UNIVERSITY OF SOUTHAMPTON

FACULTY OF ENGINEERING, SCIENCE AND MATHEMATICS

School of Mathematics

Equivariant Riemann-Roch theorems for curves over perfect fields

by

Helena Beate Fischbacher-Weitz

Thesis for the degree of Doctor of Philosophy

January 2008

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF ENGINEERING, SCIENCE AND MATHEMATICS

SCHOOL OF MATHEMATICS

Doctor of Philosophy

EQUIVARIANT RIEMANN-ROCH THEOREMS FOR CURVES OVER PERFECT FIELDS

by Helena Beate Fischbacher-Weitz

This thesis deals with the equivariant Riemann-Roch problem for curves over perfect fields, and with the related topic of geometric Galois module theory.

We generalize Köck's work on the equivariant Riemann-Roch problem for curves over algebraically closed fields, proving a "weak" equivariant Riemann-Roch formula for arbitrarily ramified Galois covers of curves over perfect fields as well as a "strong" formula for weakly ramified covers.

As an application of our results, we show that under certain conditions, the automorphism group of a geometric Goppa code acts faithfully on the code, meaning that the code has in some sense "maximal symmetry".

In the last part of this thesis, we present an alternative proof for a result of Chinburg in geometric Galois module theory, describing the equivariant Euler characteristic of the structure sheaf of a curve in terms of epsilon constants.

Contents

Annotations to the declaration of authorship

The work presented in this thesis was done wholly during my candidature for the degree of PhD at the University of Southampton, 2004-2007.

Chapters 2 and 3 are essentially my transfer thesis, which was handed in at the University of Southampton in July 2006.

A shortened version of Chapter 2 has been submitted for publication in January 2007, and has also been made available to the public via the preprint archive; for details see reference [FK] in the bibliography.

Parts of Chapter 2 have been incorporated in a thesis submitted for the German *Diplom* degree at the Universität Karlsruhe (TH) in March 2007. More concretely, my diploma thesis (see reference [Fi] in the bibliography) contains Sections 2.2 and 2.3 of this thesis, and a glance at Section 2.3; it presents a weaker version of Theorem 2.4.15, which still contains rational coefficients and only works for the tamely ramified case, and which is proved in a way that is different from the proof method used in this thesis. (See Remark 2.4.18 for details.)

All published sources that I have used are listed in the bibliography and, where applicable, quoted within the text. All other sources of help are acknowledged in the Acknowledgements section.

Acknowledgements

I would like to express my gratitude to all those who have contributed to the successful completion of this thesis.

It is with great pleasure that I express my sincere thanks to my supervisor, Bernhard Köck, for all the time and thought he has invested into supervising my research, for many insightful mathematical discussions, and also for his valuable comments on various drafts of my mathematical writings.

I would also like to thank Bernhard Köck and Manuel Breuning for their help with the proof of Proposition 4.2.3.

My candidature was supported by a grant from the EPSRC doctoral training account and a grant from the School of Mathematics at the University of Southampton, for which I would like to thank both institutions.

Furthermore, I would like to thank the Pure Mathematics group at the University of Southampton for giving me a warm, friendly welcome, and for providing an excellent environment to work in.

In particular, I would like to thank the other PhD students I have been sharing an office with for providing such good company.

Thanks also go to the Arbeitsgruppe Zahlentheorie und Algebraische Geometrie at the Universität Karlsruhe (TH) for their interest in my work, which I have found to be very encouraging. I also thank them for answering various minor questions, in particular on the topics of Chapter 4 of this thesis.

I would like to thank Stephan Wesemeyer and Markus Grassl for interesting and useful conversations about Coding Theory.

Furthermore, I would like to thank Frank Herrlich, Jürgen Wolfart, Rob de Jeu, Dorothy Buck and Holger Brenner for giving me the opportunity to present my work at conferences and external seminars, and for the valuable feedback they have given me on these occasions.

Finally, I would like to thank my family – in particular my husband, my parents and my sister – as well as all my friends, who have given me a great deal of support throughout my candidature for the degree of PhD.

Index of notations and conventions

Different notions of "characters"

For a topological group H (finite or infinite), a *quasi-character* of H is a continuous homomorphism $H \to \mathbb{C}^*$. If it has absolute value 1 (i.e. if its image lies in the unit circle), it is called a *character.*

Let now H be a finite group, endowed with the discrete topology. Then all homomorphisms $H \to \mathbb{C}^*$ are characters in the above sense.

Homomorphisms from H into the multiplicative group of a field other than $\mathbb{C}$ will also be called characters. Care has been taken to avoid confusion with the notion of a *character afforded by a representation of* H, i.e. a map of the form $h \mapsto \mathrm{Trace}(h|V)$, and the notion of a *virtual character,* i.e. a $\mathbb{Z}$-linear combination of these, which we will need in Chapter 4. However, where there is no risk of confusion, we use the word "character" indifferently.

If K is any field, then a *multiplicative character* is a character (continuous homomorphism of absolute value 1) $K^* \to \mathbb{C}^*$ of the multiplicative group of K, and an *additive character* of K is a character $K \to \mathbb{C}^*$ of the additive group of K.

The general setting and frequently used notations

Throughout this thesis, $\pi : X \to Y$ is a cover of nonsingular projective curves such that the corresponding extension of function fields, denoted $K(X)/K(Y)$, is a finite Galois extension. Its Galois group is denoted G.

The table below gives an overview of notations that are frequently used in this thesis. Where applicable, numbers at the end of entries indicate the Chapter, section and subsection in which the definition can be found.

X	a nonsingular, projective algebraic curve over a field
k	the underlying field (perfect in Chapter 2, finite in Chapters 3 and 4)
$\bar{k}$	an algebraic closure of k
$X(\bar{k})$	the set of $\bar{k}$-rational points on X, 2.2.1

G	a finite subgroup of $\mathrm{Aut}(X/k)$
Y	the nonsingular quotient curve X/G
$\lvert X\rvert$, $\lvert Y\rvert$, etc.	the set of closed points in X, in Y, etc.
$\bar{X}$	the geometric fibre $X \times_k \bar{k}$
P, Q, R	a closed point on X, $\bar{X}$, Y respectively
$\tilde{R}$	a point on X lying over $R \in Y$
$L = K(X)$, $K = K(Y)$	function fields of X, Y resp.
v, $\mathfrak{p}$	a valuation, resp. place of $K = K(Y)$
K_v, $K_\mathfrak{p}$	(for a global field K) completion of K with respect to the valuation v, the place $\mathfrak{p}$ resp.
$k[G]$	the group ring over G with coefficients in k
$K_0(G,k)$	the Grothendieck group of all $k[G]$-modules ($k[G]$-modules are always assumed to be finitely generated), 2.2.3
$K_0(k[G])$	the Grothendieck group of projective $k[G]$-modules, 2.2.3
$\mathcal{O}_X$	the structure sheaf on X
$\mathcal{O}_{X,P}$	the stalk of $\mathcal{O}_X$ at P
$\mathfrak{m}_P$	the maximal ideal of $\mathcal{O}_{X,P}$
$k(P)$	the residue field at P
$\mathcal{E}$, $\mathcal{F}$	sheaves of modules on X
$\bar{\mathcal{E}}$, $\bar{\mathcal{F}}$	pullback of $\mathcal{E}$, $\mathcal{F}$ to $\bar{X}$, 2.1.1
$\mathcal{E}(P)$	fibre of $\mathcal{E}$ at P
$G_P = G_{P,-1}$	the decomposition subgroup of G at P, 2.2.2 and 2.3.2
$I_P = G_{P,0}$	the inertia subgroup at P, 2.2.2 and 2.3.2
$G_{P,i}$	the higher ramification groups at P, 2.3.2
n	the order of G
e_P	the ramification index at P; $e_P = \lvert G_{P,0}\rvert$
e_P^t	the tame part of the ramification index; $e_P^t = \lvert G_{P,0}/G_{P,1}\rvert$
e_P^w	the wild part of the ramification index; $e_P^w = \lvert G_{P,1}\rvert$
f_P	the inertia degree at P; $f_P = [k(P) : k(\pi(P))] = (G_P : I_P)$
D	a divisor on X
$\mathcal{L}(D)$	the invertible sheaf associated to D, 2.3.1
$L(D)$	(in Chapter 3) the Riemann-Roch space of a divisor D; $L(D) = H^0(X, \mathcal{L}(D))$
$\mathcal{O}_K$	(for a local field K) the ring of integers in K
$\mathfrak{m}_K$	(for a local field K) the maximal ideal in $\mathcal{O}_K$
$\mathrm{Trace}(-\lvert V)$	(modular) character afforded by V, 4.2.3
G_{reg}	Elements of G whose order is coprime to the characteristic of k, 4.2.3

V^* (for a vector space V) the dual vector space

V^* (for a group representation V) the contragredient (dual representation)

k^* (for a field k) the multiplicative group of k

Chapter 1

Introduction

Like many other areas in Algebraic Geometry, Riemann-Roch theory originally arose from the study of Riemann surfaces.
Given a compact Riemann surface X and a map $D : X \to \mathbb{Z}$ of finite support ("divisor"), one considers the set $L(D)$ of meromorphic functions on X whose pole and zero orders are bounded by the values of D:

$$L(D) := \{f : X \to \hat{\mathbb{C}} \mid f \text{ meromorphic and } \mathrm{ord}_P(f) + D(P) \geq 0 \text{ for all } P \in X\}$$

It turns out that $L(D)$ is always a finite-dimensional vector space over $\mathbb{C}$. Its dimension, denoted $l(D)$, is computed by the **Riemann-Roch Theorem**:

$$l(D) - l(K - D) = \deg D + 1 - g$$

Here, $\deg D := \sum_{P \in X} D(P)$ is the *degree* of D, g is the genus of X and K is a *canonical divisor* of X, a divisor coming from some differential on X.
This is a very deep result that is not easy to prove. One proof of the Riemann-Roch theorem can be given by viewing Riemann surfaces as nonsingular, projective algebraic curves over $\mathbb{C}$ and by using the language of schemes and sheaves. In particular, $L(D)$ can be considered as the 0-th cohomology group of an invertible sheaf on the algebraic curve X:

$$L(D) = H^0(X, \mathcal{L}(D)),$$

where $\mathcal{L}(D)$ is the invertible sheaf associated to D by the 1-1 correspondence between invertible sheaves and divisors (as explained in [Ha], Chapter II.6).

Similarly, we have

$$L(K-D)^* = H^1(X, \mathcal{L}(D)),$$

i.e. $L(K-D)$ is dual (as a vector space over k) to the first cohomology group of $\mathcal{L}(D)$. This follows from Serre duality (cf. Chapter III.7 in [Ha]). Thus the quantity on the left-hand side of the Riemann-Roch theorem is just the *Euler characteristic*

$$\chi(X, \mathcal{L}(D)) := \dim H^0(X, \mathcal{L}(D)) - \dim H^1(X, \mathcal{L}(D)).$$

In the algebro-geometric proof of the Riemann-Roch theorem, the underlying field $\mathbb{C}$ can be replaced with no extra effort by any other algebraically closed field (see for example [Ha], proof of Theorem IV.1.3) or even by an arbitrary *perfect* field. A field is called *perfect* if all of its finite algebraic extensions are separable. This is a large class of fields including all algebraically closed fields, all fields of characteristic zero and all finite fields. Furthermore, the Riemann-Roch theorem can easily be generalized to compute the Euler characteristic of arbitrary locally free sheaves.

In *equivariant* Riemann-Roch theory, we consider the same situation as above, but additionally we fix a finite group G of automorphisms of X and we require the divisor D to be G*-equivariant*, i.e.

$$D(P) = D(\sigma(P)) \quad \text{for all} \quad P \in X, \sigma \in G.$$

(See Definition 2.2.19 for the corresponding definition for sheaves.) In this case, G also acts on the cohomology groups $H^i(X, \mathcal{L}(D))$. The equivariant Riemann-Roch problem consists in describing the isomorphism class of $H^0(X, \mathcal{L}(D))$ as a representation of G over the underlying field k, rather than just its dimension as a vector space. In analogy to the classical Riemann-Roch theorem, we seek to find a formula for the quantity

$$\chi(G, X, \mathcal{L}(D)) := [H^0(X, \mathcal{L}(D))] - [H^1(X, \mathcal{L}(D))]$$

in the *Grothendieck group of finitely generated* $k[G]$*-modules*, denoted $K_0(G,k)$, which consists of equivalence classes of finite dimensional k-representations of G and their formal inverses. More concretely, $K_0(G,k)$ is defined to be the quotient of the free abelian group over all (isomorphism classes of) finitely generated $k[G]$-modules, by the subgroup generated by all expressions $M - M' - M''$, whenever there is an exact sequence

$$0 \to M' \to M \to M'' \to 0$$

of $k[G]$-modules. $\chi(G, X, \mathcal{L}(D))$ is called the *equivariant Euler characteristic* of $\mathcal{L}(D)$.

If two *projective* $k[G]$-modules are in the same class in $K_0(G, k)$, then they are isomorphic. However, this is not true for non-projective $k[G]$-modules, which exist if the characteristic of k divides the order of G. In this case, an equivariant Riemann-Roch formula in $K_0(G, k)$ does not give sufficient information to determine the isomorphism class of $H^0(X, \mathcal{L}(D))$ as a $k[G]$-module. One way to solve this problem is to modify the formula such that both sides can be shown to be integer linear combinations of *projective* $k[G]$-modules, so that one obtains a formula in the Grothendieck group of *projective* $k[G]$-modules, denoted $K_0(k[G])$.

Chapter 2 of this thesis deals with finding equivariant Riemann-Roch formulae both in $K_0(G, k)$ and in $K_0(k[G])$, assuming that the underlying field k is perfect and of arbitrary characteristic.

An interesting special case of the results in Chapter 2 is the case where k is a finite field.

In Chapter 3, we explain how divisors on curves over finite fields give rise to linear codes, the so-called *geometric Goppa codes.* We show that in the setting from Chapter 2, with some additional conditions, the group G acts faithfully on $H^0(X, \mathcal{L}(D))$, and we interpret this fact in the context of geometric Goppa codes.

In Chapter 4, we consider once again the case of a finite underlying field. We use some results from Chapter 2 to give a more elementary proof of Chinburg's description of the equivariant Euler characteristic of the structure sheaf of X, $\chi(G, X, \mathcal{O}_X)$, in terms of *epsilon constants.* These are the constants that appear in the functional equation for Artin L-functions, so they are originally a concept from algebraic number theory. Our proof is based on suggestions made by Erez in the paper [Er].

More background information can be found in the introductory sections of each chapter.

Chapter 2

Two equivariant Riemann-Roch theorems for curves

2.1 Introduction

Let X be a nonsingular, projective, geometrically irreducible algebraic curve over a perfect field k. Let $G \leq \mathrm{Aut}(X/k)$ be a finite group of automorphisms of X over k, and let $\mathcal{E}$ be a G-sheaf on X, i.e. a locally free sheaf that carries a group action of G. This chapter is dedicated to proving a formula for the *equivariant Euler characteristic*

$$\chi(G, X, \mathcal{E}) := [H^0(X, \mathcal{E})] - [H^1(X, \mathcal{E})]$$

both in the Grothendieck group of $k[G]$-modules and in the Grothendieck group of projective $k[G]$-modules.
The problem of computing $\chi(G, X, \mathcal{L}(D))$ is called the *equivariant Riemann-Roch problem* and goes back to Chevalley and Weil [CW], who described the $\mathbb{C}[G]$-module structure of the space of global holomorphic differentials on a compact Riemann surface. Ellingsrud and Lønsted [EL] found a formula for the equivariant Euler characteristic of an arbitrary G-sheaf on a curve over an algebraically closed field of characteristic zero. Nakajima [Na] and Kani [Ka] independently generalized this to curves over arbitrary algebraically closed fields, under the assumption that the canonical morphism $X \to X/G$ be tamely ramified. These results have been revisited by Borne [Bo], who moreover found a formula that even holds for wildly ramified covers $\pi : X \to X/G$ and computes the difference

between the equivariant Euler characteristics of two G-sheaves. In the same setting, formulae for the Euler characteristic of a single G-sheaf have recently been proved by Köck ([Kö1], [Kö2]). Using these formulae, he has also given new proofs for the results of Ellingsrud-Lønsted, Nakajima and Kani. In this thesis, we consider the case where the underlying field k is only assumed perfect rather than algebraically closed.

Our "weak equivariant Riemann-Roch formula", Theorem 2.3.18, describes $\chi(G, X, \mathcal{E})$ in $K_0(G, k)$ in terms of the rank and degree of $\mathcal{E}$, the genus of the quotient curve X/G, and some local data determined by the sheaf $\mathcal{E}$ and by the ramification of the canonical morphism $\pi : X \to X/G$. In the case where the underlying field k is algebraically closed, Theorem 2.3.18 coincides with Theorem 3.1 in [Kö2]. To prove Theorem 2.3.18, we tensor the formula of Theorem 2.3.18 with an algebraic closure $\bar{k}$ over k and obtain a formula in $K_0(G, \bar{k})$. Since tensoring with $\bar{k}$ over k induces an *injective* map

$$K_0(G, k) \hookrightarrow K_0(G, \bar{k}),$$

it suffices to show that this new formula holds true in $K_0(G, \bar{k})$. The new formula describes the Euler characteristic of a locally free sheaf (namely the pullback of $\mathcal{E}$) on the "geometric fibre" $X \times_k \bar{k}$, which is a curve over $\bar{k}$. Hence we can use Köck's result to show that the new formula holds true. Here various "folklore" results from algebraic geometry and representation theory come into play. These are explained in Sections 2.1 and 2.2, where Section 2.1 is focussed on preliminary results that hold in a very general setting.

Section 2.3 is dedicated to showing a "stronger" equivariant Riemann-Roch formula. A finitely generated $k[G]$-module M is projective if and only if $M \otimes_k \bar{k}$ is a projective $\bar{k}[G]$-module. In Subsection 2.3.1, we give variants of this well-known fact for classes in $K_0(G, k)$ rather than for $k[G]$-modules M. These variants, which are much harder to prove, are then used for the proofs in Subsection 2.3.2. The first results in Subsection 2.3.2 give both necessary and sufficient conditions for $\chi(G, X, \mathcal{E})$ to lie in $K_0(k[G])$. In particular, if $\mathcal{E}$ is the invertible sheaf $\mathcal{L}(D)$ associated to some equivariant divisor D, then this holds if the canonical morphism $\pi : X \to X/G$ is weakly ramified and the coefficients of D satisfy a certain congruence relation. Provided that π is weakly ramified, we derive from the corresponding result in [Kö2] the existence of the *ramification module*

$N_{G,X}$, which is defined by the following isomorphism of $k[G]$-modules:

$$\bigoplus^{n} N_{G,X} \cong \bigoplus_{P\in X} \bigoplus_{d=1}^{e_P^t-1} \bigoplus^{e_P^w \cdot d} \mathrm{Ind}_{I_P}^{G}(\mathrm{Cov}((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d})).$$

Here Cov denotes the $k[I_P]$-projective cover and $\mathfrak{m}_P/\mathfrak{m}_P^2$ is the cotangent space at P. If moreover D is an equivariant divisor, then our "strong equivariant Riemann-Roch formula" (Theorem 2.4.15) describes $\chi(G, X, \mathcal{L}(D))$ in $K_0(k[G])$ in terms of $N_{G,X}$, $k[G]$ and the induced representations $\mathrm{Ind}_{G_P}^{G} W_{P,d}$ (for $P \in X, d \geq 0$) where $W_{P,d}$ is a projective $k[G_P]$-module defined by the following isomorphism of $k[G_P]$-modules:

$$\bigoplus^{f_P} W_{P,d} \cong \mathrm{Ind}_{I_P}^{G_P}(\mathrm{Cov}((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes(-d)})),$$

where f_P denotes the inertia degree at P. The existence of $W_{P,d}$ is shown by applying a prototype of Theorem 2.4.15 to suitably chosen divisors D. In the case where π is tamely ramified, we consider two situations where we can give a local proof of this divisibility result. One of these situations includes the important case when k is a finite field. We conclude Chapter 2 with some examples to illustrate what the two Riemann-Roch theorems say in practice.

2.2 Preliminaries

Throughout this section, let X be a scheme of finite type over a field k, and let $\bar{k}$ be an algebraic closure of k. For any (closed) point $P \in X$, let $k(P) := \mathcal{O}_{X,P}/\mathfrak{m}_P$ denote the residue field at P.

2.2.1 Geometric fibre $X \times_k \bar{k}$ and $\bar{k}$-rational points

Proposition 2.2.1. *For any closed point $P \in X$, the extension of fields $k(P)/k$ is finite.*

Proof. If $U = \mathrm{Spec}\, A$ is an affine neighbourhood of P, then A is a finitely generated k-algebra (cf. [Ha], Ex. II.3.3c), say $A = k[x_1, \ldots, x_m]$. As a closed point of $\mathrm{Spec}\, A$, P corresponds to some maximal ideal $\mathfrak{m}$ of A, and we have $k(P) = A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}} = A/\mathfrak{m}$, so the field $k(P)$ is generated as a k-algebra by the classes of $x_1, \ldots, x_m$ modulo $\mathfrak{m}$. By Hilbert's Nullstellensatz, these generators are algebraic over k (cf. Proposition I.3.2 in [Ku1]), which implies that $k(P)/k$ is a finite algebraic extension. □

Definition 2.2.2. We call the fibred product $\bar{X} := X \times_k \bar{k}$ the *geometric fibre* of X. The canonical projection $\bar{X} \to X$ will be denoted p throughout this paper.

Remark 2.2.3. The projection p is flat (because it is obtained by base extension from the flat morphism $\operatorname{Spec} \bar{k} \to \operatorname{Spec} k$). Furthermore, on any affine subset $U = \operatorname{Spec} A$ of X, p is induced by a homomorphism $A \hookrightarrow A \otimes_k \bar{k}$, and since $A \otimes_k \bar{k}$ is an integral extension of A, p is a closed morphism. p is in general not of finite type, but has an "unramifiedness" property, as we will see later. Since the property "being of finite type" is stable under base extension, the geometric fibre is a scheme of finite type over $\bar{k}$.

Notation 2.2.4. We write $|X|$, $|\bar{X}|$ for the set of closed points in X, $\bar{X}$ respectively.

Definition 2.2.5. Let k'/k be an extension of fields. Then the set

$$X(k') := \operatorname{Mor}_k(\operatorname{Spec} k', X)$$

is called the set of k'*-rational points of* X. Similarly, the set

$$\bar{X}(\bar{k}) := \operatorname{Mor}_{\bar{k}}(\operatorname{Spec} \bar{k}, \bar{X})$$

is called the set of $\bar{k}$*-rational points of* $\bar{X}$.

Remark 2.2.6. Giving a morphism from $\operatorname{Spec} k'$ to X over k is equivalent to giving a point $P \in X$ and a k-embedding from $k(P)$ to k' (cf. [Ha], Ex. II.2.7). If k'/k is an algebraic extension of fields, then such an inclusion only exists if P is a closed point. Hence, in this case, we can identify the set of k'-rational points on X with the set

$$\{(P, i_P) | P \in |X|, i_P \in \operatorname{Hom}_k(k(P), k')\}.$$

Similarly, we can identify the set of $\bar{k}$-rational points on $\bar{X}$ with the set

$$\{(Q, i_Q) | Q \in |\bar{X}|, i_Q \in \operatorname{Hom}_{\bar{k}}(k(Q), \bar{k})\}.$$

Lemma 2.2.7. *The map*

$$\bar{X}(\bar{k}) \to |\bar{X}|,\ (Q, i_Q) \mapsto Q$$

is bijective.

Proof. For every point $Q \in |\bar{X}|$, $k(Q)$ is an algebraic extension of $\bar{k}$ (by Proposition 2.2.1) and hence isomorphic to $\bar{k}$. So for every $Q \in |\bar{X}|$, $\mathrm{Hom}_{\bar{k}}(k(Q), \bar{k}) = \mathrm{Hom}_{\bar{k}}(\bar{k}, \bar{k}) = \{\mathrm{id}_{\bar{k}}\}$, which is why every $Q \in |\bar{X}|$ has exactly one pre-image (namely $(Q, \mathrm{id}_{\bar{k}})$). Hence the map is bijective. ☐

Lemma 2.2.8. *We have a canonical bijection*

$$\bar{X}(\bar{k}) \xrightarrow{\sim} X(\bar{k}).$$

Proof. Let $p : \bar{X} \to X$, $p_2 : \bar{X} \to \bar{k}$ be the canonical projections. Every morphism from $\operatorname{Spec}\bar{k}$ to $\bar{X}$ is of the form (f, g) for some $f \in \mathrm{Mor}_k(\operatorname{Spec}\bar{k}, X)$ and some $g \in \mathrm{Mor}_k(\operatorname{Spec}\bar{k}, \operatorname{Spec}\bar{k})$ satisfying $p \circ (f, g) = f$ and $p_2 \circ (f, g) = g$.

$$\begin{tikzcd}
\operatorname{Spec}\bar{k} \arrow[drr, bend left, "g"] \arrow[dr, dotted, "{(f,g)}"] \arrow[ddr, bend right, "f"'] & & \\
& \bar{X} \arrow[r, "p_2"] \arrow[d, "p"'] & \bar{k} \arrow[d] \\
& X \arrow[r] & k
\end{tikzcd}$$

Now if (f, g) is a $\bar{k}$-morphism, then by definition, $p_2 \circ (f, g)$ must be the identity morphism on $\operatorname{Spec}\bar{k}$, i.e. $g = \mathrm{id}_{\operatorname{Spec}\bar{k}}$, and vice versa. Hence we have

$$\bar{X}(\bar{k}) = \{(f, \mathrm{id}) | f \in \mathrm{Mor}_k(\operatorname{Spec}\bar{k}, X)\},$$

i.e. $f \mapsto (f, \mathrm{id})$ defines bijective map $X(\bar{k}) \to \bar{X}(\bar{k})$. ☐

Corollary 2.2.9. *The map*

$$\Phi : X(\bar{k}) \to |\bar{X}|,\ g \mapsto g((0))$$

is bijective.

