \in X$, it is true that $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$, and we also have $\mathrm{ord}_P(f+g) \geq \inf\{\mathrm{ord}_P(f), \mathrm{ord}_P(g)\}$, with equality whenever $\mathrm{ord}_P(g) \neq \mathrm{ord}_P(f)$. We call any element $t \in \mathcal{O}_{X,P}$ which has order 1 at P a ***uniformising parameter at*** P.

Proposition 2.2.2. *Any non-zero meromorphic function* f *on* X *has finitely many poles and zeroes. Moreover, the number of poles and zeroes of* f *are equal, after counting multiplicity; i.e.*

$$\sum_{P \in X} \mathrm{ord}_P(f) = 0.$$

Proof. See [Ful89, Chap. 8, §1, Prop. 1]. □

We now introduce the concept of a differential on the curve X. Let R be any commutative ring containing k and let M be an R-module. Then a k-linear map $D \colon R \to M$ satisfying $D(fg) = fD(g) + gD(f)$ is called a ***derivation*** of R in to M over k.

There exists a unique module $\Omega_k(R)$, called the ***module of differentials of*** R ***over*** k, and a derivation $d \colon R \to \Omega_k(R)$ through which all derivations of R over k must factor. We can describe $\Omega_k(R)$ more concretely as the free module generated by $[f]$ for all $f \in R$, quotiented by the relations

- $[f] + [g] = [f+g]$,
- $[cf] = c[f]$,
- $[fg] = f[g] + g[f]$,

where $f, g \in R$ and $c \in k$. Then $d(f)$ is the image of $[f]$ in this quotient.

In particular, if $R = K(X)$ then we define $\Omega_{K(X)} := \Omega_k(K(X))$. In this case we call the map $d\colon K(X) \to \Omega_{K(X)}$ the ***differential map*** and we let $df := d(f)$. We say that $\omega \in \Omega_{K(X)}$ is a ***meromorphic differential*** on X.

Proposition 2.2.3. *The module of differentials, $\Omega_{K(X)}$, is a one dimensional vector space over $K(X)$. Moreover, if $t \in K(X)$ is a uniformising parameter for any point P in X then dt is a basis of $\Omega_{K(X)}$.*

Proof. See [Sti93, Prop. 1.5.9]. □

We suppose that $P \in X$ and we choose a uniformising parameter $t \in \mathcal{O}_{X,P}$. Then for any $0 \neq \omega \in \Omega_{K(X)}$ there exists a unique $f \in K(X)$ such that $\omega = f\,dt$, by Proposition 2.2.3. We define the ***order of ω at P*** to be $\mathrm{ord}_P(\omega) := \mathrm{ord}_P(f)$, and remark that this is independent of the choice of t. The set of differentials regular at P form a module over $\mathcal{O}_{X,P}$, which we call the ***module of differentials regular at P***, and denote by $\Omega_{X,P}$.

For any $f \in \mathcal{O}_{X,P}$ we have $df \in \Omega_{X,P}$. If f is a local parameter at P this follows from the definition of $\Omega_{X,P}$, and if $\mathrm{ord}_P(f) > 1$ it then follows from this and the product rule. Finally, if f is a unit at P then it is true because $df = d(f - f(P))$, and clearly $f - f(P) \in \mathcal{M}_{X,P}$. In fact, $\Omega_{X,P}$ is the module of differentials of $\mathcal{O}_{X,P}$ over k, and it is generated by dt for any uniformising parameter $t \in \mathcal{O}_{X,P}$. Note that given a function $f \in K(X)$ and differentials $\omega, \omega' \in \Omega_{K(X)}$ we have $\mathrm{ord}_P(f\omega) = \mathrm{ord}_P(f) + \mathrm{ord}_P(\omega)$ and $\mathrm{ord}_P(\omega + \omega') \geq \inf\{\mathrm{ord}_P(\omega), \mathrm{ord}_P(\omega')\}$.

Let U be an open subset of X. We call $\omega \in \Omega_{K(X)}$ ***holomorphic on U*** if $\mathrm{ord}_P(\omega) \geq 0$ for all $P \in U$, and we let

$$H^0(U, \Omega_X) := \{\omega \in \Omega_{K(X)} | \mathrm{ord}_P(\omega) \geq 0 \text{ for all } P \in X\} \cup \{0\}$$

be ***the space of holomorphic differentials on U***. If $\omega \in \Omega_{K(X)}$ is holomorphic on X we say that ω is ***holomorphic***, and so $H^0(X, \Omega_X)$ is the space of global holomorphic differentials. As in [Ful89, Chap. 8, §2, Prop. 3], the k-vector space $H^0(X, \Omega_X)$ is finite dimensional.

Definition 2.2.4. We define the *genus* of X to be

$$g_X := \dim_k H^0(X, \Omega_X).$$

The genus is an invariant of fundamental importance in the study of algebraic curves. In particular, we remark that if $k = \mathbb{C}$ then the genus of an algebraic curve (also called the geometric genus) is the same as the topological genus of the corresponding Riemann surface (the corresponding Riemann surface being found via the equivalence of categories mentioned earlier).

We now briefly recall the notion of a ***polydifferential***. If we consider an element of the tensor product $\omega \in \Omega_{K(X)}^{\otimes m}$, for some $m \in \mathbb{Z}_{>0}$, then it can be written as $f dx_1 \otimes \ldots \otimes dx_m$, where $f, x_i \in K(X)$ for all $1 \leq i \leq m$. Let P be a point in X. Since each dx_i can be written as $f_i dt$ for some $f_i \in K(X)$ and some uniformising parameter t at P, we can rewrite ω as $f' dt \otimes \ldots \otimes dt$, where $f' = f \cdot f_1 \cdots f_m$. We then define the order of ω at P to be $\mathrm{ord}_P(\omega) := \mathrm{ord}_P(f')$. In the particular case where $\omega' = \omega^{\otimes m}$ for some $\omega \in \Omega_{K(X)}$ then we have the equality

$$\mathrm{ord}_P(\omega') = m \, \mathrm{ord}_P(\omega).$$

Finally, for any open $U \subseteq X$ we define

$$H^0(U, \Omega_{K(X)}^{\otimes m}) := \{\omega \in \Omega_{K(X)}^{\otimes m} | \mathrm{ord}_P(\omega) \geq 0 \text{ for all } P \in U\}$$

to be the ***space of holomorphic polydifferentials*** on U. We call the elements of $H^0(X, \Omega_{K(X)}^{\otimes m})$ ***global holomorphic polydifferentials*** on X.

2.3 The Riemann–Roch theorem

We now recall the relevant facts and definitions needed to state the Riemann–Roch theorem.

We first recall that a ***divisor*** on X is a finitely supported formal sum

$$D = \sum_{P \in X} n_P [P],$$

with coefficients in $\mathbb{Z}$. The set off all divisors on X forms an additive group, denoted $\mathrm{Div}(X)$. The ***degree*** of the divisor D is $\deg(D) := \sum_{P \in X} n_P$, which lies in $\mathbb{Z}$.

Given any function $f \in K(X)$ we define the ***divisor associated to*** f to be

$$\mathrm{div}(f) := \sum_{P \in X} \mathrm{ord}_P(f)[P].$$

Note that by Proposition 2.2.2 $\mathrm{div}(f)$ has finite support and degree zero. We call any divisor D which is equal to $\mathrm{div}(f)$ for some $f \in K(X)$ a ***principal divisor***. Is is clear that for any $f, g \in K(X)$ we have $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$. Also, for any $f \in K(X)$ we define $\mathrm{div}_0(f)$ and $\mathrm{div}_\infty(f)$, the ***divisor of zeroes*** and the ***divisor of poles*** of f respectively, as follows:

$$\mathrm{div}_0(f) := \sum_{\mathrm{ord}_P(f) > 0} \mathrm{ord}_P(f)[P]$$

and then

$$\mathrm{div}_\infty(f) := \mathrm{div}_0(f) - \mathrm{div}(f).$$

Now for any differential $0 \neq \omega \in \Omega_{K(X)}$ we define the ***divisor associated to*** ω to be

$$\mathrm{div}(\omega) := \sum_{P \in X} \mathrm{ord}_P(\omega)[P].$$

To show that $\mathrm{div}(\omega)$ does indeed have finite support we recall that by Proposition 2.2.3 then ω can be written in the form $f dg$ for some $f, g \in K(X)$. Then every pole of ω is a pole of f or a pole of g. Thus, by Proposition 2.2.2 it follows that ω has only finitely many poles. It can be shown that ω has finitely many zeroes in a similar fashion. If W is a divisor on X and $W = \mathrm{div}(\omega)$ for some $0 \neq \omega \in \Omega_{K(X)}$ then we say that W is a ***canonical divisor*** on X.

The principal divisors of X form a subgroup of $\mathrm{Div}(X)$, and two divisors $D, D' \in \mathrm{div}(X)$ are ***equivalent***, denoted $D \sim D'$, if their image in the quotient of $\mathrm{Div}(X)$ by the group of principal divisors is the same; i.e. if there exists $f \in K(X)$ such that $D = D' + \mathrm{div}(f)$. By the following corollary, it makes sense to refer to the (unique) canonical divisor on X, up to equivalence, which we write as K_X.

Corollary 2.3.1. *The canonical divisors on X form precisely one equivalence class on X with respect to the relation $\sim$.*

Proof. Let W be the canonical divisor associated to $\omega \in \Omega_{K(X)}$ and suppose that $D \in \mathrm{Div}(X)$ is equivalent to W. Then $D = W + \mathrm{div}(f) = \mathrm{div}(f\omega)$ is also a canonical divisor.

On the other hand, suppose W and W' are the canonical divisors associated to $\omega, \omega' \in \Omega_{K(X)}$ respectively. Then we can find a meromorphic function $f \in K(X)$ such that $\omega = f\omega'$, by Proposition 2.2.3. Then $W = W' + \mathrm{div}(f)$, and the divisors are equivalent. □

Given any divisor $D = \sum_{P \in X} n_P[P]$ we let

$$H^0(X, \mathcal{O}_X(D)) := \{f \in K(X) | \mathrm{ord}_P(f) \geq -n_P \text{ for all } P \in X\}$$

be the ***vector space of meromorphic functions associated to*** D. Similarly, we let

$$H^0(X, \Omega_X(D)) := \{\omega \in \Omega_{K(X)} | \mathrm{ord}_P(\omega) \geq -n_P \text{ for all } P \in X\}$$

be the ***vector space of meromorphic differentials associated to*** D. Both of the spaces mentioned above are also referred to as ***Riemann–Roch spaces***. Note that when D is the zero divisor we have $H^0(X, \Omega(0)) = H^0(X, \Omega_X)$, and similarly $H^0(X, \mathcal{O}_X(0)) = H^0(X, \mathcal{O}_X)$. Also, it follows immediately from Proposition 2.2.2 that if $D \in \mathrm{Div}(X)$ is a divisor with negative degree then $H^0(X, \mathcal{O}_X(D)) = \{0\}$.

Lemma 2.3.2. *Given any divisor D on X we have the following isomorphism,*

$$H^0(X, \mathcal{O}_X(D)) \cong H^0(X, \Omega_X(D-W))$$

where W is any canonical divisor on X.

Proof. Let W be a canonical divisor and chose $\omega \in \Omega_{K(X)}$ to be the associated differential. Since $\operatorname{div}(f\omega) = \operatorname{div}(f) + \operatorname{div}(\omega)$, it follows that $f \in H^0(X, \mathcal{O}_X(D))$ if and only if $f\omega \in H^0(X, \Omega_X(D-W))$. Since $\Omega_{K(X)}$ is a one dimensional vector space over $K(X)$ we can find a unique $f \in K(X)$ for every differential ω' in $H^0(X, \Omega_X(D-W)$ such that $\omega' = f\omega$. Hence the map $f \mapsto f\omega$ is an isomorphism. □

It follows from this lemma and the definition of genus that $\dim_k H^0(X, \mathcal{O}_X(W)) = g_X$ for any canonical divisor W.

We now state the celebrated Riemann–Roch theorem.

Theorem 2.3.3 (Riemann–Roch theorem). *Let g_X be the genus of X. Furthermore, let D be any divisor on X, and let W be any canonical divisor on X. Then*

$$\dim_k H^0(X, \mathcal{O}_X(D)) = \deg(D) + 1 - g_X + \dim_k H^0(X, \mathcal{O}_X(W-D)).$$

Proof. See [Har77, Chap. IV, §1, Thm. 1.3] or, for a more elementary approach, [Ful89, Chap. 8, §6]. □

We now give some corollaries to the Riemann–Roch theorem.

Corollary 2.3.4. *For any canonical divisor W on X, we have*

$$\deg(W) = 2g_X - 2.$$

Proof. The statement follows by rearranging

$$\begin{aligned} g_X &= \dim_k H^0(X, \mathcal{O}_X(W)) \\ &= \deg(W) + 1 - g_X + \dim_k H^0(X, \mathcal{O}_X(W-W)) \\ &= \deg(W) + 1 - g_X + 1, \end{aligned}$$

where the first equality is Definition 2.2.4, and the second equality follows from the Riemann–Roch theorem. □

Corollary 2.3.5. *For any divisor D of degree greater than $2g_X - 2$ we have*

$$\dim_k H^0(X, \mathcal{O}_X(D)) = \deg(D) + 1 - g_X.$$

Proof. If $\deg(D) > 2g_X - 2$ then $\deg(W - D) < 0$. Then if $f \in H^0(X, \mathcal{O}(W - D))$ it follows that f has more zeroes than poles (after counting multiplicities), which contradicts Proposition 2.2.2. □

Corollary 2.3.6. *If D is a divisor of degree greater than $2g_X - 2$ and P is any point in X then*

$$\dim_k H^0(X, \mathcal{O}_X(D + [P])) = \dim_k H^0(X, \mathcal{O}_X(D)) + 1.$$

Proof. Since $\deg(D) > 2g - 2$, it follows from Corollary 2.3.4 that $\deg(W - D) < 0$. Then $\dim_k H^0(X, \mathcal{O}_X(W - D)) = 0$. We then apply the Riemann–Roch theorem and see that

$$\begin{aligned}\dim_k H^0(X, \mathcal{O}_X(D + [P])) &= \deg(D + [P]) + 1 - g_X \\ &= \deg(D) + 1 + 1 - g_X = \dim_k H^0(X, \mathcal{O}_X(D) + 1.\end{aligned}$$

□

Using the Riemann–Roch theorem and Corollary 2.3.4 we can compute the dimension of the space of ***holomorphic polydifferentials*** of order m, denoted $H^0(X, \Omega_X^{\otimes m})$, where $m \in \mathbb{Z}_{>0}$.

Corollary 2.3.7. *Let $g_X, m \geq 2$. Then*

$$\dim_k H^0(X, \Omega_X^{\otimes m}) = (2m - 1)(g_X - 1)$$

Proof. Since $g_X \geq 2$ it follows from Corollary 2.3.4 that $\deg(W) \geq 1$, and hence we see that $\deg(mW) > \deg(W)$. Similarly to Lemma 2.3.2, we have $H^0(X, \Omega_X^{\otimes m}) \cong H^0(X, \mathcal{O}_X(mW))$. It then follows from the Riemann–Roch theorem (Theorem 2.3.3) and Corollary 2.3.4 that

$$\dim_k H^0(X, \Omega_X^{\otimes m}) = \deg(mW) + 1 - g_X = (2m - 1)(g_X - 1).$$

□

2.4 Ramification and the Riemann–Hurwitz formula

In this section we will introduce the concept of ramification, and we state the Riemann–Hurwitz formula, which relates the canonical divisor of two curves which have a morphism between them, via the ramification divisor.

Let X and Y be curves over k. We first note that given a non-constant morphism $\phi\colon X \to Y$ we have an induced ring homomorphism on the function fields,

$$\phi^*\colon K(Y) \to K(X),$$

given by composition with ϕ; i.e. $\phi^*(f) = f \circ \phi$. Moreover, it transpires that ϕ^* is an injection, and hence we can view $K(Y)$ as a subfield of $K(X)$. We then define the *degree* of ϕ, denoted $\deg(\phi)$, to be the degree of the extension $K(X)/K(Y)$, which is always finite.

We henceforth assume that $\phi\colon X \to Y$ is an arbitrary non-constant morphism of curves. Recall that we have

$$\phi^*(H^0(U, \mathcal{O}_Y)) \subseteq H^0(\phi^{-1}(U), \mathcal{O}_X).$$

Definition 2.4.1. Let P be a point in X and choose a uniformising parameter $t \in \mathcal{O}_{Y,\phi(P)}$. We define the *ramification index* e_P of ϕ at P to be

$$e_P := \mathrm{ord}_P(\phi^*(t)).$$

Note that $e_P = 1$ for almost all points $P \in X$. We say that the point $Q \in Y$ is a *branch point* of ϕ if there exists some $P \in \phi^{-1}(Q)$ for which $e_P > 1$. We say that $P \in X$ is a *ramification point* of X if $e_P > 1$.

The following theorem asserts that the degree of ϕ is the same as the number of points in the pre-image $\phi^{-1}(Q)$ for any $Q \in Y$, if we count multiplicities correctly.

Theorem 2.4.2. *Let $n := \deg(\phi)$. Then, for any $Q \in Y$, we have*

$$\sum_{P \mapsto Q} e_P = n.$$

Proof. See, for example, [Liu02, Pg. 290]. □

Suppose $P \in X$ is a ramification point. Then if $p = \mathrm{char}(k)$ divides e_P we say that P is *wildly ramified*. If p does not divide e_P we say that P is *tamely ramified*.

Definition 2.4.3. Let $D = \sum_{Q \in Y} n_Q[Q]$ be a divisor on Y. Then the *pull back* of D with respect to ϕ is

$$\phi^*(D) := \sum_{Q \in Y} \sum_{P \in \pi^{-1}(Q)} e_P \cdot n_Q[P].$$

Note that ϕ^* defines a group homomorphism $\mathrm{Div}(Y) \to \mathrm{Div}(X)$.

We also define the pullback of a differential $\omega = g \cdot df \in \Omega_{K(Y)}$ by ϕ to be

$$\phi^*(\omega) := \phi^*(g) d\phi^*(f).$$

Clearly $\phi^*(\omega)$ is a differential on X.

Now we describe the different exponent, which we require to define the ramification divisor.

Definition 2.4.4. For any $P \in X$ we choose a uniformising parameter $t \in \mathcal{O}_{Y,\phi(P)}$. Then we define the ***different exponent*** at P to be

$$\delta_P := \mathrm{ord}_P(\phi^*(dt)).$$

Note that since $\phi^*(t)$ is regular at P it follows that δ_P is non-negative for all $P \in X$.

Definition 2.4.5 (Ramification divisor). The ***ramification divisor*** of $\phi \colon X \to Y$ is

$$R := \sum_{P \in X} \delta_P [P].$$

We will see in Theorem 2.4.9 that this sum does have finite support.

The following theorem has the classical Riemann–Hurwitz formula as a corollary, but also goes further, actually relating the canonical divisors on X and Y.

Theorem 2.4.6. *If* $0 \neq \omega \in \Omega_{K(Y)}$ *then*

$$\mathrm{div}(\phi^*(\omega)) = \phi^*(\mathrm{div}(\omega)) + R. \tag{2.1}$$

In particular, we have

$$K_X \sim \phi^*(K_Y) + R.$$

Proof. See [Har77, Chap. IV, §2, Prop. 2.3] for a sheaf theoretic approach, or alternatively [Sti93, Thm. 3.4.6], for a proof involving function fields. □

Corollary 2.4.7 (Riemann–Hurwitz Formula). *We let* g_X *and* g_Y *be the genera of* X *and* Y *respectively. Then we have*

$$2g_X - 2 = n(2g_Y - 2) + \deg(R).$$

Proof. This follows from Corollary 2.3.4 and Theorem 2.4.6, by taking degrees in (2.1). □

The majority of topics considered in the thesis will be concerned with the following situation. Let G be a finite subgroup of the automorphism group of X (recall that if $g_X \geq 2$ then the automorphism group itself is finite, see, for example, [IT51]). The group G naturally acts on the function field of X, by $g \cdot f(P) := f(g \cdot P)$ for every $P \in X$ and $f \in K(X)$. Then the quotient $Y := X/G$ of X by the action of G is again a curve (see [DaSh94, Chap. 2, §1.7, Ex. 8]), and the function field of the quotient curve is the subfield of $K(X)$ fixed by this action, which we denote $K(X)^G$. We let $\pi\colon X \to Y$ be the projection of X on to the quotient. Note that G acts transitively on the fibres of π (*ibid.*). We also recall that the stabiliser of a point $P \in X$ is the subgroup $G(P) := \{g \in G | g \cdot P = P\}$ of G.

We now introduce the higher ramification groups, which we will use to state Hilbert's formula, which computes the coefficients of the ramification divisor.

Definition 2.4.8. Let G be finite subgroup of $\mathrm{Aut}(X)$ and let t be a uniformising parameter at $P \in X$. Then for $i \geq -1$ we define the i^{th} ***ramification group*** at P, denoted $G_i(P)$, to be the subgroup formed by the $s \in G_{-1}(P)$ such that $i_G(s) := \mathrm{ord}_P(s(t) - t)$ is at least $i + 1$. This is independent of the choice of t, see [Ser79, Chap. IV, §1, pg. 62].

Note that for any $P \in X$ we have that $G_{-1}(P) = G$, $G_0(P)$ is the stabiliser of P and that $G_i(P) \supseteq G_{i+1}(P)$. Also, $e_P = \mathrm{ord}(G_0(P))$ for any $P \in X$, and if n_P is the size of the fiber of $\pi(P)$ then $n = e_P \cdot n_P$, where $n = \deg(\pi)$. Less obviously, we have that $G_i(P)$ is trivial if i is sufficiently large, that G_1 is a p-group and that $\mathrm{ord}(G_0(P)/G_1(P))$ is coprime to p — see [Ser79, Chap. IV, §1] for details. In particular, ϕ is tamely ramified at P if and only if $G_1(P)$ is the trivial group.

Theorem 2.4.9 (Hilbert's Formula). *For every $P \in X$ we have*

$$\delta_P = \sum_{s \neq e} i_G(s) = \sum_{j=0}^{\infty} (\mathrm{ord}(G_i(P)) - 1),$$

where e denotes the identity in G. In particular, if P is tamely ramified then $\delta_P = e_P - 1$.

Proof. See [Ser79, Chap. IV, §1, Prop. 4] for a proof of Hilbert's formula. □

2.5 Serre duality

In this section we give the details of Serre duality, in such a way that we will be able to perform explicit computations using Serre duality in later chapters. We retain the notations of the previous sections, and in particular we recall that the notations $H^1(X, \Omega_X)$ and $H^1(X, \mathcal{O}_X)$ refer to first cohomology groups of the sheaf of differentials, Ω_X, and the sheaf of rational functions, $\mathcal{O}_X$, respectively. The following lemma gives us useful and elementary descriptions of $H^1(X, \mathcal{O}_X)$ and $H^1(X, \Omega_X)$. We will use these descriptions almost exclusively for the rest of the thesis, and as such the reader may take this as a definition if he or she wishes.

Lemma 2.5.1. *We have canonical exact sequences as follows:*

$$0 \to H^0(X, \mathcal{O}_X) \to K(X) \to \bigoplus_{P \in X} K(X)/\mathcal{O}_{X,P} \to H^1(X, \mathcal{O}_X) \to 0; \tag{2.2}$$

$$0 \to H^0(X, \Omega_X) \to \Omega_{K(X)} \to \bigoplus_{P \in X} \Omega_{K(X)}/\Omega_{X,P} \to H^1(X, \Omega_X) \to 0. \tag{2.3}$$

Remark. Note that a sketch of the proof below can be found in [Har77, Pg. 248].

Proof. We let $\underline{\Omega}_{K(X)}$ and $\underline{K}(X)$ denote the constant sheaves of $\Omega_{K(X)}$ and $K(X)$ respectively. The short exact sequence

$$0 \to \mathcal{O}_X \to \underline{K}(X) \to \underline{K}(X)/\mathcal{O}_X \to 0 \tag{2.4}$$

is a flasque resolution of $\mathcal{O}_X$ (see [Har77, Chap. II, ex. 1.16]).

For each $P \in X$ we have a natural embedding $i\colon \{P\} \hookrightarrow X$, and we view the module $K(X)/\mathcal{O}_{X,P}$ as a sheaf on the singleton $\{P\}$. Then for each $P \in X$ we have the induced sheaf $i_*(K(X)/\mathcal{O}_{X,P})$ on X. If we consider the direct sum of these induced sheaves over all points $P \in X$ we have the following isomorphism

$$\underline{K}(X)/\mathcal{O}_X \cong \bigoplus_{P \in X} i_*(K(X)/\mathcal{O}_{X,P}). \tag{2.5}$$

To explain this isomorphism we first construct a map from $\underline{K}(X)/\mathcal{O}_X$ in to the product $\prod_{P \in X} i_*(K(X)/\mathcal{O}_{X,P})$, and then show that the image of each element under this map has finite support.

Given $i\colon \{P\} \hookrightarrow X$ we have the following equalities

$$i^{-1}(\underline{K}(X)/\mathcal{O}_X) = (\underline{K}(X)/\mathcal{O}_X)_P = \underline{K}(X)_P/\mathcal{O}_{X,P} = K(X)/\mathcal{O}_{X,P}.$$

It follows that for any $P \in X$ we have the adjunction map $\underline{K}(X)/\mathcal{O}_X \to i_*(K(X)/\mathcal{O}_{X,P})$. These adjunction maps give a map $\underline{K}(X)/\mathcal{O}_X \to \prod_{P \in X}(K(X)/\mathcal{O}_{X,P})$, whose image is actually in the sum $\bigoplus_{P \in X} i_*(K(X)/\mathcal{O}_{X,P})$. The resulting map is an isomorphism because the stalk $i_*(K(X)/\mathcal{O}_{X,P})_Q$ is zero for $Q \neq P$ and is $K(X)/\mathcal{O}_{X,P}$ when $Q = P$. The isomorphism in (2.5) follows from this.

Replacing $\underline{K}(X)/\mathcal{O}_X$ by $\bigoplus_{P \in X} i_*(K(X)/\mathcal{O}_{X,P})$ in (2.4) yields

$$0 \to \mathcal{O}_X \to \underline{K}(X) \to \bigoplus_{P \in X} i_*(K(X)/\mathcal{O}_{X,P}) \to 0. \tag{2.6}$$

Taking cohomology, and recalling that $H^1(X, \underline{K}(X)) = 0$, we arrive at the exact sequence (2.2).

We now perform a similar computation to produce the second exact sequence (2.3). We start with the short exact sequence

$$0 \to \Omega_X \to \underline{\Omega}_{K(X)} \to \underline{\Omega}_{K(X)}/\Omega_X \to 0,$$

which is a flasque resolution of Ω_X (see [Har77, Chap. II, ex. 1.16]). For each $P \in X$ we again have a natural injection $i\colon \{P\} \hookrightarrow X$, giving rise to the induced sheaf $i_*(K(X)/\mathcal{O}_{X,P})$ on X. Then we have an isomorphism

$$\underline{\Omega}_{K(X)}/\Omega_X \cong \bigoplus_{P \in X} i_*\left(\Omega_{K(X)}/\Omega_{X,P}\right),$$

similar to that in (2.5).

Hence we arrive at the short exact sequence

$$0 \to \Omega_X \to \underline{\Omega}_{K(X)} \to \bigoplus_{P \in X} i_*\left(\Omega_{K(X)}/\Omega_{X,P}\right) \to 0. \tag{2.7}$$

Taking cohomology of this then yields the second exact sequence (2.3). □

Remark. When considering elements of $H^1(X, \Omega_X)$ as elements in the cokernel of the map $\Omega_{K(X)} \to \bigoplus_{P \in X} \Omega_{K(X)}/\Omega_{X,P}$ above, we will denote them by $\overline{(\omega_P)}_{P \in X}$, where $(\omega_P)_{P \in X} \in \bigoplus_{P \in X} \Omega_{K(X)}/\Omega_{X,P}$. Similarly, when considering elements of $H^1(X, \mathcal{O}_X)$ as elements of the cokernel of the map $K(X) \to \bigoplus_{P \in X} K(X)/\mathcal{O}_{X,P}$, we will denote them by $\overline{(f_P)}_{P \in X}$, where $(f_P)_{P \in X} \in \bigoplus_{P \in X} K(X)/\mathcal{O}_{X,P}$.

The residue map $\mathrm{Res}_P\colon \Omega_{K(X)} \to k$ is of fundamental importance in the computations that follow. We define the *residue map*, Res_P, to be the unique map identified in the following theorem.

Theorem 2.5.2. *For any $P \in X$ there exists a unique k-linear map $\mathrm{Res}_P\colon \Omega_{K(X)} \to k$ defined by the following properties:*

- $\mathrm{Res}_P(\omega) = 0$ *for all* $\omega \in \Omega_{X,P}$*;*
- $\mathrm{Res}_P(f^n df) = 0$ *for all* $f \in K(X)^*$ *and all* $n \neq -1$*;*
- $\mathrm{Res}_P(f^{-1} df) = \mathrm{ord}_P(f)$*, where* $\mathrm{ord}_P(f)$ *is the order of f at P.*

Proof. See [Ser88, Chap. II, §7 and §11] or [Tat68]. □

This definition implies the following explicit standard description of the residue map. Let $P \in X$ and let $t \in \mathcal{O}_{X,P}$ be a local parameter at P. We may then write any $\omega \in \Omega_{K(X)}$ in the form

$$\omega = \sum_{i=-n}^{-1} a_i t^i dt + \omega_0,$$

for some $a_{-n}, \ldots, a_{-1}$ and $\omega_0 \in \Omega_{X,P}$. Then we obviously have

$$\mathrm{Res}_P(\omega) = a_{-1}.$$

Theorem 2.5.3 (Residue Theorem). *Given any differential $\omega \in \Omega_{K(X)}$ on X then*

$$\sum_{P \in X} \mathrm{Res}_P(\omega) = 0.$$

Proof. See [Ser88, Chap. II, Prop. 6] or [Tat68, Pg. 155]. □

Since $\Omega_{X,P} \subseteq \ker(\mathrm{Res}_P)$, it follows that Res_P is a well defined function on the quotient $\Omega_{K(X)}/\Omega_{X,P}$. Hence by the residue theorem the map

$$\bigoplus_{P \in X} \Omega_{K(X)}/\Omega_{X,P} \to k, \quad (\omega_P)_{P \in X} \mapsto \sum_{P \in X} \mathrm{Res}_P(\omega_P)$$

vanishes on the image of $\Omega_{K(X)}$, which allows us to make the following definition.

Definition 2.5.4. Let $\overline{(\omega_P)}_{P \in X} \in H^1(X, \Omega_X)$. Then we define the ***trace map*** to be

$$t\colon H^1(X, \Omega_X) \to k, \qquad \overline{(\omega_P)}_{P \in X} \mapsto \sum_{P \in X} \mathrm{Res}_P(\omega_P).$$

We now use the trace map to define a pairing between the k-vector spaces $H^1(X, \mathcal{O}_X)$ and $H^0(X, \Omega_X)$. Since $\Omega_{K(X)}$ is a $K(X)$-module, we can define the product map

$$H^0(X, \Omega_X) \times H^1(X, \mathcal{O}_X) \to H^1(X, \Omega_X), \; \left(\omega, \overline{(f_P)}_{P \in X}\right) \mapsto \overline{((f\omega)_P)}_{P \in X}, \tag{2.8}$$

where $(f\omega)_P$ is the product of $f_P \in K(X)/\mathcal{O}_{X,P}$ and the residue class of ω in $\Omega_{K(X)}/\Omega_{X,P}$.

We now combine the product map in (2.8) with the trace map t to get a map

$$H^0(X, \Omega_X) \times H^1(X, \mathcal{O}_X) \to k, \quad \left(\omega, \overline{(f_P)}_{P \in X}\right) \mapsto \left\langle \omega, \overline{(f_P)}_{P \in X} \right\rangle := t\left(\overline{(f\omega)_P}\right)_{P \in X}.$$

Theorem 2.5.5. *Via the pairing $\langle \; , \; \rangle$, the k-vector spaces $H^1(X, \mathcal{O}_X)$ and $H^0(X, \Omega_X)$ are dual to each other.*

Proof. This is a specialisation of [Ser88, Chap. II, Thm. 2]. □

More explicitly, this theorem means the following. If we fix any $\omega \in H^0(X, \Omega_X)$ we produce a map $\theta(\omega)\colon H^1(X, \mathcal{O}_X) \to k$, given by $\theta(\omega)(f) = \langle \omega, f \rangle$. Similarly, if we fix any $f \in H^1(X, \mathcal{O}_X)$ then we get a map $\psi(f)\colon H^0(X, \Omega_X) \to k$. Then the maps

$$\psi\colon H^1(X, \mathcal{O}_X) \to \hom(H^0(X, \Omega_X), k) \quad \text{and} \quad \theta\colon H^0(X, \Omega_X) \to \hom(H^1(X, \mathcal{O}_X), k)$$

are isomorphisms. In particular, given a k-basis $\omega_1, \ldots, \omega_g$ of $H^0(X, \Omega_X)$, we can find a basis $f_1, \ldots, f_g$ of $H^1(X, \mathcal{O}_X)$ such that $\langle \omega_i, f_i \rangle = 1$ for all $1 \le i \le n$ and $\langle \omega_i, f_j \rangle = 0$ if $i \ne j$, and likewise, starting with a basis of $H^1(X, \mathcal{O}_X)$ we can find corresponding basis of $H^0(X, \Omega_X)$.

Chapter 3

Bases for the spaces of (poly)differentials on hyperelliptic curves

In this chapter we recall the definition and basic details of hyperelliptic curves, and then go on to compute bases for the spaces of holomorphic differentials and polydifferentials, see Propositions 3.1.2 and 3.2.5. The primary use of these concepts is to form a foundation for the next chapter. Furthermore, we also use the bases computed to illustrate all the facets of our main theorem in Chapter 5. The various attributes of hyperelliptic curves differ greatly according to whether the characteristic of the base field is two or not, and as such we split this chapter into two sections, considering these cases separately.

Before going in to the details of hyperelliptic curves we recall that a curve X is hyperelliptic if there exists a finite separable morphism $\pi\colon X \longrightarrow \mathbb{P}^1_k$ of degree two. Every hyperelliptic curve has a hyperelliptic involution σ which permutes the elements of $\pi^{-1}(a)$ for each $a \in \mathbb{P}^1_k$ (except for the finite number of points a for which $\pi^{-1}(a)$ has order one), and the quotient curve $X/\langle\sigma\rangle$ is isomorphic to $\mathbb{P}^1_k$. We let X be a hyperelliptic curve of genus g throughout the chapter, and we fix such a map π, which is unique up to an automorphism of $\mathbb{P}^1_k$ [Liu02, Prop. 7.4.29]. We also let P_a and P'_a denote the unique elements of $\pi^{-1}(a)$ for any point $a \in \mathbb{P}^1_k$ that is not a branch point. If $a \in \mathbb{P}^1_k$ is a branch point we denote the unique point in $\pi^{-1}(a)$ by P_a. We define D_a to be the divisor $\pi^*([a])$ for any $a \in \mathbb{P}^1_k$, and hence

$$D_a = \begin{cases} 2[P_a] & \text{if } a \text{ is a branch point,} \\ [P_a] + [P'_a] & \text{otherwise.} \end{cases}$$

We also have for $x \in k(x) = K(\mathbb{P}^1_k) \subseteq K(X)$, that

$$\operatorname{div}(x) = D_0 - D_\infty, \tag{3.1}$$

regardless of characteristic. Furthermore, the strong Riemann-Hurwitz formula (Theorem 2.4.6) gives us

$$\operatorname{div}_X(dx) = \pi^*(\operatorname{div}_{\mathbb{P}^1_k}(dx)) + R,$$

and since $\operatorname{div}_{\mathbb{P}^1_k}(dx) = -2[\infty]$, it follows that $\pi^*(\operatorname{div}_{\mathbb{P}^1_k}(dx)) = -2D_\infty$. Hence we conclude that

$$\operatorname{div}(dx) = R - 2D_\infty. \tag{3.2}$$

3.1 Characteristic unequal to 2

In this section we assume that $\operatorname{char}(k) = p \neq 2$. Then the extension $K(X)$ of $K(\mathbb{P}^1_k) = k(x)$ corresponding to $\pi\colon X \to \mathbb{P}^1_k$ will be $k(x,y)$, where y satisfies

$$y^2 = f(x) \tag{3.3}$$

for some polynomial $f(x) \in k[x]$ which has no repeated roots and is of degree $2g+1$ or $2g+2$ [Liu02, Prop. 7.4.24]. Moreover, by applying an automorphism of $\mathbb{P}^1_k$ if necessary, we can and will assume that $f(x)$ is monic.

If we let $d_f := \deg(f(x))$ then

$$f(x) = \prod_{i=1}^{d_f}(x - a_i) = x^{d_f} + b_{d_f-1}x^{d_f-1} + \ldots + b_0, \tag{3.4}$$

for some $a_i, b_i \in k$. We now show that the $a_i \in \mathbb{A}^1_k$, and possibly $\infty \in \mathbb{P}^1_k$, are the branch points of π.

Firstly, observe that by the Riemann-Hurwitz formula, Corollary 2.4.7,

$$\deg(R) = 2g - 2 + 2 \cdot 2 = 2g + 2.$$

Since π is of degree two and $\operatorname{char}(k) \neq 2$ it is only tamely ramified, and it follows that the coefficient of each ramification point is 1 in R. From this we conclude that each branch point has precisely one corresponding ramification point, and that there are precisely $2g+2$ ramification points. Also, since there are no repeated roots in $f(x)$, then (3.3) defines a non-singular affine curve X' with a degree two projection $\pi'\colon X' \to \mathbb{A}^1_k$. For any point $a \in \mathbb{A}^1_k$ which is not a solution to $f(x)$ there are two points in the pre-image, namely $(a, \pm\sqrt{a})$, and the point is not a branch point. On the other hand, if $a = a_i \in \mathbb{A}^1_k$ is a solution to $f(x)$, then there is only one point in the pre-image and hence it is a branch point. We let $P_i = P_{a_i}$ denote the ramification point corresponding to a_i. Since $\deg(R) = 2g+2$ we conclude that if $d_f = 2g+1$ then $\infty \in \mathbb{P}^1_k$ is also a branch point and we define $P_{2g+2} := P_\infty$ in this case. Hence the ramification divisor R of π is

$$R = \sum_{i=1}^{2g+2} [P_i].$$

In the following lemma we compute the divisor of $y \in K(X)$.

Lemma 3.1.1. *The divisor of $y \in K(X)$ is*

$$\operatorname{div}(y) = R - (g+1)D_\infty. \tag{3.5}$$

Proof. Since $\operatorname{div}(y^2) = \operatorname{div}(f(x))$ and hence $\operatorname{div}(y) = \frac{1}{2}\operatorname{div}(f(x))$, we need only compute the divisor of $f(x)$. As noted earlier, the solutions to $f(x)$ correspond to the ramification points. So for any $P \notin \pi^{-1}(\infty)$ then $\operatorname{ord}_P(y) = \frac{1}{2}\operatorname{ord}_P(f(x)) = 1$ if P is a ramification point, and $\operatorname{ord}_P(y) = \frac{1}{2}\operatorname{ord}_P(f(x)) = 0$ otherwise.

We now consider the poles of y. By Proposition 2.2.2 we know that $\sum_{P\in X}\operatorname{ord}_P(f(x)) = 0$, and we also know that the poles of $f(x)$ can only lie in $\pi^{-1}(\infty)$. Hence if ∞ is a branch point then $\operatorname{ord}_{P_\infty}(f(x)) = -\sum_{i=1}^{2g+1}\operatorname{ord}_{P_i}(f(x)) = -2(2g+1)$, and $\operatorname{ord}_{P_\infty}(y) = -(2g+1)$. On the other hand, if ∞ is not a branch point we know that $\operatorname{ord}_{P_\infty}(f(x)) + \operatorname{ord}_{P'_\infty}(f(x)) = -2(2g+2)$. Recall that $\operatorname{ord}_P(\sigma(f(x))) = \operatorname{ord}_{\sigma(P)}(f(x))$ for any automorphism $\sigma \in \operatorname{Aut}(X)$ and any point $P \in X$. In particular, if σ is the hyperelliptic involution of X then

$$\operatorname{ord}_{P_\infty}(f(x)) = \operatorname{ord}_{P_\infty}(\sigma(f(x))) = \operatorname{ord}_{\sigma(P_\infty)}(f(x)) = \operatorname{ord}_{P'_\infty}(f(x)).$$

Hence $\operatorname{ord}_{P_\infty}(y) = \operatorname{ord}_{P'_\infty}(y) = -(g+1)$ Overall, we conclude that

$$\operatorname{div}(y) = \sum_{i=1}^{2g+2}[P_i] - (g+1)D_\infty = R - (g+1)D_\infty.$$

□

Proposition 3.1.2. *Let $m \geq 1$. Let X, x and y be as above, and let $\omega := \frac{dx^{\otimes m}}{y^m}$. Then if $g \geq 2$, a basis of $H^0(X, \Omega_X^{\otimes m})$ is given by*

$\omega, x\omega, \dots, x^{g-1}\omega$	*if $m = 1$,*
$\omega, x\omega, x^2\omega$	*if $m = g = 2$,*
$\omega, x\omega, \dots, x^{m(g-1)}\omega;\ y\omega, xy\omega, \dots, x^{(m-1)(g-1)-2}y\omega$	*otherwise.*

Remark. Note that the case where $m = 1$ is treated in [Liu02, Prop. 7.4.26] and [Gri89, Ch. IV, §4, Prop. 4.3].

Proof. We first show that the elements are linearly independent over k. Since ω is fixed, it is equivalent to show that the coefficients are linearly independent over k — i.e. that $1, x, \dots, x^n, y, xy, \dots, x^l y$ are linearly independent over k for any n and l in $\mathbb{N}$. It is immediate that $1, x, \dots, x^n$ are linearly independent, and similarly that $y, yx, \dots, yx^l$ are linearly independent. Finally, the two sets of elements are linearly independent of each other, otherwise the extension $K(X)/k(x)$ would be degree 1.

To show that the differentials in the statement of the lemma are indeed holomorphic differentials, we show that their divisors are greater than 0. Recall that $\operatorname{div}(dx^{\otimes m}) = m \operatorname{div}(dx)$, as noted in the previous chapter. We now show that the differentials listed in Proposition 3.1.2 are holomorphic. We have that

$$\begin{aligned} \operatorname{div}(x^i \omega) &= \operatorname{div}\left(\frac{x^i dx^{\otimes m}}{y^m}\right) \\ &= i(D_0 - D_\infty) + m(R - 2D_\infty) - m(R - (g+1)D_\infty) \\ &= iD_0 + (mg - m - i)D_\infty \\ &= iD_0 + (m(g-1) - i)D_\infty, \end{aligned} \tag{3.6}$$

by Lemma 3.1.1, (3.1) and (3.2), which is positive for $0 \le i \le m(g-1)$. Hence all the polydifferentials in the first two cases and the first $m(g-1)+1$ differentials in the third case are holomorphic. Note that if $m = g = 2$ then there are three elements, and since $\dim_k H^0(X, \Omega_X^{\otimes 2}) = 3$ by Corollary 2.3.7, these elements form a basis. Also, if $m = 1$ then by Definition 2.2.4 $\dim_k H^0(X, \Omega_X) = g$, and we have g linearly independent elements, so they again must form a basis.

We now consider the final $(m-1)(g-1)-1$ differentials in the third case. The divisor of one of these elements is

$$\begin{aligned} \operatorname{div}(x^i y \omega) &= \operatorname{div}(x^i \omega) + R - (g+1)D_\infty \\ &= iD_0 + R + ((m-1)(g-1) - 2 - i)D_\infty, \end{aligned}$$

by Lemma 3.1.1 and (3.6), which is positive for $0 \le i \le (m-1)(g-1) - 2$. By Corollary 2.3.7 we know that

$$\dim_k H^0(X, \Omega_X^{\otimes m}) = (2m-1)(g-1).$$

Since the number of differentials listed in the last case of the proposition is precisely

$$(m-1)(g-1) - 1 + m(g-1) + 1 = 2mg - 2m - g + 1 = (2m-1)(g-1),$$

it is clear that these elements form a basis. □

3.2 Characteristic 2

In this section we assume that $\mathrm{char}(k) = p = 2$. In this case the function field $K(X)$ is $k(x,y)$, a degree two extension of the function field of one variable over k, $k(x) = k(\mathbb{P}^1_k)$, where

$$y^2 - H(x)y = F(x) \tag{3.7}$$

for some polynomials $H(x), F(x) \in k[x]$, such that $H(x)$ and $H'(x)^2F(x) + F'(x)^2$ have no common roots in k [Liu02, Prop. 7.4.24]. We have that $\deg(H(x)) \le g+1$, with equality if and only if ∞ is not a branch point, and that $\deg(F(x)) \le 2g+2$ with $\deg(F(x)) = 2g+1$ if ∞ is a branch point [Liu02, Prop. 7.4.24].

Lemma 3.2.1. *The affine plane curve X' given by* (3.7) *is smooth if and only if $H(x)$ and $H'(x)^2F(x) + F'(x)^2$ have no common zeroes in k.*

Proof. The Jacobian criterion (see, for example, [Liu02, Thm. 4.2.19]), states that if the derivatives of (3.7) with respect to x and with respect to y are zero at a point $P \in X'$ then the curve is not smooth at P, and otherwise it is. Clearly

$$\frac{d}{dy}(y^2 - H(x)y - F(x)) = H(x) \tag{3.8}$$

since the characteristic of k is 2. On the other hand,

$$\frac{d}{dx}(y^2 - H(x)y - F(x)) = H'(x)y - F'(x). \tag{3.9}$$

The affine plane curve given by (3.7) is smooth at $P \in X'$ if and only if at least one of (3.8) and (3.9) is non-zero at P. Of course, (3.9) is zero if and only its square

$$(H'(x)y - F'(x))^2 = H'(x)^2y^2 - F'(x)^2 = H'(x)^2H(x)y + H'(x)^2F(x) - F'(x)^2 \tag{3.10}$$

is zero. Finally, if $H(a) = 0$ for some $a \in k$, then (3.10) evaluated at a is $H'(a)^2F(a) - F'(a)^2$. Hence the curve is smooth if and only if $H'(x)^2F(x) - F'(x)^2$ and $H(x)$ share no roots in k. □

We first describe the ramified points of π, in order to compute the ramification divisor. By Lemma 3.2.1 if we consider the affine curve defined by this equation it will be smooth. We denote this curve by X'. Then π restricts to a map $X' \to \mathbb{A}^1_k$, the projection on to the x co-ordinate. Let $a \in \mathbb{A}^1_k$. Then if (a,b) is a point in $\pi^{-1}(a)$, so is the point $(a, b + H(a))$, which is clearly distinct if and only if $H(a) \neq 0$. Since the extension is degree two, this shows that the ramified points in the affine part correspond to the roots of $H(x)$. We let k be the number of distinct roots that $H(x)$ has and d_H the degree of $H(x)$. Then

$$H(x) = \prod_{i=1}^{k} (x - A_i)^{n_i} = x^{d_H} + B_{d_H - 1} x^{d_H - 1} + \ldots + B_1 x + B_0 \tag{3.11}$$

for some $A_i, B_i \in k$ and $n_i \in \mathbb{N}$. As above, the A_i are branch points of π and we let $P_i \in X$ be the corresponding ramification points, and $D_i = D_{P_i}$. Note that for each A_i there is a corresponding K_i, which is the square root of $F(A_i)$.

We now compute the ramification divisor of π.

Lemma 3.2.2. *Let n_i be the order of $H(x)$ at $A_i \in \mathbb{A}^1_k$. Then the coefficient δ_P of the ramification divisor R at $P \in X$ is given by*

$$\delta_P = \begin{cases} 2n_i & \text{if } P \in \{P_1, \ldots, P_k\}, \\ 2(g + 1 - d_H) & \text{if } P \in \pi^{-1}(\infty), \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We first show that it will suffice to prove that the coefficient of $[P_i]$ is $2n_i$ for $1 \leq i \leq k$. Note that by the Riemann-Hurwitz formula $\deg(R) = 2g + 2$. If ∞ is not a branch point of π then $\delta_P = 0 = 2(g + 1 - d_H)$, as stated. If ∞ is a branch point then the coefficient at P_∞ is $\deg(R) - \sum_{i=1}^{k} 2n_i = 2g + 2 - 2d_H = 2(g + 1 - d_H)$, again as stated.

Let $P = P_i$ for some $i \in \{1, \ldots, k\}$. Then $y - b_i$ is a local parameter at P. To see this, note that the maximal ideal $\mathfrak{m}_{P,X}$ of the local ring $\mathcal{O}_{X,P}$ at P is generated by $x - a_i$ and $y - b_i$. But $x - a_i \in \mathfrak{m}_P^2$ since π is ramified at P with ramification index 2. By Nakayama's lemma [AM69, Prop. 2.6], $y - b_i$ is therefore a local parameter at P.

Using Hilbert's formula, Theorem 2.4.9, we obtain

$$\begin{aligned} \delta_P &= \sum_{i \geq 0} (\mathrm{ord}(G_i(P)) - 1) \\ &= \max\{i \in \mathbb{N} | G_i(P) \neq \{1\}\} + 1 \\ &= \mathrm{ord}_P(\sigma(y - b_i) - (y - b_i)). \end{aligned}$$

From the defining equation (3.7), it is clear that the hyperelliptic involution is given by $\sigma(y) = y + H(x)$. The following calculation then concludes the proof,

$$\begin{aligned}\delta_P &= \mathrm{ord}_P(\sigma(y-b_i)-(y-b_i)) \\ &= \mathrm{ord}_P(y-b_i+H(x)-y+b_i) \\ &= 2\,\mathrm{ord}_{A_i}(H(x)) \\ &= 2n_i.\end{aligned}$$

□

The divisors of x and dx are the same as when $\mathrm{char}(k) \neq 2$, see (3.1) and (3.2). We also note that since $\mathrm{char}(k) = 2$ we have

$$dF(x) = d(y^2 + yH(x)) = d(yH(x)) = H(x)dy + ydH(x)$$

and hence

$$dy = \frac{F'(x) + yH'(x)}{H(x)}dx \tag{3.12}$$

We now compute the divisor of $H(x)$ too.

Lemma 3.2.3. *The divisor associated to $H(x)$ is*

$$\mathrm{div}(H(x)) = \sum_{i=1}^{k} n_i D_i - d_H D_\infty = R - (g+1)D_\infty.$$

Proof. If π is ramified at infinity then $\mathrm{ord}_{P_\infty}(H(x)) = -2d_H$. If it is not ramified, then $\mathrm{ord}_{P_\infty}(H(x)) = \mathrm{ord}_{P'_\infty}(H(x)) = -d_H = -(g+1)$. For the ramified points P_i, $1 \leq i \leq k$, then $\mathrm{ord}_{P_i}(H(x)) = 2n_i$. At any other point of X the order of $H(x)$ is clearly zero, and the first equality follows. □

Finally, we describe the divisor of y. In order to do this we need to distinguish the zeroes of $F(x)$. Suppose that $F(x)$ has $l \leq \deg(F(x))$ distinct zeroes, and let $\gamma_1, \ldots, \gamma_l \in k \subseteq \mathbb{P}^1_k$ be these zeroes. Then if γ_i is a branch point let $Q_i = (\gamma_i, 0)$ be the unique point in the pre-image $\pi^{-1}(\gamma_i)$. If γ_i is not a branch point then let $Q_i = (\gamma_i, 0)$ and $Q'_i = (\gamma_i, H(\gamma_i))$ be the unique points that form the pre-image $\pi^{-1}(\gamma_i)$. Also, we denote the order of the zero of $F(x)$ at $\gamma_i \in k$ by $m_i \in \mathbb{N}$.

Proposition 3.2.4. *If ∞ is a branch point, the divisor of y is*

$$\mathrm{div}(y) = \sum_{i=1}^{l} m_i[Q_i] - (2g+1)[P_\infty].$$

If ∞ is not a branch point then, after possibly swapping the notations for the two points P_∞ and P'_∞ in $\pi^{-1}(\infty)$, we have

$$\operatorname{div}(y) = \sum_{i=1}^{l} m_i[Q_i] + (g+1-\deg(F(x)))[P_\infty] - (g+1)[P'_\infty].$$

Proof. We first show that the divisor of y on the affine part of X, $U_\infty := X \backslash \pi^{-1}(\infty)$, is $\sum_{i=1}^{l} m_i[Q_i]$. Suppose $P \in U_\infty$. If $F|_P \neq 0$ then it follows that $y|_P \neq 0$, since $F(x) = y(y+H(x))$ (and similarly y does not have a pole at P). Hence $\operatorname{div}(y)$ has a coefficient of zero for any point in $U_\infty \backslash \{Q_1, \dots, Q_l\}$.