Proof. The above map is just the composition of the bijections

$$X(\bar{k}) \to \bar{X}(\bar{k}),\ f \mapsto (f, \mathrm{id})$$

and

$$\bar{X}(\bar{k}) \to |\bar{X}|,\ g \mapsto g((0))$$

from Lemma 2.2.8 and Lemma 2.2.7. □

Corollary 2.2.10. *For every $P \in |X|$, there is a bijective map $\mathrm{Hom}_k(k(P), \bar{k}) \to p^{-1}(P)$.*

Proof. From what we have seen so far, we can deduce the following sequence of bijections for any $P \in |X|$:

$$\begin{aligned}\mathrm{Hom}_k(k(P), \bar{k}) &\xrightarrow{\sim} \{(P, i_P) | i_P \in \mathrm{Hom}_k(k(P), \bar{k})\} \underset{2.2.6}{\xrightarrow{\sim}} \{f \in X(\bar{k}) | f((0)) = P\} \\ &\underset{2.2.8}{\xrightarrow{\sim}} \{(f, \mathrm{id}) \in \bar{X}(\bar{k}) | p \circ (f, \mathrm{id})((0)) = P\} = \{(f, \mathrm{id}) \in \bar{X}(\bar{k}) | (f, \mathrm{id})((0)) \in p^{-1}(P)\} \\ &\underset{2.2.6}{\xrightarrow{\sim}} \{(Q, i_Q) | Q \in p^{-1}(P),\ i_Q \in \mathrm{Hom}_{\bar{k}}(k(Q), \bar{k})\} \underset{2.2.7}{\xrightarrow{\sim}} p^{-1}(P).\end{aligned}$$

□

Corollary 2.2.11. *For every point $P \in |X|$, $p^{-1}(P)$ is finite. If the field extension $k(P)/k$ is separable, then $\# p^{-1}(P) = [k(P) : k]$.*

Proof. By Corollary 2.2.10, we have $\#(p^{-1}(P)) = \# \mathrm{Hom}_k(k(P), \bar{k})$. Galois theory yields that $\# \mathrm{Hom}_k(k(P), \bar{k}) \leq [k(P) : k]$, which is finite by Proposition 2.2.1. If $k(P)/k$ is separable, then the above inequality becomes an equality, so $\# p^{-1}(P) = [k(P) : k]$. □

2.2.2 Group actions on the geometric fibre

Let X, $\bar{X}$ be as above and let G be a finite subgroup of $\mathrm{Aut}(X/k)$. By the following lemma, we may view G as a subgroup of $\mathrm{Aut}(\bar{X}/\bar{k})$.

Lemma 2.2.12. *The homomorphism*

$$\mathrm{Aut}(X/k) \to \mathrm{Aut}(\bar{X}/\bar{k}), \sigma \mapsto \sigma \times \mathrm{id}$$

is injective.

Proof. As before, we write p for the canonical projection from $\bar{X}$ to X. Let $\sigma, \sigma' \in \mathrm{Aut}(X/k)$ such that $\sigma \times \mathrm{id} = \sigma' \times \mathrm{id}$, then by the definition of the product morphism, we have $\sigma \circ p = p \circ (\sigma \times \mathrm{id}) = p \circ (\sigma' \times \mathrm{id}) = \sigma' \circ p$. For any affine subset $U = \operatorname{Spec} A$ of X, the pre-image $\bar{U} := p^{-1}(U)$ is just the spectrum of $(A \otimes_k \bar{k})$, which is an integral extension of A. As $p|_{\bar{U}}$ is just the morphism induced by the inclusion $A \hookrightarrow A \otimes_k \bar{k}$, it is an epimorphism; hence, p is an epimorphism also, and thus $\sigma \circ p = \sigma' \circ p$ implies $\sigma = \sigma'$. $\square$

Since the elements of G act on the topological space of X as homeomorphisms, they must map closed points to closed points. Hence, G also acts on $|X|$, the set of closed points in X. A similar argument shows that G acts on the set $|\bar{X}|$ of closed points in $\bar{X}$. G also acts on $X(\bar{k})$, $\sigma \in G$ sending $f \in X(\bar{k})$ to $\sigma \circ f$.

Lemma 2.2.13. *The bijection $\Phi : X(\bar{k}) \to |\bar{X}|$ from Lemma 2.2.9 is compatible with the G-action on the two sets.*

Proof. For all $f \in X(\bar{k})$ and all $\sigma \in G$, we have

$$(\sigma \times \mathrm{id})(\Phi(f)) = (\sigma \times \mathrm{id})((f, \mathrm{id})((0))) = (\sigma \circ f, \mathrm{id})((0)) = \Phi(\sigma \circ f).$$

$$\begin{tikzcd}
\operatorname{Spec} \bar{k} \arrow[dr, dotted, "{(f,\mathrm{id})}"] \arrow[drr, bend left, "id"] \arrow[ddr, "f"'] & & & \\
& \bar{X} \arrow[r] \arrow[d, "p"] \arrow[dr, dotted, "\sigma\times\mathrm{id}"] & \bar{k} \arrow[dr, "id"] & \\
& X \arrow[dr, "\sigma"'] & \bar{X} \arrow[r] \arrow[d, "p"] & \bar{k} \arrow[d] \\
& & X \arrow[r] & k
\end{tikzcd}$$

$\square$

Definition 2.2.14. Let X, G as above, and let $P \in |X|$ or $P \in |\bar{X}|$. We define the *decomposition group* G_P and the *inertia group* I_P as follows:

$$G_P := \{\sigma \in G | \sigma(P) = P\};$$
$$I_P := \{\sigma \in G_P | \bar{\sigma} = \mathrm{id}_{k(P)}\} = \ker(G_P \to \mathrm{Aut}(k(P)/k)).$$

Here $\bar{\sigma}$ denotes the endomorphism that σ induces on $k(P)$.

Lemma 2.2.15. *For all $Q \in |\bar{X}|$, we have $G_Q = I_Q$.*

Proof. For all $Q \in |\bar{X}|$, $k(Q)$ is an algebraic extension of $\bar{k}$ (by Proposition 2.2.1) and hence isomorphic to $\bar{k}$. The Galois group of $\bar{k}/\bar{k}$ is trivial, so we have

$$I_Q = \ker(G_Q \to \mathrm{Gal}(k(Q)/k)) = G_Q.$$

□

Lemma 2.2.16. *For all $Q \in |\bar{X}|$, we have $G_Q = I_P$ where $P = p(Q) \in |X|$.*

Proof. Let $f := \Phi^{-1}(Q)$ be the element of $X(\bar{k})$ corresponding to Q. Let $\sigma \in G$. By definition, $\sigma \in G_Q$ if and only if $\sigma(Q) = Q$, which is equivalent to $\sigma \circ f = f$ by Lemma 2.2.13. According to Remark 2.2.6, this holds if and only if

$$(\sigma \circ f)((0)) = f((0)) \text{ and } \bar{f} \circ \bar{\sigma} = \bar{f}, \tag{2.1}$$

where $\bar{f}, \bar{\sigma}$ denote the induced homomorphism of residue fields. By definition,

$$P = p(Q) = p(\Phi(f)) = p((f, \mathrm{id})((0))) = (p \circ (f, \mathrm{id})((0))) = f((0)),$$

so the first part of (2.1) can be written as $\sigma(P) = P$. Since P is a closed point, the homomorphism of residue fields induced by f is an inclusion $k(P) \hookrightarrow \bar{k}$, so the second part of (2.1) holds if and only if $\bar{\sigma} = \mathrm{id}$. Sticking the two parts together again, we get that (2.1) is equivalent to $\sigma \in I_P$. □

2.2.3 Euler characteristic of sheaves on a scheme and on its geometric fibre

Let G, k, X and $\bar{X}$ be as above. Then we define the *Grothendieck group* of finitely generated $k[G]$-modules (i.e. finite dimensional k-representations of G), denoted $K_0(G, k)$, to be the quotient of the free abelian group over all (isomorphism classes of) finitely generated $k[G]$-modules, by the subgroup generated by all expressions $M - M' - M''$, whenever there is an exact sequence

$$0 \to M' \to M \to M'' \to 0$$

of $k[G]$-modules. In particular, this implies that for any two $k[G]$-modules M, N, we have $[M \oplus N] = [M] + [N]$ in $K_0(G,k)$. One can show that $K_0(G,k)$ is a free abelian group generated by the classes of *simple* $k[G]$-modules ($k[G]$-modules that don't have a proper $k[G]$-submodule).
Later in this thesis, we will also use the Grothendieck group of finitely generated *projective* $k[G]$-modules, denoted $K_0(k[G])$,which is defined by requiring all $k[G]$-modules in the above definition to be *projective*, i.e. direct summands of a free module. $K_0(k[G])$ is a free abelian group generated by the classes of *indecomposable* projective $k[G]$-modules (projective $k[G]$-modules that cannot be written as a direct sum of proper submodules). By mapping the class of a projective $k[G]$-module in $K_0(k[G])$ to the class of that module in $K_0(G,k)$, we obtain a well-defined, injective homomorphism of groups

$$c : K_0(k[G]) \hookrightarrow K_0(G,k)\,,$$

which is called the *Cartan homomorphism*. In particular, $K_0(k[G])$ is isomorphic to the subgroup of $K_0(G,k)$ generated by the classes of projective $k[G]$-modules.
As the equivalence classes in the Grothendieck group are defined via short exact sequences, the exact functor "tensoring with $\bar{k}$ over k" from the category of $k[G]$-modules to the category of $\bar{k}[G]$-modules induces a homomorphism

$$\beta : K_0(G,k) \to K_0(G,\bar{k})$$

of the corresponding Grothendieck groups.

Lemma 2.2.17. *The homomorphism β above is injective.*

Proof. See [Se2], Section 14.6. □

Lemma 2.2.18. *Let $\mathcal{E}$ be a locally free $\mathcal{O}_X$-module. Then for every $i \geq 0$ we have a natural isomorphism*

$$H^i(X,\mathcal{E}) \otimes_k \bar{k} \cong H^i(\bar{X}, p^*\mathcal{E}).$$

Proof. Let $q, \bar{q}$ be the structure morphisms $X \to k$ and $\bar{X} \to \bar{k}$, respectively. By Proposition III.8.5 in [Ha], for every $i \in \mathbb{N}_0$ we have natural isomorphisms

$$H^i(X,\mathcal{E}) \cong \Gamma(\operatorname{Spec} k, R^i q_* \mathcal{E}) \text{ and}$$
$$H^i(\bar{X}, p^*\mathcal{E}) \cong \Gamma(\operatorname{Spec} \bar{k}, R^i \bar{q}_* p^* \mathcal{E}),$$

where $R^i q_*, R^i \bar{q}_*$ are the i-th right derived functors of the direct image functors $q_*, \bar{q}_*$ respectively.

Now consider the following commutative diagram:

$$\begin{tikzcd} \bar{X} \arrow[r, "p"] \arrow[d, "\bar{q}"'] & X \arrow[d, "q"] \\ \bar{k} \arrow[r, "u"'] & k \end{tikzcd}$$

By Proposition III.9.3 in [Ha], for any $i \in \mathbb{N}_0$ we have a natural isomorphism

$$u^* R^i q_*(\mathcal{E}) \cong R^i \bar{q}_*(p^*\mathcal{E}); \text{ hence}$$

$$\begin{aligned} H^i(X, \mathcal{E}) \otimes_k \bar{k} &\cong \Gamma(\operatorname{Spec} k, R^i q_* \mathcal{E}) \otimes_k \bar{k} \cong \Gamma(\operatorname{Spec} \bar{k}, u^* R^i q_* \mathcal{E}) \\ &\cong \Gamma(\operatorname{Spec} \bar{k}, R^i \bar{q}_*(p^*\mathcal{E})) \cong H^i(\bar{X}, p^*\mathcal{E}). \end{aligned}$$

□

Definition 2.2.19. A *locally free G-sheaf* (of rank r) on X is a locally free $\mathcal{O}_X$-module $\mathcal{E}$ (of rank r) together with an isomorphism of $\mathcal{O}_X$-modules $v_\sigma : \sigma^*\mathcal{E} \to \mathcal{E}$ for every $\sigma \in G$, such that for all $\sigma, \tau \in G$, the following diagram commutes:

$$\begin{tikzcd} \sigma^*\mathcal{E} \arrow[r, "v_\sigma"] & \mathcal{E} \\ \sigma^*(\tau^*\mathcal{E}) = (\tau\sigma)^*\mathcal{E} \arrow[u, "\sigma^* v_\tau"] \arrow[ur, "v_{\tau\sigma}"'] & \end{tikzcd}$$

Remark 2.2.20. It is easy to see that if $\mathcal{E}$ is a locally free G-sheaf of finite rank, then the cohomology groups $H^i(X, \mathcal{E})$ ($i \in \mathbb{N}_0$) are k-representations of G. If moreover X is proper over k, then they are finite-dimensional and vanish for $i >> 0$ (see Theorem III.5.2 in [Ha]).

Definition 2.2.21. If X is proper over k, and $\mathcal{E}$ is a locally free G-sheaf of finite rank, then

$$\chi(G, X, \mathcal{E}) := \sum_i (-1)^i [H^i(X, \mathcal{E})] \in K_0(G, k)$$

is called the *equivariant Euler characteristic* of $\mathcal{E}$ on X.

Corollary 2.2.22. *With $X, \mathcal{E}$ as in Definition 2.2.21, we have in $K_0(G, \bar{k})$:*

$$\beta(\chi(G, X, \mathcal{E})) = \chi(G, \bar{X}, p^*\mathcal{E}),$$

where (as before) β denotes the injective homomorphism $K_0(G, k) \hookrightarrow K_0(G, \bar{k})$ defined by tensoring with $\bar{k}$ over k.

Proof. Use Lemma 2.2.18. □

2.2.4 Tensoring fibres

In this section, we compute the tensor products of certain vector spaces with $\bar{k}$. In particular, we show that for any coherent sheaf $\mathcal{F}$ on X, the tensor product of a fibre $\mathcal{F}(P)$ ($P \in |X|$) with $\bar{k}$ is isomorphic to a direct sum of fibres of $p^*\mathcal{F}$. It will turn out that if $\mathcal{F}$ is a locally free G-sheaf, then both sides of this isomorphism admit actions of the inertia group I_P and are isomorphic as I_P-representations.

Lemma 2.2.23. *For any separable finite field extension k'/k, the homomorphism*

$$\phi : k' \otimes_k \bar{k} \to \bigoplus_{\mathrm{Hom}_k(k', \bar{k})} \bar{k}$$

defined by

$$\phi(y \otimes z) := (\varphi(y) \cdot z)_{\varphi \in \mathrm{Hom}_k(k', \bar{k})}$$

is an isomorphism.

Proof. As k'/k is separable, k' is generated by a single element over k, say $k' = k(x_1)$. Let $f(X) \in k[X]$ be the minimal polynomial of x_1 over k. Then we have

$$k' = k(x_1) \cong k[X]/(f) \text{ and hence } k' \otimes_k \bar{k} \cong (k[X]/(f)) \otimes_k \bar{k} = \bar{k}[X]/(f). \tag{2.2}$$

Let $f(X) = (X - x_1) \dots (X - x_l)$ be the decomposition of f into (distinct!) linear factors in $\bar{k}[X]$. Then the Chinese Remainder Theorem yields

$$\bar{k}[X]/(f) \cong \bigoplus_{i=1}^{l} \bar{k}[X]/(X - x_i). \tag{2.3}$$

Now for every $i \in \{1, \dots, l\}$, we have an isomorphism

$$\bar{k}[X]/(X - x_i) \xrightarrow{\sim} \bar{k},\ h(X) \bmod (X - x_i) \mapsto h(x_i) = h(\varphi_i(x_1)) = \varphi_i(h(x_1)), \tag{2.4}$$

where φ_i denotes the element of $\mathrm{Hom}_k(k', \bar{k})$ given by $\varphi_i(x_1) = x_i$.
Let now $y \in k', z \in \bar{k}$, then $y = g(x_1)$ for some $g \in k[X]$, and applying the isomorphisms (2.2) and (2.3) maps $y \otimes z$ to $(g(X) \cdot z \bmod (X - x_i))_{i=1,\dots,l}$. Applying the isomorphism (2.4) to each component, we get

$$(\varphi_i(g(x_1)) \cdot z)_{i=1,\dots,l} = (\varphi_i(y) \cdot z)_{i=1,\dots,l} = \phi(y \otimes z).$$

We have now verified that the homomorphism ϕ is obtained by composing isomorphisms; hence ϕ itself is an isomorphism. □

In the following corollary, we will assume for the first time that the field k is *perfect*, i.e. that all finite algebraic extensions of k are separable.

Corollary 2.2.24. *Assume that k is perfect. Let $P \in |X|$ be a closed point with residue field $k(P)$. Then the canonical homomorphism*

$$k(P) \otimes_k \bar{k} \to \bigoplus_{Q \in p^{-1}(P)} k(Q)$$

given by

$$y \otimes z \mapsto (\bar{p}_Q(y) \cdot z)_{Q \in p^{-1}(P)}$$

is an isomorphism.
Here, $\bar{p}_Q : k(P) \to k(Q)$ denotes the homomorphism of residue fields induced by the morphism p at the point Q.

Proof. The field extension $k(P)/k$ is finite (by Proposition 2.2.1), hence separable (because k is perfect), and the homomorphism above coincides with the homomorphism defined in Lemma 2.2.23 for $k' = k(P)$; hence it is an isomorphism. □

Lemma 2.2.25. *Assume that k is perfect. Let $\mathcal{F}$ be a coherent sheaf on X, and let $\bar{\mathcal{F}} := p^*\mathcal{F}$. Let P be a closed point in X, and let $\mathcal{F}(P) = \mathcal{F}_P \otimes_{\mathcal{O}_{X,P}} k(P)$ be the fibre of $\mathcal{F}$ at P. Then the canonical homomorphism*

$$\mathcal{F}(P) \otimes_k \bar{k} \mapsto \bigoplus_{Q \in p^{-1}(P)} \bar{\mathcal{F}}(Q)$$

is an isomorphism.

Proof. Let $U = \operatorname{Spec} A$ be an affine neighbourhood of P and $\mathfrak{m}$ the maximal ideal associated to P as a closed point of U. Then the pre-image of U under $p : \bar{X} \to X$ is isomorphic to the spectrum of $\bar{A} := A \otimes_k \bar{k}$. By Lemma 2.2.11, P has finitely many pre-images under p. We will denote the corresponding prime ideals of $\bar{A}$ by $\mathfrak{n}_1, \ldots, \mathfrak{n}_l$.
In this notation, we have

$$k(P) = A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}} = A/\mathfrak{m}. \tag{2.5}$$

Analogously, for every $Q \in p^{-1}(P)$ with corresponding prime ideal $\mathfrak{n}_i$, we have

$$k(Q) = \bar{A}/\mathfrak{n}_i. \tag{2.6}$$

Since $\mathcal{F}$ is coherent, $\mathcal{F}|_U$ is the sheaf $\tilde{F}$ on $U = \operatorname{Spec} A$ associated to some A-module F (cf. Proposition II.5.4 in [Ha]), and we have

$$\mathcal{F}(P) = \mathcal{F}_P/\mathfrak{m}_P\mathcal{F}_P = F_{\mathfrak{m}}/\mathfrak{m}F_{\mathfrak{m}} = F \otimes_A A/\mathfrak{m}. \tag{2.7}$$

The restriction of the pullback $\bar{\mathcal{F}} := p^*\mathcal{F}$ to the affine subset $p^{-1}(U) = \operatorname{Spec} \bar{A}$ is the sheaf $(\bar{F})^\sim$ associated to the module $\bar{F} := F \otimes_k \bar{k}$ (by Proposition II.5.2 in [Ha]), and the following analogue of (2.7) holds for $Q \in p^{-1}(P)$ with corresponding prime ideal $\mathfrak{n}_i$:

$$\bar{\mathcal{F}}(Q) = \bar{F} \otimes_{\bar{A}} \bar{A}/\mathfrak{n}_i. \tag{2.8}$$

Hence we have canonical isomorphisms

$$\begin{aligned}
\mathcal{F}(P) \otimes_k \bar{k} &\overset{(2.7)}{=} F \otimes_A A/\mathfrak{m} \otimes_k \bar{k} \\
&= F \otimes_A \Big(\bigoplus_{i=1}^{l} \bar{A}/\mathfrak{n}_i\Big) \quad \text{(by Corollary 2.2.24)} \\
&= F \otimes_k \bar{k} \otimes_{A \otimes_k \bar{k}} \left(\bigoplus_{i=1}^{l} \bar{A}/\mathfrak{n}_i\right) \\
&= \bigoplus_{i=1}^{l} \bar{F} \otimes_{\bar{A}} \bar{A}/\mathfrak{n}_i \overset{(2.8)}{=} \bigoplus_{Q \in p^{-1}(P)} \bar{\mathcal{F}}(Q).
\end{aligned}$$

□

Proposition 2.2.26. *Assume that k is perfect. Let $\Omega_{X/k}$ be the sheaf of relative differentials of X over k. Then for every closed point $P \in |X|$, the canonical map*

$$\mathfrak{m}_P/\mathfrak{m}_P^2 \to \Omega_{X/k}(P)$$

is an isomorphism.

Proof. We use the same "affine" notation as in the proof of Lemma 2.2.25 above, replacing the coherent sheaf $\mathcal{F}$ by $\Omega_{X/k}$. The restriction of $\Omega_{X/k}$ to the affine subset $U = \operatorname{Spec} A$ is just the sheaf associated to the module $\Omega_{A/k}$ of relative differential forms of A over k (cf. Remark II.8.9.2 in [Ha]). Thus Formula (2.7) yields

$$\Omega_{X/k}(P) = \Omega_{A/k} \otimes_A A/\mathfrak{m}.$$

Furthermore, we will use that

$$\mathfrak{m}_P/\mathfrak{m}_P^2 = \mathfrak{m}A_{\mathfrak{m}}/(\mathfrak{m}A_{\mathfrak{m}})^2. \tag{2.9}$$

We now apply a result from [Ku2] taking as input two local rings, denoted R, S respectively, with a ring homomorphism $R \to S$. In our case, we take $R := k$ and $S := \mathcal{O}_{X,P} = A_{\mathfrak{m}}$ with maximal ideals $(0), \mathfrak{m}A_{\mathfrak{m}}$, respectively. Then the corresponding residue fields are k and $k(P)$, respectively. Proposition 2.2.1 and the perfectness of k yield that the field extension $k(P)/k$ is separable, so by Corollary 6.5 in [Ku2], the canonical sequence

$$0 \to \mathfrak{m}/\mathfrak{m}^2 \to \Omega_{A_{\mathfrak{m}}/k} \otimes_{A_{\mathfrak{m}}} A/\mathfrak{m} \to \Omega_{k(P)/k} \to 0$$

is exact. By Corollary 5.3 in [Ku2], $\Omega_{k(P)/k}$ is trivial, so the second arrow in the above sequence is an isomorphism. We have $\Omega_{A_{\mathfrak{m}}/k} = (\Omega_{A/k})_{\mathfrak{m}}$, so the object in the middle is equal to $\Omega_{A/k} \otimes_A A/\mathfrak{m} = \Omega_{X/k}(P)$, which proves our assertion. □

Corollary 2.2.27. *Let k be perfect. Let $\mathcal{F}$ be a coherent sheaf on X, $\bar{\mathcal{F}} := p^*\mathcal{F}$. For every $P \in |X|$ and every $d \in \mathbb{N}$, the canonical homomorphism*

$$\left(\mathcal{F}(P) \otimes_{k(P)} (\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}\right) \otimes_k \bar{k} \to \bigoplus_{Q \in p^{-1}(P)} \bar{\mathcal{F}}(Q) \otimes_{k(Q)} (\mathfrak{m}_Q/\mathfrak{m}_Q^2)^{\otimes d}$$

is an isomorphism.

Proof. By Proposition 2.2.26, the expression $\mathcal{F}(P) \otimes_{k(P)} (\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}$ on the left is just the fibre of the coherent sheaf $\mathcal{F} \otimes_{\mathcal{O}_X} \Omega_{X/k}^{\otimes d}$ on X at P. Analogously, for every $Q \in p^{-1}(P)$, the expression $\bar{\mathcal{F}}(Q) \otimes_{\bar{k}} (\mathfrak{m}_Q/\mathfrak{m}_Q^2)^{\otimes d}$ is the fibre of $\bar{\mathcal{F}} \otimes_{\mathcal{O}_{\bar{X}}} \Omega_{\bar{X}/\bar{k}}^{\otimes d} = p^*(\mathcal{F} \otimes_{\mathcal{O}_X} \Omega_{X/k}^{\otimes d})$ at Q. Applying Lemma 2.2.25 to $\mathcal{F} \otimes_{\mathcal{O}_X} \Omega_{X/k}^{\otimes d}$ completes our proof. □

In Lemma 2.2.25 and Corollary 2.2.27, we have made relatively weak assumptions on the sheaf $\mathcal{F}$. If we require $\mathcal{F}$ to be a locally free G-sheaf, then for every point $P \in |X|$, this additional structure yields an action of the inertia group I_P on the fibre $\mathcal{F}(P)$ by $k(P)$-automorphisms. For example, the action of I_P on the fibre $\Omega_X(P)$ of the sheaf of differentials corresponds to the natural action on the cotangent space $\mathfrak{m}_P/\mathfrak{m}_P^2$ via the isomorphism from Lemma 2.2.26.

By letting I_P act trivially on $\bar{k}$, we can extend this action to an action on the tensor product $\mathcal{F}(P) \otimes_k \bar{k}$. On the other hand, since $I_Q = I_P$ for any point $Q \in p^{-1}(P)$ by Lemma 2.2.16 and Lemma 2.2.15, I_P acts on the fibre $\mathcal{G}(Q)$ of any locally free G-sheaf $\mathcal{G}$ on $\bar{X}$ for any point $Q \in p^{-1}(P)$. In particular, this holds if $\mathcal{G} = p^*\mathcal{F}$ for a locally free G-sheaf $\mathcal{F}$ on X. Hence we have an I_P-action on both sides of the isomorphisms shown in Lemma 2.2.25 and Corollary 2.2.27, and it is easy to check that the following holds:

Lemma 2.2.28. *The isomorphisms shown in Lemma 2.2.25 and Corollary 2.2.27 respect the group action, i.e. they are isomorphisms of* $\bar{k}[I_P]$*-modules.*

Remark 2.2.29. We also have an action of the decomposition group G_P on any fibre $\mathcal{F}(P)$, but G_P only acts on the fibre via k-automorphisms, whereas I_P acts via $k(P)$-automorphisms.

2.3 An equivariant Riemann-Roch formula

We will now make more assumptions on X than in the previous section.

Let X be a smooth, projective curve over a perfect field k. Assume that X is geometrically irreducible, i.e. that the geometric fibre $X \times_k \bar{k}$ is irreducible. Then the curve X itself is irreducible. Indeed, if X could be written as the union of two proper closed subsets, say $X = U \cup V$, then the geometric fibre $\bar{X}$ would be the union of the two proper closed subsets $U \times_k \bar{k}$ and $V \times_k \bar{k}$.