Suppose that $P = Q_i = (\gamma_i, 0)$ is an unramified point in U_∞. Then $H(\gamma_i) \neq 0$ and $y\big|_P = 0$, so $y + H(x)$ is a unit at P. Since $y(y+H(x)) = F(x)$ we find that

$$\operatorname{ord}_P(y) = \operatorname{ord}_P\left(\frac{F(x)}{y+H(x)}\right) = \operatorname{ord}_P(F(x)) = m_i.$$

We now look at when $P = Q_i = (\gamma_i, 0)$ is a ramification point. Since $H(x)$ and $H'(x)^2F(x) + F'(x)^2$ cannot share roots it follows that $m_i = 1$. Hence the function $\tilde{F}(x) := (x-\gamma_i)^{-1}F(x)$ is a unit at P. We let $\tilde{H}(x) = (x-\gamma_i)^{-1}H(x)$.

Now

$$y^2 = F(x) - yH(x) = (x-\gamma_i)\left(\tilde{F}(x) - y\tilde{H}(x)\right),$$

and hence

$$\operatorname{ord}_P(y^2) = \operatorname{ord}_P(x-\gamma_i) + \operatorname{ord}_P(\tilde{F}(x) - y\tilde{H}(x)).$$

Since $\operatorname{ord}_P(x-\gamma_i) = 2$ and $\operatorname{ord}_P\left(\tilde{F}(x) - y\tilde{H}(x)\right) \geq 0$ we know that $\operatorname{ord}_P(y) \geq 1$. Hence $(y\tilde{H}(x))\big|_P = 0$, and since $\tilde{F}(x)$ is a unit at P, we conclude that $\tilde{F}(x) - y\tilde{H}(x)$ is a unit at P. Hence $\operatorname{ord}_P(y^2) = 2$, and so $\operatorname{ord}_P(y) = 1 = m_i$. It follows that the divisor of y restricted to U_∞ is $\sum_{i=1}^{l} m_i[Q_i]$.

We now consider the coefficients in $\operatorname{div}(y)$ of the points in $\pi^{-1}(\infty)$. If ∞ is a branch point then $\deg(F(x)) = 2g+1$ and hence $\sum_{i=1}^{l} m_i = 2g+1$. Since y can only have a pole at P_∞, we conclude that the order of this pole is $2g+1$, and hence

$$\operatorname{div}(y) = \sum_{i=1}^{l} m_i[Q_i] - (2g+1)[P_\infty].$$

If ∞ is not a branch point then there are two points at which y may have a pole, namely P_∞ and P'_∞. The hyperelliptic involution σ switches these two points. Furthermore, since $\sigma\colon y \mapsto y + H(x)$ it follows that $\operatorname{ord}_{P'_\infty}(y) = \operatorname{ord}_{P_\infty}(y+H(x))$, a fact we use below.

We now consider three cases, firstly supposing that $\mathrm{ord}_{P_\infty}(y) < -(g+1)$. Then $\mathrm{ord}_{P_\infty}(y) < \mathrm{ord}_{P_\infty}(H(x))$ and hence $\mathrm{ord}_{P_\infty}(y) = \mathrm{ord}_{P_\infty}(y+H(x))$. But this contradicts $\mathrm{ord}_{P_\infty}(y)+\mathrm{ord}_{P_\infty}(y+H(x)) = \mathrm{ord}_{P_\infty}(F(x))$, since the left hand side is less than $-2(g+1)$, which is the minimum value of the right hand side.

We now suppose that $\mathrm{ord}_{P_\infty}(y) = -(g+1)$. Since $y(y+H(x)) = F(x)$ it follows that $-(g+1)+\mathrm{ord}_{P_\infty}(y+H(x)) = \mathrm{ord}_{P_\infty}(F(x))$, and hence $\mathrm{ord}_{P'_\infty}(y) = \mathrm{ord}_{P_\infty}(y+H(x)) = -\deg(F(x))+g+1$.

We now consider the case in which $\mathrm{ord}_{P_\infty}(y) > -(g+1)$. Then, since $\mathrm{ord}_{P_\infty}(H(x)) = -(g+1)$, it follows that $\mathrm{ord}_{P'_\infty}(y) = \mathrm{ord}_{P_\infty}(y+H(x)) = -(g+1)$. It now follows from a computation similar to that in the previous paragraph that $\mathrm{ord}_{P_\infty}(y) = -\deg(F(x))+g+1$, completing the proof. □

The following proposition determines a basis of the k vector space of global holomorphic polydifferentials. The case where $m=1$ can again be found in [Liu02, Prop. 7.4.26].

Proposition 3.2.5. *We assume that* $g \geq 2$ *and let* $\omega := \frac{dx^{\otimes m}}{H(x)^m}$. *Then a basis of* $H^0(X, \Omega_X^{\otimes m})$ *is given by*

$$\begin{array}{cc} \omega, x\omega, \ldots, x^{g-1}\omega & \text{if } m=1, \\ \omega, x\omega, x^2\omega & \text{if } m=g=2, \\ \omega, x\omega, \ldots, x^{m(g-1)}\omega;\; y\omega, xy\omega, \ldots, x^{(m-1)(g-1)-2}y\omega & \text{otherwise.} \end{array}$$

Proof. We first assume that above elements are holomorphic polydifferentials, and show that they then form a basis. To show that the elements are linearly independent over k we need only show that the coefficients of ω are, since ω is fixed. The only case where this is not clear is when the coefficients contain both x and y terms. But since the y terms are all linear, and the extension is of degree two, it must follow that coefficients are linearly independent.

In the case that $m=1$ then we have that $\dim_k H^0(X, \Omega_X) = g$ by Definition 2.2.4, and there are g elements described in the statement of the proposition in this case, so they must form a basis. If $m \geq 2$ then $\dim_k H^0(X, \Omega_X^{\otimes m}) = (2m-1)(g-1)$. If $m=g=2$ then $(2m-1)(g-1) = 3$, and there are three elements listed in the proposition. On the other hand if $m \geq 2$ and $g > 2$ the proposition lists

$$m(g-1)+1+(g-1)(m-1)-2+1 = 2mg-2m-g+1 = (2m-1)(g-1)$$

elements, and again they must form a basis.

We now show that the listed polydifferentials are holomorphic, i.e. that their divisors are non-negative. Firstly we have

$$\begin{aligned}\operatorname{div}(x^i\omega) &= \operatorname{div}\left(\frac{x^i dx^{\otimes m}}{H(x)^m}\right)\\ &= i(D_0 - D_\infty) + m(R - 2D_\infty) - m(R - (g+1)D_\infty)\\ &= iD_0 + (m(g-1) - i)D_\infty\end{aligned}$$

by (3.1), (3.2) and Lemma 3.2.3, and this is clearly non-negative for $0 \le i \le m(g-1)$.

Similarly, if ∞ is a branch point, we have

$$\begin{aligned}\operatorname{div}(x^i y\omega) &= \operatorname{div}(x^i\omega) + \operatorname{div}(y)\\ &= iD_0 + (m(g-1) - i)D_\infty + \sum_{i=1}^{l} m_i[Q_i] - (2g+1)[P_\infty]\\ &= iD_0 + \sum_{i=1}^{l} m_i[Q_i] + (2m(g-1) - 2g - 1 - 2i)[P_\infty]\\ &= iD_0 + \sum_{i=1}^{l} m_i[Q_i] + (2((m-1)(g-1) - 1 - i) - 1)[P_\infty],\end{aligned}$$

by (3.1), (3.2) and Lemma 3.2.3 and Proposition 3.2.4, which is again clearly non-negative for $0 \le i \le (g-1)(m-1) - 2$.

Finally, if ∞ is not a branch then, after possibly switching P_∞ and P'_∞, we have

$$\begin{aligned}&\operatorname{div}(x^i y\omega) = \operatorname{div}(x^i\omega) + \operatorname{div}(y)\\ &\quad = iD_0 + (m(g-1) - 1)D_\infty + \sum_{i=1}^{l} m_i[Q_i] + (g + 1 - \deg(F(x)))[P_\infty] - (g+1)[P'_\infty]\\ &\qquad - mR + m(g+1)D_\infty\\ &\quad = iD_0 + \sum_{i=1}^{l} m_i[Q_i] + (mg - i - m - g - 1)[P'_\infty] + (mg - i - m + g + 1 - \deg(F(x)))[P_\infty]\\ &\quad = iD_0 + \sum_{i=1}^{l} m_i[Q_i] + ((m-1)(g-1) - 2 - i)[P'_\infty] + (mg - i - m + g + 1 - \deg(F(x)))[P_\infty],\end{aligned}$$

by Proposition 3.2.4, (3.1), (3.2) and Lemma 3.2.3. Since $0 \le i \le (g-1)(m-1) - 2$ then the coefficient of $[P'_\infty]$ is clearly non-negative. Finally, since $\deg(F(x)) \le 2g + 2$, the coefficient of $[P_\infty]$ is greater than or equal to that of $[P'_\infty]$, and we conclude that the above divisor is non-negative, completing the proof. □

Chapter 4

Group actions on algebraic de-Rham cohomology

Our aim in this chapter is to study the de Rham cohomology $H^1_{\mathrm{dR}}(X/k)$ of a hyperelliptic curve X as a module over $k[G]$, where G is a subgroup of $\mathrm{Aut}(X)$. In the first section we describe the ordinary cohomology groups $H^1(X, \mathcal{O}_X)$ and $H^1_{\mathrm{dR}}(X/k)$ via Čech cohomology. We can do this particularly elegantly in the case of a hyperelliptic curve X, since we can choose a very simple affine cover, via the natural projection any hyperelliptic curve has on to the projective line. We then use this to prove that the sequence of $k[G]$-modules

$$0 \to H^0(X, \Omega_X) \to H^1_{\mathrm{dR}}(X/k) \to H^1(X, \mathcal{O}_X) \to 0 \tag{4.1}$$

is exact, see Proposition 4.1.2. The rest of the chapter will then build towards showing that for a particular class of hyperelliptic curves this sequence does not split.

Building on the Čech cohomology computations of the previous section, we then use Serre duality and the fact that we have already computed a k vector space basis of $H^0(X, \Omega_X)$ to compute a basis of $H^1(X, \mathcal{O}_X)$ (Theorem 4.2.1), which surprisingly is the same whether $\mathrm{char}(k) = 2$ or not. As an application of this we then give a Mittag-Leffler style theorem for hyperelliptic curves, see Corollary 4.2.2.

In the next section we compute a k vector space basis of $H^1_{\mathrm{dR}}(X/k)$, which features the bases of $H^0(X, \Omega_X)$ and $H^1(X, \mathcal{O}_X)$ already mentioned, as well as other components, see Theorem 4.3.1. Unlike the basis of $H^1(X, \mathcal{O}_X)$, this basis does depend on whether $\mathrm{char}(k) = 2$ or not.

Using this basis we are able, after some computations, to determine precisely how certain automorphisms act on the de Rham cohomology of X. In particular, we look at automorphisms on X of the form $(x, y) \mapsto (x + a, y)$, for some non-zero $a \in k$. Then we prove (see

Theorem 4.4.3) that if G contains such an automorphism, and X ramifies above $\infty \in \mathbb{P}^1_k$, then the short exact sequence (4.1) does not split as a sequence of $k[G]$-modules. It should be noted that such hyperelliptic curves can occur in any genus greater than 1. After this is the final section of the chapter, giving examples to illustrate the details of what happens when the above suppositions are satisfied, and finally giving an example to demonstrate that the supposition that ∞ is a branch point is required.

4.1 Čech cohomology and de Rham cohomology for hyperelliptic curves

Throughout this chapter we assume that X is hyperelliptic of genus $g \geq 2$. We recall from Chapter 3 that a curve is hyperelliptic if there exists a finite, separable morphism of degree two from the curve to $\mathbb{P}^1_k$. We fix such a map $\pi\colon X \to \mathbb{P}^1_k$ of degree two, which is unique up to an automorphism of $\mathbb{P}^1_k$ (see [Liu02, Rem. 7.4.30]).

In this section we describe $H^1(X,\mathcal{O}_X)$ and $H^1(X,\Omega_X)$ concretely for such an X, using Čech cohomology.

By Leray's theorem [Liu02, Thm. 5.2.12] and Serre's affineness criterion [Liu02, Thm. 5.2.23] we know that, if we use an affine cover, the first Čech cohomology group of $\mathcal{O}_X$ will be isomorphic to $H^1(X,\mathcal{O}_X)$. We define $U_a = X\backslash\pi^{-1}(a)$ for any $a \in \mathbb{P}^1_k$ and we let $\mathcal{U}$ be the affine cover of X formed by U_0 and U_∞. Given any sheaf $\mathcal{F}$ on X we have the Čech differential $\check{d}\colon \mathcal{F}(U_0)\times\mathcal{F}(U_\infty) \to \mathcal{F}(U_0\cap U_\infty)$, defined by $(f_0,f_\infty)\mapsto f_0|_{U_0\cap U_\infty} - f_\infty|_{U_0\cap U_\infty}$. In general we will suppress the notation denoting the restriction map. Via this differential we have the following cochain complex

$$0 \to \mathcal{O}_X(U_0)\times\mathcal{O}_X(U_\infty) \xrightarrow{\check{d}} \mathcal{O}_X(U_0\cap U_\infty) \to 0.$$

The first cohomology group of this chain complex is $\check{H}^1(\mathcal{U},\mathcal{O}_X) = \frac{\mathcal{O}_X(U_0\cap U_\infty)}{\mathrm{Im}(\check{d})}$ and hence

$$H^1(X,\mathcal{O}_X) \cong \frac{\mathcal{O}_X(U_0\cap U_\infty)}{\mathrm{Im}(\check{d})} = \frac{\mathcal{O}_X(U_0\cap U_\infty)}{\{f_0 - f_\infty | f_i \in \mathcal{O}_X(U_i)\}}. \tag{4.2}$$

When describing elements of $H^1(X,\mathcal{O}_X)$ using the isomorphism we will denote the residue class of $f \in \mathcal{O}_X(U_0\cap U_\infty)$ in the quotient by $[f]$.

If we replace $\mathcal{O}_X$ by Ω_X in the previous paragraph then everything still holds, and we conclude that

$$H^1(X,\Omega_X) \cong \frac{\Omega_X(U_0\cap U_\infty)}{\mathrm{Im}(\check{d})} = \frac{\Omega_X(U_0\cap U_\infty)}{\{\omega_0 - \omega_\infty | \omega_i \in \Omega_X(U_i)\}}. \tag{4.3}$$

Again, we denote the residue class of $\omega \in \Omega_X(U_0 \cap U_\infty)$ in $H^1(X, \Omega_X)$ by $[\omega]$.

We now describe how the trace map acts on $H^1(X, \Omega_X)$ via the presentation (4.3).

Lemma 4.1.1. *Let $\omega \in \Omega_X(U_0 \cap U_\infty)$ with residue class $[\omega]$ in $H^1(X, \Omega_X)$. Then we have*

$$t([\omega]) = \sum_{P \in \pi^{-1}(\infty)} \mathrm{Res}_P(\omega).$$

On the right hand side we consider ω as an element of the module of differentials, $\Omega_{K(X)}$, via the canonical injection $\Omega_X(U_0 \cap U_\infty) \hookrightarrow \Omega_{K(X)}$.

Proof. We take the Čech complex of (2.7) over the cover $\mathcal{U}$, yielding the following bicomplex, with exact rows

$$\begin{array}{ccccc} \Omega_X(U_0) \times \Omega_X(U_\infty) & \hookrightarrow & \Omega_{K(X)} \times \Omega_{K(X)} & \twoheadrightarrow & \bigoplus_{P \in U_0} \Omega_{K(X)}/\Omega_{X,P} \times \bigoplus_{P \in U_\infty} \Omega_{K(X)}/\Omega_{X,P} \\ \downarrow d_1 & & \downarrow d_2 & & \downarrow d_3 \\ \Omega_X(U_0 \cap U_\infty) & \hookrightarrow & \Omega_{K(X)} & \twoheadrightarrow & \bigoplus_{P \in U_0 \cap U_\infty} \Omega_{K(X)}/\Omega_{X,P} \end{array} \tag{4.4}$$

The exactness of the rows can be derived from 2.5.1, by replacing X by U_0 and U_∞, and noting that in this case the first cohomology group will vanish, by Serre's affineness criteria [Liu02, Thm. 5.2.23].

We can now apply the snake lemma to this diagram, giving a long exact sequence. We first note that d_2 is clearly surjective — any $\omega \in \Omega_{K(X)}$ is mapped to by $(\omega, 0) \in \Omega_{K(X)} \times \Omega_{K(X)}$. Now recall that d_3 is defined by $((\omega_P)_{P \in U_0}, (\omega'_P)_{P \in U_\infty}) \mapsto (\omega_P - \omega'_P)_{P \in U_0 \cap U_\infty}$. Then given any element $(\omega_P)_{U_0 \cap U_\infty} \in \bigoplus \Omega_{K(X)}/\Omega_{X,P}$ we can define

$$(\omega'_P) := \begin{cases} \omega_P & \text{if } P \in U_0 \cap U_\infty \\ 0 & \text{if } P = \infty. \end{cases}$$

Clearly $d_3((\omega'_P)_{P \in U_0}, 0) = (\omega_P)_{P \in U_0 \cap U_\infty}$, and hence d_3 is also surjective. In particular, the fifth and sixth terms of the long exact sequence are zero. We now exhibit isomorphisms between $\ker(d_3)$ and $\mathrm{coker}(d_1)$ and, respectively, the third and fourth terms of (2.3). The fact that $H^1(X, \Omega_X) \cong \mathrm{coker}(d_1)$ follows from the above discussion of Čech cohomology. To show the isomorphism $\ker(d_3) \cong \bigoplus_{P \in X} \Omega_{K(X)}/\Omega_{X,P}$ we first observe that the kernel of d_3 is formed of pairs $((\omega_P)_{P \in U_0}, (\omega'_P)_{P \in U_\infty}) \in \left(\bigoplus_{P \in U_0} \Omega_{K(X)}/\Omega_{X,P}\right) \times \left(\bigoplus_{P \in U_\infty} \Omega_{K(X)}/\Omega_{X,P}\right)$ such that $\omega_P = \omega'_P$ for every $P \in U_0 \cap U_\infty$. From this it follows that the map

$$\bigoplus_{P \in X} \Omega_{K(X)}/\Omega_{X,P} \to \ker(d_3), \quad (\omega_P)_{P \in X} \to \left((\omega_P)_{P \in U_0}, (\omega_P)_{P \in U_\infty}\right)$$

is an isomorphism.

The proof now follows from a diagram chase on (4.4). We start with the residue class $[\omega] \in H^0(X, \Omega_X)$ of $\omega \in \Omega_X(U_0 \cap U_\infty)$. Then ω injects in to $\Omega_{K(X)}$, and since d_2 is surjective we can choose an element of $\Omega_{K(X)} \times \Omega_{K(X)}$ mapping to ω. In particular, we choose $(\omega, 0)$. This then maps to

$$\psi = ((\omega_P)_{P\in U_0}, 0) \in \left(\bigoplus_{P\in U_0} \Omega_{K(X)}/\Omega_{X,P}\right) \times \left(\bigoplus_{P\in U_\infty} \Omega_{K(X)}/\Omega_{X,P}\right).$$

By commutativity of the diagram $\psi \in \ker(d_3) \cong \bigoplus_{P\in X} \Omega_{K(X)}/\Omega_{X,P}$. This means that ω_P, and hence ψ, is zero for any $P \in U_0 \cap U_\infty$. Since ψ is also zero for $P \in \pi^{-1}(\infty)$ it follows that

$$t([\omega]) = \sum_{P\in X} \operatorname{Res}_P(\psi) = \sum_{P\in\pi^{-1}(\infty)} \operatorname{Res}_P(\omega).$$

□

We now recall how to compute the algebraic de Rham cohomology of X via Čech cohomology. Since X is a curve any differentials of degree greater than one on X are zero. Hence the de Rham complex of X is

$$0 \to \mathcal{O}_X \xrightarrow{d} \Omega_X \to 0. \tag{4.5}$$

Here d denotes the differential map $f \mapsto df$, as defined in [Har77, Chap. II, Pg. 172]. We then recall from [Gro66, Pg. 351] that the algebraic de Rham cohomology of X is defined to be the hypercohomology of (4.5).

We use the cover $\mathcal{U}$ and the Čech differentials defined earlier to give us the Čech bicomplex of (4.5), which is

$$\begin{array}{ccccccc} & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{O}_X(U_0)\times\mathcal{O}_X(U_\infty) & \longrightarrow & \Omega_X(U_0)\times\Omega_X(U_\infty) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{O}_X(U_0\cap U_\infty) & \longrightarrow & \Omega_X(U_0\cap U_\infty) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & \end{array} \tag{4.6}$$

By a generalisation of Leray's theorem [Gro61, Cor. 12.4.7] we know that the $H^1_{\mathrm{dR}}(X/k)$ is isomorphic to the first cohomology of the total complex of (4.6). Note that this requires

$\check{H}^p(U_\sigma, \mathcal{O}_X)$ and $\check{H}^p(U_\sigma, \Omega_X)$ to be zero for any σ in the nerve of $\mathcal{U}$ and any $p \geq 1$ — since U_0 and U_∞ are affine, this follows from Serre's affineness criterion [Liu02, Thm. 5.2.23].

Therefore $H^1_{\mathrm{dR}}(X/k)$ is isomorphic to the space

$$\left\{(\omega_0, \omega_\infty, f_{0,\infty}) | \omega_i \in \Omega_X(U_i), f_{0,\infty} \in \mathcal{O}_X(U_0 \cap U_\infty), d f_{0,\infty} = \omega_0|_{U_0\cap U_\infty} - \omega_\infty|_{U_0\cap U_\infty}\right\} \tag{4.7}$$

quotiented by the subspace

$$\left\{(d f_0, d f_\infty, f_0|_{U_0\cap U_\infty} - f_\infty|_{U_0\cap U_\infty}) | f_i \in \mathcal{O}_X(U_i)\right\}. \tag{4.8}$$

Via the isomorphism (4.2) and the description of $H^1_{\mathrm{dR}}(X/k)$ above, we can define the maps

$$i \colon H^0(X, \Omega_X) \to H^1_{\mathrm{dR}}(X/k), \qquad [\omega] \mapsto [(\omega, \omega, 0)] \tag{4.9}$$

and

$$p \colon H^1_{\mathrm{dR}}(X/k) \to H^1(X, \mathcal{O}_X), \qquad [(\omega_0, \omega_\infty, f_{0\infty})] \mapsto [f_{0\infty}]. \tag{4.10}$$

The following lemma shows that $H^1_{\mathrm{dR}}(X/k)$ fits in to a short exact sequence with $H^0(X, \Omega_X)$ and $H^1(X, \mathcal{O}_X)$.

Proposition 4.1.2. *The following sequence is exact:*

$$0 \to H^0(X, \Omega_X) \xrightarrow{i} H^1_{dR}(X/k) \xrightarrow{p} H^1(X, \mathcal{O}_X) \to 0.$$

Proof. Let T be the total complex of (4.6). Moreover, we let $\mathcal{O}$ and Ω be the complexes formed from the first and second (non-trivial) columns of (4.6) respectively. Then let $\Omega[1]$ denote the complex obtained from shifting Ω by one, i.e. $\Omega[1]^{n+1} = \Omega^n$. From this we obtain the following short exact sequence of complexes

$$\Omega[1] \hookrightarrow T \twoheadrightarrow \mathcal{O},$$

giving rise to the following long exact sequence

$$\begin{aligned} 0 \to & H^0_{\mathrm{dR}}(X/k) \to H^0(X, \mathcal{O}_X) \to \\ H^0(X, \Omega_X) \to & H^1_{\mathrm{dR}}(X/k) \to H^1(X, \mathcal{O}_X) \to \\ H^1(X, \Omega_X) \to & H^2_{\mathrm{dR}}(X/k) \to 0, \end{aligned} \tag{4.11}$$

where the maps in the middle line are the maps i (4.9) and p (4.10).

The map $H^0(X, \mathcal{O}_X) \to H^0(X, \Omega_X)$ is the map $f \mapsto df$. Since the only globally holomorphic functions on X are constant functions, it follows that this is the zero map, and hence $H^0(X, \Omega_X) \to H^1_{\mathrm{dR}}(X/k)$ is injective.

Since (4.11) is exact, p is surjective if and only if $\alpha\colon H^1(X,\Omega_X) \to H^2_{\mathrm{dR}}(X/k)$ is injective. Now $H^1(X,\Omega_X)$ is isomorphic to k via the trace map, and if we can show that this isomorphism factors through α it will follow that α is injective. Considering the Čech cohomology constructions of $H^1(X,\Omega_X)$ and $H^2_{\mathrm{dR}}(X/k)$, it suffices to show that the trace map is zero on $\mathrm{Im}\,(d\colon \mathcal{O}_X(U_0\cap U_\infty) \to \Omega_X(U_0\cap U_\infty))$. This follows from Theorem 2.5.2, which says that given any $f\in K(X)$ then $\mathrm{Res}_P(df)=0$ for any $P\in X$, and in particular for any $P\in\pi^{-1}(\infty)$. Hence $t([df])=0$ by Lemma 4.1.1. So the residue isomorphism factors through α, and p is surjective. □

4.2 Basis of $H^1(X,\mathcal{O}_X)$

We now give concrete elements in $\mathcal{O}_X(U_0\cap U_\infty)$ whose classes in $H^1(X,\mathcal{O}_X)$, via the isomorphism (4.2), form a basis of $H^1(X,\mathcal{O}_X)$. Note in particular that the basis is the same regardless of whether $p=2$ or $p\neq 2$. We then give a corollary which is of the same style as the Mittag-Leffler theorem [Ahl78, Chap. 5, §2, Thm. 4].

Theorem 4.2.1. *The elements $\frac{y}{x},\dots,\frac{y}{x^g}\in K(X)$ are regular on $U_0\cap U_\infty$, and their residue classes $\left[\frac{y}{x}\right],\dots,\left[\frac{y}{x^g}\right]$ form a basis of $H^1(X,\mathcal{O}_X)$.*

Proof. We start by considering the case $p\neq 2$ and first check that the functions $\frac{y}{x},\dots,\frac{y}{x^g}$ are indeed regular on $U_0\cap U_\infty$ (as required by (4.2)) by computing their divisors. From (3.1) and (3.5) we see that

$$\begin{aligned}\mathrm{div}\left(\frac{y}{x^i}\right) &= \mathrm{div}(y)-\mathrm{div}(x^i)\\ &= R-(g+1)D_\infty - iD_0 + iD_\infty\\ &= R - iD_0 - (g+1-i)D_\infty.\end{aligned}$$

Since R is a positive divisor this is non-negative on $U_0\cap U_\infty$ for all $i\in\mathbb{Z}$, and hence in particular for $i\in\{0,\dots,g-1\}$.