Let G be a finite subgroup of $\mathrm{Aut}(X/k)$, of order n. It is a well-known result that the quotient scheme $Y := X/G$ is also a smooth projective curve, with function field $K(Y) = K(X)^G$.
Note that we do not make any assumptions on the ramification of the cover $\pi : X \to Y$ in this section.

For every closed point $P \in X$, let $G_P := \{\sigma \in G \mid \sigma(P) = P\}$, $I_P := \ker(G_P \to \mathrm{Gal}(k(P)/k))$ as in Section 2.2.2. Let $\chi_P : I_P \to k(P)^*$ be the group homomorphism defined by the action of I_P on the cotangent space $\mathfrak{m}_P/\mathfrak{m}_P^2$.

2.3.1 Invariance of the degree of a locally free sheaf under pullback

Since X is integral and smooth over k, we have isomorphisms between the divisor class group $\mathrm{CH}_0(X)$, the Cartier class group $\mathrm{CaCl}\, X$ and the Picard group $\mathrm{Pic}\, X$ of X. Namely, we have the following 1-1 correspondences giving rise to these isomorphisms (see also [Ha], Section II.6):

- Let $D = \sum_{P \in X} n_P \cdot P$ be a Weil divisor on X. Then D corresponds to the Cartier divisor given by $\{(U_P, f_P)\}_{P \in |X|}$, where $\{U_P\}$ is an open cover of X and the f_P are elements of $K(X)^*$, such that for every $P \in \mathrm{Supp}\, D$ we have $\mathrm{Supp}\, D \cap U_P = \{P\}$ and for every $P \in X$ we have $v_P(f_P) = n_P$.

- Let a Cartier divisor D on X be given by $\{(U_i, f_i)\}$, where $\{U_i\}$ is an open cover of X and $f_i \in K(X)^*$ for every i. Then the invertible sheaf $\mathcal{L}(D)$ corresponding to D is the $\mathcal{O}_X$-module generated by f_i^{-1} on U_i, i.e. we have $\mathcal{L}(D)|_{U_i} = f_i^{-1}\mathcal{O}_X|_{U_i}$.

Definition 2.3.1. Let $D = \sum_{P \in |X|} n_P P$ be a Weil divisor on X. Then we define the *degree of* D to be

$$\deg D := \sum_{P \in X} n_P \cdot [k(P) : k].$$

The *degree of an invertible sheaf* $\mathcal{L}$ on X is defined to be the degree of the Weil divisor mapped to $\mathcal{L}$ under the above 1-1 correspondences.

The *degree of a locally free sheaf* $\mathcal{F}$ of rank r on X is defined to be the degree of the invertible sheaf $\bigwedge^r \mathcal{F}$, where $\bigwedge^r$ denotes the r-th exterior power (see Exercise II.5.16 and Exercise II.6.11 in [Ha]).

We apply the same definitions to Weil divisors, invertible sheaves and locally free sheaves on the geometric fibre $\bar{X}$, in the obvious way.

With this definition, linearly equivalent divisors have the same degree (see remark after Definition 1.4 in [Fu]), so the notion of degree is well-defined on the "class groups" $\mathrm{CH}_0(X)$, $\mathrm{CaCl}\,X$ and $\mathrm{Pic}\,X$.

Definition 2.3.2. We define the *pullback* of a Weil divisor on X via p by setting

$$p^*P := \sum_{Q \in p^{-1}(P)} v_Q(t_P) \cdot Q$$

for any closed point (prime divisor) $P \in |X|$, where t_P is a local parameter at P and v_Q is the valuation of the local ring $\mathcal{O}_{\bar{X},Q}$, and by extending linearly.

Remark 2.3.3. In the rare cases where p is a finite morphism, our definition coincides with the one in [Ha], Section IV.2. Furthermore, it is easy to see that our definition coincides with the one in [Fu], where the pullback of a prime divisor P is defined to be the 0-cycle associated to the inverse image scheme $p^{-1}(P)$, i.e. the divisor $\sum_{Q \in p^{-1}(P)} \mathrm{length}\, \mathcal{O}_{p^{-1}(P),Q} \cdot Q$. Hence, Theorem 1.7 in [Fu] yields that the pullback gives rise to a well-defined homomorphism

$$p^* : \mathrm{CH}_0(X) \to \mathrm{CH}_0(\bar{X})$$

between the divisor class groups.

Definition 2.3.4. Let a Cartier divisor D on X be given by $\{(U_i, f_i)\}$, where $\{U_i\}$ is an open cover of X and $f_i \in K(X)^*$ for all i. Then we define the *pullback* of D via p to be the Cartier divisor on $\bar{X}$ given by $\{(p^{-1}(U_i), f_i)\}$, where the f_i are considered as elements of $K(\bar{X})$ via the inclusion of function fields $K(X) \hookrightarrow K(\bar{X})$ induced by p.

Remark 2.3.5. D is a principal Cartier divisor if and only if all the f_i are equal. Thus, the pullback of a principal Cartier divisor is again a principal Cartier divisor, so the pullback gives rise to a well-defined homomorphism

$$p^* : \mathrm{CaCl}\,X \to \mathrm{CaCl}\,\bar{X}$$

between the Cartier class groups.

Finally, we have the well-known notion of pullback of invertible sheaves: For an invertible sheaf $\mathcal{L}$ on X, we put

$$p^*\mathcal{L} := p^{-1}\mathcal{L} \otimes_{p^{-1}\mathcal{O}_X} \mathcal{O}_{\bar{X}}.$$

This gives rise to a homomorphism

$$p^* : \operatorname{Pic} X \to \operatorname{Pic} \bar{X}$$

between the Picard groups.

Lemma 2.3.6. *The notions of pullback for the divisor class group, the Cartier class group and the Picard group are compatible with the isomorphisms between these groups; i.e. both squares in the following diagram commute, where the horizontal arrows are the isomorphisms described at the beginning of Subsection 2.3.1.*

$$\begin{tikzcd}
\mathrm{CH}_0(\bar{X}) \arrow[r, "\sim"] & \mathrm{CaCl}\,\bar{X} \arrow[r, "\sim"] & \operatorname{Pic} \bar{X} \\
\mathrm{CH}_0(X) \arrow[r, "\sim"] \arrow[u, "p^*"] & \mathrm{CaCl}\,X \arrow[r, "\sim"] \arrow[u, "p^*"] & \operatorname{Pic} X \arrow[u, "p^*"]
\end{tikzcd}$$

Proof. Straightforward. □

The following lemma reveals that although p is usually not of finite type, it can be thought of as an "unramified" morphism in the common sense.

Lemma 2.3.7. *Let $Q \in |\bar{X}|$ be a closed point, and let $P := p(Q)$. Then, with the notations from Definition 2.3.2, we have*

$$v_Q(t_P) = 1.$$

Proof. The local parameter t_P must be an element of $\mathfrak{m}_P \setminus \mathfrak{m}_P^2$, so (the equivalence class of) t_P is a generator of the one-dimensional vector space $\mathfrak{m}_P/\mathfrak{m}_P^2$ over $k(P)$. Hence, $t_P \otimes 1$ is a generator of the rank-1-module $\mathfrak{m}_P/\mathfrak{m}_P^2 \otimes_k \bar{k}$ over $k(P) \otimes_k \bar{k}$.
By Lemma 2.2.24, we have $k(P) \otimes_k \bar{k} \cong \bigoplus_{Q \in p^{-1}(P)} k(Q)$, so $\mathfrak{m}_P/\mathfrak{m}_P^2 \otimes_k \bar{k}$ is also a module of rank 1 over $\bigoplus_{Q \in p^{-1}(P)} k(Q)$ generated by $t_P \otimes 1$. By Corollary 2.2.27, we have a canonical isomorphism

$$\mathfrak{m}_P/\mathfrak{m}_P^2 \otimes_k \bar{k} \to \bigoplus_{Q \in p^{-1}(P)} \mathfrak{m}_Q/\mathfrak{m}_Q^2$$

which we can view as an isomorphism of modules over $k(P) \otimes_k \bar{k} \cong \bigoplus_{Q \in p^{-1}(P)} k(Q)$. Since this isomorphism must map $t_P \otimes 1$ to a generator of the right-hand side over $\bigoplus_{Q \in p^{-1}(P)} k(Q)$, the image of $t_P \otimes 1$ in each component $\mathfrak{m}_Q/\mathfrak{m}_Q^2$ must be a generator of $\mathfrak{m}_Q/\mathfrak{m}_Q^2$, i.e. the image of t_P under each induced homomorphism $p_Q : \mathcal{O}_{X,P} \to \mathcal{O}_{\bar{X},Q}$ must be a local parameter at Q. Thus, $e'_Q = v_Q(t_P) = 1$ for all $Q \in p^{-1}(P)$. □

Proposition 2.3.8 (Invariance of the degree under pullback). *Let $\mathcal{E}$ be a locally free G-sheaf on X. Then we have*

$$\deg \mathcal{E} = \deg(p^*\mathcal{E}).$$

Proof. Since the functor p^* on locally free $\mathcal{O}_X$-modules commutes with exterior powers, we may assume that $\mathcal{E}$ is an invertible sheaf.
Let $D = \sum_{P \in |X|} n_P \cdot P$ be the Weil divisor corresponding to $\mathcal{E}$, then by Lemma 2.3.6, the Weil divisor corresponding to $p^*\mathcal{E}$ is p^*D, which is just $\sum_{Q \in |\bar{X}|} n_{p(Q)} \cdot Q$ by Lemma 2.3.7. Hence we have

$$\begin{aligned}
\deg(p^*\mathcal{E}) = \deg(p^*D) &= \sum_{Q \in |\bar{X}|} [k(Q) : \bar{k}] \cdot n_{p(Q)} \quad \text{by definition} \\
&= \sum_{Q \in |\bar{X}|} n_{p(Q)} \quad \text{since } k(Q) = \bar{k} \quad \text{for all } Q \in \bar{X} \\
&= \sum_{P \in |X|} \# p^{-1}(P) \cdot n_P = \sum_{P \in |X|} [k(P) : k] \cdot n_P \quad \text{by Corollary 2.2.10} \\
&= \deg D = \deg \mathcal{E}.
\end{aligned}$$

□

2.3.2 Higher ramification groups

We recall the definition of the higher ramification groups (see for example [Ne], Definition 10.1 in Chapter II):

Definition 2.3.9. Let L/K be a finite Galois extension of local fields, and let v_K be a normed discrete valuation of K such that the residue field has characteristic $p > 0$. Suppose that there is a *unique* valuation w on L that extends v_K, and denote the corresponding normed valuation of L by v_L.

Let $\mathcal{O}$ denote the ring of integers in L. For every $s \geq -1$, we define the *s-th ramifcation group* of the extension L/K to be

$$G_s(L/K) := \{\sigma \in \mathrm{Gal}(L/K) | v_L(\sigma(a) - a) \geq s + 1 \text{ for all } a \in \mathcal{O}\}.$$

Definition 2.3.10. Let $P \in X$ be a closed point, $R := \pi(P) \in Y$, where $\pi : X \to Y = X/G$ is the canonical projection. Let v_P be the unique normed valuation of the function field $K(X)$ associated to P, and let v_R be the unique normed valuation of $K(Y)$ associated to R. Then v_P is equivalent to a valuation extending v_R. Let $K(X)_{v_P}$ be the completion of $K(X)$ with respect to v_P, and let $K(Y)_{v_R}$ be the completion of $K(Y)$ with respect to v_R. For $s \geq -1$, we define the *s-th ramification group* $G_{P,s}$ *at* P to be the s-th ramification group of the extension of local fields $K(X)_{v_P}/K(Y)_{v_R}$.
The canonical projection $\pi : X \to Y$ is called *unramified (tamely ramified, weakly ramified)* if $G_{P,s}$ is trivial for $s \geq 0$ $(s \geq 1, s \geq 2)$ and for all $P \in X$.

Lemma 2.3.11. *For any* $P \in X$, *we have* $G_{P,-1} = G_P$ *and* $G_{P,0} = I_P$.

Proof. Follows directly from Theorem 9.6 and Theorem 9.9 in Chapter II of [Ne]. □

Remark 2.3.12. The obvious analogue of Definition 2.3.10 is used for points on $\bar{X}$, and the analogue of Lemma 2.3.11 clearly holds for these points as well.

Notation 2.3.13. We denote the ramification index of $\pi : X \to Y$ at the place P by e_P, its wild part by e_P^w and its tame part by e_P^t. In other words, if t_R is a local parameter at $R := \pi(P)$, then we have $e_P = v_P(t_R) = |G_{P,0}|$, $e_P^w = |G_{P,1}|$ and $e_P^t = |G_{P,0}/G_{P,1}|$.

Proposition 2.3.14. *For any point* $P \in |X|$, *the character* $\chi_P : G_{P,0} \to k(P)^*$ *afforded by the action of* $G_{P,0}$ *on the cotangent space* $\mathfrak{m}_P/\mathfrak{m}_P^2$ *factors through* $G_{P,1}$, *inducing an injective homomorphism* $\bar{\chi}_P : G_{P,0}/G_{P,1} \to k(P)^*$. *The character group* $\mathrm{Hom}(G_{P,0}/G_{P,1}, k(P)^*)$ *is cyclic of order* e_P^t *and is generated by* $\bar{\chi}_P$.

Proof. Let t_P be a local parameter at P. Let $\bar{t}_P$ denote the class of t_P in $\mathfrak{m}_P/\mathfrak{m}_P^2$. Then a defining equation for the character $\chi_P : G_{P,0} \to k(P)^*$ is given by

$$\sigma(\bar{t}_P) = \chi_P(\sigma) \cdot \bar{t}_P \text{ in } \mathfrak{m}_P/\mathfrak{m}_P^2 \text{ for all } \sigma \in G_{P,0}.$$

Since completion of the field extension with respect to the valuation v_P changes neither the inertia group nor the residue field, we can apply Proposition 7 in Chapter IV in [Sel], which implies that χ_P factors through G_1, inducing an injective homomorphism

$$\bar{\chi}_P : G_0/G_1 \to k(P)^*.$$

Corollary 1 of Proposition 7 in Chapter IV in [Sel] implies that $G_{P,0}/G_{P,1}$ is cyclic.
Let ρ be a generator of $G_{P,0}/G_{P,1}$, i an integer. Then we have $\chi_P^i(\rho) = \chi_P(\rho^i) = 1$ if and only if $\rho^i = \mathrm{id}$, i.e. if and only if i is a multiple of e_P^t. Hence χ_P has order e_P^t in $\mathrm{Hom}(G_{P,0}/G_{P,1}, k(P)^*)$, i.e. it generates a cyclic subgroup of order e_P^t. But as every element of $\mathrm{Hom}(I_P, k(P)^*)$ is determined by the image of ρ, which has to be an e_P^t-th root of unity in $k(P)$, $\mathrm{Hom}(G_{P,0}/G_{P,1}, k(P)^*)$ has at most e_P^t elements. Hence χ_P generates the whole character group. □

Remark 2.3.15. For $d = 0, \ldots, e_P - 1$, the action of I_P on $(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}$ is given by the character χ_P^d.

The following proposition shows that the higher ramification groups at a point on the geometric fibre of X are just the same as at its image under the projection $p : \bar{X} \to X$.

Proposition 2.3.16. *Let $Q \in \bar{X}$ be a closed point, $P := p(Q) \in X$. Then for every $s \geq 0$, we have $G_{Q,s} = G_{P,s}$.*

Proof. Lemma 2.3.11, Lemma 2.2.15 and Lemma 2.2.16 yield that

$$G_{Q,0} = I_Q = I_P = G_{P,0}.$$

Now Proposition 5 in Chapter IV in [Sel] yields that an element σ of $G_{Q,0}$ belongs to $G_{Q,s}$ (with $s \geq 0$) if and only if

$$\frac{\sigma(t_Q)}{t_Q} \equiv 1 \mod \mathfrak{m}_Q^s \tag{2.10}$$

for some local parameter t_Q at Q. (This result is only formulated for complete fields, but completing does not change the valuation of elements.) Let t_P be a local parameter at P, and let $p^\#$ denote the homomorphism of local rings from $\mathcal{O}_{X,P}$ to $\mathcal{O}_{\bar{X},Q}$ induced by p. Then by Lemma 2.3.7,

$p^{\#}(t_P)$ is a local parameter at Q, i.e. we can replace t_Q by $p^{\#}(t_P)$ in the condition (2.10).
Furthermore, since the morphism of sheaves $p^{\#}$ commutes with σ, we have

$$\frac{\sigma(t_Q)}{t_Q} = \frac{\sigma(p^{\#}t_P)}{p^{\#}t_P} = p^{\#}(\frac{\sigma(t_P)}{t_P}),$$

so the condition (2.10) is equivalent to

$$\frac{\sigma(t_P)}{t_P} \equiv 1 \mod (p^{\#})^{-1}(\mathfrak{m}_Q^s) = \mathfrak{m}_P^s.$$

Using the fact that σ is an element of $G_{P,0} = G_{Q,0}$ and applying Proposition 5 in Chapter IV in [Se1] again, we see that this condition holds if and only if σ is an element of $G_{P,s}$, which proves our assertion. □

Corollary 2.3.17. *If $Q \in \tilde{X}$ is a closed point and $P = p(Q) \in X$, then we have $e_P = e_Q$, $e_P^w = e_Q^w$ and $e_P^t = e_Q^t$.*

2.3.3 A formula for the equivariant Euler characteristic

We keep the assumptions and notations stated at the beginning of Section 2.3: Let X be a smooth, projective, geometrically irreducible curve over a perfect field k, and let $G \leq \mathrm{Aut}(X/k)$ be finite, of order n. Let π denote the projection $X \to Y = X/G$. Let $\mathcal{E}$ be a locally free G-sheaf of finite rank r on X. Then the equivariant Euler characteristic of $\mathcal{E}$ on X (cf. Definition 2.2.21) is

$$\chi(G, X, \mathcal{E}) = [H^0(X, \mathcal{E})] - [H^1(X, \mathcal{E})] \in K_0(G, k).$$

We denote the genus of X and the genus of Y by g_X and g_Y, respectively.

Theorem 2.3.18 ("Weak" equivariant Riemann-Roch formula). *We have in $K_0(G, k)$:*

$$n \cdot \chi(G, X, \mathcal{E}) = C_{G,X,\mathcal{E}} \cdot [k[G]] - \sum_{P \in |X|} e_P^w \sum_{d=0}^{e_P^t - 1} d[\mathrm{Ind}_{I_P}^G(\mathcal{E}(P) \otimes_{k(P)} (\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d})], \tag{2.11}$$

where

$$C_{G,X,\mathcal{E}} = n(1-g_Y)r + \deg\mathcal{E} - \frac{r}{2}\sum_{P\in X}[k(P):k]\left((e_P^w - 1)(e_P^t + 1) + \sum_{s\geq 2}(|G_{P,s}| - 1)\right).$$

Remark 2.3.19. The constant $C_{G,X,\mathcal{E}}$ can be written in a simpler way as follows:

$$C_{G,X,\mathcal{E}} = r(1-g_X) + \deg\mathcal{E} + \frac{r}{2}\sum_{P\in|X|}[k(P):k](e_P^t - 1).$$

Proof of Remark 2.3.19. By Theorem 3.13 in [Ne] (Riemann-Hurwitz formula for function fields) we have

$$1 - g_X = n(1-g_Y) + \frac{1}{2}\deg\mathfrak{C}_{K(X)/K(Y)}, \tag{2.12}$$

where $\mathfrak{C}_{K(X)/K(Y)}$ is the codifferent of $K(X)/K(Y)$ and the *degree* of a complete fractional ideal $\mathfrak{a} = \prod_{\mathfrak{p}}\mathfrak{p}^{v_{\mathfrak{p}}}$ of $K(X)$ is defined as the degree of the divisor $\sum_{\mathfrak{p}} v_{\mathfrak{p}}\cdot\mathfrak{p}$, i.e.

$$\deg(\mathfrak{a}) := \sum_{\mathfrak{p}} v_{\mathfrak{p}}\deg(\mathfrak{p}).$$

(Here the index variable $\mathfrak{p}$ runs through the places of $K(X)$, and $\deg\mathfrak{p}$ is the degree of the residue field at $\mathfrak{p}$ over k.)
Let $\mathfrak{D}_{K(X)/K(Y)} := (\mathfrak{C}_{K(X)/K(Y)})^{-1}$ denote the different, then by Corollary 2.3 in Chapter III in [Ne], we have $\mathfrak{D}_{K(X)/K(Y)} = \prod_{P\in X}\mathfrak{D}_{K(X)_{v_P}/K(Y)_{v_{\pi(P)}}}$. Hence Proposition 4 in Chapter IV in [Se1] yields

$$\deg\mathfrak{C}_{K(X)/K(Y)} = -\deg\mathfrak{D}_{K(X)/K(Y)} = -\sum_{P\in|X|}[k(P):k]\deg\mathfrak{D}_{K(X)_{v_P}/K(Y)_{v_{\pi(P)}}}$$
$$= -\sum_{P\in|X|}[k(P):k]v_P(\mathfrak{D}_{K(X)_{v_P}/K(Y)_{v_{\pi(P)}}}) = \sum_{P\in|X|}[k(P):k]\sum_{s\geq 0}(|G_{P,s}| - 1),$$

so formula (2.12) can be re-written as

$$1 - g_X = n(1-g_Y) - \frac{1}{2}\sum_{P\in|X|}\sum_{s\geq 0}(|G_{P,s}| - 1).$$

Hence we have

$$\begin{aligned} C_{G,X,\mathcal{E}} = r(1 - g_X + \frac{1}{2}\sum_{P\in|X|}[k(P):k]\sum_{s=0}^{1}(|G_{P,s}|-1)) + \deg\mathcal{E} \\ - \frac{r}{2}\sum_{P\in|}[k(P):k](e_P^w - 1)(e_P^t + 1) \end{aligned}$$

and hence

$$\begin{aligned} C_{G,X,\mathcal{E}} &= r(1-g_X) + \frac{r}{2}\sum_{P\in|X|}[k(P):k](e_P - 1 + e_P^w - 1) + \deg\mathcal{E} \\ &\quad - \frac{r}{2}\sum_{P\in|}[k(P):k](e_P^w e_P^t + e_P^w - e_P^t - 1)) \\ &= r(1-g_X) + \deg\mathcal{E} + \frac{r}{2}\sum_{P\in|X|}[k(P):k](e_P^t - 1). \end{aligned}$$

□

Proof of Theorem 2.3.18. In the case where the underlying field k is algebraically closed, Theorem 2.3.18 has been shown by Köck (Theorem 3.1 in [Kö2]). We have seen (Corollary 2.2.22) that the injective homomorphism $\beta : K_0(G,k) \to K_0(G,\bar{k})$ maps the Euler characteristic of a locally free G-module $\mathcal{E}$ on X to the Euler characteristic of $\bar{\mathcal{E}} = p^*\mathcal{E}$ on the geometric fibre $\bar{X}$. We know from Köck's result that Formula (2.11) holds on $\bar{X}$, so it suffices to show that β maps the right-hand-side of (2.11) (applied to X, $\mathcal{E}$) to the right-hand-side of (2.11) (applied to $\bar{X}$, $\bar{\mathcal{E}}$).

By Lemma 2.2.28, we have for every $P \in |X|$ and every $d \in \{1, \dots e_P\}$:

$$(\mathcal{E}(P) \otimes_{k(P)} (\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}) \otimes_k \bar{k} \cong \bigoplus_{Q\in p^{-1}(P)} \bar{\mathcal{E}}(Q) \otimes_{k(Q)} (\mathfrak{m}_Q/\mathfrak{m}_Q^2)^{\otimes d}$$

as $\bar{k}[I_P]$-modules, where $\bar{\mathcal{E}} := p^*\mathcal{E}$. Since $G_Q = I_P$ (by Lemma 2.2.16) and $k(Q) = \bar{k}$ (by Proposition 2.2.1) for every $Q \in p^{-1}(P)$, and since induction of representations commutes with direct sums, this implies

$$\beta\left([\mathrm{Ind}_{I_P}^G(\mathcal{E}(P) \otimes_{k(P)} (\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d})]\right) = \sum_{Q\in p^{-1}(P)} [\mathrm{Ind}_{G_Q}^G(\bar{\mathcal{E}}(Q) \otimes_{\bar{k}} (\mathfrak{m}_Q/\mathfrak{m}_Q^2)^{\otimes d})] \tag{2.13}$$

in $K_0(G,\bar{k})$. For any $Q \in p^{-1}(P)$, we have $e^t_P = e^t_Q$, $e^w_P = e^w_Q$ and $e_P = e_Q$ by Corollary 2.3.17. Hence we have

$$\beta\left(\sum_{P\in|X|} e^w_P \sum_{d=0}^{e^t_P-1} d\left[\mathrm{Ind}^G_{I_P}\left(\mathcal{E}(P)\otimes_{k(P)}(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}\right)\right]\right)$$

$$= \sum_{P\in|X|} e^w_P \sum_{d=0}^{e^t_P-1} d \sum_{Q\in p^{-1}(P)} \left[\mathrm{Ind}^G_{G_Q}\left(\bar{\mathcal{E}}(Q)\otimes_{\bar{k}}(\mathfrak{m}_Q/\mathfrak{m}_Q^2)^{\otimes d}\right)\right]$$

$$= \sum_{Q\in|\bar{X}|} e^w_Q \sum_{d=0}^{e^t_Q-1} d\left[\mathrm{Ind}^G_{G_Q},\left(\bar{\mathcal{E}}(Q)\otimes_{\bar{k}}(\mathfrak{m}_Q/\mathfrak{m}_Q^2)^{\otimes d}\right)\right].$$

We are now going to show that $C_{G,X,\mathcal{E}} = C_{G,\bar{X},\bar{\mathcal{E}}}$, i.e. that

$$n(1-g_Y)r + \deg\mathcal{E} - \frac{r}{2}\sum_{P\in X}[k(P):k]\ \left(\ (e^w_P-1)(e^t_P+1) + \sum_{s\geq 2}(|G_{P,s}|-1)\ \right)$$

$$= n(1-g_{\bar{Y}})\bar{r} + \deg\bar{\mathcal{E}} - \frac{\bar{r}}{2}\sum_{Q\in\bar{X}}\ \left(\ (e^w_Q-1)(e^t_Q+1) + \sum_{s\geq 2}(|G_{Q,s}|-1)\ \right),$$

where $\bar{r}$ denotes the rank of $\bar{\mathcal{E}}$. By Lemma 2.2.18, we have

$$g_{\bar{Y}} = \dim_{\bar{k}} H^1(\bar{Y},\mathcal{O}_{\bar{Y}}) = \dim_{\bar{k}}(H^1(Y,\mathcal{O}_Y)\otimes_k \bar{k}) = \dim_k H^1(Y,\mathcal{O}_Y) = g_Y.$$

Furthermore, we have $\deg\bar{\mathcal{E}} = \deg\mathcal{E}$ (by Proposition 2.3.8), and $\operatorname{rank}\bar{\mathcal{E}} = \operatorname{rank}\mathcal{E}$. Using that $G_{P,s} = G_{Q,s} (s \geq 0)$ for any $P \in |X|$ and any pre-image $Q \in p^{-1}(P)$ (Proposition 2.3.16), and that the number of such pre-images Q equals $[k(P):k]$ (Corollary 2.2.11), we get the desired equality $C_{G,X,\mathcal{E}} = C_{G,\bar{X},\bar{\mathcal{E}}}$.

Hence, applying the homomorphism β to the right-hand side of our formula (2.11) gives

$$\beta\left(C_{G,X,\mathcal{E}}[k[G]] - \sum_{P\in|X|}\sum_{d=0}^{e_P-1} d[\mathrm{Ind}^G_{I_P}(\mathcal{E}(P)\otimes_{k(P)}(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d})]\right)$$

$$= C_{G,\bar{X},\bar{\mathcal{E}}}[\bar{k}[G]] - \sum_{Q\in|\bar{X}|} e^w_Q \sum_{d=0}^{e_Q-1} d[\mathrm{Ind}^G_{G_Q}(\bar{\mathcal{E}}(Q)\otimes_{\bar{k}}(\mathfrak{m}_Q/\mathfrak{m}_Q^2)^{\otimes d})],$$

which proves the assertion. $\square$

2.4 An equivariant Riemann-Roch formula in terms of projective $k[G]$-modules

In this section, we investigate under which conditions the Euler characteristic $\chi(G, X, \mathcal{E})$ lies in the Grothendieck group of *projective* modules. Under these conditions, one can find a formula for $\chi(G, X, \mathcal{E})$ as an integral linear combination of *projective* $k[G]$-modules. We call this a "strong" equivariant Riemann-Roch formula because equality in $K_0(k[G])$ is stronger than in $K_0(G, k)$. More concretely, two modules which are in the same class in $K_0(k[G])$ must be isomorphic, which is not the case in $K_0(G, k)$, as can be seen from the following example.

Example 2.4.1. Let $k = \mathbb{F}_p$, $G = C_p$ (the cyclic group of order p) for some prime number p. Let σ be a generator of C_p, let C_p act on $\mathbb{F}_p[x]/(x^2)$ via $\sigma.\overline{x} := \overline{x+1}$ and let C_p act trivially on $\mathbb{F}_p$. Then we have short exact sequences of $\mathbb{F}_p[C_p]$-modules

$$0 \to \mathbb{F}_p \to \mathbb{F}_p \oplus \mathbb{F}_p \to \mathbb{F}_p \to 0$$

and

$$0 \to \mathbb{F}_p \to \mathbb{F}_p[x]/(x^2) \to \mathbb{F}_p \to 0,$$

whence $[\mathbb{F}_p \oplus \mathbb{F}_p] = [\mathbb{F}_p[x]/(x^2)]$ in $K_0(C_p, \mathbb{F}_p)$. However, the two $k[G]$-modules $\mathbb{F}_p \oplus \mathbb{F}_p$ and $\mathbb{F}_p[x]/(x^2)$ are clearly not isomorphic, since G acts trivially on the first one and non-trivially on the second one.

In this section, we make the same assumptions as in the previous section; in particular, we assume that k is a perfect field.

2.4.1 A Cartesian diagram of Grothendieck groups

Recall that we have reduced Theorem 2.3.18 to the case of an algebraically closed base field by applying the map

$$\beta : K_0(G, k) \to K_0(G, \bar{k})$$

to both sides of the formula. In this subsection, we will see that the map β "conserves projectivity" in a strong sense. This will later enable us to use essentially the same proof technique for a projective analogue of Theorem 2.3.18.

Let $K_0(k[G])$ denote the Grothendieck group of finitely generated projective $k[G]$-modules. This is a free group generated by the isomorphism classes of indecomposable projective $k[G]$-modules. Since the tensor product of a projective $k[G]$-module with $\bar{k}$ is always a projective $\bar{k}[G]$-module, the exact functor "tensoring with $\bar{k}$ over k" from the category of $k[G]$-modules to the category of $\bar{k}[G]$-modules maps the subcategory of *projective* $k[G]$-modules into the subcategory of *projective* $\bar{k}[G]$-modules. Thus, besides the homomorphism $\beta : K_0(G, k) \to K_0(G, \bar{k})$ introduced in Subsection 2.2.3, the functor also induces a homomorphism

$$\alpha : K_0(k[G]) \to K_0(\bar{k}[G])$$

between the corresponding "projective" Grothendieck groups.

By Proposition (16.22) in [CR], both homomorphisms β, α are split injections. Furthermore, the Cartan homomorphisms $c : K_0(k[G]) \to K_0(G, k)$ and $\bar{c} : K_0(\bar{k}[G]) \to K_0(G, \bar{k})$ are injective (see for example [Se2], 16.1, Corollary 1 of Theorem 35, or [CR], Theorem (21.22)).

Proposition 2.4.2. *The following diagram with injective arrows is Cartesian, i.e. it commutes and viewing the injections as inclusions, we have* $K_0(\bar{k}[G]) \cap K_0(G, k) = K_0(k[G])$.

$$\begin{tikzcd} K_0(k[G]) \arrow[r, "\alpha"] \arrow[d, "c"'] & K_0(\bar{k}[G]) \arrow[d, "\bar{c}"] \\ K_0(G, k) \arrow[r, "\beta"'] & K_0(G, \bar{k}) \end{tikzcd}$$

In other words, given a class $\mathcal{C}$ in $K_0(G, k)$, $\mathcal{C}$ lies in the image of c if and only if $\beta(\mathcal{C})$ lies in the image of $\bar{c}$.

Proof. The commutativity is obvious. Now consider the extended diagram (with exact rows)

$$\begin{tikzcd} 0 \arrow[r] & K_0(k[G]) \arrow[r, "\alpha"] \arrow[d, "c"'] & K_0(\bar{k}[G]) \arrow[r] \arrow[d, "\bar{c}"'] & M \arrow[r] \arrow[d, "f"'] & 0 \\ 0 \arrow[r] & K_0(G, k) \arrow[r, "\beta"] & K_0(G, \bar{k}) \arrow[r] & N \arrow[r] & 0 \end{tikzcd}$$

where $M := \operatorname{cok} \alpha$ is the cokernel of α, $N := \operatorname{cok} \beta$ is the cokernel of β and f is the homomorphism $M \to N$ induced by $\bar{c}$. By the Snake Lemma, there is an exact sequence of abelian groups

$$0 \to \ker c \to \ker \bar{c} \to \ker f \to \operatorname{cok} c \to \operatorname{cok} \bar{c},$$

the first two modules being trivial since c and $\bar{c}$ are injective. Since α is a split injection, $M = \operatorname{cok} \alpha$ is free over $\mathbb{Z}$, and therefore $\ker f \subseteq M$ must also be free over $\mathbb{Z}$. On the other hand, by Theorem (21.22) in [CR], we have $|G| \cdot \operatorname{cok} c = 0$, so $\operatorname{cok} c$ is a torsion module. Using the exactness of the sequence above, this implies $\ker f = 0$. Therefore $\operatorname{cok} c$ is embedded in $\operatorname{cok} \bar{c}$.

Any element of $K_0(\bar{k}[G]) \cap K_0(G,k)$ maps to zero in $\operatorname{cok} \bar{c}$, hence in $\operatorname{cok} c$, and therefore must be an element of $K_0(k[G])$. □

Proposition 2.4.3. *Let C be a class in $K_0(G,k)$. Then C is the class of a projective $k[G]$-module if and only if $\beta(C)$ is the class of a projective $\bar{k}[G]$-module.*

Proposition 2.4.3 is the main result of this subsection, and we will use it several times in the following subsections. Before proving Proposition 2.4.3, we will need to prove a few preliminary results on $k[G]$-modules.

Recall that a $k[G]$-module is called *simple* if it is nonzero and has no proper $k[G]$-submodules, and *indecomposable* if it is nonzero and is not a direct sum of proper $k[G]$-submodules.

Definition 2.4.4. A *basic set of simple $k[G]$-modules* is a set of representatives of the (finitely many) isomorphism classes of simple $k[G]$-modules. Once such a set has been fixed, its elements will be called *basic simple $k[G]$-modules.* Analogously, a *basic set of indecomposable modules* is a set of representatives of the isomorphism classes of indecomposable projective (!) $k[G]$-modules, and its elements are called *basic indecomposable modules.*

Lemma 2.4.5. *There exists a finite algebraic extension E/k such that every simple $\bar{k}[G]$-module can be realized as a simple $E[G]$-module, i.e. every simple $\bar{k}[G]$-module M can be written as $M = N \otimes_E \bar{k}$ for some simple $E[G]$-module N.*

Proof. Let M be a simple $\bar{k}[G]$-module. Then M is generated by a single element, say α, over $\bar{k}[G]$, and we have a projection

$$p_M : \bar{k}[G] \to M \quad \text{given by } 1_{\bar{k}[G]} = 1 \cdot [\mathrm{id}_G] \mapsto \alpha.$$

The kernel of p_M is a finitely generated $\bar{k}[G]$-module. We choose a generating set, say $\{\beta_1, \ldots, \beta_m\}$, and obtain a projection

$$p'_M : \bar{k}[G]^m \to \ker p_M, \quad \epsilon_i \mapsto \beta_i,$$

where $\{\epsilon_i\}_{i=1,\ldots,m}$ is the standard basis for $\bar{k}[G]^m$.
Let ι denote the inclusion $\ker p_M \hookrightarrow \bar{k}[G]$. Then obviously $\mathrm{im}(\iota \circ p'_M) \cong \mathrm{im}\, p'_M \cong \ker p_M$, and hence the following sequence is exact:

$$\bar{k}[G]^m \xrightarrow{\iota \circ p'_M} \bar{k}[G] \xrightarrow{p_M} M \longrightarrow 0$$

Let $A = (a^1, \ldots, a^m) \in \bar{k}[G]^{m \times 1}$ be the matrix representing the homomorphism $\iota \circ p'_M$ with respect to the bases $(\epsilon_1, \ldots, \epsilon_m)$ and $1_{\bar{k}[G]}$ of $\bar{k}[G]^m$ and $\bar{k}[G]$, respectively.
The entries $a^1, \ldots, a^m$ of A are elements of $\bar{k}[G]$, i.e. they can be written in the form

$$a^i = \sum_{g \in G} b^i_g \cdot [g] \quad \text{where } b^i_g \in \bar{k} \text{ for all } g \in G.$$

We define

$$E(M) := k\left(\{b^i_g \mid i \in \{1, \ldots, m\}, g \in G\}\right),$$

i.e. $E(M)$ is the field obtained from k by adjoining the elements b^i_j. Since G is a finite group, we have adjoined only finitely many elements, i.e. $E(M)/k$ is a finite algebraic extension of fields.
Let now $\{M_1, \ldots, M_s\}$ be a basic set of simple $\bar{k}[G]$-modules, and let

$$E := [E(M_1), \ldots, E(M_s)],$$

i.e. E is the composite of all the extensions $E(M_j)$. Then E is a finite algebraic extension of k.
Let now M be an arbitrary simple $\bar{k}[G]$-module. Then there is a basic $\bar{k}[G]$-module M_j such that $M \cong M_j$. We choose bases and determine the matrix $A = (a^1, \ldots, a^m) \in \bar{k}[G]^{m \times 1}$ as described above. By construction, the group ring $E(M_j)[G]$ contains all the entries of A, and so does $E[G]$ (since $E \geq E(M_j)$). Hence, using the standard bases of $E[G]^m$ and $E[G]$, the matrix A defines a homomorphism

$$q : E[G]^m \to E[G].$$

Let N be the cokernel of q, then we have an exact sequence

$$E[G]^m \xrightarrow{q} E[G] \longrightarrow N \longrightarrow 0$$

We apply the functor "tensoring with $\bar{k}$ over E" to this sequence and obtain another exact sequence:

$$\bar{k}[G]^m \xrightarrow{q\otimes\mathrm{id}} \bar{k}[G] \longrightarrow N \otimes_E \bar{k} \longrightarrow 0$$

The "lifted" homomorphism $q \otimes \mathrm{id}$ is still represented by the matrix A with respect to standard bases. Therefore we have $q \otimes \mathrm{id} = \iota \circ p'_M$, where the latter map is defined as explained at the beginning of the proof. Hence we have

$$N \otimes_E \bar{k} = \mathrm{cok}(\iota \circ p_M) \cong M.$$

Furthermore, N is a simple $E[G]$-module. Indeed if N contained a proper $E[G]$-submodule, say N', then M would contain $N' \otimes_k \bar{k}$ as a proper submodule, but this can't happen as M is simple. □

Proposition 2.4.6. *(a) For every simple $k[G]$-module M, the $\bar{k}[G]$-module $M \otimes_k \bar{k}$ is semisimple.*

(b) Let $\{P_1, \dots, P_s\}$ be a basic set of indecomposable $k[G]$-modules, and let

$$P_i \otimes_k \bar{k} = \bigoplus_{j=1}^{r_i} \bar{Q}_{ij}, \quad \bar{Q}_{ij} \text{ indecomposable projective } \bar{k}[G]\text{-modules.}$$

Then every indecomposable $\bar{k}[G]$-module is isomorphic to some $\bar{Q}_{ij}$. Further $\bar{Q}_{ij} \cong \bar{Q}_{i'j'}$ implies that $i = i'$, i.e. there is no overlap between the sets of indecomposable $\bar{k}[G]$-modules which come from different indecomposable $k[G]$-modules.

Proof. (a) By Lemma 2.4.5, there is a finite algebraic extension E/k such that every simple $\bar{k}[G]$-module can be realized as a simple $E[G]$-module. Since k is perfect, E/k is a separable extension of fields. Hence, Proposition 7.4 and Proposition 7.7 in [CR] imply that for any simple $k[G]$-module M, the $E[G]$-module $M \otimes_k E$ is semisimple. (This is also stated at the beginning of Theorem 7.9 in [CR].) Thus, part (a) is proven.

(b) For every basic indecomposable $k[G]$-module P_i, let

$$M_i := P_i / \operatorname{rad} P_i.$$

It is well-known that this gives a 1-1 correspondence between the isomorphism classes of simple $k[G]$-modules and the isomorphism classes of indecomposable projective $k[G]$-modules, whose inverse is given by taking $k[G]$-projective covers. A $k[G]$*-projective cover* (or just *projective cover*) of a $k[G]$-module M is a projective $k[G]$-module P together with an epimorphism $f : P \to M$, such that for all projective $k[G]$-modules P' and all homomorphisms $g : P' \to M$, there is an epimorphism $\varphi : P' \to P$ making the following diagram (with exact rows and columns) commute.

$$\begin{tikzcd} P' \arrow[d, dashed, "\varphi"'] \arrow[dr, "g"] & & \\ P \arrow[r, "f"'] \arrow[d] & M \arrow[r] & 0 \\ 0 & & \end{tikzcd}$$

A projective cover exists for any $k[G]$-module M and is unique up to isomorphism, so we can speak of "the" projective cover of M.

The 1-1 correspondence just described means that $\{M_1, \ldots, M_s\}$ is a basic set of simple $k[G]$-modules, and for every i we have $P_i \cong \operatorname{Cov}(M_i)$ where Cov denotes the projective cover. Part (a) implies that for every i, the $\bar{k}[G]$-module $M_i \otimes_k \bar{k}$ is semisimple, i.e. we can write

$$M_i \otimes_k \bar{k} = \bigoplus_{i=1}^{r_i} \bar{N}_{ij}, \;\; \bar{N}_{ij} \text{ simple } \bar{k}[G]\text{-modules.} \tag{2.14}$$

Hence, for every i, we obtain a decomposition of $P_i \otimes_k E$ into indecomposable projective $\bar{k}[G]$-modules in the following way:

$$
\begin{aligned}
P_i \otimes_k \bar{k} &= (\operatorname{Cov} M_i) \otimes_k \bar{k} \\
&= \operatorname{Cov}(M_i \otimes_k \bar{k}) \quad \text{by Lemma 2.4.7 below} \\
&= \operatorname{Cov}(\bigoplus_{i=1}^{r_i} \bar{N}_{ij}) \quad \text{by (2.14)} \\
&= \bigoplus_{i=1}^{r_i} \operatorname{Cov}(\bar{N}_{ij}) \quad \text{by additivity of projective covers (Corollary 6.25(iii) in [CR]).}
\end{aligned}
$$

By Lemma 2.4.5, there exist $E[G]$-modules N_{ij} such that $\bar{N}_{ij} = N_{ij} \otimes_E \bar{k}$ for every i, j. Let $Q_{ij} := \operatorname{Cov} N_{ij}$ and $\bar{Q}_{ij} := \operatorname{Cov} \bar{N}_{ij}$ for every i, j. This yields the decomposition

$$P_i \otimes_k \bar{k} = \bigoplus_{j=1}^{r_i} \bar{Q}_{ij}$$

from the proposition (uniquely determined up to isomorphism and re-ordering). Moreover, Lemma 2.4.7 below implies that $Q_{ij} \otimes_E \bar{k} \cong (\operatorname{Cov} N_{ij}) \otimes_E \bar{k} \cong \operatorname{Cov}(\bar{N}_{ij}) \cong \bar{Q}_{ij}$ for every i, j. By Theorem 7.9(ii) in [CR], every simple $E[G]$-module is isomorphic to some N_{ij}. By Lemma 2.4.5, this implies that every simple $\bar{k}[G]$-module is isomorphic to some $\bar{N}_{ij}$. Every indecomposable projective $E[G]$-module is isomorphic to the projective cover of a simple one, and hence isomorphic to $\operatorname{Cov}(\bar{N}_{ij}) = \bar{Q}_{ij}$ for some i, j. This proves the first assertion of part (b). Now if $\bar{Q}_{ij} \cong \bar{Q}_{i'j'}$, then $Q_{ij} \cong Q_{i'j'}$ and hence $\operatorname{rad} Q_{ij} = \operatorname{rad} Q_{i'j'}$, so we have $N_{ij} = Q_{ij}/\operatorname{rad} Q_{ij} \cong Q_{i'j'}/\operatorname{rad} Q_{i'j'} = N_{i'j'}$. By Theorem 7.9(ii) in [CR], this implies that $i = i'$, which completes the proof of part (b). □

Lemma 2.4.7. *Let $f : P \to M$ be a surjective homomorphism of $k[G]$-modules, with P projective. If $f : P \to M$ is a projective cover, then so is $\bar{f} : \bar{P} \to \bar{M}$, where $\bar{P} := P \otimes_k \bar{k}$ and $\bar{M} := M \otimes_k \bar{k}$.*

Proof. Assume that $f : P \to M$ is a projective cover. By Corollary 6.25(i) in [CR], this is equivalent to saying that $\ker f \subseteq NP$, where

$N := \operatorname{rad} k[G]$. Hence we have the following diagram of $k[G]$-modules, with exact rows and diagonals:

$$\begin{tikzcd}
& 0 \arrow[dr] & & & & \\
& & NP \arrow[dr] & & & \\
0 \arrow[r] & \ker f \arrow[ur] \arrow[rr] & & P \arrow[r, "f"'] & M \arrow[r] & 0 \\
0 \arrow[ur] & & & & &
\end{tikzcd}$$

We can now "lift" this diagram by applying the exact functor $- \otimes_k \bar{k}$. We thus obtain the following diagram of $\bar{k}[G]$-modules, still with exact rows and diagonals:

$$\begin{tikzcd}
& 0 \arrow[dr] & & & & \\
& & (NP) \otimes_k \bar{k} \arrow[dr] & & & \\
0 \arrow[r] & \ker \bar{f} \arrow[ur] \arrow[rr] & & \bar{P} \arrow[r, "\bar{f}"'] & \bar{M} \arrow[r] & 0 \\
0 \arrow[ur] & & & & &
\end{tikzcd}$$

This shows that we have $\ker \bar{f} \subseteq (NP) \otimes_k \bar{k}$. By Proposition 2.4.6, for every simple $k[G]$-module S, the $\bar{k}[G]$-module $S \otimes_k \bar{k}$ is semisimple. By Theorem 7.9 in [CR], this implies that

$$(\operatorname{rad} k[G]) \otimes_k \bar{k} = \operatorname{rad} \bar{k}[G].$$

Hence we have

$$\ker \bar{f} \subseteq (NP) \otimes_k \bar{k} \cong (N \otimes_k \bar{k})(P \otimes_k \bar{k}) = (\operatorname{rad} \bar{k}[G])\bar{P}.$$

By Corollary 6.25(i) in [CR], this implies that $\bar{f}$ is a projective cover. $\square$

Proof of Proposition 2.4.3. The "only if" direction is obvious. For the "if" direction, we note first of all that if $\mathcal{C}$ is a class in $K_0(G,k)$ and $\beta(\mathcal{C})$ is the class of a projective $\bar{k}[G]$-module, then Proposition 2.4.2 yields that $\mathcal{C}$ can be viewed as a class in $K_0(k[G])$. Hence it suffices to show the "if" direction for classes $\mathcal{C} \in K_0(k[G])$, replacing the homomorphism β by its restriction α.

Let $\{P_1, \ldots, P_s\}$ be a basic set of indecomposable $k[G]$-modules, and let

$$P_i \otimes_k \bar{k} = \bigoplus_{j=1}^{r_i} Q_{ij}, \quad Q_{ij} \text{ indecomposable } \bar{k}[G]\text{-modules.}$$

Every $\mathcal{C} \in K_0(k[G])$ can now be written as a $\mathbb{Z}$-linear combination of the classes $[P_i]$. The integer coefficients in this linear combination are all nonnegative if and only if $\mathcal{C}$ is the class of a projective module. Suppose that $\mathcal{C}$ is *not* the class of a projective module, i.e. without loss of generality,

$$\mathcal{C} = \sum_{i=1}^{s'} a_i[P_i] - \sum_{i=s'+1}^{s} a_i[P_i]$$

where $1 \leq s' < s$, $a_i \geq 0$ for all i and $a_i > 0$ for at least one $i \geq s'+1$. By definition of α, this implies

$$\alpha(\mathcal{C}) = \sum_{i=1}^{s'} a_i[P_i \otimes_k \bar{k}] - \sum_{i=s'}^{s} a_i[P_i \otimes_k \bar{k}] = \sum_{i=1}^{s'} \sum_{j=1}^{r_i} a_i[Q_{ij}] - \sum_{i=s'}^{s} \sum_{j=1}^{r_i} a_i[Q_{ij}].$$

Now Proposition 2.4.6 yields that the indecomposable modules Q_{ij} appearing in the first sum are all different from those appearing in the second sum, so $\alpha(\mathcal{C})$ is not a proper sum of the classes $[Q_{ij}]$. Therefore $\alpha(\mathcal{C})$ cannot be the class of a projective $\bar{k}[G]$-module. □

The following variation of Proposition 2.4.3 can directly be derived from Lemma 2.4.7.

Lemma 2.4.8. *A $k[G]$-module M is projective if and only if $M \otimes_k \bar{k}$ is a projective $\bar{k}[G]$-module.*

2.4.2 The equivariant Euler characteristic in terms of projective $k[G]$-modules

Recall that we are still working with the same assumptions and notations as at the beginning of section 2.3. In particular, π denotes the canonical projection $X \to Y = X/G$, and p denotes the projection $\bar{X} = X \times_k \bar{k} \to X$. Additionally, let $\bar{\pi}$ denote the canonical projection $\bar{X} \to \bar{Y} := \bar{X}/G = Y \otimes_k \bar{k}$, and let $\tilde{p}$ denote the projection $\bar{Y} \to Y$. We have the following commutative diagram:

$$\begin{array}{ccc} \bar{X} & \xrightarrow{p} & X \\ {\scriptstyle \bar{\pi}}\downarrow & & \downarrow{\scriptstyle \pi} \\ \bar{Y} & \xrightarrow{\tilde{p}} & Y \end{array}$$

Theorem 2.4.9. *If π is tamely ramified and $\mathcal{E}$ is a locally free G-sheaf on X, then the equivariant Euler characteristic $\chi(G, X, \mathcal{E})$ lies in the image of the Cartan homomorphism $c : K_0(k[G]) \to K_0(G, k)$.*

Proof. Follows directly from Theorem 1 in [Na]. □

Recall that π is called *weakly ramified* if $G_{P,i}$ is trivial for all $P \in |X|$ and all $i \geq 2$ (see Definition 2.3.10).

Theorem 2.4.10. *Let $D = \sum_{P\in|X|} n_P P$ be a G-equivariant divisor on X.*

(a) If π is weakly ramified and $n_P \equiv -1 \mod e_P^w$ for all $P \in X$, then the equivariant Euler characteristic $\chi(G, X, \mathcal{L}(D))$ lies in the image of the Cartan homomorphism $c : K_0(k[G]) \to K_0(G, k)$. If moreover one of the cohomology groups $H^i(X, \mathcal{L}(D))$, $i = 0, 1$, vanishes, then the other one is a projective $k[G]$-module.

(b) Let $\deg D > 2g_X - 2$. If the $k[G]$-module $H^0(X, \mathcal{L}(D))$ is projective, then π is weakly ramified and $n_P \equiv -1 \mod e_P^w$ for all $P \in |X|$.

Proof. In the case where k is algebraically closed, this theorem has been proven by Köck (Theorem 2.1 in [Kö1]). We can deduce Theorem 2.4.10 from the case where k is algebraically closed by using the following facts:

- Write $p^*D = \sum_{Q\in|\bar{X}|} n_Q Q$. Then by Lemma 2.3.7 and Corollary 2.3.17, we have $n_Q = n_{p(Q)}$ and $e_Q = e_{p(Q)}$ for all $Q \in |\bar{X}|$, and hence $n_P \equiv -1 \mod e_P^w$ for all $P \in |X|$ if and only if $n_Q \equiv -1 \mod e_Q^w$ for all $Q \in |\bar{X}|$.

- By Proposition 2.3.16, π is weakly ramified if and only if $\bar{\pi} : \bar{X} \to \bar{Y}$ is weakly ramified.

- By Lemma 2.3.6, Lemma 2.2.22 and Proposition 2.4.2, $\chi(G, X, \mathcal{L}(D)$ lies in the image of c if and only if $\beta(\chi(G, X, \mathcal{L}(D)) = \chi(G, \bar{X}, \mathcal{L}(p^*D))$ lies in the image of $\bar{c}$.