Recall that the differentials $y^{-1}dx,\dots,x^{g-1}y^{-1}dx$ form a basis of $H^0(X,\Omega_X)$ (see Proposition 3.1.2). By Lemma 4.1.1 we know that $\langle x^iy^{-1}dx, yx^{-j}\rangle = \sum_{P\in\pi^{-1}(\infty)}\mathrm{Res}_P(x^{i-j}dx)$. It follows immediately from Theorem 2.5.2 that $\sum_{P\in\pi^{-1}(\infty)}\mathrm{Res}_P(x^{i-j}dx)=-2$ if $i-j=-1$ and is zero otherwise (regardless of whether ∞ is a branch point). It then follows from Theorem 2.5.5 that the residue classes $\left[yx^{-1}\right],\dots,[yx^{-g}]$ form a basis of $H^1(X,\mathcal{O}_X)$.

We now suppose that $p = 2$, and again start by checking that for $i \in \{1,\dots,g\}$ the function yx^{-i} is regular on $U_0 \cap U_\infty$. This follows once we compute the divisor of yx^{-i}, which is

$$\begin{aligned}\operatorname{div}\left(\frac{y}{x^i}\right) &= \operatorname{div}(y) - i\operatorname{div}(x)\\ &= \sum_{i=1}^{l} m_i[Q_i] - iD_0 - (2g+1-2i)[P_\infty]\end{aligned}$$

if ∞ is a branch point and

$$\begin{aligned}\operatorname{div}\left(\frac{y}{x^i}\right) &= \operatorname{div}(y) - i\operatorname{div}(x)\\ &= \sum_{i=1}^{l} m_i[Q_i] - iD_0 + (g+1-\deg(F(x))+i)[P_\infty] - (g+1-i)[P'_\infty]\end{aligned}$$

otherwise. These equalities follow from Proposition 3.2.4 and (3.1). The divisors are clearly positive on $U_0 \cap U_\infty$ for all $i \in \mathbb{Z}$, and hence for $i \in \{1,\dots,g\}$.

Next we recall from Proposition 3.2.5 that if $p = 2$ a basis of $H^0(X,\Omega_X)$ is given by $\frac{1}{H(x)}dx,\dots,\frac{x^{g-1}}{H(x)}dx$. We then deduce from Lemma 4.1.1 that when ∞ is not a branch point

$$\left\langle \frac{x^i}{H(x)}dx, \frac{y}{x^j}\right\rangle = \operatorname{Res}_{P_\infty}\left(\frac{yx^{i-j}}{H(x)}dx\right) + \operatorname{Res}_{P'_\infty}\left(\frac{yx^{i-j}}{H(x)}dx\right).$$

Then recall that in characteristic two we have an involution $\sigma\colon X \to X$ given by $(x,y) \mapsto (x, y+H(x))$, and that $\operatorname{Res}_P(\sigma^*(\omega)) = \operatorname{Res}_{\sigma(P)}(\omega)$ for any $P \in X$ and $\omega \in H^0(X,\Omega_X)$. Then it follows that

$$\begin{aligned}\left\langle \frac{x^i}{H(x)}dx, \frac{y}{x^j}\right\rangle &= \operatorname{Res}_{P_\infty}\left(\frac{yx^{i-j}}{H(x)}dx\right) + \operatorname{Res}_{P_\infty}\left(\frac{(y+H(x))x^{i-j}}{H(x)}dx\right)\\ &= 2\operatorname{Res}_{P_\infty}\left(\frac{yx^{i-j}}{H(x)}dx\right) + \operatorname{Res}_{P\infty}(x^{i-j}dx)\\ &= \operatorname{Res}_{P_\infty}(x^{i-j}dx),\end{aligned}$$

since we are assuming that $\operatorname{char}(k) = 2$. As in the previous case, it follows from the definition of Res_P that $\operatorname{Res}_{P_\infty}(x^{i-j}dx) = -1$ if $i - j = -1$ and is zero otherwise. Hence , by Theorem 2.5.5, the residue classes of $\frac{y}{x}|_{U_0\cap U_\infty},\dots,\frac{y}{x^g}|_{U_0\cap U_\infty}$ form a basis of $H^1(X,\mathcal{O}_X)$ when $p = 2$ and ∞ is not ramified.

If P_∞ is a branch point then we compute the divisor of $\frac{y}{x^j} \cdot \frac{x^i}{H(x)} dx$, using (3.1), (3.2), Lemma 3.2.3 and Proposition 3.2.4:

$$\begin{aligned}
&\operatorname{div}\left(\frac{yx^{i-j}}{H(x)}dx\right) = \operatorname{div}(y) + \operatorname{div}(x^{i-j}) + \operatorname{div}(dx) - \operatorname{div}(H(x)) \\
&= \sum_{i=1}^{l} m_i[Q_i] - (2g+1)[P_\infty] + (i-j)D_0 - (i-j)D_\infty + R - 2D_\infty - R + (g+1)D_\infty \\
&= \sum_{i=1}^{l} m_i[Q_i] + (2j-3-2i)[P_\infty] + (i-j)D_0.
\end{aligned}$$

We see that there is a pole of order one at P_∞ precisely if $2j-3-2i = -1$, or equivalently if $j = i+1$. Hence $\left\langle \frac{x^i}{H(x)}dx, \frac{y}{x^j} \right\rangle = \operatorname{Res}_{P_\infty}\left(\frac{yx^{i-j}}{H(x)}dx\right) \neq 0$ in this case.

We also check that if $j \neq i+1$ then $\left\langle \frac{x^i}{H(x)}dx, \frac{y}{x^j} \right\rangle = 0$. Indeed, if $j - i \geq 2$ then clearly $\frac{yx^{i-j}}{H(x)}dx$ does not have a pole at P_∞. On the other hand, if $j - i \leq 0$ then the differential $\frac{yx^{i-j}}{H(x)}dx$ is regular on U_∞, and hence the residue on this set is zero. Since $X \backslash U_\infty = \{P_\infty\}$ it follows from the residue theorem (Theorem 2.5.3) that the residue of $\frac{yx^{i-j}}{H(x)}dx$ at P_∞ is also zero, and hence the residue classes of the elements $\left[\frac{y}{x}\right], \ldots, \left[\frac{y}{x^g}\right]$ form a basis of $H^1(X, \mathcal{O}_X)$, in all cases. □

We now give a corollary to Theorem 4.2.1, which is of the same style as the Mittag-Leffler theorem. For a description of the classical Mittag-Leffler problem see [Mir95, Pgs. 180-181].

Corollary 4.2.2. *For each $P \in X$ we fix $f_P \in K(X)/\mathcal{O}_{X,P}$, such that $f_P = 0$ for almost all $P \in X$. Then there exist unique $\alpha_1, \ldots, \alpha_g \in k$ such that, after replacing f_P by $f_P - \left(\alpha_1 \frac{y}{x} + \ldots + \alpha_g \frac{y}{x^g}\right)$ for $P \in \pi^{-1}(\infty)$, we can find an $f \in K(X)$ which has a Laurent tail of f_P at P for all $P \in X$.*

Proof. Since $f_P = 0$ for almost all $P \in X$ then $(f_P)_{P\in X} \in \bigoplus_{P \in X} K(X)/\mathcal{O}_{X,P}$. From Lemma 2.5.1 we have the following exact sequence

$$0 \to H^0(X, \mathcal{O}_X) \to K(X) \to \bigoplus_{P \in X} K(X)/\mathcal{O}_{X,P} \to H^1(X, \mathcal{O}_X) \to 0,$$

and we let δ denote the map $\bigoplus_{P\in X} K(X)/\mathcal{O}_{X,P} \to H^1(X, \mathcal{O}_X)$. By Theorem 4.2.1 the residue classes $\gamma_1 = \left[\frac{y}{x}\right], \ldots, \gamma_g = \left[\frac{y}{x^g}\right]$ form a basis of $H^1(X, \mathcal{O}_X)$, and it follows that there exist unique $\alpha_1, \ldots, \alpha_g \in k$ such that

$$\delta\left((f_P)_{P\in X}\right) - \left(\alpha_1\gamma_1 + \ldots + \alpha_g\gamma_g\right) = 0.$$

We can derive the exact sequence (2.2) by applying the snake lemma to the Čech complex of (2.6) over $\mathcal{U}$, which is

$$\begin{array}{ccccc}
\mathcal{O}_X(U_0)\times\mathcal{O}_X(U_\infty) & \hookrightarrow & K(X)\times K(X) & \twoheadrightarrow & \bigoplus_{P\in U_0} K(X)/\mathcal{O}_{X,P}\times\bigoplus_{P\in U_\infty} K(X)/\mathcal{O}_{X,P} \\
\downarrow d_1 & & \downarrow d_2 & & \downarrow d_3 \\
\mathcal{O}_X(U_0\cap U_\infty) & \hookrightarrow & K(X) & \twoheadrightarrow & \bigoplus_{P\in U_0\cap U_\infty} K(X)/\mathcal{O}_{X,P}
\end{array}$$

where the rows are exact. In particular, the surjectivity of the right hand horizontal maps follows from the fact the exact sequence (2.3) still holds if we replace X by an affine curve, and that in this case the final term of the sequence is zero. Now δ is the differential map $\ker(d_3)=\bigoplus_{P\in X}K(X)/\mathcal{O}_{X,P}\to\operatorname{coker}(d_1)=H^1(X,\mathcal{O}_X)$ in the statement of the snake lemma [Wei94, Lem. 1.3.2]. Hence we can perform a diagram chase to find the element in $\ker(d_3)$ which maps to $\left(\alpha_1\gamma_1+\ldots+\alpha_g\gamma_g\right)\in H^1(X,\mathcal{O}_X)$ via this differential. Firstly, it is clear that $\alpha_1\gamma_1+\ldots+\alpha_g\gamma_g$ pulls back to

$$\left(\left(\left(\alpha_1\frac{y}{x}+\ldots+\alpha_g\frac{y}{x^g}\right)\right)_{P\in U_0},0\right)\in\bigoplus_{P\in U_0}K(X)/\mathcal{O}_{X,P}\times\bigoplus_{P\in U_\infty}K(X)/\mathcal{O}_{X,P}. \tag{4.12}$$

Since $\alpha_i x^i/y$ is regular on $U_\infty\cap U_0$, then (4.12) is equal to $\left((g_P)_{P\in U_0},0\right)$, where

$$g_P=\begin{cases}\alpha_1\frac{y}{x}+\ldots+\alpha_g\frac{y}{x^g} & \text{if } P\in\pi^{-1}(\infty),\\ 0 & \text{else.}\end{cases}$$

Clearly $\left((g_P)_{P\in U_0},0\right)\in\ker(d_3)=\bigoplus_{P\in X}K(X)/\mathcal{O}_{X,P}$, and $\delta\left((g_P)_{P\in U_0},0\right)=\alpha_1\gamma_1+\ldots+\alpha_g\gamma_g$. Hence $\delta((f_P)_{P\in X}-(g_P)_{P\in X})=0$, and by the exactness of (2.2) it follows that there exists an $f\in K(X)$ which has Laurent tail f_P-g_P at each $P\in X$, as required in the statement of the corollary. □

4.3 Basis of $H^1_{\mathrm{dR}}(X/k)$

In order to state a basis of $H^1_{\mathrm{dR}}(X/k)$, as well as to shorten the proof of the following theorem, we define the following polynomials. We suppose that $1\le i\le g$. Then when $p\ne 2$ we define

$$s_i(x):=xf'(x)-2if(x)\in k[x]$$

and when $p=2$ we define

$$S_i(x,y):=xF'(x)+y(xH'(x)+iH(x))\in k[x]\oplus yk[x]\subseteq k(x,y). \tag{4.13}$$

We now decompose these polynomials into two parts, which will be used in the sequel. Firstly, we write $s_i(x)$ as $s_i(x) = \phi_i(x) + \psi_i(x)$, where $\psi_i(x), \phi_i(x) \in k[x]$ are the unique polynomials such that the degree of $\psi_i(x)$ is at most $g+1$ and x^{g+2} divides $\phi_i(x)$. Secondly, we define $A_{j,i} \in k$ for $1 \le j \le 2g+2$, and $B_{k,i} \in k$ for $0 \le k \le g+1$ by the equation

$$S_i(x,y) = A_{2g+2,i}x^{2g+2} + \ldots + A_{1,i}x + y(B_{g+1,i}x^{g+1} + \ldots + B_{1,i}x + B_{0,i}).$$

Note that many of these coefficients may be zero. In particular we remark that the x^i term of $xH'(x) + iH(x)$ is always zero, since $B_{i,i}x^i = x \cdot iB_i x^{i-1} + iB_i x^i = 2iB_i x^i = 0$. We now define the following polynomials:

$$\begin{aligned} \Phi_i^x(x) &= A_{2g+2,i}x^{2g+2} + \ldots + A_{i+1,i}x^{i+1}, \\ \Psi_i^x(x) &= A_{i,i}x^i + \ldots + A_{1,i}x, \\ \Phi_i^y(x) &= B_{g+1,i}x^{g+1} + \ldots B_{i+1,i}x^{i+1}, \\ \Psi_i^y(x) &= B_{i-1,i}x^{i-1} + \ldots + B_{1,i}x + B_{0,i}. \end{aligned} \tag{4.14}$$

Finally, we define $\Phi_i(x,y) = \Phi_i^x(x) + y\Phi_i^y(x)$ and $\Psi_i(x,y) = \Psi_i^x(x) + y\Psi_i^y(x)$, so that $S_i(x,y) = \Phi_i(x,y) + \Psi_i(x,y)$.

Viewing $H^1_{\mathrm{dR}}(X/k)$ as the quotient of (4.7) by (4.8), we now give a k-vector space basis of $H^1_{\mathrm{dR}}(X/k)$.

Theorem 4.3.1. *If $p \neq 2$ then the residue classes*

$$\left[\left(\left(\frac{\psi_i(x)}{2yx^{i+1}}\right)dx, \left(\frac{-\phi_i(x)}{2yx^{i+1}}\right)dx, x^{-i}y\right)\right], i = 1, \ldots, g, \tag{4.15}$$

along with the residue classes

$$\left[\left(\frac{x^i}{y}dx, \frac{x^i}{y}dx, 0\right)\right], i = 0, \ldots, g-1, \tag{4.16}$$

form a k-basis of $H^1_{dR}(X/k)$.

On the other hand, if $p = 2$ then the residue classes

$$\left[\left(\left(\frac{\Psi_i(x,y)}{x^{i+1}H(x)}\right)dx, \left(\frac{\Phi_i(x,y)}{x^{i+1}H(x)}\right)dx, x^{-i}y\right)\right], i = 1, \ldots, g, \tag{4.17}$$

together with the residue classes

$$\left[\left(\frac{x^i}{H(x)}dx, \frac{x^i}{H(x)}dx, 0\right)\right], i = 0, \ldots, g-1, \tag{4.18}$$

form a k-basis of $H^1_{dR}(X/k)$.

Before proving this theorem we use it to prove the following corollaries.

Corollary 4.3.2. *Let G be a subgroup of the automorphism group* $\mathrm{Aut}(X)$*. Then the action of G on $H^1_{dR}(X/k)$ is faithful unless G contains a hyperelliptic involution and $p = 2$, in which case the action of the hyperelliptic involution is trivial.*

Proof. Recall from Proposition 4.1.2 that $H^0(X, \Omega_X)$ injects into $H^1_{\mathrm{dR}}(X/k)$. Then if $p \neq 2$ or G does not contain a hyperelliptic involution it follows from Theorem 5.3.1 that G acts faithfully on $H^0(X, \Omega_X)$, and hence G acts faithfully on $H^1_{\mathrm{dR}}(X/k)$.

We now suppose that $p = 2$ and that G contains a hyperelliptic involution, which we denote by σ. Again by Theorem 5.3.1, we know that σ acts trivially on $H^0(X, \Omega_X)$.

Since $H^0(X, \Omega_X)$ is dual to $H^1(X, \mathcal{O}_X)$ then σ also acts trivially on $H^1(X, \mathcal{O}_X)$. We can study exactly why this is from the view of Čech cohomology, and this will also help to determine the action of σ on $H^1_{\mathrm{dR}}(X/k)$. If we fix a natural number $i \in \{1, \ldots, g\}$ then σ maps $\frac{y}{x^i}$ to $\frac{y}{x^i} + \frac{H(x)}{x^i}$. Now we can write the rational function $\frac{H(x)}{x^i}$ as follows,

$$\frac{H(x)}{x^i} = \frac{B_{i-1}x^{i-1} + \ldots + B_1 x + B_0}{x^i} - \left(-\frac{x^{d_H} + B_{d_H - 1}x^{d_H - 1} + \ldots + B_i x^i}{x^i} \right),$$

where B_j and d_H are as in (3.11). Since this is clearly the difference of an element of $\mathcal{O}_X(U_0)$ and an element of $\mathcal{O}_X(U_\infty)$ we see that $\frac{H(x)}{x^i}$ is zero in $H^1(X, \mathcal{O}_X)$. We let

$$H_{1,i}(x) = B_{i-1}x^{i-1} + \ldots + B_1 x + B_0 \quad \text{and} \quad H_{2,i}(x) = -(x^d + B_{d-1}x^{d-1} + \ldots + B_i x^i).$$

We now consider the action of σ on the entries in (4.17). Firstly we see that

$$\begin{aligned}
\sigma\left(\frac{-\Psi_i(x,y)}{x^{i+1}H(x)}dx\right) &= \frac{-\sigma(\Psi_i(x,y))}{x^{i+1}H(x)}dx \\
&= \frac{-\Psi_i(x,y)}{x^{i+1}H(x)}dx + \frac{H(x)(xH'_{1,i}(x) + iH_{1,i}(x))}{x^{i+1}H(x)}dx \\
&= \frac{-\Psi_i(x,y)}{x^{i+1}H(x)}dx + \frac{xH'_{1,i}(x) + iH_{1,i}(x)}{x^{i+1}}dx \\
&= \frac{-\Psi_i(x,y)}{x^{i+1}H(x)}dx + \frac{H'_{1,i}(x)}{x^i}dx + \frac{iH_{1,i}(x)}{x^{i+1}}dx \\
&= \frac{-\Psi_i(x,y)}{x^{i+1}H(x)}dx + \frac{1}{x^i}d\left(H_{1,i}(x)\right) + H_{1,i}(x)d\left(\frac{1}{x^i}\right) \\
&= \frac{-\Psi_i(x,y)}{x^{i+1}H(x)}dx + d\left(\frac{H_{1,i}(x)}{x^i}\right),
\end{aligned}$$

where the second equality follows from (4.13) and the fact that $\sigma(y) = y + H(x)$.

Similarly we can derive

$$\sigma\left(\frac{\Phi_i(x,y)}{x^{i+1}H(x)}dx\right) = \frac{\Phi_i(x,y)}{x^{i+1}H(x)}dx + d\left(\frac{H_{2,i}(x)}{x^i}\right).$$

Lastly, it is clear that $\sigma(x^{-i}y) = x^{-i}(y + H(x))$.

We can now describe exactly how σ acts on the elements of (4.17) using $H_{1,i}(x)$ and $H_{2,i}(x)$:

$$\sigma\left(\left[\left(\left(\frac{-\Psi_i(x,y)}{x^{i+1}H(x)}\right)dx, \left(\frac{\Phi_i(x,y)}{x^{i+1}H(x)}\right)dx, x^{-i}y\right)\right]\right) =$$
$$\left[\left(\left(\frac{-\Psi_i(x,y)}{x^{i+1}H(x)}\right)dx + d\left(\frac{H_{1,i}(x)}{x^i}\right), \left(\frac{\Phi_i(x,y)}{x^{i+1}H(x)}\right)dx + d\left(\frac{H_{2,i}(x)}{x^i}\right), \frac{y+H(x)}{x^i}\right)\right].$$

So the action of σ on the basis elements in (4.17) amounts to adding the residue class

$$\left[\left(d\left(\frac{H(x)_{1,i}}{x^i}\right), d\left(\frac{H(x)_{2,i}}{x^i}\right), \frac{H(x)}{x^i}\right)\right],$$

which is clearly an element of (4.8) and hence is zero. So the action of the involution σ on $H^1_{\mathrm{dR}}(X/k)$ is trivial and hence the action of the group G is not faithful. □

Corollary 4.3.3. *Let $p \neq 2$. Then the hyperelliptic involution acts on $H^1_{dR}(X/k)$ by multiplication with -1.*

Proof. The hyperelliptic involution σ acts by $(x,y) \mapsto (x,-y)$. Hence, if we let

$$\gamma_i = \left[\left(\left(\frac{\psi_i(x)}{2yx^{i+1}}\right)dx, \left(\frac{-\phi_i(x)}{2yx^{i+1}}\right)dx, x^{-i}y\right)\right],$$

then clearly $\sigma(\gamma_i) = -\gamma_i$. Similarly, if

$$\lambda_i = \left[\left(\frac{x^i}{y}dx, \frac{x^i}{y}dx, 0\right)\right]$$

then $\sigma(\lambda_i) = -\lambda_i$. Hence σ acts by multiplication with -1 on $H^1_{\mathrm{dR}}(X/k)$. □

We now prove Theorem 4.3.1.

Proof. We make use of the fact that the short exact sequence in Proposition 4.1.2 splits as a sequence of vector spaces over k, and that we know bases of the outer two terms.

It is clear that the elements in (4.16) and (4.18) are elements of (4.7). In fact, it follows from Propositions 3.1.2 and 3.2.5 that they are the image of a basis of $H^0(X,\Omega_X)$ in $H^1_{\mathrm{dR}}(X/k)$.

Moreover, it is obvious that if the elements in (4.15) and (4.17) are well defined elements of the space (4.7) then they will map to the basis of $H^1(X, \mathcal{O}_X)$ given in Theorem 4.2.1. So we need only show that the terms in (4.15) and (4.17) satisfy the conditions stated in (4.7). For the rest of the proof we fix $i \in \{1, \dots, g\}$.

We start with the case $p \neq 2$, and observe that

$$\begin{aligned}
\left(\frac{\psi_i(x)}{2yx^{i+1}} - \frac{-\phi_i(x)}{2yx^{i+1}}\right)dx &= \frac{s_i(x)}{2yx^{i+1}}dx \\
&= \frac{1}{2yx^i}\left(f(x)' - \frac{2if(x)}{x}\right)dx \\
&= \frac{x^i}{2y}\left(\frac{f(x)'}{x^{2i}}dx - \frac{2if(x)}{x^{2i+1}}dx\right) \\
&= \frac{x^i}{2y}\left(f(x)d\left(\frac{1}{x^{2i}}\right) + \frac{1}{x^{2i}}df(x)\right) \\
&= \frac{x^i}{2y}d(f(x)x^{-2i}) \\
&= \frac{x^i}{2y}d\left(\left(yx^{-i}\right)^2\right) \\
&= d(yx^{-i}),
\end{aligned}$$

with the penultimate line following from the defining equation (3.3). This shows that the elements in (4.15) satisfy $df_{0,\infty} = \omega_0 - \omega_\infty$, one of the conditions of (4.7). Since we saw in the proof of Theorem 4.2.1 that $\frac{y}{x^i}$ is regular on $U_0 \cap U_\infty$ it only remains to show that $\frac{\phi_i(x)}{2yx^{i+1}}dx$ and $\frac{-\psi_i(x)}{2yx^{i+1}}dx$ are regular on U_∞ and U_0 respectively.

In order to do this we fix $\alpha_{j,i} \in k$ for $0 \leq j \leq 2g+2$ satisfying the equation

$$s_i(x) = \alpha_{2g+2,i}x^{2g+2} + \ldots + \alpha_{0,i},$$

so that

$$\phi_i(x) = \alpha_{2g+2,i}x^{2g+2} + \ldots + \alpha_{g+2,i}x^{g+2}$$

and

$$\psi_i(x) = \alpha_{g+1,i}x^{g+1} + \ldots + \alpha_{0,i}.$$

Note that it is possible for any of $\alpha_{j,i}$ to be zero. In fact, it is possible for either $\phi_i(x)$ or $\psi_i(x)$ to be zero. Whenever they are non-zero we denote their degrees as polynomials in x by d_ϕ and d_ψ respectively. From the definition of $\phi_i(x)$ and $\psi_i(x)$ we know that $0 \leq d_\psi \leq g+1$ and $g+1 < d_\phi \leq 2g+2$.

We now show that $\frac{-\phi_i(x)}{2yx^{i+1}}dx$ and $\frac{\psi_i(x)}{2yx^{i+1}}dx$ are regular on U_∞ and U_0 respectively. We may assume that $\phi_i(x)$ and $\psi_i(x)$ are non-zero, since the zero function is regular everywhere.

The divisor of $\frac{-\phi_i(x)}{2yx^{i+1}}dx$ is

$$\begin{aligned}
\operatorname{div}\left(\frac{-\phi_i(x)}{2yx^{i+1}}dx\right) &= \operatorname{div}(\phi_i(x)) - \operatorname{div}(y) - \operatorname{div}(x^{i+1}) + \operatorname{div}(dx) \\
&= \operatorname{div}(\phi_i(x)) - (R - (g+1)D_\infty) - ((i+1)D_0 - (i+1)D_\infty) \\
&\quad + (R - 2D_\infty) \\
&= \left(\operatorname{div}_0\left(\frac{\phi_i(x)}{x^{g+2}}\right) + (g+2)D_0 - d_\phi D_\infty\right) - (i+1)D_0 + (g+i)D_\infty \\
&\geq \operatorname{div}_0\left(\frac{\phi_i(x)}{x^{g+2}}\right) + (g+2)D_0 - (2g+2)D_\infty - (i+1)D_0 + (g+i)D_\infty \\
&= \operatorname{div}_0\left(\frac{\phi_i(x)}{x^{g+2}}\right) + (i-g-2)D_\infty + (g-i+1)D_0,
\end{aligned}$$

where the second equality makes use of (3.1) and (3.5). Since $i \leq g$ the differential $\frac{-\phi_i(x)}{2yx^{i+1}}dx$ is regular on $U_\infty = X\backslash\pi^{-1}(\infty)$.

Similarly the divisor of $\frac{\psi_i(x)}{2yx^{i+1}}dx$ is

$$\begin{aligned}
\operatorname{div}\left(\frac{\psi_i(x)}{2yx^{i+1}}dx\right) &= \operatorname{div}(\psi_i(x)) - \operatorname{div}(y) - \operatorname{div}(x^{i+1}) + \operatorname{div}(dx) \\
&= \operatorname{div}(\psi_i(x)) - (R - (g+1)D_\infty) - ((i+1)D_0 - (i+1)D_\infty) \\
&\quad + (R - 2D_\infty) \\
&= \operatorname{div}(\psi_i(x)) + (g+i)D_\infty - (i+1)D_0 \\
&= (\operatorname{div}_0(\psi_i(x)) - d_\psi D_\infty) + (g+i)D_\infty - (i+1)D_0 \\
&\geq (\operatorname{div}_0(\psi_i(x)) - (g+1)D_\infty) + (g+i)D_\infty - (i+1)D_0 \\
&= \operatorname{div}_0(\psi_i(x)) + (i-1)D_\infty - (i+1)D_0.
\end{aligned}$$

Again, the second equality uses (3.1) and (3.5), and since $i \geq 1$ we conclude that $\frac{\psi_i(x)}{2yx^{i+1}}dx$ is regular on $U_0 = X\backslash\pi^{-1}(0)$, completing the $p \neq 2$ case.