- Let $i \in \{0, 1\}$. By Lemma 2.3.6, Lemma 2.2.18 and Proposition 2.4.3, $H^i(X, \mathcal{L}(D)$ is projective if and only if $H^i(\bar{X}, \mathcal{L}(p^*D))$ is.

- $\deg D = \deg p^*D$ (by Lemma 2.19) and $g_X = g_{\bar{X}}$.

□

The following theorem generalizes Theorem 4.3 in [Kö2] and will be used in the formulation of the (main) Theorem 2.4.15.

Theorem 2.4.11. *Let π be weakly ramified. Then there is a projective $k[G]$-module $N_{G,X}$ such that*

$$\bigoplus^{n} N_{G,X} \cong \bigoplus_{P\in|X|} \bigoplus_{d=1}^{e_P^t - 1} \bigoplus^{e_P^w \cdot d} \mathrm{Ind}_{I_P}^G(\mathrm{Cov}((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d})), \tag{2.15}$$

where Cov *denotes the $k[I_P]$-projective cover (as defined in the proof of Proposition 2.4.6).*
The class of $N_{G,X}$ in $K_0(G,k)$ is given by

$$[N_{G,X}] = (1 - g_Y)[k[G]] - \chi(G, X, \mathcal{L}(E)) \tag{2.16}$$

where E denotes the G-equivariant divisor $E := \sum_{P\in X}(e_P^w - 1) \cdot P$.

Remark 2.4.12. The projective module $N_{G,X}$ is sometimes called *ramification module* because it "encodes" the ramification of the cover $\pi : X \to Y$.

Note that $N_{G,X}$ is determined by what happens at the ramification points of the cover $\pi : X \to Y$, so it is determined by "local" data. However, in order to obtain the divisibility by the group order n, one must sum over all these points, so the existence of $N_{G,X}$ is actually a "global" result (as pointed out by Köck in [Kö2]).

Unlike our equivariant Riemann-Roch formula from Theorem 2.3.18 (and unlike the "strong" equivariant Riemann-Roch formula we will prove later in Theorem 2.4.15), Theorem 2.4.11 does not involve the additional data of a locally free G-sheaf $\mathcal{E}$ or an equivariant divisor D on X.

If π is assumed to be *tamely* ramified, then the defining equation for $N_{G,X}$ has the following somewhat simpler shape:

$$\bigoplus^{n} N_{G,X} = \bigoplus_{P\in X} \bigoplus_{d=1}^{e_P-1} \bigoplus^{d} \mathrm{Ind}_{I_P}^{G}((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}).$$

For the case where π is tamely ramified and k is algebraically closed, the existence of $N_{G,X}$ has already been shown by Nakajima (Theorem 2 in [Na]), and later with other methods by Borne (Theorem 3.16 in [Bo]) and Köck (Corollary 1.4(a) in [Kö1]).

Furthermore, if π is tamely ramified, then the divisor E in the theorem is the zero divisor, so we have $\mathcal{L}(E) = \mathcal{O}_X$ and hence

$$[N_{G,X}] = (1 - g_Y)[k[G]] - \chi(G, X, \mathcal{O}_X), \tag{2.17}$$

which can be considered as an equivariant Hurwitz formula. For the case where π is tamely ramified and k is algebraically closed, formula (2.17) has been proven by Borne (Theorem 3.16 in [Bo]) and Köck (Remark 1.5 in [Kö1]).

Proof of Theorem 2.4.11. Theorem 4.3 in [Kö2] yields that there is a projective $\bar{k}[G]$-module $N_{G,\bar{X}}$ such that

$$\bigoplus^{n} N_{G,\bar{X}} \cong \bigoplus_{Q\in|\bar{X}|} \bigoplus_{d=1}^{e_Q^t-1} \bigoplus^{e_Q^w \cdot d} \mathrm{Ind}_{G_Q}^{G}(\mathrm{Cov}((\mathfrak{m}_Q/\mathfrak{m}_Q^2)^{\otimes d})), \tag{2.18}$$

and that the class of $N_{G,\bar{X}}$ is given by

$$[N_{G,\bar{X}}] = (1 - g_{\bar{Y}})[\bar{k}[G]] - \chi(G, X, \mathcal{L}(\bar{E})) \tag{2.19}$$

where $\bar{E}$ is the G-equivariant divisor $\bar{E} := \sum_{Q\in\bar{X}}(e_Q^w - 1)\cdot Q$. Since $\bar{E} = p^*E$ (by Lemma 2.3.7 and Corollary 2.3.17), this is just the image of the class

$$\mathcal{C} := (1 - g_Y)[k[G]] - \chi(G, X, \mathcal{L}(E)) \in K_0(G, k)$$

under β. Hence, we can apply Proposition 2.4.3 to see that $\mathcal{C}$ is the class of some projective $k[G]$-module, say $N_{G,X}$. Now we have in $K_0(\bar{k}[G])$:

$$\begin{aligned}
\beta(n[N_{G,X}]) = n\,\beta(\mathcal{C}) = n\,[N_{G,\bar{X}}] &\overset{(2.18)}{=} \left[\bigoplus_{Q\in|\bar{X}|}\bigoplus_{d=1}^{e_Q^t-1}\bigoplus^{e_Q^w\cdot d}\mathrm{Ind}_{G_Q}^G(\mathrm{Cov}((\mathfrak{m}_Q/\mathfrak{m}_Q^2)^{\otimes d}))\right] \\
&= \left[\bigoplus_{P\in|X|}\bigoplus_{Q\in p^{-1}(P)}\bigoplus_{d=1}^{e_Q^t-1}\bigoplus^{e_Q^w\cdot d}\mathrm{Ind}_{G_Q}^G(\mathrm{Cov}((\mathfrak{m}_Q/\mathfrak{m}_Q^2)^{\otimes d}))\right] \\
&= \left[\bigoplus_{P\in|X|}\bigoplus_{d=1}^{e_P^t-1}\bigoplus^{e_P^w\cdot d}\mathrm{Ind}_{I_P}^G(\mathrm{Cov}(\bigoplus_{Q\in p^{-1}(P)}(\mathfrak{m}_Q/\mathfrak{m}_Q^2)^{\otimes d}))\right].
\end{aligned}$$

Here we have used that $e_P^t = e_Q^t, e_P^w = e_Q^w, I_P = G_Q$ if $Q \in p^{-1}(P)$. We have also used the additivity of projective covers (Corollary 6.25(ii) in [CR]) and the additivity of induction (Proposition 10.6 in [CR]). Lemma 2.2.28 now yields that $\bigoplus_{Q\in p^{-1}(P)}(\mathfrak{m}_Q/\mathfrak{m}_Q^2)^{\otimes d} \cong ((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}) \otimes_k \bar{k}$ as $k[I_P]$-modules, and hence

$$\begin{aligned}
\beta(n\,[N_{G,X}]) &= \left[\bigoplus_{P\in|X|}\bigoplus_{d=1}^{e_P^t-1}\bigoplus^{e_P^w\cdot d}\mathrm{Ind}_{I_P}^G(\mathrm{Cov}((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d})\otimes_k\bar{k})\right] \\
&= \beta\left(\left[\bigoplus_{P\in|X|}\bigoplus_{d=1}^{e_P^t-1}\bigoplus^{e_P^w\cdot d}\mathrm{Ind}_{I_P}^G((\mathrm{Cov}(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}))\right]\right)
\end{aligned}$$

since we have $\mathrm{Ind}_{I_P}^G(V\otimes_k\bar{k}) \cong (\mathrm{Ind}_{I_P}^G(V))\otimes_k\bar{k}$ (by Corollary 10.20 in [CR]) and $\mathrm{Cov}(V\otimes_k\bar{k}) \cong (\mathrm{Cov}\,V)\otimes_k\bar{k}$ (by Lemma 2.4.7) for any $k[I_P]$-module V. Cov has been used to denote projective covers with respect to $k[I_P]$ as well as $k[G]$, $\bar{k}[G]$ and $\bar{k}[I_P]$, depending on the context. Since β is injective, the above yields that equation (2.15) holds for $N_{G,X}$. By construction, equation (2.16) holds as well. □

Notation 2.4.13. For any $P \in X$, we denote the inertia degree $[k(P) : k(\pi(P))]$ by f_P.

Lemma 2.4.14. *For every point $R \in Y$, the number of pre-images of R under π is equal to $\frac{n}{e_P f_P}$, where P is any point in $\pi^{-1}(R)$. In particular, if the base field k is algebraically closed, then the number of pre-images is $\frac{n}{e_P}$.*

Proof. The number of pre-images of R is obviously equal to the length of the G-orbit of P,

$$\#\pi^{-1}(R) = \#(G \cdot P) = \frac{|G|}{|G_P|} = \frac{n}{|G_P|}.$$

By Theorem 9.9 in [Ne], the sequence

$$1 \to I_P \to G_P \to \mathrm{Gal}(k(P)/k(R)) \to 1$$

is exact, so we have $|G_P| = |I_P||\mathrm{Gal}(k(P)/k(R))| = e_P f_P$. □

Theorem 2.4.15 ("Strong" equivariant Riemann-Roch formula). *Let $\pi : X \to Y$ be weakly ramified.*

(a) Let $P \in |X|$ be a closed point. For every $d \in \{0, \ldots, e_P^t - 1\}$, there is a unique projective $k[G]$-module $W_{P,d}$ such that

$$\mathrm{Ind}_{I_P}^{G_P}(\mathrm{Cov}((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes(-d)})) \cong \bigoplus^{f_P} W_{P,d}$$

as $k[G_P]$-modules.

(b) Let $D = \sum_{P \in |X|} n_P \cdot P$ be a G-equivariant divisor on X with $n_P \equiv -1 \mod e_P^w$ for all $P \in X$. For any $P \in X$, we write

$$n_P = (e_P^w - 1) + (l_P + m_P e_P^t) e_P^w$$

with $l_P \in \{0, \ldots, e_P^t - 1\}$ and $m_P \in \mathbb{Z}$. Furthermore, for any $R \in Y$, fix a point $\tilde{R} \in \pi^{-1}(R)$. Then we have in $K_0(k[G])$:

$$\begin{aligned}&\chi(G, X, \mathcal{L}(D)) \\ &= -[N_{G,X}] + \sum_{R \in Y} \sum_{d=1}^{l_{\tilde{R}}} [\mathrm{Ind}_{G_{\tilde{R}}}^G (W_{\tilde{R},d})] + \Big(1 - g_Y + \sum_{R \in Y} [k(R) : k] m_{\tilde{R}}\Big) [k[G]].\end{aligned} \tag{2.20}$$

Proof. We first show that under the conditions of (b), the following holds in the Grothendieck group with rational coefficients $K_0(k[G])_{\mathbb{Q}}$:

$$\chi(G,X,\mathcal{L}(D))$$
$$= -[N_{G,X}]+\sum_{R\in Y}\frac{1}{f_{\tilde{R}}}\sum_{d=1}^{l_{\tilde{R}}}[\mathrm{Ind}_{I_{\tilde{R}}}^{G}(\mathrm{Cov}((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes(-d)}))]+\left(1-g_Y+\sum_{R\in Y}[k(R):k]m_{\tilde{R}}\right)[k[G]] \tag{2.21}$$

With suitably chosen divisors D, Formula (2.21) will be used to show part (a). Formula (2.21) and part (a) obviously imply part (b).
For curves over algebraically closed fields, formula (2.21) coincides with Theorem 4.5 in [Kö2]. We have seen (Lemma 2.2.18) that the injective homomorphism $\beta: K_0(G,k) \to K_0(G,\bar{k})$ maps $\chi(G,X,\mathcal{E})$ to $\chi(G,\bar{X},p^*\mathcal{E})$, and by Theorem 2.4.10, both of these Euler characteristics lie in the image of the respective Cartan homomorphisms. Hence, by the injectivity of α and of the Cartan homomorphism, it suffices to show that β maps every summand of the right-hand side of formula 2.20 (applied to X, D) to the corresponding summand of the right-hand side applied to $\bar{X}, p^*D$.
From the proof of Theorem 2.4.11, we see that $\beta([N_{G,X}]) = [N_{G,\bar{X}}]$.
Now write $p^*D = \sum_{Q\in X} n_Q \cdot Q$. Then we have (by Lemma 2.3.7 and Proposition 2.3.17) $n_Q = n_P$, $e_P = e_Q$, $e_P^t = e_Q^t$ and $e_P^w = e_Q^w$ if $Q \in p^{-1}(P)$. This also implies that $l_Q = l_P$ and $m_Q = m_P$ if $Q \in p^{-1}(P)$.
For any $S \in |\bar{Y}|$, fix a point $\tilde{S} \in \bar{\pi}^{-1}(S)$. Then we have

$$\beta\left(\sum_{R\in Y}\frac{1}{f_{\tilde{R}}}\sum_{d=1}^{l_{\tilde{R}}}[\mathrm{Ind}_{I_{\tilde{R}}}^{G}(\mathrm{Cov}((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes(-d)}))]\right)$$
$$= \beta\left(\sum_{P\in X}\left(\frac{n}{e_P f_P}\right)^{-1}\frac{1}{f_P}\sum_{d=1}^{l_P}[\mathrm{Ind}_{I_P}^{G}(\mathrm{Cov}((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes(-d)}))]\right) \quad \text{(by Lemma 2.4.14)}$$
$$= \sum_{Q\in\bar{X}}\frac{e_P}{n}\sum_{d=1}^{l_Q}[\mathrm{Ind}_{G_Q}^{G}(\mathrm{Cov}((\mathfrak{m}_Q/\mathfrak{m}_Q^2)^{\otimes(-d)}))] \quad \text{(by Section 2.2)}$$
$$= \sum_{S\in\bar{Y}}\sum_{d=1}^{l_{\tilde{S}}}[\mathrm{Ind}_{G_{\tilde{S}}}^{G}(\mathrm{Cov}((\mathfrak{m}_{\tilde{S}}/\mathfrak{m}_{\tilde{S}}^2)^{\otimes(-d)}))].$$

Moreover, we have

$$\begin{aligned}
&\beta\left(\left(1-g_Y+\sum_{R\in Y}[k(R):k]m_{\tilde{R}}\right)\ [k[G]]\right)\\
&=\beta\left(\left(1-g_{\bar{Y}}+\sum_{S\in \bar{Y}}m_{\tilde{S}}\right)\ [k[G]]\right) \qquad \text{(by Lemma 2.2.10)}\\
&=\left(1-g_{\bar{Y}}+\sum_{S\in\bar{Y}}m_{\tilde{S}}\right)[\bar{k}[G]].
\end{aligned}$$

Since we know that Formula (2.21) holds for the cover $\bar{\pi}:\bar{X}\to\bar{Y}$ of curves over $\bar{k}$, this proves Formula (2.21) for the cover $\pi: X\to Y$.

We now prove part (a). Let $P\in X$ be a closed point. For $d=0$, the statement is obvious because $(\mathfrak{m}_P/\mathfrak{m}_P^2)^0$ is the trivial one-dimensional $k(P)$-representation of I_P, so it decomposes into f_P copies of the trivial one-dimensional $k(R)$-representation of I_P, where $R:=\pi(P)$. Hence we only need to do the inductive step from d to $d+1$, for $d\in\{0,\ldots,e_P^t-2\}$. If π is unramified at P, then $e_P=1$, so there is no $d\in\{0,\ldots,e_P^t-2\}$. Hence we may assume that π is ramified at P. Set $H:=G_P$, the decomposition group at P, and let π' denote the projection $X\to X/H=:Y'$. For every closed point $Q\in|X|$ and for every $s\geq -1$, let $H_{Q,s}$ be the s-th ramification group at Q with respect to that cover, as in Definition 2.3.10. It follows directly from the definitions that we have $H_{Q,s}=G_P\cap G_{Q,s}$ for every $s\geq-1$ and every $Q\in|X|$. In particular, if π is weakly ramified, then so is π'. For $Q=P$, we get $H_{P,s}=G_{P,s}$ for all $s\geq -1$; in particular, the ramification indices and inertia degrees of π and π' at P are equal.

Let now $D:=\sum_{Q\in|X|}n_Q\cdot Q$ be the H-equivariant divisor with coefficients

$$n_Q=\begin{cases}(d+2)e_Q^w-1 & \text{if}\quad Q=P\\ e_Q^w-1 & \text{otherwise}\end{cases}$$

Then formula (2.21) applied to H,X,D gives

$$\begin{aligned}
\chi(H,X,\mathcal{L}(D)) &= -[N_{H,X}]+\frac{1}{f_P}\sum_{n=1}^{d}[\mathrm{Ind}_{I_P}^H(\mathrm{Cov}((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes(-n)}))]\\
&\quad+\frac{1}{f_P}[\mathrm{Ind}_{I_P}^H(\mathrm{Cov}((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes(-(d+1))}))]+(1-g_{Y'})[k[H]] \qquad (2.22)
\end{aligned}$$

in $K_0(k[H])_{\mathbb{Q}}$. By the induction hypothesis, the sum from $n = 1$ to d in this formula is divisible by f_P in $K_0(k[H])$; hence the remaining fractional term $\frac{1}{f_P}[\mathrm{Ind}_{I_P}^{H}(\mathrm{Cov}((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes(-(d+1))}))]$ must lie in $K_0(k[H])$. In particular, when writing $\mathrm{Ind}_{I_P}^{H}(\mathrm{Cov}((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes(-(d+1))})$ as a direct sum of indecomposable projective $k[H]$-modules, every summand occurs with a multiplicity divisible by f_P. This proves the assertion. □

In the proof of Theorem 2.4.15(a), we have used a *global* argument to show the divisibility of $\mathrm{Ind}_{I_P}^{G_P}(\mathrm{Cov}((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes(-d)}))$ by f_P. This tells us very litte about the structure of the summands $W_{P,d}$, which leads to the question whether one could find a "local" proof for the divisibility. In two different situations, the following proposition provides such a proof, yielding a concrete description of $W_{P,d}$. Note that in both of these situations, the cover $\pi : X \to Y = X/G$ has to be *tamely* ramified.

Proposition 2.4.16. *Assume that π is tamely ramified and let $P \in |X|$ and $d \in \{1, \ldots, e_P^t - 1\}$.*

(a) If $\mathrm{Gal}(k(P)/k(\pi(P)))$ is abelian, then we have $W_{P,d} \cong (\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes(-d)}$ as $k[G_P]$-modules.

(b) If I_P is central in G_P, then $W_{P,d}$ is of the form $W_{P,d} = \mathrm{Ind}_{I_P}^{G}(\chi_d)$ for some $k[I_P]$-module χ_d. If moreover $G_P \cong I_P \times G_P/I_P$, then $W_{P,d} \cong (\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes(-d)}$ as $k[G_P]$-modules.

Note that since every Galois extension of a finite field is cyclic, the first part of this proposition gives a "local" proof of Theorem 2.4.15(a) for the important case where π is tamely ramified and the underlying field k is finite.

Proposition 2.4.16 can be deduced from the following purely algebraic result. Note that, in this result, we don't use the notations introduced earlier in this paper; when Proposition 2.4.17 is being applied to prove Proposition 2.4.16, the fields k and l become the fields $k(\pi(P))$ and $k(P)$, respectively, the group G becomes G_P and V becomes $(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes(-d)}$ which is viewed only as a representation of I_P (and not of G_P) in Theorem 2.4.15.

Proposition 2.4.17. *Let l/k be a finite Galois extension of fields. Let G be a finite group, and let I be a cyclic normal subgroup of G, such that*

$G/I \cong \mathrm{Gal}(l/k)$, i.e. we have a short exact sequence

$$1 \to I \to G \to \mathrm{Gal}(l/k) \to 1.$$

Let V be a one-dimensional vector space over l such that G acts semilinearly on V, that is, for any $g \in G, \lambda \in l, v, w \in V$, we have $g.(\lambda v + w) = \bar{g}(\lambda)(g.v) + g.w$, where $\bar{g}$ denotes the image of g in $\mathrm{Gal}(l/k)$. In particular, V is then a $k[G]$-module and an $l[I]$-module. Assume furthermore that I acts faithfully on V.

(a) If $\mathrm{Gal}(l/k)$ is abelian, then we have $\mathrm{Ind}_I^G \mathrm{Res}_I^G(V) \cong \bigoplus^{(G:I)} V$ as $k[G]$-modules.

(b) If I is central in G, then there is a (non-trivial) one-dimensional k-representation χ of I such that $\mathrm{Res}_I^G(V) \cong \bigoplus^{(G:I)} \chi$ as $k[I]$-modules.

If moreover $G = I \times \mathrm{Gal}(l/k)$, then we have $\mathrm{Ind}_I^G \chi \cong V$ and $\mathrm{Ind}_I^G \mathrm{Res}_I^G(V) \cong \bigoplus^{(G:I)} V$ as $k[G]$-modules.

Proof. (a) We have (isomorphisms of $k[G]$-modules):

$$\begin{aligned}
&\mathrm{Ind}_I^G \mathrm{Res}_I^G(V) \\
&\quad \cong V \otimes_k \mathrm{Ind}_I^G(k) && \text{by Corollary 10.20 in [CR]} \\
&\quad \cong V \otimes_k k[G/I] && \text{(cf. §10A in [CR])} \\
&\quad \cong V \otimes_k k[\mathrm{Gal}(l/k)] && \text{as } \mathrm{Gal}(l/k) \cong G/I \\
&\quad \cong V \otimes_k l \\
&\quad \cong \bigoplus_{\sigma \in \mathrm{Gal}(l/k)} V.
\end{aligned}$$

The last two isomorphisms can be derived as follows. By the normal basis theorem, there is an element $x_0 \in l$ such that $\{g(x_0) | g \in \mathrm{Gal}(l/k)\}$ is a basis of l over k. The resulting isomorphism

$$\begin{aligned}
&k[\mathrm{Gal}(l/k)] \to l \quad \text{given by} \\
&\qquad [g] \mapsto g(x_0) \quad \text{for every } g \in \mathrm{Gal}(l/k).
\end{aligned}$$

is obviously $k[G]$-linear. This is the penultimate isomorphism. For the last one, we define

$$\begin{aligned}\varphi : l \otimes_k V &\to \bigoplus_{\sigma \in \mathrm{Gal}(l/k)} V \quad \text{by} \\ a \otimes v &\mapsto (\sigma(a) \cdot v)_{\sigma \in \mathrm{Gal}(l/k)} \quad \text{for every } a \in l, v \in V.\end{aligned}$$

φ is an isomorphism of vector spaces over k, by the Galois descent lemma. If $\mathrm{Gal}(l/k)$ is commutative, then φ is also compatible with the G-action on both sides: Let $a \in l$, $v \in V$, $g \in G$, then we have

$$\begin{aligned}\varphi(g.(a \otimes v)) = \varphi(\bar{g}(a) \otimes g.v) = ((\sigma\bar{g})(a) \cdot g.v)_{\sigma \in \mathrm{Gal}(l/k)} &= ((\bar{g}\sigma)(a) \cdot g.v)_{\sigma \in \mathrm{Gal}(l/k)} \\ &= g.((\sigma(a) \cdot v)_{\sigma \in \mathrm{Gal}(l/k)}) = g.\varphi(a \otimes v).\end{aligned}$$

(b) Since I is cyclic and acts faithfully on V, it acts by multiplication with e-th roots of unity, where $e = |I|$. If I is central in G, then it follows that the e-th roots of unity are contained in k. For if h is a generator of I and $h.v = \zeta_e \cdot v$ for all $v \in V$, ζ_e an e-th root of unity, then we have for all $g \in G$ and all $v \in V$:

$$\bar{g}(\zeta_e)(g.v) = g.(\zeta_e v) = (gh).v = (hg).v = \zeta_e(g.v).$$

Hence for every $\bar{g} \in \mathrm{Gal}(l/k)$, we have $\bar{g}(\zeta_e) = \zeta_e$, which means that ζ_e lies in k. Let now $\{x_1, \ldots, x_f\}$ be a k-basis of V, where $f = (G : I)$. Then we have $V = kx_0 \oplus \ldots \oplus kx_f$ not only as vector spaces over k, but also as $k[I]$-modules, since

$$Ix_i = \{\zeta_e^j x_i | j = 0, \ldots, e-1\} \subseteq kx_i$$

for every basis vector x_i. Furthermore, the summands kx_i are isomorphic as $k[I]$-modules because I acts on each of them by multiplication with the same roots of unity in k. Setting for example $kx_1 =: \chi$, we can write

$$\mathrm{Res}_I^G(V) \cong \bigoplus^f \chi$$

as required.

Assume now that $G = I \times \mathrm{Gal}(l/k)$ Then by the Galois descent lemma, we have

$$V \cong l \otimes_k V^{\mathrm{Gal}(l/k)}$$

as $k[G]$-modules, where I acts trivially on l and $\mathrm{Gal}(l/k)$ acts trivially on $V^{\mathrm{Gal}(l/k)}$. This is isomorphic to $l \otimes_k \chi$, where χ is viewed as a $k[G]$-module via the projection $G = I \times \mathrm{Gal}(l/k) \to I$. By the normal basis theorem, we have

$$l \otimes_k \chi \cong \mathrm{Ind}_I^G(k) \otimes \chi = \mathrm{Ind}_I^G(\chi),$$

so $V \cong \mathrm{Ind}_I^G(\chi)$ as requested. Together with what we have shown before, this implies the last identity of the proposition:

$$\mathrm{Ind}_I^G \mathrm{Res}_I^G(V) = \mathrm{Ind}_I^G(\bigoplus^f \chi) = \bigoplus^f V.$$

□

Remark 2.4.18. In the case of an algebraically closed underlying field, Theorem 2.4.11 and formula 2.21 coincide with Theorem 4.3 and Theorem 4.5, respectively, in [Kö2]. He deduces both theorems from his weak equivariant Riemann-Roch formula, Theorem 3.1 in [Kö2].

An alternative approach to the results of this section is to exactly imitate this method and derive both Theorem 2.4.11 and formula 2.21 from our weak equivariant Riemann-Roch formula, Theorem 2.3.18. For the case where π is tamely ramified, this has been realised in the author's diploma thesis [Fi]. But if one were to do the same for the weakly ramified case, it would become quite lengthy and would probably be less elegant than the approach taken in this thesis. In particular, one would have to find an alternative proof of Theorem 2.4.10 and do some quite tedious calculations to show the result in the weakly ramified case.

The following Corollary of Theorem 2.4.15 is similar to a result stated (but not proven) in [Kö2]. It will be useful for finding an equivariant Riemann-Roch formula whose coefficients are *nonnegative* integers rather than just integers (see Chapter 3).

Corollary 2.4.19. *Assume that π is tamely ramified. Let S be a G-stable subset of X containing all the ramification points of π. Furthermore, let $\Sigma_{\pi(S)} := \sum_{R\in\pi(S)} R$ and let $N^*_{G,X}$ denote the dual $k[G]$-module of $N_{G,X}$. Then we have in $K_0(k[G])$:*

$$[N^*_{G,X}] + \sum_{R\in\pi(S)} [\mathrm{Ind}^G_{I_{\tilde{R}}}(k(R))] + [N_{G,X}] = (\deg \Sigma_{\pi(S)})[k[G]]. \tag{2.23}$$

Proof. By Remark 2.4.12, we have in $K_0(k[G])_{\mathbb{Q}}$:

$$[N_{G,X}] = \frac{1}{n}\sum_{P\in X}\sum_{d=1}^{e_P-1} d\,[\mathrm{Ind}^G_{I_P}((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d})] = \sum_{R\in Y}\sum_{d=1}^{e_{\tilde{R}}-1}\frac{d}{e_{\tilde{R}}f_{\tilde{R}}}[\mathrm{Ind}^G_{I_{\tilde{R}}}((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes d})]$$
$$= \sum_{R\in Y}\frac{1}{f_{\tilde{R}}}\sum_{d=1}^{e_{\tilde{R}}-1}\frac{d}{e_{\tilde{R}}}[\mathrm{Ind}^G_{I_{\tilde{R}}}((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes d})].$$

Here we have used that $\#\{P'\in X|\pi(P')=\pi(P)\} = \frac{n}{e_Pf_P}$ for any $P\in X$. By Proposition 2.3.14, the character group $\mathrm{Hom}(I_P, k(P)^*)$ is cyclic of order e_P and generated by the character χ_P which represents the I_P-action on $\mathfrak{m}_P/\mathfrak{m}_P^2$. Hence the one-dimensional $k(P)[I_P]$-modules are just the $(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}$ $(d=0,\dots,e_P-1)$. For every d, I_P acts on $(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}$ by χ_P^d and on its dual by χ_P^{-d}, so the dual of $(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}$ is $(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes(e_P-d)}$. Hence we have

$$[N^*_{G,X}] = \sum_{R\in Y}\frac{1}{f_{\tilde{R}}}\sum_{d=1}^{e_{\tilde{R}}-1}\frac{d}{e_{\tilde{R}}}[\mathrm{Ind}^G_{I_{\tilde{R}}}((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes(e_{\tilde{R}}-d)})]$$
$$= \sum_{R\in Y}\frac{1}{f_{\tilde{R}}}\sum_{d=1}^{e_{\tilde{R}}-1}\frac{e_{\tilde{R}}-d}{e_{\tilde{R}}}[\mathrm{Ind}^G_{I_{\tilde{R}}}((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes d})]$$
$$= \sum_{R\in Y}\frac{1}{f_{\tilde{R}}}\sum_{d=1}^{e_{\tilde{R}}-1}(1-\frac{d}{e_{\tilde{R}}})[\mathrm{Ind}^G_{I_{\tilde{R}}}((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes d})]$$
$$= \sum_{R\in Y}\frac{1}{f_{\tilde{R}}}\sum_{d=1}^{e_{\tilde{R}}-1}[\mathrm{Ind}^G_{I_{\tilde{R}}}((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes d})] + \sum_{R\in Y}\frac{1}{f_{\tilde{R}}}\sum_{d=1}^{e_{\tilde{R}}-1}\frac{-d}{e_{\tilde{R}}}[\mathrm{Ind}^G_{I_{\tilde{R}}}((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes d})].$$

For any $P\in|X|$, the representation $(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes 0}$ is the trivial one-dimensional $k(P)$-representation of I_P, or equivalently, a direct sum of

f_P copies of the one-dimensional $k(R)$-representation of I_P, where $R = \pi(P)$. So for any $R \in Y$, we have in $K_0(k[G])_{\mathbb{Q}}$:

$$[\mathrm{Ind}_{I_{\tilde{R}}}^G(k(R))] = \frac{1}{f_{\tilde{R}}}[\mathrm{Ind}_{I_{\tilde{R}}}^G(\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes 0}].$$

Hence we have

$$\begin{aligned}
&[N_{G,X}^*] + \sum_{R\in\pi(\mathcal{S})} [\mathrm{Ind}_{I_{\tilde{R}}}^G(k(R))] + [N_{G,X}] \\
&= \sum_{R\in Y} \frac{1}{f_{\tilde{R}}} \sum_{d=1}^{e_{\tilde{R}}-1} [\mathrm{Ind}_{I_{\tilde{R}}}^G((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes d})] + \sum_{R\in Y} \frac{1}{f_{\tilde{R}}} \sum_{d=1}^{e_{\tilde{R}}-1} \frac{-d}{e_{\tilde{R}}}[\mathrm{Ind}_{I_{\tilde{R}}}^G((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes d})] \\
&\quad + \sum_{R\in\pi(\mathcal{S})} \frac{1}{f_{\tilde{R}}}[\mathrm{Ind}_{I_{\tilde{R}}}^G((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes 0}) + \sum_{R\in Y} \frac{1}{f_{\tilde{R}}} \sum_{d=1}^{e_{\tilde{R}}-1} \frac{d}{e_{\tilde{R}}}[\mathrm{Ind}_{I_{\tilde{R}}}^G((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes d})] \\
&= \sum_{R\in\pi(\mathcal{S})} \frac{1}{f_{\tilde{R}}} \sum_{d=0}^{e_{\tilde{R}}-1} [\mathrm{Ind}_{I_{\tilde{R}}}^G((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes d})] = \sum_{R\in\pi(\mathcal{S})} \frac{1}{f_{\tilde{R}}}[\mathrm{Ind}_{I_{\tilde{R}}}^G(\bigoplus_{d=0}^{e_{\tilde{R}}-1}((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes d}))] \\
&= \sum_{R\in\pi(\mathcal{S})} \frac{1}{f_{\tilde{R}}}[\mathrm{Ind}_{I_{\tilde{R}}}^G(k(\tilde{R})[I_{\tilde{R}}])] = \sum_{R\in\pi(\mathcal{S})} \frac{1}{f_{\tilde{R}}}[k(\tilde{R})[G]] = \sum_{R\in\pi(\mathcal{S})} \frac{[k(\tilde{R}):k]}{f_{\tilde{R}}}[k[G]] \\
&\qquad = \sum_{R\in\pi(\mathcal{S})} [k(R):k][k[G]] = (\deg \Sigma_{\pi(\mathcal{S})})[k[G]],
\end{aligned}$$

where we have used that the sum of all irreducible representations of a finite group is the group ring. □

2.5 Some examples

The aim of this section is to give some examples to illustrate the results of the previous sections, in particular to apply the equivariant Riemann-Roch formulae from Theorem 2.3.18 and 2.4.15 and to give some idea of what the ramification module $N_{G,X}$ can look like.

We start with some examples where both X and Y are projective 1-space over some field whose characteristic does not divide the group order, so that we have a tamely ramified cover. Then we consider a class of examples that yields covers with weak ramification.

In most of the examples, we will use the fact that if $\deg D > 2g_X - 2$, then $H^1(X, \mathcal{L}(D))$ is trivial, which follows, for example, from Lemma 3.2.2.

2.5.1 C_3 acting on $\mathbb{P}^1_{\mathbb{C}}$

Let $X := \mathbb{P}^1_{\mathbb{C}}$, viewed as a curve over $k = \mathbb{C}$. Since $\mathbb{C}$ is algebraically closed, a point on X is $\mathbb{C}$-rational if and only if it is a closed point (cf. [Ha], Exercise II.2.15). We can identify the set of rational points on X with the Riemann Sphere or the set $\mathbb{C} \cup \infty$, as usual. The function field $K(X)$ of X is the field of rational functions in one variable, $\mathbb{C}(x)$, and the automorphisms of X over $\mathbb{C}$ are of the form $x \mapsto \frac{ax+b}{cx+d}$ with $a, b, c, d \in \mathbb{C}$. Let σ denote the automorphism given by $x \mapsto \frac{1}{1-x}$. Then σ generates a subgroup of order 3 of $\mathrm{Aut}(X/\mathbb{C})$, which we denote G. σ acts on the Riemann sphere with exactly two fixed points, $F_1 = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ and $F_2 = \frac{1}{2} - i\frac{\sqrt{3}}{2}$. All other points have orbits of length 3, e.g. 0 is mapped to 1, 1 to ∞ and ∞ to 0. Hence the cover $\pi : X \to X/G$ is (tamely) ramified at F_1 and F_2, with ramification index 3, and unramified everywhere else. By the classical Hurwitz formula (Corollary 2.4 in [Ha]), we have

$$-2 = 2g_X - 2 = 3 \cdot (2g_Y - 2) + \sum_{P \in X} (e_P - 1) = 3 \cdot (2g_Y - 2) + 4,$$

so $g_Y = 0$, i.e. $Y = \mathbb{P}^1_{\mathbb{C}}$.

Remark 2.5.1. One can show with a similar computation that for any cover $\pi : X \to Y = X/G$ as in the previous sections, then we have $g_X \geq g_Y$. In particular, if X is projective 1-space over a perfect field, then X/G also is projective 1-space over that field.

Let $\zeta_3 := -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, a primitive 3rd root of unity. Then G can act on $\mathbb{C}$ in three ways: Either G acts trivially, or $\sigma.z = \zeta_3 \cdot z$ for all $z \in \mathbb{C}$, or $\sigma.z = \zeta_3^2 \cdot z$ for all $z \in \mathbb{C}$. $\mathbb{C}$ with these G-actions will be denoted $\mathbb{C}_0$, $\mathbb{C}_1$, $\mathbb{C}_2$ respectively. The ramification module $N_{G,X}$ must satisfy equation (2.16), so we have

$$[N_{G,X}] = (1-g_Y)[\mathbb{C}[G]] - \chi(G, X, \mathcal{O}_X) = [\mathbb{C}[G]] - [H^0(X, \mathcal{O}_X)] + [H^1(X, \mathcal{O}_X)]$$

in $K_0(G, \mathbb{C})$, since $g_Y = 0$. $H^0(X, \mathcal{O}_X)$ is the set of holomorphic functions on X, so it consists only of the constant functions from X to $\mathbb{C}$; hence it is isomorphic to $\mathbb{C}_0$ as a $\mathbb{C}[G]$-module. Furthermore, since $\deg \mathcal{O}_X = 0 > 2g_X - 2$, $H^1(X, \mathcal{O}_X)$ vanishes. In other words, there are no holomorphic differentials on X. Hence we have

$$[N_{G,X}] = [\mathbb{C}[G]] - [\mathbb{C}_0] = [\mathbb{C}_1] + [\mathbb{C}_2],$$

using that $\mathbb{C}_0, \mathbb{C}_1, \mathbb{C}_2$ are exactly the one-dimensional representations of G, so that their sum is $\mathbb{C}[G]$.

Let now

$$D := [0] + [1] + [\infty],$$

then D is a G-equivariant divisor on X, with support disjoint from the ramification locus of π. The decomposition of the coefficients of $D = \sum_{P \in |X|} n_P P$ in the form $n_P = m_P e_P + l_P$ gives $l_P = 0$ for all $P \in X$, $m_P = 1$ if $P \in \{0, 1, \infty\}$ and $m_P = 0$ otherwise. By Theorem 2.4.15, we have

$$\chi(G, X, \mathcal{L}(D))$$
$$= -[N_{G,X}] + \sum_{R \in Y} \frac{1}{f_{\tilde{R}}} \sum_{d=1}^{l_{\tilde{R}}} [\mathrm{Ind}_{G_{\tilde{R}}}^{G}(\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)] + \left(1 - g_Y + \sum_{R \in Y} [k(R) : \mathbb{C}] m_{\tilde{R}}\right) [\mathbb{C}[G]].$$

The first sum over $R \in Y$ vanishes because $l_P = 0$ for all P. Since $g_Y = 0$ and since $\mathbb{C}$ is algebraically closed, whence $k(R) = \mathbb{C}$ for all $R \in Y$, we obtain

$$\chi(G, X, \mathcal{L}(D)) = -[N_{G,X}] + \left(1 + \sum_{R \in Y} m_{\tilde{R}}\right) [k[G]] = -[N_{G,X}] + 2[\mathbb{C}[G]],$$

since the only points on X where $m_P \neq 0$ are $0, 1$ and ∞, and they all map to one point $R \in Y$, for which $m_{\tilde{R}} = 1$.

As $\deg D > 2g - 2$, we have $H^1(X, \mathcal{L}(D)) = 0$, and using again that the sum of the one-dimensional representations of G is the group ring, the above yields

$$[H^0(X, \mathcal{L}(D))] = -[\mathbb{C}_1 \oplus \mathbb{C}_2] + 2[\mathbb{C}[G]] = [\mathbb{C}_0] + [\mathbb{C}[G]].$$

Indeed, $H^0(X, \mathcal{L}(\mathcal{D}))$ can be viewed as the set

$$\{f \in K(X) | \operatorname{ord}_P(f) + n_P \geq 0 \quad \text{for all} \quad P \in |X|\},$$

which is generated by the rational functions $1, x, \frac{1}{x-1}$ and $\frac{1}{x}$ as a vector space over $\mathbb{C}$, and on which σ acts by transforming the variable x:

$$\sigma.(f(x)) := f(\sigma^{-1}(x)).$$

The subspace generated by 1 is the space of constant functions, on which G acts trivially; the space spanned by the three other generators can be written as $\langle x, \frac{1}{1-x}, 1-\frac{1}{x}\rangle$, which shows that it is isomorphic to $\mathbb{C}[G]$ as a $\mathbb{C}[G]$-module.

2.5.2 C_3 acting on $\mathbb{P}^1_{\mathbb{R}}$

Let now $X = \mathbb{P}^1_{\mathbb{R}}$. The set of closed points of X can be identified with the compactified upper half plane

$$\bar{\mathbb{H}} := \mathbb{H} \cup \mathbb{R} \cup \{\infty\} = \{z \in \mathbb{C} : \Im z \geq 0\} \cup \{\infty\}.$$

In this model, the $\mathbb{R}$-rational points of $\mathbb{P}^1_{\mathbb{R}}$ correspond to the points of $\mathbb{R} \cup \{\infty\}$, whereas the non-rational closed points (which all have residue field $\mathbb{C}$) correspond to the points in $\mathbb{H}$. The function field of X is the field of rational functions in one variable over $\mathbb{R}$, $\mathbb{R}(x)$, and its automorphisms are of the form $x \mapsto \frac{ax+b}{cx+d}$ with $a, b, c, d \in \mathbb{R}$ and determinant $ad - bc > 0$. Hence the map $\sigma : x \mapsto \frac{1}{1-x}$ from above defines an automorphism of X. σ generates a subgroup of order 3 of $\mathrm{Aut}(X/\mathbb{R})$, which we denote G. Out of the two fixed points of σ on $\mathbb{C} \cup \{\infty\}$, only one lies in $\bar{\mathbb{H}}$, namely $F := F_1 = \frac{1}{2} + i\frac{\sqrt{3}}{2}$. Hence σ has exactly one fixed point on X; the orbits of all other points have length 3. The cover π is (tamely) ramified at F, with ramification index 3, and unramified everywhere else. The defining equation of $N_{G,X}$ (2.15) says that

$$\begin{aligned}\bigoplus^{3} N_{G,X} &= \bigoplus_{P\in X} \bigoplus_{d=1}^{e_P-1} \bigoplus^{d} \mathrm{Ind}_{I_P}^{G}((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}) = \bigoplus_{d=1}^{2} \bigoplus^{d} ((\mathfrak{m}_F/\mathfrak{m}_F^2)^{\otimes d}) \\ &= \mathfrak{m}_F/\mathfrak{m}_F^2 \oplus (\mathfrak{m}_F/\mathfrak{m}_F^2)^{\otimes 2} \oplus (\mathfrak{m}_F/\mathfrak{m}_F^2)^{\otimes 2}\end{aligned}$$

The cotangent space $\mathfrak{m}_F/\mathfrak{m}_F^2$ is one-dimensional over $k(F) = \mathbb{C}$ and carries a non-trivial G-action. Hence with the notations from Example 2.5.1, we have either $\mathfrak{m}_F/\mathfrak{m}_F^2 \cong \mathbb{C}_1$ and $(\mathfrak{m}_F/\mathfrak{m}_F^2)^{\otimes 2} \cong \mathbb{C}_2$ or vice versa. But $\mathbb{C}_1$ and $\mathbb{C}_2$ are isomorphic as $\mathbb{R}[G]$-modules, since complex conjugation yields an isomorphism between them (note that this is not an isomorphism of $\mathbb{C}$-vector spaces!). Hence the above can be rewritten as

$$\bigoplus^3 N_{G,X} \cong \bigoplus^3 \mathbb{C}_1,$$

so

$$N_{G,X} \cong \mathbb{C}_1.$$

This gives an easy example of the fact that $N_{G,X} \otimes_{\mathbb{R}} \mathbb{C} = N_{G,\tilde{X}}$, shown in the proof of Theorem 2.4.11.

Let now $D = [0] + [1] + [\infty]$ as in the previous example. Theorem 2.4.15 yields

$$\begin{aligned}&\chi(G, X, \mathcal{L}(D))\\ &= -[N_{G,X}] + \sum_{R \in Y} \sum_{d=1}^{l_{\tilde{R}}} [\mathrm{Ind}_{G_{\tilde{R}}}^{G}(\mathfrak{m}_P/\mathfrak{m}_P^2)] + \left(1 - g_Y + \sum_{R \in Y} [k(R):\mathbb{R}] m_{\tilde{R}}\right)[\mathbb{R}[G]]\end{aligned}$$

In analogy to the previous example, we have $l_P = 0$ for all $P \in |X|$, $m_P = 1$ for $P = 0, 1, \infty$ and $m_P = 0$ everywhere else. Furthermore, $H^1(X, \mathcal{L}(D))$ vanishes, since $\deg D > 2g - 2$. Hence we have

$$[H^0(X, \mathcal{L}(D))] = -[\mathbb{C}_1] + 2[\mathbb{R}[G]] = [\mathbb{C}_1] + 2[\mathbb{R}[G]] = [\mathbb{R}] + [\mathbb{R}[G]].$$

Indeed, as above, $H^0(X, \mathcal{L}(D))$ is generated by $1, x, 1-x$ and $\frac{1}{1-x}$ over $\mathbb{R}$ and thus decomposes into the trivial representation $\langle 1 \rangle$ and the regular representation $\langle x, 1-x, \frac{1}{1-x} \rangle = \langle x, \frac{1}{1-x}, 1 - \frac{1}{x} \rangle$.

2.5.3 S_3 acting on $\mathbb{P}^1_{\mathbb{C}}$

As in Subsection 2.5.1, let $X = \mathbb{P}^1_{\mathbb{C}}$ and $\sigma(x) := \frac{1}{1-x}$. Furthermore, let $\tau(x) := \frac{1}{x}$. Then σ and τ are Möbius transformations (i.e. automorphisms of $\mathbb{P}^1_{\mathbb{C}}$) of order 3 and 2 respectively. An easy calculation shows that the group generated by σ and τ contains exactly the following elements.

$$\begin{aligned}&\mathrm{id} = \sigma^3 = \tau^2,\\ &\sigma(x) &&= \tfrac{1}{1-x},\\ &\sigma^2(x) &&= 1 - \tfrac{1}{x},\\ &\tau(x) &&= \tfrac{1}{x},\\ &\sigma\tau(x) &&= 1 - \tfrac{1}{1-x} = \tau\sigma^2(x)\\ &\sigma^2\tau(x) &&= 1 - x = \tau\sigma(x).\end{aligned}$$

Hence a presentation of $G := \langle \sigma, \tau \rangle$ is given by

$$G := \langle \sigma, \tau \rangle \cong \langle s, t | s^3 = t^2 = 1, s^2 t = ts \rangle.$$

This is is the presentation of the dihedral group D_3, which is also isomorphic to the symmetric group S_3.

By the *natural permutation representation* of S_3 we shall mean the representation which consists of three copies of $\mathbb{C}$ that are permuted by S_3 just like S_3 permutes the numbers 1, 2, 3. The natural permutation representation is reducible; namely, it decomposes into a trivial representation (generated by $(1,1,1)^T$) and a two-dimensional irreducible complement.

The irreducible representations of S_3 are:

- The trivial one-dimensional representation, which we will denote $\mathbb{C}$.
- The sign representation: one-dimensional, σ acts trivially and τ acts by multiplication with -1.
- The non-trivial part of the natural permutation representation (two-dimensional), which will be denoted U.

The following points on $X = \mathbb{P}^1_{\mathbb{C}}$ have nontrivial decomposition group (i.e. they are fixed by some nontrivial element of G).

P_1	$:= \frac{1}{2} + i\frac{\sqrt{3}}{2}$	is fixed by	σ and σ^2
P_2	$:= \frac{1}{2} - i\frac{\sqrt{3}}{2}$	is fixed by	σ and σ^2
P_3	$:= 1$	is fixed by	τ
P_4	$:= -1$	is fixed by	τ
P_5	$:= 0$	is fixed by	$\sigma\tau$
P_6	$:= 2$	is fixed by	$\sigma\tau$
P_7	$:= \frac{1}{2}$	is fixed by	$\sigma^2\tau$
P_8	$:= \infty$	is fixed by	$\sigma^2\tau$

Since $\mathbb{C}$ is algebraically closed, we must have $f_{P_i} = 1$ for all i. Therefore we have $I_{P_i} \cong C_3$ for $i = 1, 2$ and $I_{P_i} \cong C_2$ for $i = 3, \ldots, 8$, and the ramification index at P_i is 3 for $i = 1, 2$ and 2 for $i = 3, \ldots, 8$.

By Remark 2.5.1, the quotient curve Y is again the Riemann sphere.

Let us now compute the ramification module $N_{G,X}$. By definition, we have in the Grothendieck group $K_0(\mathbb{C}[G])$:

$$
\begin{aligned}
[N_{G,X}] &= \frac{1}{n}\sum_{P\in|X|}\sum_{d=1}^{e_P-1} d\ \mathrm{Ind}_{I_P}^{G}(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d} \\
&= \frac{1}{6}\Big([\mathrm{Ind}_{C_3}^{G}(\mathfrak{m}_{P_1}/\mathfrak{m}_{P_1}^2)] + 2[\mathrm{Ind}_{C_3}^{G}(\mathfrak{m}_{P_1}/\mathfrak{m}_{P_1}^2)^{\otimes 2}] \\
&\quad + [\mathrm{Ind}_{C_3}^{G}(\mathfrak{m}_{P_2}/\mathfrak{m}_{P_2}^2)] + 2[\mathrm{Ind}_{C_3}^{G}(\mathfrak{m}_{P_2}/\mathfrak{m}_{P_2}^2)^{\otimes 2}] \\
&\quad + \sum_{i=3}^{8}[\mathrm{Ind}_{C_2}^{G}(\mathfrak{m}_{P_i}/\mathfrak{m}_{P_i}^2)] \Big).
\end{aligned}
$$

Let $W_{1,2}$ denote the two different nontrivial one-dimensional $\mathbb{C}$-representations of C_3, and let V denote the unique nontrivial one-dimensional $\mathbb{C}$-representation of C_2.
As in Subsection 2.5.1, the cotangent spaces at the complex conjugates P_1 and P_2 are isomorphic to W_1 and W_2, respectively. Furthermore, the cotangent spaces at the other ramification points are nontrivial one-dimensional representations of C_2, so they are all isomorphic to V. Therefore we get

$$
\begin{aligned}
[N_{G,X}] &= \frac{1}{6}\Big([\mathrm{Ind}_{C_3}^{G}(W_1)] + 2[\mathrm{Ind}_{C_3}^{G}(W_2)] + [\mathrm{Ind}_{C_3}^{G}(W_2)] \\
&\quad + 2[\mathrm{Ind}_{C_3}^{G}(W_1)] + \sum_{i=3}^{8}[\mathrm{Ind}_{C_2}^{G}(V)] \Big) \\
&= \frac{1}{2}\Big([\mathrm{Ind}_{C_3}^{G}(W_1)] + [\mathrm{Ind}_{C_3}^{G}(W_2)] \Big) + [\mathrm{Ind}_{C_2}^{G}(V)].
\end{aligned}
$$

The following lemma explains how $N_{G,X}$ can be expressed without fractions, and in terms of the irreducible representations of G.

Lemma 2.5.2. *We have the following isomorphisms of $\mathbb{C}[G]$-modules.*

(a)

$$\mathrm{Ind}_{C_2}^{G}(V) \cong \mathrm{sign} \oplus \mathrm{U}$$

(b)

$$\mathrm{Ind}_{C_3}^{G}(W_1) \cong \mathrm{Ind}_{C_3}^{G}(W_2) \cong U.$$

Proof. By definition, $\mathrm{Ind}_{C_2}^G(V) = V \otimes_{\mathbb{C}[C_2]} \mathbb{C}[G]$ is a three dimensional complex vector space with basis indexed by the cosets $\{[\mathrm{id}], [\sigma], [\sigma^2]\}$ modulo C_2. σ acts on this space by cyclically permuting the coordinates. τ acts on the first coordinate, $[\mathrm{id}]$, by multiplication with -1, as it does on V. However, τ must permute the other two coordinates in order to make the action compatible with the relations in G. Therefore we have with respect to the above basis:

$$\sigma, \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} y \\ z \\ x \end{pmatrix}, \quad \tau. \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -x \\ -z \\ -y \end{pmatrix}.$$

The subspace generated by the vector $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ is obviously G-invariant and isomorphic to the sign representation. Its complement is the 2-dimensional space

$$\{\begin{pmatrix} x \\ y \\ z \end{pmatrix} | x + y + z = 0\}$$

with G-action given by

$$\sigma, \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} y \\ z \\ x \end{pmatrix}, \quad \tau. \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ z \\ y \end{pmatrix};$$

which is isomorphic to U.

Hence part (a) is shown.

In part (b), the induced representation $\mathrm{Ind}_{C_3}^G(W_1)$ is two-dimensional, with basis indexed $[id], [\tau]$. τ permutes the two coordinates, and σ acts on the first coordinate by multiplication with a nontrivial third root of unity, which we denote ζ_3. Hence we have, with respect to the above basis:

$$\sigma. \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \zeta_3 x \\ a \end{pmatrix}, \sigma^2. \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \zeta_3^2 x \\ b \end{pmatrix}, \tau. \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix}$$

where a, b are linear functions of x, y yet to be determined.