We now suppose that $p = 2$. We remind the reader that this allows us to change signs between positive and negative as we wish. We see that

$$\begin{aligned}\left(\left(\frac{\Psi_i(x,y)}{x^{i+1}H}\right)+\left(\frac{\Phi_i(x,y)}{x^{i+1}H}\right)\right)dx &= \frac{S_i(x,y)}{x^{i+1}H(x)}dx\\ &= \left(\frac{F(x)'}{x^iH(x)}+\frac{yH(x)'}{x^iH(x)}+\frac{iy}{x^{i+1}}\right)dx\\ &= \frac{1}{x^i}\left(\frac{F(x)'+yH(x)'}{H(x)}\right)dx+\frac{iy}{x^{i+1}}dx\\ &= x^{-i}dy+yd\left(x^{-i}\right)\\ &= d\left(yx^{-i}\right),\end{aligned}$$

with the fourth equality following from (3.12). We have also already seen in the proof of Theorem 4.2.1 that $\frac{y}{x^i}$ is regular on $U_0 \cap U_\infty$. So in order to prove that for $i \in \{1,\dots,g\}$ the elements of (4.17) are satisfy the conditions of (4.7) it only remains to show that the differentials $\frac{\Phi_i(x,y)}{x^{i+1}H(x)}dx$ and $\frac{\Psi_i(x,y)}{x^{i+1}H(x)}dx$ are regular on U_∞ and U_0 respectively. We denote the degrees of the polynomials defined in (4.14) by $d^x_\Phi, d^x_\Psi, d^y_\Phi$ and d^y_Ψ.

By (4.14) we have $\Phi_i(x,y) = \Phi^x_i(x) + y\Phi^y_i(x)$ and $\Psi_i(x,y) = \Psi^x_i(x) + y\Psi^y_i(x)$, and we will use these splittings to show that $\frac{\Phi_i(x,y)}{x^{i+1}H(x)}dx$ and $\frac{\Psi_i(x,y)}{x^{i+1}H(x)}dx$ are regular on U_∞ and U_0 respectively.

We start by computing the divisor of $\frac{1}{x^{i+1}H(x)}dx$, since it is a common component to all the differentials we will consider. This yields

$$\begin{aligned}\operatorname{div}\left(\frac{1}{x^{i+1}H(x)}dx\right) &= \operatorname{div}(dx)-\operatorname{div}(x^{i+1})-\operatorname{div}(H(x))\\ &= (R-2D_\infty)-((i+1)D_0-(i+1)D_\infty)-(R-(g+1)D_\infty)\\ &= (g+i)D_\infty-(i+1)D_0,\end{aligned}$$

using (3.1), (3.2) and Lemma 3.2.3. We now use this along with Proposition 3.2.4 and the polynomials (4.14) to complete the proof.

We begin by computing the divisors associated to $\Phi_i(x,y)$. Firstly,

$$\begin{aligned}\operatorname{div}\left(\frac{\Phi^x_i(x)}{x^{i+1}H(x)}dx\right) &= \operatorname{div}(\Phi^x_i(x))-(i+1)D_0+(g+i)D_\infty\\ &= \left(\operatorname{div}_0(\Phi^x_i(x))-d^x_\Phi D_\infty\right)-(i+1)D_0+(g+i)D_\infty\\ &\geq \operatorname{div}_0(\Phi^x_i(x))-(2g+2)D_\infty-(i+1)D_0+(g+i)D_\infty\\ &= \operatorname{div}_0(\Phi^x_i(x))-(i+1)D_0+(i-2-g)D_\infty\\ &= \operatorname{div}_0\left(\frac{\Phi^x_i(x)}{x^{i+1}}\right)+(i-g-2)D_\infty.\end{aligned}$$

From this we see that the differential $\frac{\Phi_i^x(x)}{x^{i+1}H(x)}dx$ is clearly regular on $U_\infty = X\backslash\pi^{-1}(\infty)$.

We now compute the divisor of the other half of $\frac{\Phi_i(x,y)}{x^{i+1}H(x)}dx$, namely

$$\begin{aligned}
\operatorname{div}\left(\frac{y\Phi_i^y(x)dx}{x^{i+1}H(x)}\right) &= \operatorname{div}(y) + \operatorname{div}(\Phi_i^y(x)) - (i+1)D_0 + (g+i)D_\infty \\
&= \operatorname{div}(y) + \operatorname{div}_0(\Phi_i^y(x)) - d_\Phi^y D_\infty - (i+1)D_0 + (g+i)D_\infty \\
&\geq \operatorname{div}(y) + \operatorname{div}_0(\Phi_i^y(x)) - (g+1)D_\infty - (i+1)D_0 + (g+i)D_\infty \\
&= \operatorname{div}(y) + \operatorname{div}_0\left(\frac{\Phi_i^y(x)}{x^{i+1}}\right) + (i-1)D_\infty.
\end{aligned}$$

From Proposition 3.2.4 we see that y only has poles at points in $\pi^{-1}(\infty)$, and hence $\frac{\Phi_i(x,y)}{x^{i+1}H(x)}dx$ is regular on $U_\infty = X\backslash\pi^{-1}(\infty)$.

Now we complete the same computations on $\Psi_i(x,y)$, starting with $\Psi_i^x(x)$:

$$\begin{aligned}
\operatorname{div}\left(\frac{\Psi_i^x(x)}{x^{i+1}H(x)}dx\right) &= \operatorname{div}(\Psi_i^x(x)) - (i+1)D_0 + (g+i)D_\infty \\
&= (\operatorname{div}_0(\Psi_i^x(x)) - d_\Psi^x D_\infty) - (i+1)D_0 + (g+i)D_\infty \\
&\geq \operatorname{div}_0(\Psi_i^x(x)) - iD_\infty - (i+1)D_0 + (g+i)D_\infty \\
&= \operatorname{div}_0(\Psi_i^x(x)) - (i+1)D_0 + gD_\infty,
\end{aligned}$$

and it is clear that the divisor is positive on $U_0 = X\backslash\pi^{-1}(0)$.

For the other half of the differential we need to consider separate cases. If we assume that ∞ is a branch point then using Proposition 3.2.4 we see that

$$\begin{aligned}
\operatorname{div}\left(\frac{y\Psi_i^y(x)}{x^{i+1}H(x)}dx\right) &= \operatorname{div}_0(y) - (2g+1)[P_\infty] + \operatorname{div}(\Psi_i^y(x)) - (i+1)D_0 + 2(g+i)[P_\infty] \\
&= \operatorname{div}_0(y) + \operatorname{div}(\Psi_i^y(x)) - (i+1)D_0 + (2i-1)[P_\infty] \\
&= \operatorname{div}_0(y) + \operatorname{div}_0(\Psi_i^y(x)) - 2d_\Psi^y[P_\infty] - (i+1)D_0 + (2i-1)[P_\infty] \\
&\geq \operatorname{div}_0(y) + \operatorname{div}_0(\Psi_i^y(x)) - (i-1)[P_\infty] - (i+1)D_0 + (2i-1)[P_\infty] \\
&= \operatorname{div}_0(y) + \operatorname{div}_0(\Psi_i^y(x)) - (i+1)D_0 + [P_\infty],
\end{aligned}$$

which is clearly positive on U_0. On the other hand, if ∞ is not a branch point then we have

$$\begin{aligned}\operatorname{div}\left(\frac{y\Psi_i^y(x)}{x^{i+1}H(x)}dx\right) &= \operatorname{div}(y) + \operatorname{div}(\Psi_i^y(x)) - (i+1)D_0 + (g+i)D_\infty \\ &= \operatorname{div}(y) + \operatorname{div}_0(\Psi_i^y(x)) - (i+1)D_0 + (g+i-d_\Psi^y)D_\infty \\ &\geq \operatorname{div}(y) + \operatorname{div}_0(\Psi_i^y(x)) - (i+1)D_0 + (g+1)D_\infty.\end{aligned}$$

Since we know from Proposition 3.2.4 that y cannot have a pole of order greater $g+1$ at P_∞ or P'_∞, and only has poles at these points, it follows that the differential $\frac{y\Psi_i^y(x)}{x^{i+1}H(x)}dx$ is regular on $U_0 = X\backslash\pi^{-1}(0)$. Thus we have completed the proof.

□

4.4 Splitting of the short exact sequence

We keep the assumptions of the previous section, and we also assume that $\operatorname{char}(k) = p \geq 3$.

In the previous section we found a basis for the de Rham cohomology of any hyperelliptic curve using Čech cohomology, with respect to the cover $\mathcal{U} = \{U_0, U_\infty\}$ (Theorem 4.3.1). We let λ_i and γ_i denote the elements of this basis by defining

$$\lambda_i = \left[\left(\frac{x^i}{y}dx, \frac{x^i}{y}dx, 0\right)\right], \quad i = 0, \ldots, g-1$$

and

$$\gamma_i = \left[\left(\frac{\psi_i(x)}{2yx^{i+1}}dx, \frac{-\phi_i(x)}{2yx^{i+1}}dx, x^{-i}y\right)\right], \quad i = 1, \ldots, g.$$

In this section we further study the covers $\mathcal{U}' = \{U_a, U_\infty\}$ and $\mathcal{U}'' = \{U_0, U_a, U_\infty\}$ for some fixed $a \in \mathbb{P}_k^1\backslash\{0,\infty\}$. Then $H^1_{\mathrm{dR}}(X/k)$ is isomorphic to the k-vector space

$$\Big\{(\omega_0, \omega_a, \omega_\infty, f_{0a}, f_{0\infty}, f_{a\infty}) | \omega_i \in \Omega_X(U_i), f_{ij} \in \mathcal{O}_X(U_i \cap U_j), \\ f_{0a} - f_{0\infty} + f_{a\infty} = 0, df_{ij} = \omega_i - \omega_j\Big\} \tag{4.19}$$

quotiented by the subspace

$$\{(df_0, df_a df_\infty, f_0 - f_a, f_0 - f_\infty, f_a - f_\infty) | f_i \in \mathcal{O}_X(U_i)\}. \tag{4.20}$$

We introduce Čech cohomology notation for the different representations of $H^1_{\mathrm{dR}}(X/k)$ we have used, letting $\check{H}^1_{\mathrm{dR}}(\mathcal{U})$ and $\check{H}^1_{\mathrm{dR}}(\mathcal{U}'')$ be the quotient of (4.7) by (4.8) and (4.19) by (4.20) respectively. Then we have a canonical isomorphism $\rho\colon \check{H}^1_{\mathrm{dR}}(\mathcal{U}'') \to \check{H}^1_{\mathrm{dR}}(\mathcal{U})$, given by the projection

$$\rho\colon (\omega_0, \omega_a, \omega_\infty, f_{0a}, f_{0\infty}, f_{a\infty}) \mapsto (\omega_0, \omega_\infty, f_{0\infty}). \tag{4.21}$$

The next proposition explicitly describes the pre-image of the basis element γ_i under ρ. To this end, we define the following polynomials for $1 \le i \le g$:

$$r_i(x) := \sum_{k=0}^{i-1} (-1)^{g-k} \binom{g}{k} a^{g-k} x^k$$

and

$$t_i(x) := \sum_{k=i}^{g} (-1)^{g-k} \binom{g}{k} a^{g-k} x^k.$$

These split the polynomial $(x-a)^g$ in to two parts.

Proposition 4.4.1. *The pre-image $\rho^{-1}(\gamma_i)$ for $i \in \{1, \ldots, g\}$ is the residue class of*

$$\nu_i = \left(\frac{\psi_i(x)}{2yx^{i+1}} dx, \frac{(\psi_i(x)t_i(x) - \phi_i(x)r_i(x))(x-a) + 2if(x)(-1)^{g-i+1}\binom{g}{i} a^{g-i+1} x^i}{2yx^{i+1}(x-a)^{g+1}} dx, \right.$$
$$\left. \frac{-\phi_i(x)}{2yx^{i+1}} dx, \frac{r_i(x)y}{x^i(x-a)^g}, \frac{y}{x^i}, \frac{t_i(x)y}{x^i(x-a)^g} \right).$$

Proof. In order to be able to refer to the entries in ν_i more succinctly we let

$$\nu_i = (\omega_{0i}, \omega_{ai}, \omega_{\infty i}, f_{0ai}, f_{0\infty i}, f_{a\infty i}).$$

First, note that it follows from the proof of Theorem 4.3.1 that $d(f_{0\infty i}) = \omega_{0i} - \omega_{\infty i}$, and that $f_{0\infty i}, \omega_{0i}$ and $\omega_{\infty i}$ are regular on the appropriate open sets.

Since $r_i(x) + t_i(x)$ is the binary expansion of $(x-a)^g$ then

$$\begin{aligned} f_{0ai} - f_{0\infty i} + f_{a\infty i} &= \frac{r_i(x)y}{x^i(x-a)^g} - \frac{y}{x^i} + \frac{t_i(x)y}{x^i(x-a)^g} \\ &= \frac{y(r_i(x) + t_i(x) - (x-a)^g)}{x^i(x-a)^g} \\ &= 0. \end{aligned}$$

We now check that the differentials and functions in v_i are regular on the appropriate open sets by computing the relevant divisors. Firstly, by (3.1) and (3.5),

$$\begin{aligned}\operatorname{div}(f_{0ai}) &= \operatorname{div}\left(\frac{r_i(x)y}{x^i(x-a)^g}\right)\\ &= \operatorname{div}(r_i(x)) + \operatorname{div}(y) - i\operatorname{div}(x) - g\operatorname{div}(x-a)\\ &\geq \operatorname{div}_0(r_i(x)) - (i-1)D_\infty + R - (g+1)D_\infty - iD_0 + iD_\infty - gD_a + gD_\infty\\ &= \operatorname{div}_0(r_i(x)) + R - iD_0 - gD_a,\end{aligned}$$

which is non-negative on $U_0 \cap U_a$. Note that the second and third line are not necessarily equal, since the coefficient of x^{i-1} in $r_1(x)$ may be divisible by p, and hence zero in k. On the other hand, again by (3.1) and (3.5),

$$\begin{aligned}\operatorname{div}(f_{a\infty i}) &= \operatorname{div}\left(\frac{t_i(x)y}{x^i(x-a)^g}\right)\\ &= \operatorname{div}\left(\frac{t_i(x)}{x^i}\right) + \operatorname{div}(y) - g\operatorname{div}(x-a)\\ &= \operatorname{div}_0\left(\frac{t_i(x)}{x^i}\right) - (g-i)D_\infty + R - (g+1)D_\infty - gD_a + gD_\infty\\ &= \operatorname{div}_0\left(\frac{t_i(x)}{x^i}\right) + R - gD_a - (g-i+1)D_\infty,\end{aligned}$$

where the third equality holds because $t_i(x)/x^i$ is regular on U_∞. We conclude that $f_{a\infty i}$ is regular on $U_a \cap U_\infty$.

To show that

$$\omega_{ai} = \frac{(\psi_i(x)t_i(x) - \phi_i(x)r_i(x))(x-a) + 2if(x)(-1)^{g-i+1}\binom{g}{i}a^{g-i+1}x^i}{2yx^{i+1}(x-a)^{g+1}}dx \tag{4.22}$$

is regular on U_a we first compute the divisor

$$\begin{aligned}&\operatorname{div}\left(\frac{dx}{2yx^{i+1}(x-a)^{g+1}}\right) = \operatorname{div}(dx) - \operatorname{div}(y) - (i+1)\operatorname{div}(x) - (g+1)\operatorname{div}(x-a)\\ &= R - 2D_\infty - R + (g+1)D_\infty - (i+1)D_0 + (i+1)D_\infty - (g+1)D_a + (g+1)D_\infty\\ &= (2g+i+1)D_\infty - (i+1)D_0 - (g+1)D_a,\end{aligned}$$

using (3.1), (3.2) and (3.5). We next show that the numerator of (4.22),

$$(\psi_i(x)t_i(x) - \phi_i(x)r_i(x))(x-a) + 2if(x)(-1)^{g-i+1}\binom{g}{i}a^{g-i+1}x^i, \tag{4.23}$$

has degree less than $2g+i+2$, from which it follows that (4.22) doesn't have a pole at the point(s) in $\pi^{-1}(\infty)$. The degree of $\psi_i(x)t_i(x)(x-a)$ is at most $2g+2$, which is less than $2g+2+i$ for all $i \geq 1$. If $\deg(f(x)) = 2g+1$, then clearly

$$\deg\left(\phi_i(x)r_i(x)(x-a)\right) = \deg(\phi_i) + \deg(r_i(x)) + \deg(x-a) \leq 2g+1+i-1+1 = 2g+i+1$$

and

$$\deg\left(2if(x)(-1)^{g-i+1}\binom{g}{i}a^{g-i+1}x^i\right) \leq 2g+1+i.$$

Lastly, if $\deg(f(x)) = 2g+2$ then the term of degree $2g+i+2$ in $-\phi_i(x)r_i(x)(x-a)$ is

$$\begin{aligned}
-((2g+2)a_{2g+2}x^{2g+2} - 2ia_{2g+2}x^{2g+2})&\left((-1)^{g-i+1}\binom{g}{i-1}a^{g-i+1}x^i\right) \\
&= 2(-1)^{g-i+2}\left((g-i+1)\binom{g}{i-1}\right)a_{2g+2}a^{g-i+1}x^{2g+i+2} \\
&= 2(-1)^{g-i}\left(\frac{g!}{(i-1)!(g-i)!}\right)a_{2g+2}a^{g-i+1}x^{2g+i+2} \\
&= 2i(-1)^{g-i}\binom{g}{i}a_{2g+2}a^{g-i+1}x^{2g+i+2},
\end{aligned}$$

which cancels with the term of the same degree in $2if(x)(-1)^{g-i+1}\binom{g}{i}a^{g-i+1}x^i$. Since these terms cancel, we again have the that the degree of (4.23) is at most $2g+i+1$, and (4.22) has no pole(s) at the point(s) in $\pi^{-1}(\infty)$.

Finally, we show that (4.23) is divisible by x^{i+1}. By definition $x^{g+2}|\phi_i(x)$, and since $i \leq g$ it follows that $x^{i+1}|\phi_i(x)r_i(x)(x-a)$. On the other hand, the lowest degree terms of $2if(x)(-1)^{g-i+1}\binom{g}{i}a^{g-i+1}x^i$ and $\psi_i(x)t_i(x)(x-a)$ which can be non-zero are, respectively,

$$2ia_0(-1)^{g-i+1}\binom{g}{i}a^{g-i+1}x^i$$

and

$$(-2ia_0)\left((-1)^{g-i}\binom{g}{i}a^{g-i}x^i\right)(-a).$$

When adding $\psi_i(x)t_i(x)(x-a)$ and $2if(x)(-1)^{g-i+1}\binom{g}{i}a^{g-i+1}x^i$ these two terms obviously cancel. Hence the numerator (4.23) is divisible by x^{i+1}.

It only remains to show that $\omega_{ai} = \omega_{0i} - df_{0ai}$. We begin this by computing df_{0ai}, which is

$$\begin{aligned}
df_{0ai} &= d\left(\frac{yr_i(x)}{x^i(x-a)^g}\right) \\
&= \frac{r_i(x)}{x^i(x-a)^g}dy + yd\left(\frac{r_i(x)}{x^i(x-a)^g}\right) \\
&= \frac{f'(x)r_i(x)}{2yx^i(x-a)^g}dx + y\left(\frac{r_i'(x)}{x^i(x-a)^g} - \frac{ir_i(x)}{x^{i+1}(x-a)^g} - \frac{gr_i(x)}{x^i(x-a)^{g+1}}\right)dx \\
&= \frac{xf'(x)r_i(x)(x-a) + 2f(x)(xr_i'(x)(x-a) - i(x-a)r_i(x) - gxr_i(x))}{2yx^{i+1}(x-a)^{g+1}}dx.
\end{aligned}$$

Hence $\omega_{0i} - df_{0ai}$ expands to

$$\frac{\psi_i(x)(x-a)^{g+1} - xf'(x)r_i(x)(x-a) - 2f(x)\left(xr_i'(x)(x-a) - i(x-a)r_i(x) - gxr_i(x)\right)}{2yx^{i+1}(x-a)^{g+1}}dx.$$

Now

$$(x-a)^{g+1} = (x-a)^g(x-a) = (r_i(x) + t_i(x))(x-a)$$

and

$$\begin{aligned}
xf'(x)r_i(x)(x-a) - 2if(x)r_i(x)(x-a) &= r_i(x)(x-a)(xf'(x) - 2if(x)) \\
&= r_i(x)(x-a)(\psi_i(x) + \phi_i(x)).
\end{aligned}$$

So

$$\psi_i(x)(x-a)^{g+1} - xf'(x)r_i(x)(x-a) + 2if(x)r_i(x)(x-a) = (\psi_i(x)t_i(x) - \phi_i(x)r_i(x))(x-a).$$

We now compute $(x-a)r_i'(x) - gr_i(x)$. First, we note that

$$\begin{aligned}
r_i'(x) &= \sum_{k=1}^{i-1} k(-1)^{g-k}\binom{g}{k}a^{g-k}x^{k-1} \\
&= \sum_{k=0}^{i-2}(k+1)(-1)^{g-k-1}\binom{g}{k+1}a^{g-k-1}x^k.
\end{aligned}$$

From this it follows that

$$\begin{aligned}
r_i'(x)(x-a) &= x\sum_{k=1}^{i-1} k(-1)^{g-k}\binom{g}{k}a^{g-k}x^{k-1} - a\sum_{k=0}^{i-2}(k+1)(-1)^{g-k-1}\binom{g}{k+1}a^{g-k-1}x^k \\
&= \sum_{k=1}^{i-1} k(-1)^{g-k}\binom{g}{k}a^{g-k}x^k + \sum_{k=0}^{i-2}(k+1)(-1)^{g-k}\binom{g}{k+1}a^{g-k}x^k \\
&= gr_i(x) + (-1)^{g-i+2}i\binom{g}{i}a^{g-i+1}x^{i-1},
\end{aligned}$$

since

$$\begin{aligned}
k\binom{g}{k} + (k+1)\binom{g}{k+1} &= k\left(\frac{g!}{k!(g-k)!}\right) + (k+1)\left(\frac{g!}{(k+1)!(g-k-1)!}\right) \\
&= \frac{g!}{(k-1)!(g-k)!} + \frac{g!}{k!(g-k-1)!} \\
&= \frac{g\cdot g!}{k!(g-k)!} \\
&= g\binom{g}{k}.
\end{aligned}$$

Hence $x(r_i'(x)(x-a) - gr_i(x)) = (-1)^{g-i+2}i\binom{g}{i}a^{g-i+1}x^i$.

Combining the above we conclude that

$$\omega_{0i} - df_{0ai} = \frac{(\psi_i(x)t_i(x) - \phi_i(x)r_i(x))(x-a) + 2if(x)(-1)^{g-i+1}\binom{g}{i}a^{g-i+1}x^i}{2yx^{i+1}(x-a)^{g+1}}dx = \omega_{ai}.$$

Note that the last relation ($df_{a\infty i} = \omega_{ai} - \omega_{\infty i}$) holds, since

$$df_{a\infty i} = df_{0\infty i} - df_{0ai} = \omega_{0i} - \omega_{\infty i} - \omega_{0i} + \omega_{ai} = \omega_{ai} - \omega_{\infty i}. \qquad \square$$

Recall that the hyperelliptic involution σ is in the centre of $\operatorname{Aut}(X)$ (see [Liu02, Cor. 7.4.31]). Then, given any $\tau \in \operatorname{Aut}(X)$, we have an induced map $\bar{\tau}\colon \mathbb{P}^1_k \to \mathbb{P}^1_k$, since $\mathbb{P}^1_k$ is the quotient of X by the hyperelliptic involution. Hence the following diagram commutes

$$\begin{array}{ccc}
X & \xrightarrow[\tau]{} & X \\
\downarrow \pi & & \downarrow \pi \\
\mathbb{P}^1_k & \xrightarrow[\bar{\tau}]{} & \mathbb{P}^1_k
\end{array}$$

Lemma 4.4.2. *Suppose there exists $\tau \in \operatorname{Aut}(X)$ such that the induced automorphism $\bar{\tau}\colon \mathbb{P}^1_k \to \mathbb{P}^1_k$ is given by $x \mapsto x + a$ for some $0 \neq a \in k$. Then the action of τ^* on y is given by $\tau^*(y) = y$ or $\tau^*(y) = -y$ and moreover if such an automorphism of X exists, then p divides the degree of $f(x)$.*

Proof. We first show that $\tau^*(y) = \pm y$. Since $y^2 \in k(x)$ then there exist $g_1(x), g_2(x) \in k(x)$ such that

$$\tau^*(y) = g_1(x)y + g_2(x) \in k(x,y).$$

Hence

$$f(x+a) = \tau^*(y^2) = (\tau^*(y))^2 = g_1(x)^2 f(x) + 2g_1(x)g_2(x)y + g_2(x)^2. \tag{4.24}$$

Firstly, note that if neither $g_1(x)$ nor $g_2(x)$ are zero then

$$y = \frac{f(x+a) - g_1(x)^2 f(x) - g_2(x)^2}{2g_1(x)g_2(x)},$$

which contradicts the fact that $K(X)$ is a degree two extension of $k(x)$. Hence one of $g_1(x)$ or $g_2(x)$ must be zero.

If $g_1(x) = 0$ then τ^* would not be an automorphism, since y would not be in the image. Hence $\tau^*(y) = g_1(x)y$. Also, by comparing the degrees in (4.24) we see that $\deg(g_1(x)) = 0$, and then by comparing coefficients in the same equation we see that $g_1(x)^2 = 1$. Hence $\tau^*(y) = \pm y$.

We now show that $d_f := \deg(f(x))$ is divisible by p. We derived above that $f(x) = f(x+a)$. Comparing the terms of degree $d_f - 1$ on each side we see that $d_f a - b_{d_f-1} = b_{d_f-1}$ (where b_{d_f-1} is as in (3.4)). It follows that $d_f = 0$ in k, and hence $p \mid d_f$. □

Recall from Proposition 4.1.2 that we have a canonical short exact sequence

$$0 \to H^0(X,\Omega_X) \to H^1_{\mathrm{dR}}(X/k) \to H^1(X,\mathcal{O}_X) \to 0. \tag{4.25}$$

Theorem 4.4.3. *Suppose there exists $\tau \in \mathrm{Aut}(X)$ such that the induced automorphism $\bar{\tau}\colon \mathbb{P}^1_k \to \mathbb{P}^1_k$ is given by $x \mapsto x + a$ for some $0 \neq a \in k$. We let $G = \langle \tau \rangle$ be the subgroup of $\mathrm{Aut}(X)$ generated by τ, and we further suppose that $\infty \in \mathbb{P}^1_k$ is a branch point of $\pi\colon X \to \mathbb{P}^1_k$. Then the sequence (4.25) does not split as a sequence of $k[G]$-modules.*

Proof. By Lemma 4.4.2 we have $\tau^*(y) = y$ or $\tau^*(y) = -y$. Without loss of generality we can and will assume that $\tau^*(y) = y$ since, if $\tau^*(y) = -y$, we replace τ by $\tau \circ \sigma$ (where σ is the hyperelliptic involution of X). Notice that the sequence (4.25) splits as a sequence of $K[G]$-modules if and only if it splits as a sequence of $K[\langle \tau \circ \sigma \rangle]$-modules (see Corollary 4.3.3).

We now suppose that the sequence (4.25) does split, and that $s\colon H^1(X,\mathcal{O}_X) \to H^1_{\mathrm{dR}}(X/k)$ is a splitting map. Then it follows that for all $\alpha \in H^1(X,\mathcal{O}_X)$ we have

$$s(\tau^*(\alpha)) = \tau^*(s(\alpha)) \in H^1_{\mathrm{dR}}(X/k). \tag{4.26}$$

We will show that this equality gives rise to a contradiction when α is the residue class $\left[\frac{y}{x^g}\right]$ in $H^1(X,\mathcal{O}_X)$ (see (4.2) and Theorem 4.2.1). It will then follow that no splitting map can exist.

We first compute the action of τ^* on the residue class $\left[\frac{y}{x^g}\right]$. In order to do this we consider the following obvious commutative diagram of isomorphisms:

$$\begin{array}{ccccc} H^1(X,\mathcal{O}_X) & \xleftarrow{\sim} & \check{H}^1(\mathcal{U},\mathcal{O}_X) & \xleftarrow{\rho} & \check{H}^1(\mathcal{U}'',\mathcal{O}_X) \\ \tau^* \downarrow & & & & \rho' \downarrow \\ H^1(X,\mathcal{O}_X) & \xleftarrow{\sim} & \check{H}^1(\mathcal{U},\mathcal{O}_X) & \xleftarrow{\tau^*} & \check{H}^1(\mathcal{U}',\mathcal{O}_X) \end{array}$$

where ρ and ρ' are the canonical projections. From Proposition 4.4.1 we know that $\rho^{-1}\left(\left[\frac{y}{x^g}\right]\right)$ is the residue class

$$\left[\left(\frac{r_g(x)y}{x^g(x-a)^g}, \frac{y}{x^g}, \frac{t_g(x)y}{x^g(x-a)^g}\right)\right] = \left[\left(\frac{((x-a)^g - x^g)y}{x^g(x-a)^g}, \frac{y}{x^g}, \frac{y}{(x-a)^g}\right)\right] \in \check{H}^1(\mathcal{U}'',\mathcal{O}_X).$$

Therefore

$$\begin{aligned} \tau^*\left(\left[\frac{y}{x^g}\right]\right) &= \tau^*\left(\rho'\left(\rho^{-1}\left(\left[\frac{y}{x^g}\right]\right)\right)\right) \\ &= \tau^*\left(\rho'\left(\left[\left(\frac{((x-a)^g - x^g)y}{x^g(x-a)^g}, \frac{y}{x^g}, \frac{y}{(x-a)^g}\right)\right]\right)\right) \\ &= \tau^*\left(\left[\frac{y}{(x-a)^g}\right]\right) \\ &= \left[\frac{y}{x^g}\right], \end{aligned}$$

i.e. $\left[\frac{y}{x^g}\right]$ in $H^1(X,\mathcal{O}_X)$ is fixed by τ^*.

Since the canonical projection $H^1_{\mathrm{dR}}(X/k) \to H^1(X,\mathcal{O}_X)$ maps γ_g to the residue class $\left[\frac{y}{x^g}\right]$ it follows that

$$\tau^*(\gamma_g) = \gamma_g + \sum_{i=0}^{g-1} c_i \lambda_i$$

for some $c_0,\dots,c_{g-1} \in k$. On the other hand, we also have

$$s\left(\left[\frac{y}{x^g}\right]\right) = \gamma_g + \sum_{i=0}^{g-1} d_i \lambda_i$$

for some $d_0, \dots, d_{g-1} \in k$. Now the action of τ^* on λ_i for $0 \le i \le g-1$ is easily seen to be given by

$$\begin{aligned} \tau^*(\lambda_i) &= \tau^*\left(\left[\left(\frac{x^i}{y}dx, \frac{x^i}{y}dx, 0\right)\right]\right) \\ &= \left[\left(\frac{(x+a)^i}{y}dx, \frac{(x+a)^i}{y}dx, 0\right)\right] \\ &= \sum_{k=0}^{i} \binom{i}{k} a^{i-k}\lambda_k. \end{aligned}$$

Then, by (4.26), it follows that

$$\begin{aligned} \gamma_g + \sum_{i=0}^{g-1} d_i\lambda_i &= s\left(\left[\frac{y}{x^g}\right]\right) \\ &= s\left(\tau^*\left(\left[\frac{y}{x^g}\right]\right)\right) \\ &= \tau^*\left(\gamma_g + \sum_{i=0}^{g-1} d_i\lambda_i\right) \\ &= \left(\gamma_g + \sum_{i=0}^{g-1} c_i\lambda_i\right) + \sum_{i=0}^{g-1} d_i\left(\sum_{k=0}^{i}\binom{i}{k}a^{i-k}\lambda_k\right). \end{aligned}$$

By comparing coefficients of the basis elements λ_{g-1}, we see that $c_{g-1} = 0$. We now show that we must have $c_{g-1} = a/4$ for the defining equation

$$\tau^*(\gamma_g) = \gamma_g + \sum_{i=0}^{g-1} c_i\lambda_i$$

to hold. Since we assumed that $a \neq 0$ this will give us the contradiction we desire.

To compute $\tau^*(\gamma_g)$ we consider the following commutative diagram of isomorphisms

$$\begin{array}{ccccc} H^1_{\mathrm{dR}}(X/k) & \stackrel{\sim}{\longleftarrow} & \check{H}^1_{\mathrm{dR}}(\mathcal{U}) & \stackrel{\rho}{\longleftarrow} & \check{H}^1_{\mathrm{dR}}(\mathcal{U}'') \\ \tau^*\downarrow & & & & \rho'\downarrow \\ H^1_{\mathrm{dR}}(X/k) & \stackrel{\sim}{\longleftarrow} & \check{H}^1_{\mathrm{dR}}(\mathcal{U}) & \stackrel{\tau^*}{\longleftarrow} & \check{H}^1_{\mathrm{dR}}(\mathcal{U}') \end{array} \tag{4.27}$$

where ρ is the canonical projection (4.21) and ρ' is given by

$$\rho' \colon (\omega_0, \omega_a, \omega_\infty, f_{0a}, f_{0\infty}, f_{a,\infty}) \mapsto (\omega_a, \omega_\infty, f_{a\infty}).$$

Then

$$\begin{aligned}\tau^*(\gamma_g) &= \tau^*(\rho'(\rho^{-1}(\gamma_g)))\\ &= \tau^*\left(\left[\omega_{ag}, \frac{-\phi_g(x)}{2yx^{g+1}}dx, \frac{y}{(x-a)^g}\right)\right]\\ &= \left[\left(\tau^*(\omega_{ag}), \frac{-\phi_g(x+a)}{2y(x+a)^{g+1}}dx, \frac{y}{x^g}\right)\right],\end{aligned} \tag{4.28}$$

where ω_{ag} is the second entry in ν_g, as in the proof of Proposition 4.4.1. On the other hand, we have

$$\gamma_g + \sum_{i=0}^{g-1} c_i\lambda_i = \left[\left(\frac{\psi_g(x)}{2yx^{g+1}}dx, \frac{-\phi_g(x)}{2yx^{g+1}}dx, \frac{y}{x^g}\right)\right] + \sum_{i=0}^{g-1} c_i\left[\left(\frac{x^i}{y}dx, \frac{x^i}{y}dx, 0\right)\right]. \tag{4.29}$$

Note that the third entry in both (4.28) and (4.29) is $\frac{y}{x^g}$. Since any element of the form $(\omega_0, \omega_\infty, 0)$ in the subspace (4.8) of the space (4.7) is in fact zero, we conclude, by comparing the second entries of (4.28) and (4.29), that

$$-\frac{\phi_g(x+a)}{2y(x+a)^{g+1}}dx = -\frac{\phi_g(x)}{2yx^{g+1}}dx + \sum_{i=0}^{g-1} c_i\frac{x^i}{y}dx$$

in $\Omega_{K(X)}$.

Since dx is a basis of $\Omega_{K(X)}$ considered as a $K(X)$-vector space, and as $K(X) = k(x) \oplus y^{-1}k(x)$, the equation above is equivalent to

$$\frac{\phi_g(x+a)}{2(x+a)^{g+1}} = \frac{\phi_g(x)}{2x^{g+1}} - \sum_{i=0}^{g-1} c_i x^i,$$

in $k[x]$, and this, in turn, is equivalent to

$$\phi_g(x+a)x^{g+1} = \phi_g(x)(x+a)^{g+1} - 2(x+a)^{g+1}x^{g+1}\sum_{i=0}^{g-1} c_i x^i,$$

also in $k[x]$.

Recall from Chapter 3, Section 3.1, that the assumption that $\infty \in \mathbb{P}^1_k$ is a branch point of π implies that the degree of $f(x)$ is precisely $2g+1$. The terms of highest degree in $\phi_g(x)$ are the same as the terms of highest degree in

$$s_g(x) = xf'(x) - 2gf(x) = x^{2g+1} + 0 \cdot x^{2g} + \dots.$$

We therefore obtain

$$\Big((x+a)^{2g+1} + 0\cdot(x+a)^{2g} + \ldots\Big)x^{g+1}$$
$$= (x^{2g+1} + 0\cdot x^{2g} + \ldots)(x+a)^{g+1} - 2(x+a)^{g+1}x^{g+1}(c_{g-1}x^{g-1} + \ldots),$$

and hence

$$(2g+1)ax^{3g+1} = (g+1)ax^{3g+1} - 2c_{g-1}x^{3g+1}.$$

Finally, since $2g+1 = \deg(f(x)) \equiv 0 \mod p$ (by Lemma 4.4.2) then $g = -\frac{1}{2}$ in k. Hence we obtain

$$c_{g-1} = \frac{((g+1)-(2g+1))a}{2} = \frac{a}{4},$$

as claimed above. This concludes the proof of theorem 4.4.3. □

4.5 Examples

In this section we give a number of examples and specialisations of Theorem 4.4.3, as well as an example which demonstrates the necessity of the supposition that ∞ is a branch point of $\pi\colon X \to \mathbb{P}^1_k$.

Applying Theorem 4.4.3 to the hyperelliptic curve given by $y^2 = x^p - x$ we obtain Theorem 3.1 in Hortsch's paper [Hor12]. Conversely, the following lemma shows that Hortsch's theorem implies Theorem 4.4.3 if $\deg(f(x)) = p$.

Lemma 4.5.1. *Let $p \geq 3$. Suppose that $deg(f(x)) = p$ and that there exists $\tau \in \mathrm{Aut}(X)$ such that the induced automorphism $\bar{\tau}\colon \mathbb{P}^1_k \to \mathbb{P}^1_k$ is given by $x \mapsto x+a$ for some $0 \neq a \in k$. Then the curve X is isomorphic to the hyperelliptic curve given by $y^2 = x^p - x$.*

Proof. Suppose that we have

$$f(x) = x^p + a_{p-1}x^{p-1} + \ldots + a_1x + a_0,$$

for some $a_i \in k$. We first show, by induction, that $a_i = 0$ for $i \in \{2,\ldots,p-1\}$, and that $a_1 = -a^{p-1}$. Since $f(x) = f(x+a)$, we can compare coefficients, and for x^{p-2} this yields the equality $a_{p-2} = a_{p-1}(p-1)a + a_{p-2}$, which is equivalent to $a_{p-1}a = 0$. Since we assumed that $a \neq 0$ we conclude that $a_{p-1} = 0$. We now assume that $a_{p-1} = a_{p-2} = \ldots = a_{k+1} = 0$, where $k > 1$. Then the coefficient of x^{k-1} in $f(x+a)$ is $a_{k-1} + ka_ka$, and after comparing to the coefficient of x^{k-1} in $f(x)$, which is a_{k-1}, we conclude that $ka_ka = 0$. Since $a \neq 0$ by assumption, and also $k \neq 0$, it follows that $a_k = 0$.

Finally, comparing the constant coefficients of $f(x)$ and $f(x+a)$ gives us $a_0 = a_0 + a_1 a + a^p$, and so $a_1 = -a^{p-1}$. So we now have

$$f(x) = x^p - a^{p-1}x + a_0.$$

If $b \in k$ is a root of $f(x)$ then the map $x \mapsto x + b$, $y \mapsto y$ is an isomorphism of $K(X)$ to the function field of the hyperelliptic curve X' given by $y^2 = f(x) = x^p - a^{p-1}x$. Further, the map $x \mapsto ax$, $y \mapsto a^{\frac{p}{2}}y$ is an isomorphism of $K(X')$ to the function field of the hyperelliptic curve given by $y^2 = f(x) = x^p - x$. Combining these isomorphisms we see that our original curve is isomorphic to that defined by $y^2 = x^p - x$, concluding the proof. □

Since we do not, a priori, enforce any conditions on the degree of $f(x)$, it is plausible that Theorem 4.4.3 is much more general that Hortsch's theorem. In fact the following example is a simple and general method to obtain polynomials $f(x)$ of any odd degree, and hence any genus, such that Theorem 4.4.3 applies to the curve given by $y^2 = f(x)$. Of course this will only hold in a finite number of characteristics for any fixed genus.

Example 4.5.2. Let $g(x) \in k[x]$ be a polynomial of odd degree without repeated roots. Then the combined polynomial $f(x) = g(x^p - x)$ obviously has no repeated roots, and it is also clear that $f(x+1) = f(x)$, and hence we have an automorphism τ, as in the statement of Theorem 4.4.3.

Moreover, if $g \geq 2$ and p divides $2g+1$, and if we choose $h(x)$ to be a polynomial of degree $n := (2g+1)/p$ then the curve defined by $y^2 = f(x) := h(x^p - x)$ is of genus g, and satisfies the criteria of Theorem 4.4.3.

We now examine hyperelliptic curves that satisfy the requirements of Theorem 4.4.3 of genus 4 in full generality.

Example 4.5.3. Let $p = 3$. Given $0 \neq a \in k$, it is straightforward to verify that a monic polynomial $f(x)$ of degree $9 = 2 \cdot 4 + 1$ satisfies $f(x+a) = f(x)$ if and only if it is of the form

$$f(x) = x^9 + a_6x^6 + a^2a_6x^4 + a_3x^3 + a^4a_6x^2 + 2(a^8 + a^2a_3)x + a_0,$$

for some $a_6, a_3, a_0 \in k$. Now we fix $a_6, a_3 \in k$, such that a_6 or $a_3 + a^6$ is non-zero.

Then $f'(x) = a^2a_6x^3 + 2a^4a_6x + 2(a^8 + a^2a_3)$ is non-zero. If $a_6 = 0$ the $f'(x)$ has no roots, and hence $f(x)$ and $f'(x)$ are coprime, so $f(x)$ has no repeated roots. Otherwise $f'(x)$ has three roots, which may or may not be distinct, which we denote β_1, β_2 and β_3. Then we define $\beta_i' := f(\beta_i) - a_0$ for $i = 1, 2, 3$. If $a_0 \in k \backslash \{-\beta_1', -\beta_2', -\beta_3'\}$ it is clear that $f'(x)$ and $f(x)$ do not share any roots, and hence $f(x)$ has no repeated roots.

From this it follows that the equation $y^2 = f(x)$ defines a genus 4 hyperelliptic curve over k, for which the exact sequence in Proposition 4.1.2 does not split, by Theorem 4.4.3.

We conclude this chapter with an example which demonstrates that the requirement in Theorem 4.4.3 for ∞ to be a branch point X is a necessary condition.

Example 4.5.4. Let $p = 3$. By [KY10, Table 1], the modular curve $X_0(22)$ is the hyperelliptic curve of genus 2 defined by

$$y^2 = f(x) = x^6 + 2x^4 + x^3 + 2x^2 + 1,$$

and the automorphism group of $X_0(22)$ is D_6. We will show that the short exact sequence in Proposition 4.1.2 splits as a sequence of $k[\langle\tau\rangle]$-modules, where τ is a generator of the unique order three subgroup of D_6. However, in order to describe τ, we need to adjust our defining equation. We first notice that the map $x \mapsto x - 1$, $y \mapsto y$ is an isomorphism of $K(X_0(22))$ to the function field of the curve defined by $y^2 = f(x) = x^6 + 2x^4 + 2x^2 + 2$. We now apply a further isomorphism to this curve. In general, if $g(x) = a_s x^s + \ldots + a_0$, and $a_0 \neq 0 \neq a_s$ we can define $g^*(x) := a_0^{-1} x^s g\left(\frac{1}{x}\right)$. It is stated after Lemma 2.6 in [KY10] that if $y^2 = g(x)$ defines a hyperelliptic curve, and s is even, then the curve defined by $y^2 = g^*(x)$ is isomorphic. In this case we conclude that the curve defined by

$$y^2 = f(x) = x^6 + x^4 + x^2 + 2$$

is isomorphic to $X_0(22)$, and we let X be the curve defined by this equation, and we fix $f(x) = x^6 + x^4 + x^2 + 2$ for the rest of the example. Note that $f'(x) = x^3 + 2x$ and $f(x) = f'(x)^2 + 2$, and hence $f'(x)$ and $f(x)$ are coprime. In particular, this verifies that $f(x)$ has no repeated roots. Moreover, it is clear that $f'(x+1) = f'(x)$, and from this it follows that

$$f(x+1) = f'(x+1)^2 + 2 = f'(x)^2 + 2 = f(x).$$

Hence the map $\tau\colon (x,y) \mapsto (x+1,y)$ is an automorphism of X.

By Theorem 4.3.1 a basis of $\check{H}^1_{\mathrm{dR}}(\mathcal{U})$ is given by

$$\begin{aligned}
\lambda_1 &= \left[\left(\frac{1}{y}dx, \frac{1}{y}dx, 0\right)\right] \\
\lambda_2 &= \left[\left(\frac{x}{y}dx, \frac{x}{y}dx, 0\right)\right] \\
\gamma_1 &= \left[\left(\frac{1}{yx^2}dx, \frac{x^4 + 2x^2}{y}dx, \frac{y}{x}\right)\right] \\
\gamma_2 &= \left[\left(\frac{x^2 + 1}{2yx^3}dx, \frac{2x^3}{y}dx, \frac{y}{x^2}\right)\right],
\end{aligned}$$

and we let $\bar{\gamma}_i$ be the image in $H^1(X,\mathcal{O}_X)$ of γ_i under the projection $p\colon H^1_{\mathrm{dR}}(X/k) \to H^1(X,\mathcal{O}_X)$. In particular, $\bar{\gamma}_1$ and $\bar{\gamma}_2$ form a basis of $H^1(X,\mathcal{O}_X)$.

Then we can define a map of k vector spaces

$$s\colon H^1(X,\mathcal{O}_X) \to H^1_{\mathrm{dR}}(X/k)$$

by

$$\bar{\gamma}_1 \mapsto \gamma_1 \quad \text{and} \quad \bar{\gamma}_2 \mapsto \gamma_2 + \lambda_2.$$

Clearly $p \circ s$ is the identity map on $H^1(X,\mathcal{O}_X)$, and hence if s is $k[\langle\tau\rangle]$-linear the sequence in Proposition 4.1.2 does split as a sequence of $k[\langle\tau\rangle]$-modules.

We now show that s is $k[\langle\tau\rangle]$-linear. Applying Proposition 4.4.1 to the basis above we see that the pre-images of γ_1 and γ_2 in $\check{H}^1_{\mathrm{dR}}(\mathcal{U}'')$ are the residue classes of

$$\nu_1 = \left(\frac{1}{yx^2}dx, \frac{x^4+2x^3+2x^2}{2y(x-1)^3}dx, \frac{x^4+2x^2}{y}dx, \frac{y}{x(x-1)^2}, \frac{y}{x}, \frac{y(x+1)}{(x-1)^2}\right)$$

and

$$\nu_2 = \left(\frac{1+x^2}{2yx^3}dx, \frac{x^3+x^2+x+1}{2y(x-1)^3}dx, \frac{2x^3}{y}dx, \frac{y(x+1)}{x^2(x-1)^2}, \frac{y}{x^2}, \frac{y}{(x-1)^2}\right).$$

Using a computation similar to (4.27) it is easy to verify that

$$\tau^*(\gamma_1) = \tau^*(\rho'(\nu_1)) = 2\lambda_2 + 2\gamma_2 + \gamma_1$$

and that

$$\tau^*(\gamma_2) = \tau^*(\rho'(\nu_2)) = \gamma_2 + 2\lambda_1.$$

Furthermore, we note that

$$\tau^*(\lambda_1) = \lambda_1 \quad \text{and} \quad \tau^*(\lambda_2) = \lambda_2 + \lambda_1.$$

Finally we conclude that

$$s(\tau^*(\bar{\gamma}_1)) = s(\bar{\gamma}_1 + 2\bar{\gamma}_2) = \gamma_1 + 2\lambda_2 + 2\gamma_2 = \tau^*(\gamma_1) = \tau^*(s(\bar{\gamma}_1))$$

and

$$s(\tau^*(\bar{\gamma}_2)) = s(\bar{\gamma}_2) = \gamma_2 + \lambda_2 = \tau^*(\gamma_2 + \lambda_2) = \tau^*(s(\bar{\gamma}_2)).$$

Hence s is $k[\langle\tau\rangle]$-linear, and the sequence in Proposition 4.1.2 splits.

Chapter 5

Faithful actions on Riemann–Roch spaces

In this chapter our main aim is to determine when a subgroup of the automorphism group of an algebraic curve acts faithfully on the space of global holomorphic differentials and polydifferentials. Our approach uses the obvious fact that if any finite group G does not act faithfully on $H^0(X, \Omega_X^{\otimes m})$ then there exists a subgroup of G which fixes at least one element of this k vector space.

Given this, it will be useful to know whether the fixed space is non-zero, and for this reason we start by computing the dimension of the fixed space $H^0(X, \Omega_X^{\otimes m})^G$. We discover (Proposition 5.1.2) that the dimension relies primarily on the genus of the quotient curve $Y := X/G$, m and the ramification divisor of $\pi\colon X \to Y$.

Then we use this dimension formula, along with results from the second chapter, to compute exactly when a cyclic group of prime order will act trivially on $H^0(X, \Omega_X^{\otimes m})$, considering the cases $m = 1$ and $m \geq 2$ in Proposition 5.2.1 and Proposition 5.2.2 respectively. When we are considering holomorphic differentials (i.e. when $m = 1$), this depends solely on the characteristic of k, whilst for polydifferentials (i.e. when $m \geq 2$) this is actually independent of $\mathrm{char}(k)$, and is determined by the genus of X, m and the order of the group. In the same section we also extend these results to more general Riemann–Roch spaces, see Corollary 5.2.4.

We then move on to the main theorem (Theorem 5.3.1), which answers the question of when G acts faithfully on $H^0(X, \Omega_X^{\otimes m})$. After proving this theorem we give examples which illustrate both when we do and do not have faithful actions. In particular, we use results of Chapter 3 to explicitly show the result holds for hyperelliptic curves.

We close the chapter with an alternative proof of when a cyclic group of prime order acts faithfully on $H^0(X, \Omega_X)$, by studying the $k[G]$-module structure of $H^0(X, \Omega_X)$, which was determined in [VM81].

The results of this chapter appear in [KT14].

5.1 Dimension formulae

Throughout this chapter, unless otherwise stated, we assume that X is an algebraic curve over an algebraically closed field k of characteristic $p \geq 0$. We furthermore assume that G is a finite group of order n that acts faithfully on X. Note that G also induces an action on the vector space $H^0(X, \Omega_X^{\otimes m})$ of global holomorphic poly-differentials of order m. We let Y denote the quotient curve X/G, and we let $\pi \colon X \to Y$ be the canonical projection. Finally, we denote by g_X and g_Y the genus of X and Y respectively, and we let K_X and K_Y be canonical divisors on X and Y.

In this section we compute the dimension of $H^0(X, \Omega_X^{\otimes m})$ and of $H^0(X, \Omega_X^{\otimes m})^G$, the subspace of $H^0(X, \Omega_X^{\otimes m})$ fixed by G. We first recall that $\dim_k H^0(X, \Omega_X) = g_X$ by Definition 2.2.4. We also computed the dimension of $H^0(X, \Omega_X^{\otimes m})$ when $g_X, m \geq 2$ in Corollary 2.3.7. Finally, as we will see in examples (a) and (b) in Section 5.4, if g_X is zero or one then $\dim_k(H^0(X, \Omega_X^{\otimes m}) = g_X$, for all $m \in \mathbb{Z} \geq 1$.

We now introduce some notations. Let $D = \sum_{P \in X} n_P[P]$ be a G-invariant divisor on X (i.e. $n_{\sigma(P)} = n_P$ for all $\sigma \in G$ and $P \in X$) and let $\mathcal{O}_X(D)$ denote the corresponding equivariant invertible $\mathcal{O}_X$-module. Furthermore, let $\pi_*^G(\mathcal{O}_X(D))$ denote the sub-sheaf of the direct image $\pi_*(\mathcal{O}_X(D))$ fixed by the obvious action of G on $\pi_*(\mathcal{O}_X(D))$. We also let $\left\lfloor \frac{\pi_*(D)}{n} \right\rfloor$ denote the divisor on Y obtained from the push-forward $\pi_*(D)$ by replacing the coefficient m_Q of Q in $\pi_*(D)$ with the integral part $\left\lfloor \frac{m_Q}{n} \right\rfloor$ of $\frac{m_Q}{n}$ for each $Q \in Y$. The function fields of X and Y are denoted by $K(X)$ and $K(Y)$ respectively. Finally, for any $P \in X$ let ord_P and ord_Q denote the respective valuations of $K(X)$ and $K(Y)$ at P and $Q := \pi(P)$.

The next lemma is the main idea in the proof of our formula for $\dim_k H^0(X, \Omega_X^{\otimes m})^G$, see Proposition 5.1.2.