The relations in G mean that we must have

$$\tau\sigma. \begin{pmatrix} x \\ y \end{pmatrix} = \sigma^2\tau. \begin{pmatrix} x \\ y \end{pmatrix},$$

i.e.

$$\begin{pmatrix} a \\ \zeta_3 x \end{pmatrix} = \begin{pmatrix} \zeta_3^2 y \\ b \end{pmatrix}$$

and thus

$$a = \zeta_3^2 y, \quad b = \zeta^3 x.$$

Hence the induced representation is given by

$$\sigma.\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \zeta_3 x \\ \zeta_3^2 y \end{pmatrix}, \sigma^2.\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \zeta_3^2 x \\ \zeta_3 y \end{pmatrix}, \tau.\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix}$$

The map

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y \\ x \end{pmatrix}$$

gives an isomorphism between $\mathrm{Ind}_{C_3}^G(W_1)$ and $\mathrm{Ind}_{C_3}^G(W_2)$. Furthermore, the above description of the group action makes it easy to see that $\mathrm{Ind}_{C_3}^G(W_1)$ is isomorphic to U.

□

It follows that

$$N_{G,X} \cong \text{sign} \oplus \mathrm{U} \oplus \mathrm{U}.$$

We can verify the equivariant Hurwitz formula:
Since the group ring is the sum of all irreducible representations V with multiplicity $\dim V$, we have

$$\mathbb{C}[G] = \mathbb{C} \oplus \text{sign} \oplus \mathrm{U} \oplus \mathrm{U}$$

and hence

$$[N_{G,X}] = [\text{sign} \oplus \mathrm{U} \oplus \mathrm{U}] = [\mathbb{C}[\mathrm{G}]] - [\mathbb{C}] = (1 - \mathrm{g_Y})[\mathbb{C}[\mathrm{G}]] - \chi(\mathrm{G}, \mathrm{X}, \mathcal{O}_\mathrm{X}).$$

Of course we could also have used the equivariant Hurwitz formula to determine $N_{G,X}$ more quickly.
Let us now look at the divisor from Subsection 2.5.1,

$$D := [0] + [1] + [\infty].$$

D is G-equivariant as 0, 1, ∞ form a single G-orbit. If we make the decomposition

$$n_P = e_P m_P + l_P$$

as in Theorem 2.4.15, we get $m_P = 0$ for all P, $l_P = 1$ if $P \in \{0, 1, \infty\}$ and $l_P = 0$ otherwise. Hence Theorem 2.4.15 yields

$$\begin{aligned}
&\chi(G,X,\mathcal{L}(D)) \\
&\quad = -[N_{G,X}] + \sum_{R \in |Y|} \sum_{d=1}^{l_{\tilde{R}}} [\mathrm{Ind}_{I_{\tilde{R}}}^{G}(\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes(-d)}] + (1 - g_Y + \deg D_1)[\mathbb{C}[G]] \\
&\quad = -([\mathbb{C}[G]] - [\mathbb{C}]) + [\mathrm{Ind}_{I_0}^{G}(\mathfrak{m}_0/\mathfrak{m}_0^2)^{\otimes(-1)}] + [\mathbb{C}[G]] \\
&\quad = [\mathbb{C}] + [\mathrm{Ind}_{I_{P_5}}^{G}(\mathfrak{m}_{P_5}/\mathfrak{m}_{P_5}^2)^{\otimes(-1)}] \\
&\quad = [\mathbb{C}] + [\mathrm{Ind}_{C_2}^{G}(V)] \\
&\quad = [\mathbb{C}] + [\mathrm{sign}] + [\mathrm{U}]
\end{aligned}$$

with the notations U, V from above.

To verify this, we first note that as in Subsection 2.5.1, we have $\chi(G,X,\mathcal{L}(D)) = [H^0(X,\mathcal{L}(D))]$, and the latter is a complex vector space generated by the functions $1, x, \frac{1}{x}, \frac{1}{1-x}$. With respect to this basis of $H^0(X,\mathcal{L}(D)$, the generators of G have the following matrix representations:

$$\sigma \hat{=} S := \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \quad \tau \hat{=} T := \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Let now

$$f(x) := x + \sigma.x + \sigma^2.x = x + (1 - \frac{1}{x}) + \frac{1}{1-x},$$

and let

$$g(x) := \tau.f(x)$$

Then $f(x) - g(x)$ is invariant under σ, and $\tau.(f(x) - g(x)) = g(x) - f(x)$. Hence, $f(x) - g(x)$ generates a copy of the sign representation.

With respect to the basis chosen above, we have

$$f(x) \hat{=} \begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \end{pmatrix}, \quad g(x) \hat{=} T \begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \quad f(x) - g(x) \hat{=} \begin{pmatrix} -1 \\ 2 \\ -2 \\ 2 \end{pmatrix}.$$

Now we need to find a complement to $\langle \begin{pmatrix} -1 \\ 2 \\ -2 \\ 2 \end{pmatrix} \rangle$ that is isomorphic to the natural permutation representation of G. A necessary condition for this is that some vector $\mathbf{v}$ in this complement has to have the same image under σ and τ, and that this image is linearly independent of $\mathbf{v}$. Hence we solve the linear system of equations

$$(S-T)\mathbf{v} = 0.$$

The space of solutions of this system of equations is spanned by $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$, so we take $\mathbf{v} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$.

Next we put $\mathbf{v}' := S\mathbf{v} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ -1 \end{pmatrix}$ and $\mathbf{v}'' := S^2\mathbf{v} = \begin{pmatrix} 2 \\ -1 \\ -1 \\ 0 \end{pmatrix}$.

We see that σ permutes these three vectors cyclically, whilst τ swaps $\mathbf{v}$ and $\mathbf{v}'$ but leaves $\mathbf{v}''$ invariant. Hence $\mathbf{v}$, $\mathbf{v}'$ and $\mathbf{v}''$ generate the natural permutation representation. The trivial representation that it contains is recovered by considering the subspace generated by $\mathbf{v} + \mathbf{v}' + \mathbf{v}'' = \begin{pmatrix} 3 \\ 0 \\ 0 \\ 0 \end{pmatrix}$.

Furthermore, if we add the vector $\begin{pmatrix} -1 \\ 2 \\ -2 \\ 2 \end{pmatrix}$ to the collection then we obtain a linearly independent set, which therefore is a full basis of $H^0(X, \mathcal{L}(D))$:

$$H^0(X, \mathcal{L}(D)) = \langle \begin{pmatrix} -1 \\ 2 \\ -2 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ -1 \\ -1 \\ 0 \end{pmatrix} \rangle.$$

2.5.4 S_3 acting on $\mathbb{P}^1_{\mathbb{F}_5}$

Let now $X := \mathbb{P}^1_{\mathbb{F}_5}$. The function field of X is the field $\mathbb{F}_5(x)$ of rational functions over $\mathbb{F}_5$, and the automorphisms of X over $\mathbb{F}_5$ (resp. of its function field) are the maps $x \mapsto \frac{ax+b}{cx+d}$ with coefficients in $\mathbb{F}_5$. Hence the assignments $\sigma(z) = \frac{1}{1-z}$, $\tau(z) = \frac{1}{z}$ from the previous subsection define automorphisms of X, and they generate a subgroup G of $\mathrm{Aut}(X/\mathbb{F}_5)$ that is isomorphic to $D_3 \cong S_3$.

Note that $\mathbb{F}_5$ is not large enough with respect to this group, because it does not contain any nontrivial third roots of unity. Here a field k is called *large enough* with respect to a group G if k contains the m-th roots of unity, where m is the p-primary part of the least common multiple of the orders of elements in G.

The quadratic extension $\mathbb{F}_5(\sqrt{3})$ is large enough with respect to S_3, since the nontrivial third roots of unity are $\zeta_3 = 2 + \sqrt{3}$ and $\zeta_3^2 = 2 - \sqrt{3}$. Because it is large enough, the irreducible $\mathbb{F}_5(\sqrt{3})$-representations of the abelian subgroup C_3 are all one-dimensional; we call them $\mathbb{F}_5(\sqrt{3})$, W_1 and W_2.

When viewed as $\mathbb{F}_5$-representations of C_3, W_1 and W_2 are still irreducible, and they are isomorphic as $\mathbb{F}_5$-representations. (Cf. the analogous situation over $\mathbb{R}$, $\mathbb{C}$ respectively in Subsection 2.5.2.)

$\mathbb{F}_5$ is large enough with respect to the subgroup C_2, and therefore there is a nontrivial one-dimensional $\mathbb{F}_5$-representation of C_2, which we denote V.

The irreducible representations of G over $\mathbb{F}_5$ are essentially the same as over $\mathbb{C}$ – the trivial representation, simply denoted $\mathbb{F}_5$, the sign representation, and the nontrivial part of the natural permutation representation, denoted U.

All rational points of X have a nontrivial decomposition group:

P_1	$:= 1$	is fixed by	τ
P_2	$:= 4$	is fixed by	τ
P_3	$:= 0$	is fixed by	$\sigma\tau$
P_4	$:= 2$	is fixed by	$\sigma\tau$
P_5	$:= 3$	is fixed by	$\sigma^2\tau$
P_6	$:= \infty$	is fixed by	$\sigma^2\tau$

The automorphism σ has exactly one fixed point on X, namely the non-rational point corresponding to $3 \pm \sqrt{3}$, with residue field $\mathbb{F}_5(\sqrt{3})$. We call this point P_7.

For combinatorial reasons, we must have $f_{P_i} = 1$ for all i, i.e. the decomposition group is always equal to the inertia group. Therefore we have $I_{P_i} \cong C_2$ for $i = 1, \ldots, 6$ and $I_{P_7} \cong C_3$. The ramification index at P_i is 2 for $i = 1, \ldots, 6$ and the ramification index at P_7 is 3.

The classical Hurwitz formula yields that $Y = X/G$ is another copy of $\mathbb{P}^1_{\mathbb{F}_5}$.

Let us now compute $N_{G,X}$. By definition, we have

$$\begin{aligned}
[N_{G,X}] &= \frac{1}{n} \sum_{P \in |X|} \sum_{d=1}^{e_P - 1} d\,[\mathrm{Ind}_{I_P}^G (\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}] \\
&= \frac{1}{6} \Big(\sum_{i=1}^{6} [\mathrm{Ind}_{C_2}^G(V)] + [\mathrm{Ind}_{C_3}^G(W_1)] + 2[\mathrm{Ind}_{C_3}^G(W_2)] \Big)
\end{aligned}$$

,

where V denotes the nontrivial one-dimensional $\mathbb{F}_5$-representation of C_2, and $W_{1,2}$ denote the nontrivial one-dimensional $\mathbb{F}_5(\sqrt{3})$-representations of C_3, viewed as two-dimensional $\mathbb{F}_5$-representations.

The analogue of Lemma 2.5.2 yields that $\mathrm{Ind}_{C_3}^G(W_1)$ is the irreducible 2-dimensional $\mathbb{F}_5(\sqrt{3})$-representation of G. As an $\mathbb{F}_5$-representation, it is therefore isomorphic to two copies of the irreducible two-dimensional $\mathbb{F}_5$-representation U of G.

Furthermore, an analogue of Lemma 2.5.2(a) even holds over $\mathbb{F}_5$, since $\mathbb{F}_5$ is large enough for C_2. This yields

$$\mathrm{Ind}_{C_2}^G(V) \cong \mathrm{sign} \oplus \mathrm{U}$$

with the notations from Subsection 2.5.3.

Hence we can write

$$\begin{aligned}
[N_{G,X}] &= \frac{1}{6}\ \big(\sum_{i=1}^{6}[\mathrm{Ind}_{C_2}^{G}(V)] + [\mathrm{Ind}_{C_3}^{G}(W_1)] + 2[\mathrm{Ind}_{C_3}^{G}(W_2)]\ \big)\\
&= \frac{1}{6}\ \big(\sum_{i=1}^{6}[\mathrm{Ind}_{C_2}^{G}(V)] + 3[\mathrm{Ind}_{C_3}^{G}(W_1)]\ \big)\\
&= \ [\mathrm{Ind}_{C_2}^{G}(V)] + \frac{1}{2}[\mathrm{Ind}_{C_3}^{G}(W_1)]\\
&= \ [\mathrm{sign} \oplus \mathrm{U}] + \frac{1}{2}[\mathrm{U} \oplus \mathrm{U}]\\
&= \ [\mathrm{sign}] + 2[\mathrm{U}].
\end{aligned}$$

This is the same expression as in the example over $\mathbb{C}$, and we can verify the equivariant Hurwitz formula in the same way.

Let us now look at the divisor from the previous subsections,

$$D = [0] + [1] + [\infty].$$

With exactly the same calculation as before, we get

$$\chi(G, X, \mathcal{L}(D)) = [\mathbb{F}_5] + [\mathrm{sign}] + [\mathrm{U}]$$

This can be verified exactly like in the previous subsection.

2.5.5 Artin-Schreier curves

Example 2.5 in Köck's paper [Kö2], which had also been mentioned by Hasse [Has], shows how to construct classes of covers of curves with arbitrarily wild ramification. It goes as follows.

Let k be a perfect field of positive characteristic p, and let $r \in N$ be coprime to p. Let $k(x,y)$ be the field extension of the rational function field $k(x)$ given by the Artin-Schreier equation $y^p - y = x^r$. The field extension $k(x,y)/k(x)$ is Galois with group $G = C_p$, the cyclic group with p elements. Let $\pi : X \to \mathbb{P}_k^1$ denote the corresponding cover of nonsingular algebraic curves. Then π is unramified precisely over $\mathbb{A}_k^1 \subseteq \mathbb{P}_k^1$, and at the unique point $\infty \in X$ lying over $\infty \in \mathbb{P}_k^1$, the higher ramification group $G_{\infty,s}$ are trivial for $s > r$ but nontrivial (cyclic of order p) for $s \leq r$. Furthermore, the genus of X is equal to $\frac{(r-1)(p-1)}{2}$. .

In particular, for $r = 1$ the cover is weakly ramified, but not tamely ramified. At the point at infinity, the ramification index is $e_P = p$, the tame ramification index is $e_P^t = 1$, and the weak ramification index is $e_P^w = p$. The ramification module $N_{G,X}$ is defined by

$$\bigoplus^{n} N_{G,X} \cong \bigoplus_{P\in X} \bigoplus_{d=1}^{e_P^t-1} \bigoplus^{e_P^w \cdot d} \mathrm{Ind}_{I_P}^G(\mathrm{Cov}((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d})).$$

Since $e_P^t = 1$ for all P (even for the point at infinity), the sums in the formula all vanish, so

$$N_{G,X} = 0.$$

Let now D be the equivariant divisor

$$D = (p-1)[\infty]$$

on X. Then D satisfies the condition $n_P \equiv e_P^w - 1$ for all $P \in X$. Hence we can apply Theorem 2.4.15. If we make the decomposition

$$n_P = (e_P^w - 1) + (l_P + m_P e_P^t) e_P^w$$

with $l_P \in \{0, \ldots, e_P^t - 1\}$ and $m_P \in \mathbb{Z}$, we get $l_P = m_P = 0$ everywhere (even at the point at infinity).Therefore we obtain in $K_0(k[G])$:

$$\begin{aligned}
&\chi(G, X, \mathcal{L}(D)) \\
&= -[N_{G,X}] + \sum_{R\in Y} \sum_{d=1}^{l_{\tilde{R}}} [\mathrm{Ind}_{G_{\tilde{R}}}^G(W_{\tilde{R},d})] + \Big(1 - g_Y + \sum_{R\in Y} [k(R) : k] m_{\tilde{R}}\Big) [k[G]] \\
&= 0 + 0 + (1 - g_Y + 0)[k[G]] \\
&= [k[G]]
\end{aligned}$$

Since the genus of X is $\frac{(r-1)(p-1)}{2} = 0$, we have $\deg D > 2g_X - 2$ and hence $H^1(X, \mathcal{L}(D)) = \{0\}$. Furthermore, the above calculation was done in the Grothendieck group of projective modules, so it yields an isomorphism of $k[G]$-modules

$$H^0(X, \mathcal{L}(D)) \cong k[G].$$

Indeed, we have

$$H^0(X, \mathcal{L}(D)) = \langle 1, y, \ldots, y^{p-1} \rangle \cong k[G].$$

Chapter 3

On the automorphism group of geometric Goppa codes

3.1 What is Coding Theory?

If a message is to be sent over a distance, then there are two major problems one has to deal with. Firstly, the message could be read by an unauthorized third party while it is on its way. Secondly, one can never fully avoid transmission errors caused by technical unreliability, however optimized the transmission procedure may be.

The first problem is a main subject in *Cryptography*, whilst *Coding Theory* tackles the second problem.

The message is normally represented as a binary sequence rather than as a sequence of characters A-Z. In the encoding process, this binary sequence is split up into small parts of equal length, say m. Every m-tuple is then substituted by a longer tuple (say, an n-tuple), so that the message becomes longer without gaining more content. This redundancy is what we need in order to recognize and correct possible transmission errors.

The n-tuples that the encoded message consists of are called *codewords*; the ensemble of codewords is called the *code*. The codewords can be binary n-tuples, or they can be n-tuples over some finite field other than $\mathbb{F}_2$. The number n is called the *length* of the code.

If transmission errors occur in the process of sending the encoded message, these errors are unlikely to turn a codeword into a different codeword, but will in general produce an n-tuple that is not a codeword. Hence we can recognize that an error has occurred. By looking for the codeword which is "closest" to the n-tuple received, we can even correct the error. How well this works is largely determined by the choice of the code, which is why a big part of Coding Theory just deals with the problem of finding "good" codes.

Example 3.1.1. We assume that the message is given as a binary sequence. We split the sequence up into binary pairs (in the terminology above, this means $m = 2$) and substitute every pair by a binary 4-tuple (i.e. $n = 4$) according to the following rules:

$$\begin{aligned} 00 &\to 0000 \\ 01 &\to 0111 \\ 10 &\to 1001 \\ 11 &\to 1110 \end{aligned}$$

We will now be able to recognize errors as long as they flip no more than one bit per 4-tuple, but we will not always be able to correct them; e.g.:

- tuple received: *1100* $\to$ closest codeword: *1110* $\to$ correction to 1110 and decoding to 11.
- tuple received: 1111 $\to$ there are two closest codewords, 1110 and 0111; error is recognized but cannot be corrected.

In the second case, the correction of the error is not possible because we have two codewords that are too close together (namely 1110 and 0111). Note that this is a property of the code, not of the encoding procedure.

3.2 Geometric Goppa codes

By what we said in the last section, a *code* is just an arbitrary set of n-tuples over some finite field, i.e. a subset of $\mathbb{F}_q^n$ for some prime power q. Now we will look at codes that are vector spaces over $\mathbb{F}_q$, i.e. sub-vector spaces of $\mathbb{F}_q^n$. Such codes are called *linear codes.*

Geometric Goppa codes are linear codes which are constructed from divisors on algebraic curves. Some of them have very good properties, and the rich structure of the underlying curves makes it possible to investigate them thoroughly. We will now describe how geometric Goppa codes are constructed.

Let X be a geometrically irreducible, nonsingular projective curve of genus g over a finite field $\mathbb{F}_q$. Let $|X|$ denote the set of closed points of X, and let $X(\mathbb{F}_q) := \{P \in X : k(P) \cong \mathbb{F}_q\}$, the set of $\mathbb{F}_q$-rational points on X. (This set is in 1-1 correspondence with the set $\mathrm{Mor}_{\mathbb{F}_q}(\mathrm{Spec}\,\mathbb{F}_q, X)$ which we called $X(\mathbb{F}_q)$ in Chapter 2.) Assume that $X(\mathbb{F}_q)$ is nonempty, i.e. that X has rational points. Let $D = \sum_{P \in |X|} n_P P$ be a divisor on X, and let

$$E := P_1 + \ldots + P_n$$

where the P_i are distinct points in $X(\mathbb{F}_q) \setminus \mathrm{Supp}\, D$. In particular, n must be less than or equal to the number of rational points of X.

Following the conventions used in the existing literature on Coding Theory (e.g. [HvLP]), the 0-th cohomology group $H^0(X, \mathcal{O}_X(D)$ shall be called the *Riemann-Roch space* of the divisor D and denoted $L(D)$. Recall that $L(D)$ can be defined as follows:

$$L(D) := \{f \in K(X) | v_P(f) \geq -n_P \text{ for all } P \in X\}$$

Here $K(X)$ denotes the function field of X, and $v_P(f)$ denotes the order of f at P.

The elements of $L(D)$ have poles at most at those points P where $n_P > 0$. Since $\mathrm{Supp}\, E \cap \mathrm{Supp}\, D = \emptyset$, they do not have any poles at the points $P_1, \ldots, P_n$. Furthermore, since $P_1, \ldots, P_n$ are $\mathbb{F}_q$-rational points, they actually take values in $\mathbb{F}_q$ at these points. Hence we have a well-defined homomorphism

$$L(D) \to \mathrm{Maps}(\mathrm{Supp}\, E, \mathbb{F}_q).$$

Composing this with the natural isomorphism

$$\mathrm{Maps}(\mathrm{Supp}\, E, \mathbb{F}_q) \xrightarrow{\sim} \mathbb{F}_q^n$$

gives rise to another evaluation map

$$\mathrm{ev}_{D,E} : L(D) \to \mathbb{F}_q^n, f \mapsto (f(P_1), \ldots, f(P_n)),$$

which is again a homomorphism of vector spaces over $\mathbb{F}_q$.

We now define the *geometric Goppa code* $C(D, E)$ to be the image of this second evaluation map,

$$C(D, E) := \operatorname{im} \mathrm{ev}_{D,E}\,.$$

Lemma 3.2.1 ([Ha]; [HvLP]). *If* $n > \deg D$, *then* $\mathrm{ev}_{D,E}$ *is injective.*

Proof. Assume $n > \deg D$. Let $f \in L(D)$ such that $\mathrm{ev}_{D,E}(f) = 0$. This means $f(P_i) = 0$ for $i = 1, \ldots, n$, i.e. the order of f at P_i is positive. Since the divisors D and E have disjoint supports, this implies that f is an element of the Riemann-Roch space $L(D - E)$. On the other hand, we have $\deg(D - E) = \deg D - \deg E = \deg D - n < 0$, and hence $L(D - E) = \{0\}$ by lemma 3.2.2 below. Thus, we have $f = 0$. □

Lemma 3.2.2 ([HvLP]). *Let* A *be a divisor on* X. *If* $\deg A < 0$, *then* $L(A) = \{0\}$.

Proof. Suppose there was an element $f \in L(A) \setminus \{0\}$. Then by definition, $(f) + A \succeq 0$, and hence $\deg((f) + A) \geq 0$. On the other hand, we have $\deg((f) + A) = \deg(f) + \deg A = 0 + \deg A < 0$, which is a contradiction. □

It follows from Lemma 3.2.1 and from the definition of $C(D, E)$ that $C(D, E)$ is isomorphic to the Riemann-Roch space $L(D)$ if $n > \deg D$. Then we can use the classical Riemann-Roch theorem to compute the dimension of the code, which is an important parameter if it comes to measuring the quality of a linear code. In particular, if $n > \deg D > 2g - 2$, and if K denotes the canonical divisor on X, then we have $\deg(K - D) = 2g - 2 - \deg D < 0$, so $L(K - D)$ vanishes by Lemma 3.2.2, and hence the Riemann-Roch theorem yields

$$\dim C(D, E) = \dim L(D) = \deg D + 1 - g.$$

3.3 Faithful group actions on Riemann-Roch spaces

Let X be an algebraic curve as before, and let $G \leq \mathrm{Aut}(X/\mathbb{F}_q)$ be a finite group of automorphisms of X. Assume that the canonical projection $\pi : X \to Y := X/G$ is tamely ramified.

Since every automorphism of X over $\mathbb{F}_q$ induces an automorphism of the function field $K(X)$ fixing $\mathbb{F}_q$, G can also be viewed as a subgroup of $\mathrm{Aut}(K(X)/\mathbb{F}_q)$. If the elements of $K(X)$ are considered as functions from X to $\mathbb{P}^1_{\mathbb{F}_q}$, then the action of G can be written in the following way:

$$(\sigma.f)(P) = f(\sigma^{-1}(P)) \quad (\sigma \in G, f \in K(X), P \in X).$$

If D is a G-*equivariant* divisor, then $L(D)$ is stable under the action of G on $K(X)$. The group action we get in this way is the same that we obtained in a more abstract way in Chapter 2.

We can use the strong equivariant Riemann-Roch formula, Theorem 2.4.15, to describe the isomorphism class of $L(D)$ as an $\mathbb{F}_q$-representation of G. Since all finite algebraic extensions of a finite field are cyclic and hence abelian, we can apply Proposition 2.4.16 on the structure of the spaces $W_{P,d}$ and get the following refined formula.

Theorem 3.3.1. *Let $D = \sum_{P\in|X|} n_P P$ be a G-equivariant divisor on X. For any $P \in X$, we write*

$$n_P = l_P + m_P e_P$$

with $l_P \in \{0,\dots,e_P-1\}$ and $m_P \in \mathbb{Z}$. Furthermore, for any $R \in Y$, fix a point $\tilde{R} \in \pi^{-1}(R)$. Then we have in $K_0(\mathbb{F}_q[G])$:

$$\begin{aligned}&\chi(G, X, \mathcal{L}(D))\\ &= -[N_{G,X}] + \sum_{R\in Y}\sum_{d=1}^{l_{\tilde{R}}}[\mathrm{Ind}^G_{G_{\tilde{R}}}((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}^2_{\tilde{R}})^{\otimes e_P - d})] + \Big(1 - g_Y + \sum_{R\in Y}[k(R):\mathbb{F}_q] m_{\tilde{R}}\Big)[\mathbb{F}_q[G]],\end{aligned} \tag{3.1}$$

where $N_{G,X}$ is a projective $\mathbb{F}_q[G]$-module satisfying

$$\bigoplus^{|G|}[N_{G,X}] = \bigoplus_{P\in X}\bigoplus_{d=1}^{e_P-1}\bigoplus^{d}\mathrm{Ind}^G_{I_P}(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}.$$

and all other modules on the right-hand side of formula (3.1) are projective as well.

Remark 3.3.2. If π is unramified, then formula (3.1) has the following simple form:

$$[L(D)] - [L(K-D)] = (1 - g_Y + \frac{1}{|G|}\deg D)[\mathbb{F}_q[G]].$$

Note that this is still a formula with integer coefficients, since in the unramified case, $\deg D$ is divisible by $|G|$.

Theorem 3.3.1 yields a representation of $[L(D)] - [L(K-D)]$ as a formal $\mathbb{Z}$-linear combination of projective $\mathbb{F}_q[G]$-modules. In order to say more about $L(D)$ as an $\mathbb{F}_q[G]$-module, it is useful to have a formula representing $L(D)$ as a proper sum of projective $\mathbb{F}_q[G]$-modules, i.e. with purely non-negative coefficients, because then we can leave the Grothendieck group and write $L(D)$ as a direct sum of the projective modules in question.