Lemma 5.1.1. *Let $D = \sum_{P \in X} n_P[P]$ be a G-invariant divisor on X. Then the sheaves $\pi_*^G(\mathcal{O}_X(D))$ and $\mathcal{O}_Y\left(\left\lfloor \frac{\pi_*(D)}{n} \right\rfloor\right)$ are equal as subsheaves of the constant sheaf $K(Y)$ on Y. In particular, the sheaf $\pi_*^G(\mathcal{O}_X(D))$ is an invertible $\mathcal{O}_Y$-module.*

Proof. For every open subset V of Y we have

$$\pi_*^G(\mathcal{O}_X(D))(V) = \mathcal{O}_X(D)(\pi^{-1}(V))^G \subseteq K(X)^G = K(Y).$$

In particular, both sheaves are subsheaves of the constant sheaf $K(Y)$ as stated. It therefore suffices to check that their stalks are equal. For any $Q \in Y$ and $P \in \pi^{-1}(Q)$, we have

$$\begin{aligned}\pi_*^G(\mathcal{O}_X(D))_Q &= \mathcal{O}_X(D)_P \cap K(Y)\\ &= \{f \in K(Y) : \mathrm{ord}_P(f) \geq -n_P\}\\ &= \left\{f \in K(Y) : \mathrm{ord}_Q(f) \geq -\frac{n_P}{e_P}\right\}\\ &= \left\{f \in K(Y) : \mathrm{ord}_Q(f) \geq -\left\lfloor\frac{n_P}{e_P}\right\rfloor\right\}\\ &= \mathcal{O}_Y\left(\left\lfloor\frac{\pi_*(D)}{n}\right\rfloor\right)_Q,\end{aligned}$$

as desired. □

The following proposition contains the aforementioned formula for the dimension of the subspace of $H^0(X, \Omega_X^{\otimes m})$ fixed by G. In particular we see that this dimension is completely determined by m, g_Y and $\deg\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor$.

Proposition 5.1.2. *Let $m \geq 1$. Then the dimension of $H^0(X, \Omega_X^{\otimes m})^G$ is equal to*

$$\dim_k\left(H^0(X, \Omega_X^{\otimes m})^G\right) = (2m-1)(g_Y - 1) + \deg\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor,$$

unless

- $m = 1$ *and* $\deg\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor = 0$ *or*
- $g_Y = 1$ *and* $\deg\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor = 0$ *or*
- $g_Y = 0$ *and* $\deg\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor < 2m - 1$,

in which case

$$\dim_k\left(H^0(X, \Omega_X^{\otimes m})^G\right) = g_Y.$$

Proof. Let E denote the divisor $\left\lfloor\frac{\pi_*(mK_X)}{n}\right\rfloor$ on Y. As $K_X = \pi^*(K_Y) + R$ by Theorem 2.4.6 we have

$$E = \left\lfloor\frac{\pi_*\pi^*(mK_Y) + \pi_*(mR)}{n}\right\rfloor = mK_Y + \left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor.$$

Using the previous lemma we conclude that $\pi_*^G(\Omega_X^{\otimes m}) \cong \mathcal{O}_Y(E)$ and finally that

$$\dim_k H^0(X, \Omega_X^{\otimes m})^G = \dim_k H^0\left(Y, \pi_*^G(\Omega_X^{\otimes m})\right) = \dim_k H^0(Y, \mathcal{O}_Y(E)).$$

We now show that $\dim_k H^0(X,\Omega_X^{\otimes m}) = g_Y$ in the exceptional cases listed in the proposition. Firstly if $m = 1$ and $\deg\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor = 0$, then $\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor$ is the zero divisor and we conclude that

$$\dim_k H^0(X,\Omega_X)^G = \dim_k H^0(Y,\Omega_Y) = g_Y.$$

In the second case $\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor$ is again the zero divisor. Furthermore, as $g_Y = 1$, the divisor K_Y is equivalent to the zero divisor, and hence mK_Y is too. This means that

$$\dim_k H^0(X,\Omega_X^{\otimes m})^G = \dim_k H^0(Y,\mathcal{O}_Y(E)) = \dim_k H^0(Y,\mathcal{O}_Y(0)) = 1.$$

For the third case, by [Har77, Chap. IV, Ex. 1.3.4] it suffices to show that $\deg(E) < 0$. As $g_Y = 0$ we have $\deg(K_Y) = -2$, so $\deg(mK_Y) = -2m$, and $\deg(E)$ is indeed negative.

We will show below that in all other cases $\deg(E) > \deg(K_Y)$, and then the Riemann–Roch formula (Theorem 2.3.3) will give

$$\begin{aligned}\dim_k H^0(X,\Omega_X^{\otimes m})^G &= \dim_k H^0(Y,\mathcal{O}_Y(E))\\ &= 1 - g_Y + \deg\left(mK_Y + \left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor\right)\\ &= (2m-1)(g_Y-1) + \deg\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor,\end{aligned}$$

completing the proof for the main case.

All that remains is to show that $\deg(E) > \deg(K_Y)$ in all other cases. Firstly, if $g_Y = 0$ and $\deg\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor \geq 2m-1$ then, since $\deg(mK_Y) = -2m$, we have

$$\deg(E) \geq -1 > -2 = \deg(K_Y).$$

Similarly, if $g_Y = 1$ and $\deg\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor > 0$ then, as $\deg(mK_Y) = 0$, we have $\deg(E) > 0 = \deg(K_Y)$. If $m = 1$ and $\deg\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor > 0$ then clearly $\deg(E) > \deg(K_Y)$. Lastly, if $m \geq 2$ and $g_Y \geq 2$ then $\deg(K_Y) > 0$ and we have

$$\deg(E) \geq \deg(mK_Y) > \deg(K_Y).$$

So in all other cases $\deg(E) > \deg(K_Y)$, and the proof is complete. □

If $m = 1$ we reformulate Proposition 5.1.2 in the following slightly more concrete way. Let S denote the set of all points $Q \in Y$ such that π is not tamely ramified at Q and let s denote the cardinality of S. Note that $s = 0$ if p does not divide n.

In the next corollary for any $Q \in Y$ we let $\delta_Q = \delta_P$ and $e_Q = e_P$, for any $P \in \pi^{-1}(Q)$.

Corollary 5.1.3. *We have*

$$\dim_k H^0(X,\Omega_X)^G = \begin{cases} g_Y & \text{if } s = 0, \\ g_Y - 1 + \sum_{Q\in S} \left\lfloor \frac{\delta_Q}{e_Q} \right\rfloor & \text{otherwise.} \end{cases}$$

Proof. We have

$$\deg \left\lfloor \frac{\pi_*(R)}{n} \right\rfloor = \sum_{Q\in Y} \left\lfloor \sum_{P\mapsto Q} \frac{\delta_P}{n} \right\rfloor = \sum_{Q\in Y} \left\lfloor \frac{\delta_Q}{e_Q} \right\rfloor .$$

Furthermore we have $\left\lfloor \frac{\delta_Q}{e_Q} \right\rfloor = 0$ if and only if $\delta_Q < e_Q$, i.e. if and only if $Q \notin S$. Thus Corollary 5.1.3 follows from Proposition 5.1.2. □

Remark. Note that if $p > 0$ and G is cyclic then Corollary 5.1.3 can be derived from [KaKo13, Prop. 6.].

5.2 Trivial action in the cyclic case

In this section we will look at the case where G is a cyclic group of prime order, or a power of a prime, and determine when G acts trivially on $H^0(X,\Omega_X^{\otimes m})$. Compared to arbitrary groups, it is considerably easier to compute when these groups act trivially, and we will later see that we can reduce to this case, regardless of what the structure of G is.

Throughout this section, $P_1,\dots,P_r \in X$ denote the ramification points of π and we write e_i and δ_i for e_{P_i} and δ_{P_i}. Also, for $i = 1,\dots,r$, we define $N_i \in \mathbb{N}$ by $\mathrm{ord}_{P_i}(\sigma(\pi_i)-\pi_i) = N_i + 1$, where π_i is a local parameter at the ramification point P_i and σ is a generator of $G(P_i)$. We also assume that $g_X \geq 2$.

Proposition 5.2.1. *Let $p > 0$ and let G be cyclic of order p. Furthermore, we assume that $g_Y = 0$. Then G acts trivially on $H^0(X,\Omega_X)$ if and only if $p = 2$.*

Proof. From [Nak86, Lem. 1] we know that p does not divide N_i for $i = 1,\dots,r$, a fact we will use several times below. Let $N := \sum_{i=1}^r N_i$. Using the Riemann–Hurwitz formula, Corollary 2.4.7, we obtain

$$2g_X - 2 = -2p + (N + r)(p-1) \tag{5.1}$$

and hence

$$\dim_k H^0(X,\Omega_X) = g_X = \frac{(N+r-2)(p-1)}{2}.$$

Since $g_X \geq 0$ we obtain $r \geq 1$; that is, π is not unramified. As $\mathrm{char}(k) = p = \mathrm{ord}(G)$, the morphism π is not tamely ramified, and the cardinality s defined before Corollary 5.1.3 is not zero. Therefore we have

$$\deg\left\lfloor\frac{\pi_*(R)}{p}\right\rfloor = \sum_{i=1}^{r}\left\lfloor\frac{(N_i+1)(p-1)}{p}\right\rfloor \geq \sum_{i=1}^{r}\left\lfloor\frac{2(p-1)}{p}\right\rfloor = r > 0.$$

From Corollary 5.1.3 we then conclude that

$$\begin{aligned}\dim_k H^0(X,\Omega_X)^G &= g_Y - 1 + \sum_{i=1}^{r}\left\lfloor\frac{\delta_i}{e_i}\right\rfloor \\ &= -1 + N + r + \sum_{i=1}^{r}\left\lfloor -\frac{N_i+1}{p}\right\rfloor.\end{aligned}$$

If $p = 2$, the dimension of both $H^0(X,\Omega_X)$ and $H^0(X,\Omega_X)^G$ is therefore equal to $\frac{N+r-2}{2}$. This shows the if-direction in Proposition 5.2.1.

To prove the other direction we now assume that G acts trivially on $H^0(X,\Omega_X)$. For each $i = 1,\dots,r$, we write $N_i = s_i p + t_i$ with $s_i \in \mathbb{N}$ and $t_i \in \{1,\dots,p-1\}$. We furthermore put $S := \sum_{i=1}^r s_i$ and $T := \sum_{i=1}^r t_i \geq r$. Then we have

$$\frac{(N+r-2)(p-1)}{2} = \dim_k H^0(X,\Omega_X) = \dim_k H^0(X,\Omega_X)^G = N - S - 1.$$

Rearranging this equation we obtain

$$(3-p)N - 2S = (r-2)(p-1) + 2$$

and hence

$$(-p^2 + 3p - 2)S = (r-2)(p-1) + 2 - (3-p)T.$$

Assuming that $p \geq 3$ this equation implies that

$$S = \frac{(r-2)(1-p) - 2 + T(3-p)}{(p-1)(p-2)}.$$

since $-p^2 + 3p - 2 = -(p-1)(p-2)$.

Because $S \geq 0$, the numerator of this fraction is non-negative, that is

$$\begin{aligned}0 &\leq (r-2)(1-p) - 2 + T(3-p) \\ &\leq (r-2)(1-p) - 2 + r(3-p) \\ &= 2(r-1)(2-p).\end{aligned}$$

Hence we have that $r = 1$ and that the numerator is 0. We conclude that $S = 0$ and hence that $T = 1$ or $p = 3$. If $T = 1$ we also have $N = 1$ and finally

$$g_X = \frac{(N + r - 2)(p - 1)}{2} = 0,$$

a contradiction. If $T \neq 1$ and $p = 3$ we obtain $N = T = 2$ and finally

$$g_X = \frac{(N + r - 2)(p - 1)}{2} = 1,$$

again a contradiction. □

Remark. In Section 5.5 we show that it is possible to give an alternative, but rather involved, proof of the above lemma, using the deep and intricate results of [VM81].

Proposition 5.2.2. *Let $m \geq 2$. Suppose that G is a cyclic group of prime order l (which may or may not be equal to p) and that $g_Y = 0$. Then G acts trivially on $H^0(X, \Omega_X^{\otimes m})$ if and only if $g_X = m = l = 2$.*

Proof. We have different proofs according to whether or not the order l of the group is the same as the characteristic p of the field.

First we assume that $l = p$. As in the proof of Proposition 5.2.1, we let $N = \sum_{i=1}^{r} N_i$, and we let $M = N + r$. Then due to (5.1) we have

$$2g_X - 2 = -2p + M(p - 1), \tag{5.2}$$

and combining this with Corollary 2.3.7 we can write

$$\dim_k H^0(X, \Omega_X^{\otimes m}) = (2m - 1)(g_X - 1) = (2m - 1)\left(\frac{M(p - 1) - 2p}{2}\right). \tag{5.3}$$

Furthermore, we have

$$\deg\left\lfloor \frac{m\pi_*(R)}{p} \right\rfloor = \sum_{i=1}^{r} \left\lfloor \frac{m(N_i + 1)(p - 1)}{p} \right\rfloor = mM + \sum_{i=1}^{r} \left\lfloor \frac{-m(N_i + 1)}{p} \right\rfloor. \tag{5.4}$$

If we have $p = g_X = m = 2$, then on the one hand we see that $\dim_k H^0(X, \Omega_X^{\otimes m}) = 3$. On the other hand, we first note that (5.2) implies $M = 6$. So

$$\deg\left\lfloor \frac{m\pi_*(R)}{p} \right\rfloor = 2M - M = 6 > 3 = 2m - 1.$$

Then, by Proposition 5.1.2, we obtain

$$\dim_k H^0(X,\Omega_X^{\otimes m})^G = (2m-1)(g_Y-1)+\deg\left\lfloor \frac{m\pi_*(R)}{p}\right\rfloor = -3+6=3.$$

So the two dimensions are equal and the action of G on $H^0(X,\Omega_X^{\otimes m})$ is trivial. This completes the if direction of the proof.

Now we assume that the action is trivial. We first note that this implies that $\deg\left\lfloor \frac{m\pi_*(R)}{p}\right\rfloor \geq 2m-1$. Indeed, if this was not the case then by Proposition 5.1.2 we would have

$$0 = \dim_k H^0(X,\Omega_X^{\otimes m})^G = \dim_k H^0(X,\Omega_X^{\otimes m}) = (2m-1)(g_X-1),$$

which is clearly a contradiction. So, using (5.4), (5.3) and Proposition 5.1.2 we see that

$$\begin{aligned}(2m-1)\frac{M(p-1)-2p}{2} &= \dim_k H^0(X,\Omega_X^{\otimes m})\\ &= \dim_k H^0(X,\Omega_X^{\otimes m})^G\\ &= 1-2m+mM+\sum_{i=1}^{r}\left\lfloor\frac{-m(N_i+1)}{p}\right\rfloor\\ &\leq 1-2m+mM+\sum_{i=1}^{r}\frac{-m(N_i+1)}{p}\\ &= 1-2m+mM-\frac{mM}{p}. \end{aligned} \tag{5.5}$$

After multiplying by $2p$ and rearranging we obtain

$$\begin{aligned}0 &\geq (2mM-M-4m+2)p^2+(-4mM+M-2+4m)p+2mM\\ &= (M-2)(2m-1)p^2-((M-2)(2m-1)+2mM)p+2mM\\ &= (p-1)((M-2)(2m-1)p-2mM). \end{aligned} \tag{5.6}$$

Furthermore from (5.1) we obtain that $-2p+M(p-1)=2g_X-2\geq 2$ and hence that

$$M \geq \frac{2+2p}{p-1} = 2+\frac{4}{p-1} > 2. \tag{5.7}$$

So from (5.6) and (5.7) we see that

$$\begin{aligned} p &\leq \frac{2mM}{(M-2)(2m-1)} \\ &= \frac{M}{M-2} \cdot \frac{2m}{2m-1} \\ &= \left(1 + \frac{2}{M-2}\right)\left(1 + \frac{1}{2m-1}\right) \\ &\leq 4, \end{aligned} \tag{5.8}$$

i.e. $p = 2$ or $p = 3$.

Suppose that $p = 3$. Then from (5.7) we have $M \geq 4$. However, from (5.8) we also have that

$$\begin{aligned} 3 &\leq \left(1 + \frac{2}{M-2}\right)\left(1 + \frac{1}{2m-1}\right) \\ &\leq \left(1 + \frac{2}{M-2}\right)\frac{4}{3} \\ &\leq \frac{8}{3}, \end{aligned}$$

a contradiction.

Lastly, we come to the case when $p = 2$. From (5.8) we see that $2 \leq \left(1 + \frac{2}{M-2}\right)\frac{4}{3}$ and hence $M \leq 6$. However, from (5.7) we know that $M \geq 6$, so $M = 6$. Then from (5.5) we obtain that $2m-1 = 1-2m+6m-3m$ and hence that $m = 2$. Finally, (5.1) gives us that $2g_X-2 = -4+6 = 2$ and hence $g_X = 2$. This completes the only if direction of the proof when $l = p$.

Now if $l \neq p$ then we know that all the coefficients δ_i of the ramification divisor are equal to $l-1$. To show the if direction in this case, first note that $\dim_k H^0(X, \Omega_X^{\otimes m}) = 3$ by Corollary 2.3.7. On the other hand, the Riemann–Hurwitz formula (Corollary 2.4.7) implies that $2 = 2g_X - 2 = -2l + \deg(R) = -2l + r(l-1)$, and hence that $r = 6$. Finally Proposition 5.1.2 gives us

$$\dim_k H^0(X, \Omega_X^{\otimes m})^G = -(2m-1) + \sum_{i=1}^{r} \left\lfloor \frac{m \cdot \delta_i}{l} \right\rfloor = -3 + \sum_{i=1}^{6} \left\lfloor \frac{m(l-1)}{l} \right\rfloor = 3,$$

since $m = l = 2$. As the dimensions of $H^0(X, \Omega_X^{\otimes m})$ and $H^0(X, \Omega_X^{\otimes m})^G$ are equal, the action is trivial.

For the final section of the proof we suppose that G acts trivially on the space $H^0(X, \Omega_X^{\otimes m})$. We then show that this implies that $g_X = l = m = 2$.

From Corollary 2.3.7 and Proposition 5.1.2 we obtain

$$\begin{aligned}(2m-1)(g_X-1) &= \dim_k H^0(X,\Omega_X^{\otimes m}) \\ &= \dim_k H^0(X,\Omega_X^{\otimes m})^G \\ &= -(2m-1)+\sum_{i=1}^{r}\left\lfloor\frac{m\cdot\delta_i}{l}\right\rfloor\end{aligned}$$

and hence

$$(2m-1)g_X=\sum_{i=1}^{r}\left\lfloor\frac{m\cdot\delta_i}{l}\right\rfloor=\sum_{i=1}^{r}\left\lfloor\frac{m(l-1)}{l}\right\rfloor=r\left(m+\left\lfloor\frac{-m}{l}\right\rfloor\right).$$

By choosing $s\in\{1,\ldots,l\}$ and $q\in\mathbb{N}$ such that $m=ql+s$ we can rewrite this as

$$(2m-1)g_X=r(m-q-1). \tag{5.9}$$

If we multiply (5.9) by $l-1$ and then substitute in for the $r(l-1)$ term in the Riemann-Hurwitz formula (Corollary 2.4.7) we get

$$(2m-1)(l-1)g_X=(2g_X+2(l-1))(m-q-1).$$

By rearranging we are able to compute g_X in terms of m, l and q:

$$\begin{aligned}g_X &= \frac{2(l-1)(m-q-1)}{(2m-1)(l-1)-2(m-q-1)} \\ &= 1+\frac{2(m-q-1)-(2q+1)(l-1)}{(2m-1)(l-1)-2(m-q-1)} \\ &= 1+\frac{2s-1-l}{(2m-1)(l-1)-2(m-q-1)} \\ &= 1+\frac{2(s-1)+1-l}{(2m-1-2q)(l-1)-2(s-1)}.\end{aligned} \tag{5.10}$$

First, we show that if $l\geq 3$ the equation cannot hold whilst $g_X\geq 2$. Observe that the denominator is strictly greater than $l-1$, remembering that $m=ql+s$:

$$\begin{aligned}(2m-1-2q)(l-1)-2(s-1) &= ((2q(l-1)+2s-1)(l-1)-2(s-1) \\ &\geq (2s-1)(l-1)-2(s-1) \\ &\geq (2s-1)(l-1)-2(s-1)(l-1) \\ &= l-1;\end{aligned}$$

here the two inequalities are equalities if and only if $q=0$ and $s=1$, respectively, and, as $m\geq 2$, not both inequalities can be equalities. Now the numerator is at most $l-1$, occurring when $s=l$. Hence if $l\geq 3$ the fraction in (5.10) will be less than one and $g_X<2$, contradicting our assumption. If $l = 2$, then s is either 1 or 2. If $s = 1$ the fraction is negative, and $g_X < 1$, which again contradicts our assumption. Finally, if $s = 2$ then $g_X \leq 2$, with equality if and only if $q = 0$, i.e. if and only if $m = 2$. So if $g_X \geq 2$ then the action being trivial implies that $g_X = l = m = 2$, and the proof is complete. □

For the rest of this section we assume that $p > 0$ and that G is a cyclic group of order p^l for some $l \in \mathbb{N}$. What we are now going to do will not be used in the proof of the main theorem, but is included because it generalises the previous results. More precisely, we do not restrict ourselves to looking at $H^0(X, \Omega_X^{\otimes m})$, but using a comparatively deep result from [KaKo13] we study $H^0(X, \mathcal{O}(D))$ for any G-invariant divisor D such that $\deg(D) > 2g_X - 2$.

We first introduce some notation. Let $D = \sum_{P \in X} n_P[P]$ be a G-invariant divisor on X. Then let $\langle a \rangle$ denote the fractional part of any $a \in \mathbb{R}$, i.e. $\langle a \rangle = a - \lfloor a \rfloor$. Also, for any $Q \in Y$ let n_Q be equal to n_P for any $P \in \pi^{-1}(Q)$.

Proposition 5.2.3. *Suppose $p > 0$ and G is a cyclic group of order p^l for some $l \geq 1$. Let D be a G-invariant divisor on X such that* $\deg(D) > 2g_X - 2$. *Then the action of G on $H^0(X, \mathcal{O}_X(D))$ is trivial if and only if*

$$(p^l - 1)\deg(D) = p^l \left(g_X - g_Y - \sum_{Q \in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle \right).$$

Proof. We first remind the reader of the notation in [KaKo13]. Let σ be a generator of G. Let V be the $k[G]$ module with k-basis $e_1, \ldots, e_{p^l}$ and G-action defined by $\sigma(e_i) = e_i + e_{i-1}$ for $1 \leq i \leq p^l$, where $e_0 = 0$. Then V_j, defined to be the subspace of V spanned by $e_1, \ldots, e_j$ over k, is also a $k[G]$ module. In fact, the modules $V_1, \ldots, V_{p^l}$ form a complete set of representatives for the set of isomorphism classes of indecomposable $k[G]$-modules. For each $j = 1, \ldots, p^l$ let m_j denote the multiplicity of V_j in the $k[G]$-module $H^0(X, \mathcal{O}_x(D))$, i.e. we have $H^0(X, \mathcal{O}_x(D)) \cong \bigoplus_{j=1}^{p^l} m_j V_j$.

First note that the action of G on $H^0(X, \mathcal{O}_X(D))$ is trivial if and only if

$$\dim_k H^0(X, \mathcal{O}_X(D))^G = \dim_k H^0(X, \mathcal{O}_X(D)).$$

It is clear that the G-invariant part of each submodule V_j is spanned by e_1. It then follows that $\dim_k H^0(X, \mathcal{O}_X(D))^G = \sum_{j=1}^{p^l} m_j$. By [KöKo12, Thm. 2.1], which relies on [Bor06], we have

$$\begin{aligned}\sum_{j=1}^{p^l} m_j &= 1 - g_Y + \sum_{Q\in Y} \left\lfloor \frac{n_Q}{e_Q} \right\rfloor \\ &= 1 - g_Y + \sum_{Q\in Y} \left(\frac{n_Q}{e_Q} - \left\langle \frac{n_Q}{e_Q} \right\rangle \right) \\ &= 1 - g_Y + \frac{1}{p^l} \deg(D) - \sum_{Q\in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle.\end{aligned}$$

Now as $\deg(D) > 2g_X - 2$ we have $\dim_k H^0(X, \mathcal{O}_X(D)) = \deg(D) + 1 - g_X$ by the Riemann–Roch theorem. So the action of G on $H^0(X, \mathcal{O}_X(D))$ is trivial if and only if

$$\deg(D) + 1 - g_X = 1 - g_Y + \frac{1}{p^l} \deg(D) - \sum_{Q\in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle.$$

This then rearranges to $(p^l - 1)\deg(D) = p^l \left(g_X - g_Y - \sum_{Q\in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle \right)$, as desired. □

Corollary 5.2.4. *Suppose that* $\deg(D) \geq 2g_X$. *Then the action of* G *on* $H^0(X, \mathcal{O}_X(D))$ *is trivial if and only if* $g_Y = 0$, $e_Q | n_Q$ *for all* $Q \in Y$, $\deg(D) = 2g_X$ *and either* $g_X = 0$ *or* $p^l = 2$.

Proof. The following inequalities always hold under the stated assumptions:

$$\begin{aligned}(p^l - 1)\deg(D) \geq (p^l - 1)2g_X \geq p^l g_X \geq p^l g_X - p^l \sum_{Q\in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle \\ \geq p^l \left(g_X - g_Y - \sum_{Q\in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle \right).\end{aligned}$$

Now the first inequality is an equality if and only if $\deg(D) = 2g_X$. The second is an equality if and only if either $g_X = 0$ or $p^l = 2$. The third inequality is an equality if and only if $\sum_{Q\in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle = 0$, which is the case if and only if each n_Q is divisible by e_Q. Lastly, the fourth inequality is an equality if and only if $g_Y = 0$. Given these observations, Proposition 5.2.3 implies Corollary 5.2.4. □

The following Corollary slightly strengthens the only if direction of the $l = p$ part of Proposition 5.2.2 (from $\mathrm{ord}(G) = p$ to $\mathrm{ord}(G) = p^l$) and also provides a different proof for it; note that this new proof relies on the comparatively deep result in section 7 of [Bor06].

Corollary 5.2.5. *Let* $m \geq 2$ *and let* G *be a cyclic group of order* p^l *for some* l. *If* G *acts trivially on* $H^0(X, \Omega_X^{\otimes m})$, *then* $g_Y = 0$ *and* $p^l = g_X = m = 2$.

Proof. As $g_X \geq 2$ and $m \geq 2$ we have $\deg(mK_X) \geq 2g_X$. So, if the action of G on $H^0(X, \Omega_X^{\otimes m})$ is trivial, we obtain from Corollary 5.2.4 that $\deg(mK_X) = 2g_X$, $p^l = 2$ and $g_y = 0$. Now $\deg(mK_X) = 2g_X$ implies that $m(2g_X - 2) = 2g_X$, so $m(g_X - 1) = g_X$ and hence $m = g_X = 2$. □

Similarly to the case $\deg(D) \geq 2g_X$ in Corollary 5.2.4, the following corollary derives necessary and sufficient conditions for trivial action from Proposition 5.2.3 in the case $\deg(D) = 2g_X - 1$.

Corollary 5.2.6. *Suppose that* $\deg(D) = 2g_X - 1$ *and that* $g_Y = 0$. *Then the action of* G *on* $H^0(X, \mathcal{O}_X(D))$ *is trivial if and only if one of the following conditions hold:*

- $p^l = 2$ *and* $\sum_{Q \in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle = \frac{1}{2}$*;*
- $g_X = 2$, $p^l = 3$ *and* $e_Q \mid n_Q$ *for all* $Q \in Y$.

Remark. It can easily be shown that in the last case the Riemann–Hurwitz formula implies that the number of ramification points r is at most 4. Furthermore, if $r = 1$ then the conditions "$\sum_{Q \in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle = \frac{1}{p^l}$" and "$e_Q \mid n_Q$ for all $Q \in Y$" are already implied by "$\deg(D) = 2g_X - 1$".

Proof. Firstly, if $g_X = 0$ then $\deg(D) = -1 < 0$, so $\dim_k H^0(X, \mathcal{O}_X(D)) = 0$ and the action is trivial.

Now note that, as $\deg(D) = 2g_X - 1$, we conclude from Proposition 5.2.3 that the action is trivial if and only if

$$(p^l - 1)(2g_X - 1) = p^l \left(g_X - \sum_{Q \in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle \right).$$

If $p^l = 2$ then this is equivalent to $2g_X - 1 = 2g_X - 2\sum_{Q \in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle$ and hence to $\sum_{Q \in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle = \frac{1}{2}$.

If $g_X = 1$ then this is equivalent to $p^l - 1 = p^l - p^l \sum_{Q \in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle$ and hence is also equivalent to $\sum_{Q \in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle = \frac{1}{p^l}$.

Lastly, if $p^l \geq 3$ and $g_X \geq 2$ then we have that $g_X \geq \frac{p^l - 1}{p^l - 2}$ which is equivalent to the first inequality in the chain

$$(p^l - 1)(2g_X - 1) \geq p^l g_X \geq p^l g_X - p^l \sum_{Q \in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle \geq p^l \left(g_X - g_Y - \sum_{Q \in Y} \left\langle \frac{n_Q}{e_Q} \right\rangle \right).$$

Hence the action is trivial if and only if both inequalities are equalities, which is the case if and only if $p^l = 3$, $g_X = 2$, $e_Q \mid n_Q$ for all $Q \in Y$ and $g_Y = 0$. □

5.3 The main theorem

In this section we prove the main theorem of this chapter, describing exactly when G will act faithfully on $H^0(X,\Omega_X^{\otimes m})$.

Theorem 5.3.1. *Suppose that $g_X \geq 2$ and let $m \geq 1$. Then G does not act faithfully on $H^0(X,\Omega_X^{\otimes m})$ if and only if G contains a hyperelliptic involution and one of the following two sets of conditions holds:*

- *$m = 1$ and $p = 2$;*
- *$m = 2$ and $g_X = 2$.*

Proof. We first show the if direction. In the case when $m = 1$, the hyperelliptic involution contained in G generates a subgroup of order 2. Since $p = 2$, this acts trivially by Proposition 5.2.1, and hence G does not act faithfully. In the case when $m = 2$, then again looking at the subgroup generated by the hyperelliptic involution, we have a group of order 2 acting on $H^0(X,\Omega_X^{\otimes m})$. So, by Proposition 5.2.2 and since $g_X = m = 2$, the action of this subgroup is trivial, and again, this means that G does not act faithfully.

We now start the proof of the only if direction, supposing that G does not act faithfully on $H^0(X,\Omega_X^{\otimes m})$. By replacing G with the (non-trivial) kernel H if necessary, we may assume that G is non-trivial and acts trivially on $H^0(X,\Omega_X^{\otimes m})$.

We start the proof by showing that $g_Y = 0$, which is shown separately for the cases when $m = 1$ and when $m \geq 2$. In the case when $m = 1$ we start by showing that $\deg\left\lfloor \frac{\pi_*(R)}{n} \right\rfloor > 0$ by contradiction. Suppose that $\deg\left\lfloor \frac{\pi_*(R)}{n} \right\rfloor = 0$. As G acts trivially it follows from Proposition 5.1.2 that:

$$g_X = \dim_k H^0(X,\Omega_X) = \dim_k H^0(X,\Omega_X)^G = g_Y.$$

Substituting this into the Riemann–Hurwitz formula (Corollary 2.4.7) yields the desired contradiction because $g_X \geq 2, n \geq 2$ and $\deg(R) \geq 0$.

Thus $\deg\left(\left\lfloor \frac{\pi_*(R)}{n} \right\rfloor\right) > 0$. Now Proposition 5.1.2 gives us that

$$g_X = \dim_k H^0(X,\Omega_X) = \dim_k H^0(X,\Omega_X)^G = g_Y - 1 + \deg\left\lfloor \frac{\pi_*(R)}{n} \right\rfloor.$$

Substituting this in to the Riemann–Hurwitz formula we see that

$$2\left(g_Y - 1 + \deg\left\lfloor \frac{\pi_*(R)}{n} \right\rfloor - 1\right) = 2n(g_Y - 1) + \deg(R).$$

For any $Q \in Y$ we let δ_Q denote the coefficient of the ramification divisor R at any $P \in \pi^{-1}(Q)$ and let $e_Q := e_P$ for any $P \in \pi^{-1}(Q)$. Rewriting the previous equation then yields

$$\begin{aligned}(2n-2)g_Y &= 2n-4+2\deg\left\lfloor\frac{\pi_*(R)}{n}\right\rfloor - \deg(R)\\ &= 2\left(n-2+\sum_{Q\in Y}\left(\left\lfloor\frac{n}{e_Q}\frac{\delta_Q}{n}\right\rfloor - \frac{n}{e_Q}\frac{\delta_Q}{2}\right)\right)\\ &= 2\left(n-2+\sum_{Q\in Y}\left(\left\lfloor\frac{\delta_Q}{e_Q}\right\rfloor - \frac{\delta_Q}{e_Q}\frac{n}{2}\right)\right)\\ &\leq 2(n-2),\end{aligned}$$

because $\frac{n}{2} \geq 1$ and $\left\lfloor\frac{\delta_Q}{e_Q}\right\rfloor \leq \frac{\delta_Q}{e_Q}$ for all $Q \in Y$. Hence we obtain $g_Y \leq \frac{n-2}{n-1} < 1$ and therefore $g_Y = 0$, as desired.

We now show that $g_Y = 0$ when $m \geq 2$. Since $g_X \geq 2$ we have that $\deg(mK_X) = m(2g_X - 2) > 2g_X - 2 = \deg(K_X)$. By Corollary 2.3.7, and as both m and g_X are at least 2, then $\dim_k H^0(X, \Omega_X^{\otimes m})^G = \dim_k H^0(X, \Omega_X^{\otimes m}) = (2m-1)(g_X - 1) > 1$. There is only one case in Proposition 5.1.2 such that $m \geq 2$ and $\dim_k H^0(X, \Omega_X^{\otimes m})^G > 1$, which yields

$$(2m-1)(g_X-1) = (2m-1)(g_Y-1) + \deg\left(\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor\right).$$

Combining this with the Riemann–Hurwitz formula, Corollary 2.4.7, we see that

$$\begin{aligned}2(2m-1)(g_Y-1) + 2\deg\left(\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor\right) &= 2(2m-1)(g_X-1)\\ &= 2n(2m-1)(g_Y-1) + (2m-1)\deg(R),\end{aligned}$$

which can be re-arranged as

$$(2m-1)(2n-2)(g_Y-1) = 2\deg\left(\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor\right) - (2m-1)\deg(R).$$

So if we can show that the right hand side of this equation is negative then we will have $g_Y - 1 < 0$ and hence $g_Y = 0$, as desired.

Using the same notation as in the case when $m = 1$, we calculate:

$$\begin{aligned}2\deg\left(\left\lfloor\frac{m\pi_*(R)}{n}\right\rfloor\right)-(2m-1)\deg(R) &= \sum_{Q\in Y}\left(2\left\lfloor m\cdot\frac{n}{e_Q}\frac{\delta_Q}{n}\right\rfloor - n(2m-1)\frac{\delta_Q}{e_Q}\right)\\ &\leq \sum_{Q\in Y}\left(2m\cdot\frac{\delta_Q}{e_Q} - n(2m-1)\frac{\delta_Q}{e_Q}\right)\\ &= (2m-n(2m-1))\sum_{Q\in Y}\frac{\delta_Q}{e_Q}.\end{aligned}$$

Now as $n, m \geq 2$ then we have $2m - n(2m-1) \leq 2m - 2(2m-1) = 2(1-m) < 0$ and we are done as $\sum_{Q\in Y}\frac{\delta_Q}{e_Q}$ is positive.

So we have shown for all $m \geq 1$, if the group G acts trivially on $H^0(X, \Omega_X^{\otimes m})$ then $g_Y = 0$. Now if $m \geq 2$ then first note that G must contain a cyclic subgroup of prime order, say H, such that H acts trivially on $H^0(X, \Omega_X^{\otimes m})$. Now Proposition 5.2.2 tells us that $m = g_X = 2$, and that the order of H must also be 2. Hence $X/H \cong \mathbb{P}_k^1$, and this completes the only if direction for $m \geq 2$.

Similarly, the $m = 1$ case of the only if direction will follow from Proposition 5.2.1 after we show that $p > 0$ and there is a cyclic subgroup of G of order p. This is true since π cannot be tamely ramified. Indeed, if it were then $R = \sum_{P\in X}(e_P - 1)[P]$ [Har77, Chap. IV, Cor. 2.4], and $\deg\left\lfloor\frac{\pi_*(R)}{n}\right\rfloor = 0$, which we have already shown cannot be the case. Hence p must be positive, and there is a cyclic subgroup of order p which acts trivially. □

Remark. Note that the existence of a hyperelliptic involution σ in G means not only that the genus of $X/\langle\sigma\rangle$, but also the genus of $Y = X/G$, is 0 (by the Riemann–Hurwitz formula). Moreover, if $p = 2$, then the canonical projection $X \to X/\langle\sigma\rangle$ is not unramified (again by the Riemann–Hurwitz formula) and hence not tamely ramified; then π cannot be tamely ramified either.

Remark. If X is not hyperelliptic and $m = 1$, or if $g_X \geq 3$ and $m \geq 2$, we can give a short proof of the "only-if" direction of Theorem 5.3.1 using [Har77, Chap. IV, Prop. 5.2] and [Har77, Chap. IV, Cor. 3.2]. The map $X \to \mathbb{P}(H^0(X, \Omega_X))$ is a G-equivariant closed embedding. Then, since G acts faithfully on X, G also acts faithfully on $H^0(X, \Omega_X)$.

5.4 Examples

We will now give some examples of a finite group acting on a curve, and the consequent action on the holomorphic poly-differentials. We start with some examples in which G acts trivially on $H^0(X, \Omega_X^{\otimes m})$. We then follow this with the example of hyperelliptic curves, for which we compute an explicit basis of $H^0(X,\Omega_X^{\otimes m})$, allowing us to see when the action is trivial.

(a) Let $g_X = 0$, i.e. $X \cong \mathbb{P}^1_k$. Then $\deg(K_X) = -2$ and so $\deg(mK_X) < 0$ for $m \geq 1$. Hence $H^0(X,\Omega_X^{\otimes m}) = \{0\}$ by [Har77, Lem. 2, Pg. 295] and G acts trivially on $H^0(X,\Omega_X^{\otimes m})$ for all $m \geq 1$.

(b) Let $g_X = 1$, i.e. X is an elliptic curve. If G is a finite subgroup of $X(k)$ acting on X by translations, then G leaves invariant any global non-vanishing holomorphic differential ω and hence G acts trivially on $H^0(X,\Omega_X)$; since $\omega^{\otimes m}$ is a basis of $H^0(X,\Omega_X^{\otimes m})$ this means that G acts trivially on $H^0(X,\Omega_X^{\otimes m})$ for all $m \geq 1$.

If $p > 0$ and G is a p-group, then the multiplicative character $G \to k^*$ afforded by the one-dimensional representation $H^0(X,\Omega_X^{\otimes m})$ of G has to be trivial because k doesn't contain any p^{th} roots of unity; in particular the action of G on $H^0(X,\Omega_X^{\otimes m})$ is trivial as well. On the other hand, if $p \neq 2$ and X is given by the Weierstrass equation of the form $y^2 = f(x)$, then the involution $\sigma\colon (x,y) \to (x,-y)$ maps the invariant differential $\omega = \frac{dx}{y}$ to $-\omega$.

(c) Let X be a hyperelliptic curve and G the subgroup of $\mathrm{Aut}(X)$ generated by the hyperelliptic involution. We recall that in Propositions 3.1.2 and 3.2.5 we gave bases of $H^0(X,\Omega_X^{\otimes m})$ for $m \geq 1$. In particular, if $p \neq 2$ we let $\omega = \frac{dx^{\otimes m}}{y^m}$, and if $p = 2$ we let $\omega = \frac{dx^{\otimes m}}{H(x)^m}$.

We first suppose that $p \neq 2$. Then σ acts by multiplication by -1 on $x^i\omega$ and $yx^i\omega$ if m is, respectively, odd and even. Hence if $m = 1$ or either $m > 2$ or $g_X > 2$ the action of σ is non-trivial. Finally, if m is even then σ acts trivially on ω and x, and so σ acts trivially, and hence non-faithfully, on $H^0(X,\Omega_X^{\otimes 2})$.

Now we suppose that $p = 2$. In this case σ acts trivially on x, and hence also on ω. So the action is trivial, and hence non-faithful, on $H^0(X,\Omega_X)$, and also on $H^0(X,\Omega_X^{\otimes 2})$ if $g_X = 2$. On the other hand, $\sigma(y) = y + H(x)$, so σ acts non-trivially on $yx^i\omega$, and the action is faithful if $m \geq 2$ and $g_X > 2$.

5.5 $K[G]$-module structure of $H^0(X,\Omega_X)$ when $|G| = p$

In this subsection we give an alternative proof of Proposition 5.2.1, using a sophisticated result of Valentini and Madan [VM81]. We suppose that G is a subgroup of $\mathrm{Aut}(X)$ of order $p = \mathrm{char}(k)$ and that $g_X \geq 2$ and $g_Y = 0$. The $k[G]$-module structure of $H^0(X,\Omega_X)$ is computed in [VM81, Thm. 1], and from this we will show that the action of G on $H^0(X,\Omega_X)$ is trivial if and only if $p = 2$.

We remark that in [VM81] it is assumed that $|G| = p^n$ for some $n \in \mathbb{N}$. We have assumed that $n = 1$, since this will greatly simplify our computations, and we do not require the general case.

Let σ be a generator of G. There are p unique indecomposable representations of G, which are

$$M_k := k[G]/((\sigma - 1)^k), \qquad k = 1, \dots, p.$$

Note that the elements $e := \sigma^0, \sigma = \sigma^1, \dots, \sigma^k$ form a k-vector space basis of M_k.

We let d_k denote the number of times that M_k occurs in the decomposition of the $k[G]$-module $H^0(X, \Omega_X)$ in to indecomposable $k[G]$-modules, so that

$$H^0(X, \Omega_X) \cong \bigoplus_{k=1}^{p} \bigoplus_{i=1}^{d_k} M_k. \tag{5.11}$$

Now if the action of G on $H^0(X, \Omega_X)$ is trivial then the only indecomposable submodule of $H^0(X, \Omega_X)$ will be the trivial module M_1. Hence the action of G is trivial if and only if $d_1 = g_X$ and $d_k = 0$ for $k \in \{2, \dots, p\}$.

We let $Q_1, \dots, Q_s \in Y$ be the branch points of π, and we let $P_1, \dots, P_s$ be the corresponding ramification points (note that since $|G|$ is prime it follows that there is only one point in $\pi^{-1}(Q_i)$ for $1 \le i \le s$). For each $i \in \{1, \dots, s\}$ we let m_i denote the largest integer such that $G_i(P_i)$ is non-trivial, which is coprime to p by [KöKo12, App. 5, Lem. 5.1]. From Hilbert's formula (Theorem 2.4.9) we conclude that

$$\delta_i = \sum_{j=0}^{\infty} (\mathrm{ord}(G_j(P_i)) - 1 = \sum_{j=0}^{m_i} (p-1) = (p-1)(m_i + 1).$$

In particular, the second equality holds since $G_j(P_i)$ is trivial for $j > m_i$, and hence we have $\mathrm{ord}(G_j(P_i)) - 1 = 0$ for any such j. Now we set

$$\gamma_{i,k} = \left\lfloor \frac{\delta_i - k m_i}{p} \right\rfloor, \qquad k = 0, \dots, p-1,$$

where $\lfloor c \rfloor$ denotes the largest integer less than c, for any $c \in \mathbb{R}$. We let $\Gamma_k = \sum_{i=1}^{s} \gamma_{i,k}$. Note that $\Gamma_k \le \Gamma_{k-1}$ for all k.

We now state the main theorem of [VM81].

Theorem 5.5.1. *Let G be a cyclic group of automorphisms of X of order p. Let $Y := X/G$ be the quotient of X by the action of G, with genus g_Y. The regular representation M_p of G occurs g_Y times in the representation of G on $H^0(X, \Omega_X)$. The indecomposable representation M_{p-1} occurs*

$\Gamma_{p-2} - \Gamma_{p-1} - 1$ *times, whilst for* $k = 1, \ldots, p-2$, *the indecomposable representation* M_k *of degree* k *occurs* $\Gamma_{k-1} - \Gamma_k$ *times.*

Proof. See [VM81, Thm. 1]. □

Using the above theorem we now give an alternative proof of Lemma 5.2.1.

Proof of Proposition 5.2.1. We first show that if $p = 2$ then the action is trivial. In this case there are only two representations - the regular representation and the trivial representation. By Theorem 5.5.1, the regular representation occurs g_Y times. Since we assumed that $g_Y = 0$ it follows that the action of G on $H^0(X, \Omega_X)$ only affords the trivial representation, and hence G acts trivially.

We now prove the other direction, supposing that $p > 2$ and that the action of G on $H^0(X, \Omega_X)$ is trivial. We will see that this yields a contradiction.

We first observe that for any $i \in \{1, \ldots, s\}$ we have

$$\gamma_{i,p-1} = \left\lfloor \frac{\delta_i - (p-1)m_i}{p} \right\rfloor = \left\lfloor \frac{(p-1)(m_i+1) - (p-1)m_i}{p} \right\rfloor = \left\lfloor \frac{p-1}{p} \right\rfloor = 0.$$

and hence $\Gamma_{p-1} = \sum_{i=1}^{s} \gamma_{i,p-1} = 0$.

Now since we are assuming that the action of G is trivial, it must follow that $d_k = 0$ for all $k \neq 1$, as previously discussed. Then by Theorem 5.5.1 we have that $\Gamma_{p-2} - \Gamma_{p-1} - 1 = 0$, and hence $\Gamma_{p-2} = 1$. We can then conclude inductively that for $1 \leq k \leq p-2$ we have $\Gamma_k = 1$, using the relation $\Gamma_{k-1} - \Gamma_k = 0$ from Theorem 5.5.1. Finally, we also have $\Gamma_0 = g_X + \Gamma_1 = g_X + 1$.

Since

$$1 = \Gamma_{p-2} = \sum_{i=1}^{s} \left\lfloor \frac{\delta_i - (p-2)m_i}{p} \right\rfloor = \sum_{i=1}^{s} \left\lfloor \frac{(p-1)(m_i+1) - (p-2)m_i}{p} \right\rfloor = \sum_{i=1}^{s} \left\lfloor \frac{m_i + p - 1}{p} \right\rfloor,$$

it follows that $m_i \neq 0$ for exactly one i, and for that i we have $1 \leq m_i \leq p$. Furthermore, since all m_i are coprime to p, we actually have $1 \leq m_i \leq p-1$. Note that actually $s = 1$ because $m_i = 0$ cannot occur, since $G_0(P) = G_1(P)$ for any ramified $P \in X$. We let $m = m_1$ and $\delta = \delta_1$.

We now determine m, as follows:

$$1 + g_X = \Gamma_0 = \left\lfloor \frac{\delta}{p} \right\rfloor = \left\lfloor \frac{(p-1)(m+1)}{p} \right\rfloor = m + 1 + \left\lfloor \frac{-m-1}{p} \right\rfloor = m, \tag{5.12}$$

with the last equality following since $0 \geq -m-1 \geq 2-p$.

On other hand, from the Hurwitz Formula (Corollary 2.4.7) and Hilbert's Formula (Theorem 2.4.9), we can conclude that

$$2g_X - 2 = -2p + (p-1)(m+1),$$

which, together with (5.12), implies that

$$g_X(p-3) = 0.$$

Hence we conclude that $p = 3$. But applying (5.12) and the fact that $m \leq p-1$, we conclude that $1 + g_X = m < 3$, which contradicts our assumption that $g_X \geq 2$. □

Bibliography

[Ahl78] Lars V. Ahlfors, *Complex analysis*, third ed., McGraw-Hill Book Co., New York, 1978, An introduction to the theory of analytic functions of one complex variable, International Series in Pure and Applied Mathematics. MR 510197 (80c:30001)

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR 0242802 (39 #4129)

[Bor06] Niels Borne, *Cohomology of G-sheaves in positive characteristic*, Adv. Math. **201** (2006), no. 2, 454–515. MR 2211535 (2007a:14014)

[Bro87] S. A. Broughton, *The homology and higher representations of the automorphism group of a Riemann surface*, Trans. Amer. Math. Soc. **300** (1987), no. 1, 153–158. MR 871669 (88m:30098)

[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** (1934), no. 1, 358–361. MR 3069638

[DaSh94] V. I. Danilov and V. V. Shokurov, *Algebraic geometry. I*, Encyclopaedia of Mathematical Sciences, vol. 23, Springer-Verlag, Berlin, 1994. MR 1287418 (95b:14001)

[DeIl87] Pierre Deligne and Luc Illusie, *Relèvements modulo p^2 et décomposition du complexe de de Rham*, Invent. Math. **89** (1987), no. 2, 247–270. MR 894379 (88j:14029)

[deR31] Georges de Rham, *Sur les périodes des intégrales de première espèce attachées à une variété algébrique*, Comment. Math. Helv. **3** (1931), no. 1, 151–153. MR 1509430

[Ful89] W. Fulton, *Algebraic curves*, Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989, An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original. MR 1042981 (90k:14023)

[Gre74] Leon Greenberg, *Maximal groups and signatures*, Discontinuous groups and Riemann surfaces (Proc. Conf., Univ. Maryland, College Park, Md., 1973), Princeton Univ. Press, Princeton, N.J., 1974, pp. 207–226. Ann. of Math. Studies, No. 79. MR 0379835 (52 #740)

[Gri89] P. A. Griffiths, *Introduction to algebraic curves*, Translations of Mathematical Monographs, vol. 76, American Mathematical Society, Providence, RI, 1989, Translated from the Chinese by Kuniko Weltin. MR 1013999 (90i:14028)

[Gro61] A. Grothendieck, *Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. I*, Inst. Hautes Études Sci. Publ. Math. (1961), no. 11, 167. MR 0217085 (36 #177c)

[Gro66] ______, *On the de Rham cohomology of algebraic varieties*, Inst. Hautes Études Sci. Publ. Math. (1966), no. 29, 95–103. MR 0199194 (33 #7343)

[Har77] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, No. 52, Springer-Verlag, New York, 1977. MR 0463157 (57 #3116)

[Hor12] Ruthi Hortsch, *On the canonical representation of curves in positive characteristic*, New York J. Math. **18** (2012), 911–924. MR 3007205

[IT51] Kenkichi Iwasawa and Tsuneo Tamagawa, *On the group of automorphisms of a function field*, J. Math. Soc. Japan **3** (1951), 137–147. MR 0043832 (13,325b)

[Kan86] E. Kani, *The Galois-module structure of the space of holomorphic differentials of a curve*, J. Reine Angew. Math. **367** (1986), 187–206. MR 839131 (88f:14024)

[KaKo13] S. Karanikolopoulos and A. Kontogeorgis, *Representation of cyclic groups in positive characteristic and Weierstrass semigroups*, J. Number Theory **133** (2013), no. 1, 158–175. MR 2981406

[KöKo12] Bernhard Köck and Aristides Kontogeorgis, *Quadratic differentials and equivariant deformation theory of curves*, Ann. Inst. Fourier (Grenoble) **62** (2012), no. 3, 1015–1043. MR 3013815

[KT14] Bernhard Köck and Joseph Tait, *Faithfulness of actions on Riemann-Roch spaces*, To appear, 2014.

[KY10] Aristides Kontogeorgis and Yifan Yang, *Automorphisms of hyperelliptic modular curves $X_0(N)$ in positive characteristic*, LMS J. Comput. Math. **13** (2010), 144–163. MR 2638986 (2012a:11079)

[Lew63] Joseph Lewittes, *Automorphisms of compact Riemann surfaces*, Amer. J. Math. **85** (1963), 734–752. MR 0160893 (28 #4102)

[Liu02] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications. MR 1917232 (2003g:14001)

[Mir95] Rick Miranda, *Algebraic curves and Riemann surfaces*, Graduate Studies in Mathematics, vol. 5, American Mathematical Society, Providence, RI, 1995. MR 1326604 (96f:14029)

[Nak84] S. Nakajima, *On Galois module structure of the cohomology groups of an algebraic variety*, Invent. Math. **75** (1984), no. 1, 1–8. MR 728135 (85j:14021)

[Nak86] ———, *Action of an automorphism of order p on cohomology groups of an algebraic curve*, J. Pure Appl. Algebra **42** (1986), no. 1, 85–94. MR 852320 (88d:14018)

[Ser79] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg. MR 554237 (82e:12016)

[Ser88] ———, *Algebraic groups and class fields*, Graduate Texts in Mathematics, vol. 117, Springer-Verlag, New York, 1988, Translated from the French. MR 918564 (88i:14041)

[Sti93] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993. MR 1251961 (94k:14016)

[Tat68] John Tate, *Residues of differentials on curves*, Ann. Sci. École Norm. Sup. (4) **1** (1968), 149–159. MR 0227171 (37 #2756)

[VM81] Robert C. Valentini and Manohar L. Madan, *Automorphisms and holomorphic differentials in characteristic p*, J. Number Theory **13** (1981), no. 1, 106–115. MR 602451 (83d:14011)

[Wei94] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR 1269324 (95f:18001)

[Wey52] Hermann Weyl, *Symmetry*, Princeton University Press, Princeton, N. J., 1952. MR 0048449 (14,16a)