First of all, we have to make sure that $L(D)$ is in fact a projective module. By Theorem 2.4.10 (a), this is certainly true if $L(K-D)$ vanishes, and as we have seen in Subsection 3.2, $L(K-D)$ vanishes if $\deg D > 2g_X - 2$. Therefore, we will assume $\deg D > 2g_X - 2$.

Furthermore, in order to eliminate the $-[N_{G,X}]$ term, we can use the following result, which follows directly from Corollary 2.4.19.

Let $\operatorname{br}\pi \subseteq Y$ be the set of branch points of π. Let $N^*_{G,X}$ denote the dual (contragredient) of $N_{G,X}$ as a $k[G]$-module. Then we have in $K_0(k[G])$, the Grothendieck group of projective $k[G]$-modules:

$$-[N_{G,X}] = [N^*_{G,X}] + \sum_{R \in \operatorname{br}\pi} [\operatorname{Ind}^G_{I_{\tilde{R}}}(k(R))] - (\deg \Sigma_{\operatorname{br}\pi})[k[G]].$$

Together with Theorem 3.3.1, this yields the following result.

Corollary 3.3.3. *Suppose that* $\deg D > 2g - 2$. *Then we have in* $K_0(k[G])$*:*

$$[L(D)] = [N^*_{G,X}] + \sum_{R \in \operatorname{br}\pi} [\operatorname{Ind}^G_{I_{\tilde{R}}}(k(R))] + \sum_{R \in Y} \sum_{d=1}^{l_{\tilde{R}}} [\operatorname{Ind}^G_{G_{\tilde{R}}}((\mathfrak{m}_{\tilde{R}}/\mathfrak{m}^2_{\tilde{R}})^{\otimes d})] + (1 - g_Y + \deg D_1 - \deg \Sigma_{\operatorname{br}\pi})\,[k[G]], \quad (3.2)$$

where $D_1 := \sum_{R \in |Y|} m_{\tilde{R}} \cdot R$ *with* $m_{\tilde{R}}$ *defined as in Theorem 3.3.1.*

If additionally

$$\deg D_1 \geq \deg \Sigma_{\mathrm{br}(\pi)} + g_Y - 1, \tag{3.3}$$

then formula (3.2) gives an explicit representation of $L(D)$ as a direct sum of projective $k[G]$-modules. It will be fairly easy to show that the group action of G on $L(D)$ is faithful in this case; we just have to show that the action is faithful on one of the summands, because then it will be faithful on the whole sum. (See Theorem 3.3.7).

Remark 3.3.4. (a) Note that the assumption $\deg D > 2g_X - 2$ does not imply Condition (3.3) in general. For example, choose X and G such that $g_Y = 0$ and $\deg \Sigma_{\mathrm{br}\,\pi} > 1$. Now let $D := R_\pi := \sum_{P \in |X|}(e_P - 1) \cdot P$. Then we have

$$\begin{aligned} 2g_X - 2 &= |G|(2g_Y - 2) + \deg R_\pi && \text{by the Hurwitz formula} \\ &= -2|G| + \deg R_\pi && \text{since } g_Y = 0 \\ &< \deg R_\pi = \deg D, \end{aligned}$$

so $\deg D > 2g_X - 2$. However, we obviously have $D_1 = 0$ and hence

$$\deg \Sigma_{\mathrm{br}\,\pi} + g_Y - 1 > 1 + 0 - 1 = 0 = \deg D_1,$$

i.e. Condition (3.3) does not hold in this case.

(b) Condition (3.3) holds, for example, if $e_P | n_P$ for every $P \in X$ and $g_Y > \frac{1}{|G|} \deg \Sigma_{\mathrm{ram}(\pi)} + 1$, where $\mathrm{ram}(\pi) \subseteq X$ is the set of ramification points of π and $\Sigma_{\mathrm{ram}(\pi)} := \sum_{P \in \mathrm{ram}(\pi)} P$. Indeed, in this case we have $\pi^* D_1 = D$; since $\pi^* \Sigma_{\mathrm{br}(\pi)} = \sum_{P \in X} e_P \cdot P = R_\pi + \Sigma_{\mathrm{ram}(\pi)}$, this yields

$$\begin{aligned} &\deg D_1 - \deg \Sigma_{\mathrm{br}(\pi)} \\ &\quad = \frac{1}{|G|} \deg D - \frac{1}{|G|}(\deg R_\pi + \deg \Sigma_{\mathrm{ram}(\pi)}) \\ &\quad > \frac{1}{|G|}(2g_X - 2) - \frac{1}{|G|} \deg R_\pi - \frac{1}{|G|} \deg \Sigma_{\mathrm{ram}(\pi)} \\ &\quad = 2g_Y - 2 - \frac{1}{|G|} \deg \Sigma_{\mathrm{ram}(\pi)} \qquad \text{(Hurwitz formula)} \\ &\quad = g_Y - 1 + g_Y - (1 + \frac{1}{|G|} \deg \Sigma_{\mathrm{ram}(\pi)}) > g_Y - 1. \end{aligned}$$

Lemma 3.3.5. *If* $\operatorname{br}\pi \neq \emptyset$, *then* G *acts faithfully on* $N^*_{G,X}$.

Proof. Let P be a closed point of X. Then by Proposition 2.3.14 the character group $\operatorname{Hom}(I_P, k(P)^*)$ is cyclic of order e_P and generated by χ_P, where χ_P describes the action of I_P on $(\mathfrak{m}_P/\mathfrak{m}_P^2)$. For $d = 1, \dots, e_P - 1$, the I_P-action on $(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}$ is described by χ_P^d. Thus the kernel of the I_P-action on $(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}$ is just the kernel of χ_P^d, which is trivial since χ_P is injective (cf. proof of Proposition 2.3.14). Hence I_P acts faithfully on $(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}$, which implies that G acts faithfully on $\operatorname{Ind}_{I_P}^G((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d})$ by Lemma 3.3.6 below. Thus G acts faithfully on the sum

$$\bigoplus_{P \in |X|} \bigoplus_{d=1}^{e_P - 1} \bigoplus^{d} \operatorname{Ind}_{I_P}^G((\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}) \cong \bigoplus^{n} N_{G,X}.$$

(Note that the sum is nonempty since π has at least one branch point.) This implies that G also acts faithfully on $N_{G,X}$, for if there was an element of G acting as the identity on $N_{G,X}$, then this element would act as the identity on the whole sum, and the action on the sum would not be faithful. □

Lemma 3.3.6. *Let* H *be a normal subgroup of* G, *and let* V *be a* k*-representation of* H. *Then the kernel of the* G*-action on* $\operatorname{Ind}_H^G(V)$ *lies inside the kernel of the* H*-action on* V.

Proof. The induced representation $\operatorname{Ind}_H^G(V)$ can be written as

$$\sum_{\sigma \in G/H} \sigma.V,$$

where σ runs through a system of representatives of G/H (cf. [CR], §10A). We use the symbol $\sum$ in order to indicate that this does not decompose as a direct sum of $k[G]$-modules. The elements of G that are not in H act on the sum by permuting the summands, whilst the elements of H act on every translate of V as they do on V itself. Let now $g \in G$ belong to the kernel of the G-action on $\operatorname{Ind}_H^G(V)$. This means that g acts as the identity on $\operatorname{Ind}_H^G(V)$. In particular, we must have $g.(\operatorname{id}.V) = \operatorname{id}.V$, i.e. g fixes the summand $\operatorname{id}.V$ as a set, and hence $g \in H$. Furthermore, g must even fix $\operatorname{id}.V$ pointwise, i.e. it must act as the identity on V. Hence g belongs to the kernel of the H-action on V. □

Theorem 3.3.7. *Suppose that* $\deg D > 2g_X - 2$ *and that moreover one of the following conditions holds:*

1. π *is ramified at at least one point, and Condition 3.3 holds, or*
2. π *is unramified and* $g_Y \geq 1$, *or*
3. π *is unramified,* $g_Y = 0$ *and* $\deg D > 2g_X - 2 + |G|$.

Then G *acts faithfully on* $L(D)$.

Proof. 1. If π is ramified at at least one point, then by Lemma 3.3.5, G acts faithfully on $N_{G,X}$. Thus it also acts faithfully on the dual $N^*_{G,X}$. If additionally Condition (3.3) holds, then Corollary 3.3.3 gives a representation of $L(D)$ as a direct sum of projective $k[G]$-modules where one of the direct summands is $N^*_{G,X}$. Hence G also acts faithfully on $L(D)$.

2. If π is unramified and $g_Y \geq 1$, then by Remark 3.3.2, $L(D)$ is a free $\mathbb{F}_q[G]$-module of rank

$$\begin{aligned}
1 - g_Y + \frac{1}{|G|}\deg D &> 1 - g_Y + \frac{1}{|G|}(2g_X - 2) \\
&= 1 - g_Y + 2g_Y - 2 \qquad\qquad \text{(Hurwitz formula)} \\
&= g_Y - 1 \geq 0.
\end{aligned}$$

Hence $L(D)$ has at least one copy of $\mathbb{F}_q[G]$ as a direct summand. Since G acts faithfully on $\mathbb{F}_q[G]$, it acts faithfully on $L(D)$.

3. If π is unramified, $g_Y = 0$ and $\deg D > 2g_X - 2 + |G|$, then by Remark 3.3.2, $L(D)$ is a free $\mathbb{F}_q[G]$-module of rank

$$\begin{aligned}
1 - g_Y + \frac{1}{|G|}\deg D &= 1 + \frac{1}{|G|}\deg D \\
&> 1 + \frac{1}{|G|}(2g_X - 2 + |G|) \\
&= 2 + \frac{1}{|G|}(2g_X - 2) \\
&= 2 + 2g_Y - 2 \qquad\qquad \text{(Hurwitz formula)} \\
&= 0.
\end{aligned}$$

With the same argument as before, we can now see that G acts faithfully on $L(D)$.

□

3.4 Automorphisms of codes

Let C be a linear code of length n over some finite field $\mathbb{F}_q$. We now consider two groups that act on C via automorphisms, the $\mathbb{F}_q$*-automorphism group* and the *permutation automorphism group* of C. The $\mathbb{F}_q$*-automorphism group* $\mathrm{Aut}_{\mathbb{F}_q} C$ is just the group of vector space automorphisms of C. The *permutation automorphism group* is obtained as follows: Let S_n act on $\mathbb{F}_q^n$ by permutation of the coordinates. This is obviously an action by $\mathbb{F}_q$-automorphisms. The *permutation automorphism group* $\mathrm{Aut}_P(C)$ is defined as the subgroup of S_n which fixes C as a set, i.e.

$$\mathrm{Aut}_P(C) := \{\sigma \in S_n | \forall\, c \in C : \sigma(c) \in C\}.$$

Caution 3.4.1. Note that the permutation automorphism group does not necessarily act faithfully on the code. For example, the definitions would admit $C = \{(0,0,0,0)\}$ as a code of length 4 over, say, $\mathbb{F}_7$; the permutation automorphism group would be the whole of S_4, and it would obviously not act faithfully.

We will now see how group actions on algebraic curves relate to automorphisms of geometric Goppa codes.

In the setting of Section 3.2, the divisor $E = P_1 + \ldots + P_n$ is equivariant if and only if the set $\mathrm{Supp}\, E$ is stable under the action of G on X, which means that G acts on $\mathrm{Supp}\, E$ by permutations. In other words, we have a group homomorphism $G \to S_n$ such that the following diagram (of sets) commutes:

$$\begin{array}{ccc}
G \times \mathrm{Supp}\, E & \longrightarrow & \mathrm{Supp}\, E \\
\downarrow \quad \downarrow \cong & & \downarrow \cong \\
S_n \times \{1, \ldots, n\} & \longrightarrow & \{1, \ldots, n\}
\end{array}$$

The functor $\mathrm{Maps}(-, \mathbb{F}_q)$ now induces another commutative diagram, namely:

$$\begin{tikzcd} G \times \mathrm{Maps}(\mathrm{Supp}\, E, \mathbb{F}_q) \arrow[r] \arrow[d] & \mathrm{Maps}(\mathrm{Supp}\, E, \mathbb{F}_q) \arrow[d, "\cong"] \\ S_n \times \mathbb{F}_q^n \arrow[r] & \mathbb{F}_q^n \end{tikzcd}$$

In particular, G acts on $\mathbb{F}_q^n$ by permutation of the coordinates. The action of G on $\mathrm{Maps}(\mathrm{Supp}\, E, \mathbb{F}_q)$ explicitly looks like this:

$$\sigma.\alpha = \alpha \circ (\sigma^{-1}|_{\mathrm{Supp}\, E}) \text{ for all } \sigma \in G, \alpha \in \mathrm{Maps}(\mathrm{Supp}\, E, \mathbb{F}_q).$$

If the divisor D is equivariant, then G acts on $L(D)$ via

$$\sigma.f := f \circ \sigma^{-1}.$$

The homomorphism $L(D) \to \mathrm{Maps}(\mathrm{Supp}\, E, \mathbb{F}_q)$ obviously respects the group action on both sides, and its image in $\mathrm{Maps}(\mathrm{Supp}\, E, \mathbb{F}_q)$ is G-stable. Since the geometric Goppa Code $C(D, E)$ is defined as the image of

$$\mathrm{ev}_{D,E} : L(D) \to \mathrm{Maps}(E, \mathbb{F}_q) \xrightarrow{\sim} \mathbb{F}_q^n,$$

$C(D, E)$ is a G-stable subset of $\mathbb{F}_q^n$. In other words, every permutation of coordinates in $\mathbb{F}_q^n$ that comes from an element of G lies in the permutation automorphism group $\mathrm{Aut}_P(C(D, E))$, i.e. we have a homomorphism

$$\phi : G \to \mathrm{Aut}_P\, C(D, E).$$

The following is our main result related to Coding Theory.

Theorem 3.4.2. *Assume that $n > \deg D > 2g_X - 2$, and assume further that one of the conditions of Theorem 3.3.7 holds. Then G acts faithfully on the code $C(D, E)$. In particular, the map $\phi : G \to \mathrm{Aut}_P(C(D, E))$ is injective.*

Proof. By Theorem 3.3.7, G acts faithfully on $L(D)$. Since $n > \deg D$, the map $\mathrm{ev}_{D,E}$ is injective, as seen in Subsection 3.2. Hence $L(D)$ is isomorphic to $C(D, E) = \mathrm{im}\, \mathrm{ev}_{D,E}$ as an $\mathbb{F}_q[G]$-module, and therefore the G-action on $C(D, E)$ must be faithful as well.

To show the injectivity of ϕ, consider the following commutative diagram of groups:

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d] & \mathrm{Aut}_P(C(D,E)) \arrow[d] \\ \mathrm{Aut}_{\mathbb{F}_q} L(D) \arrow[r, "\cong"] & \mathrm{Aut}_{\mathbb{F}_q}(C(D,E)) \end{tikzcd}$$

The map $G \to \mathrm{Aut}_{\mathbb{F}_q} L(D)$ is injective because G acts faithfully on $L(D)$. Hence the map $G \to \mathrm{Aut}_{\mathbb{F}_q}(C(D,E))$ is also injective. Since the injectivity of any composition of maps implies the injectivity of the first map, this proves that ϕ is injective. □

Remark 3.4.3. The permutation automorphism group $\mathrm{Aut}_P(C(D,E))$ acts faithfully on $C(D,E)$ if and only if the map $\mathrm{Aut}_P(C(D,E)) \to \mathrm{Aut}_{\mathbb{F}_q}(C(D,E))$ is injective. Under the assumptions of Theorem 3.4.2, this is not necessarily the case.

Wesemeyer [Wes] investigates some (classes of) examples where ϕ is actually an isomorphism. In this case, the map in question is indeed injective, and hence $\mathrm{Aut}_P(C(D,E))$ acts faithfully on $C(D,E)$. This is particularly useful for further applications since it helps to describe, store and manage the code efficiently.

Remark 3.4.4. The map ϕ has also been investigated by Stichtenoth and by Joyner and Ksir. Stichtenoth shows that ϕ is injective whenever $n > 2g_X + 2$ (see Proposition 3.3(b) in Chapter III in [St]). Joyner and Ksir show the same, but with the additional assumption that $\deg D > 2g$ (see Lemma 11 in [JK]).

Chapter 4

Geometric Galois Module Theory: A result of Chinburg revisited

4.1 Introduction

In this chapter, we link our results in equivariant Riemann-Roch theory to work of Chinburg, Erez, Pappas and Taylor, more concretely regarding their programme to generalize the ideas of Galois module theory to a geometric setting.

Classically, Galois module theory is a branch of algebraic number theory and deals with the following problem. Let L/K be a Galois extension of number fields with group $G = \mathrm{Gal}(L/K)$. If L/K is tamely ramified, then the ring $\mathcal{O}_L$ of integers in L is a projective $\mathbb{Z}[G]$-module, and one would like to describe its class in $K_0(\mathbb{Z}[G])$, the Grothendieck group of projective $\mathbb{Z}[G]$-modules.

In [Tay], Taylor proved Fröhlich's conjecture that this class is equal to another invariant, the *root number class* $W_{L/K}$. It is defined in terms of root numbers, also known as epsilon constants, of symplectic representations of G. The epsilon constant of a representation can be defined by means of Artin L-functions, and appears in Tate's functional equation for the Artin L-function of a representation.

Chinburg, Erez, Pappas and Taylor have conducted a programme to prove a generalized version of Fröhlich's conjecture, as well as generalisations of other results in the field, in a geometric setting. Here the Galois extension L/K is replaced by a tame G-cover $X \to Y$ of schemes of finite type over a noetherian ring, and instead of the $\mathbb{Z}[G]$-isomorphism class of the ring $\mathcal{O}_L$, one considers the equivariant Euler characteristic (in $K_0(\mathbb{Z}[G])$) of a suitable bounded complex of G-sheaves on X. In particular, one considers the equivariant Euler characteristic of the de Rham complex,

$$\psi(X/Y) := \sum_{i=0}^{d-1} \sum_{j \in \mathbb{Z}} (-1)^{i+j} (d-i)[H^j(X, \Omega^i_X)] \in K_0(\mathbb{Z}[G]),$$

where d is the dimension of X. To recover the classical case, let L/K be a Galois extension of number fields, $X := \operatorname{Spec} \mathcal{O}_L$ and $Y := \operatorname{Spec} \mathcal{O}_K$, viewed as schemes over $\mathbb{Z}$. Then $\psi(X/Y)$ is just the class of $\mathcal{O}_L$ in $K_0(\mathbb{Z}[G])$.

For the important case of schemes of finite type *over a finite field*, Chinburg [Ch] describes $\psi(X/Y)$ in terms of epsilon constants of representations of the Galois group G. His proof uses crystalline cohomology and is quite complicated, which is not surprising in such a general setting. In a later paper [Er], Erez states the following equivalent of Chinburg's result: Let g be an element of G of order coprime to p. Then we have

$$\sum_{\chi} v_p(\varepsilon(V_\chi))\chi(g) = \operatorname{Trace}(g|\psi(X/Y)), \tag{4.1}$$

where Trace denotes the modular character (Brauer character), the sum runs over the irreducible complex characters χ of G, and V_χ denotes the irreducible representation affording the virtual character χ.

In the case of curves, Erez [Er] outlines a more elementary proof of this result. Some basic ideas are sketched in [Er], but in order to give a full account of the proof, a lot of details need filling in. This was supposed to be done in a further paper by Chinburg, Erez, Pappas and Taylor, but that paper was never published and in particular not available to the author. Instead of using the Lefschetz fixed point formula as suggested by Erez, we use our equivariant Hurwitz formula, Formula 2.16 from Theorem 2.4.11, in order to re-write the right-hand side of formula (4.1). Note, however, that in order to prove Theorem 2.4.11, we rely on results by Köck which were proved using the Lefschetz fixed point formula as well.

4.2 Preliminaries

For the convenience of the reader, we recall some basic definitions and results from algebraic number theory and modular representation theory.

4.2.1 Global and local fields

Definition 4.2.1. A *global field* is a finite algebraic extension of either the field $\mathbb{Q}$ or the field $\mathbb{F}_p(t)$ of rational functions over $\mathbb{F}_p$ for some prime number p.

A *local field* is a field that is complete with respect to some discrete valuation v and whose residue field is finite. Equivalently, a local field is a finite algebraic extension of the field $\mathbb{Q}_p$ of p-adic numbers or of the field $\mathbb{F}_p((t))$ of formal power series over $\mathbb{F}_p$, for some prime number p (see Theorem II.5.2 in [Ne]).

An *algebraic number field* (*p-adic number field*) is a finite algebraic extension of $\mathbb{Q}$ (of $\mathbb{Q}_p$).

For any underlying field k, a *function field* in one variable over k is a field extension of k of transcendence degree 1.

In particular, a field K is an algebraic number field (p-adic number field) if and only if it is a global field (local field) of characteristic zero. Any function field in one variable over a finite field is a global field of positive characteristic.

Definition 4.2.2. If K is a global field, an equivalence class $\mathfrak{p}$ of non-archimedian valuations of K is called a *finite place* of K. An equivalence class of archimedian valuations is called an *infinite place* of K. In the case of finite places, we will write $K_\mathfrak{p}$ for the completion of K with respect to $\mathfrak{p}$. If L/K is a finite algebraic extension, any non-archimedian valuation of K can be extended to a non-archimedian valuation of L. We choose one way doing so and write $L_\mathfrak{p}$ for the completion of L with respect to this valuation.

During this chapter, we will often reduce problems over a global field to analogous problems over its completions $K_\mathfrak{p}$. These are local fields of the same characteristic as K.

We will mainly be dealing with the positive characteristic case. If X is a curve over the finite field $\mathbb{F}_q$ (of characteristic p), then its function field

$L := K(X)$ is a function field over $\mathbb{F}_p$, and hence a global field of characteristic p. The closed points of X are in 1-1-correspondence with the finite places of L. If P is a closed point on X and $\mathfrak{p}$ is the corresponding place of L, then the local ring $\mathcal{O}_{X,P}$ is the valuation ring of $\mathfrak{p}$, and the residue field $k(P)$ is its residue field. Equivalently, $k(P)$ is the residue field of the local field $L_{\mathfrak{p}}$.

4.2.2 Some local class field theory

Local class field theory is the theory of the abelian extensions L/K of a given local field K. The theory is fully explained in Chapters IV and V of [Ne]. For a quicker read, a nice summary of the basic ideas can be found at the beginning of §IV.3 in [Ne].

One of the most important results of local class field theory is the *local reciprocity law* (Theorem V.1.3 in [Ne]): For every finite Galois extension L/K (not necessarily abelian) of local fields, one has a canonical isomorphism

$$r_{L/K} : \mathrm{Gal}(L/K)^{ab} \to K^*/N_{L/K}(L^*),$$

where $\mathrm{Gal}(L/K)^{ab}$ denotes the largest abelian quotient of $\mathrm{Gal}(L/K)$.

The inverse of $r_{L/K}$ is called the *norm residue symbol* and can be viewed as a surjective map

$$(-, L/K) : K^* \to \mathrm{Gal}(L/K)^{ab}$$

with kernel $N_{L/K}(L^*)$.

Let now L/K be a finite Galois extension of local fields, of group G. Let χ be a character of G, i.e. a homomorphism $G \to \mathbb{C}^*$. Since $\mathbb{C}^*$ is abelian, χ factors through G^{ab}, i.e. there is a homomorphism $\chi^{ab} : G^{ab} \to \mathbb{C}^*$ such that the following diagram commutes:

$$\begin{tikzcd} G \arrow[r, "\chi"] \arrow[d] & \mathbb{C}^* \\ G^{ab} \arrow[ur, dashed, "\chi^{ab}"'] & \end{tikzcd}$$

By the local reciprocity law, χ induces a homomorphism

$$\chi_K : K^* \to \mathbb{C}^*$$

making the following diagram commute.

$$\begin{tikzcd} K^* \arrow[r, "{(-,L/K)}"] \arrow[dr, "\chi_K"'] & G^{ab} \arrow[d, "\chi^{ab}"] \\ & \mathbb{C}^* \end{tikzcd}$$

Let now L/K be a finite *abelian* extension of local fields, $G = \mathrm{Gal}(L/K) = \mathrm{Gal}(L/K)^{ab}$. Let G_s $(s \geq -1)$ denote the higher ramification groups of L/K, see Definition 2.3.10. Define a function

$$\eta : [-1, \infty) \to [-1, \infty)$$

by

$$\eta(s) := \int_0^s \frac{dx}{(G_0 : G_x)},$$

where $(G_0 : G_x)$ shall mean the inverse of $(G_x : G_0)$ for $-1 \leq x < 0$. For $0 < m \in \mathbb{N}$, we have

$$\eta(m) = \frac{1}{|G_0|}(|G_1| + \ldots + |G_m|)$$

(see §II.10 in [Ne]).
In particular, we have

$$\eta(-1) = -1, \ \eta(0) = 0,$$

and if L/K is tamely ramified with ramification index e, then we have

$$\eta(e) = \frac{1}{|G_0|}(|G_1| + \ldots + |G_e|) = \frac{1}{e}(1 + \ldots 1) = 1.$$

The function η is strictly monotonously growing on $[-1, \infty)$ and hence has an inverse η^{-1} on $[-1, \infty)$.
Let now $\mathfrak{m}_K$ denote the maximal ideal in the ring of integers of K. Then Theorem V.6.2 in [Ne] states that for every $s \geq 0$, the subgroup $U^{(s)} = 1 + \mathfrak{m}_K^s$ of K^* is mapped to the ramification group $G_{\eta^{-1}(s)}$ under the norm residue symbol. In particular, $U^0 = \mathcal{O}_K^*$ is mapped to G_0, the inertia group of L/K, and if L/K is tamely ramified with ramification index e, then $U^1 = 1 + \mathfrak{m}_K$ is mapped to $G_e = \{1\}$. Hence in the tamely ramified case, the norm residue symbol induces a surjective homomorphism

$$\alpha : k^* = \mathcal{O}_K^*/1 + \mathfrak{m}_K \to I$$

from the multiplicative group of the residue class field k of K to the inertia group.

Here are two diagrams to illustrate the situation. The first diagram commutes.

$$\begin{tikzcd} 1 + \mathfrak{m}_K \arrow[r] \arrow[d] & \mathcal{O}_K^* \arrow[r] \arrow[d] & K^* \arrow[d, "{(-,L/K)}"] \\ \{1\} \arrow[r] & I \arrow[r] & G \end{tikzcd}$$

$$\begin{tikzcd} k^* = \mathcal{O}_K^*/1 + \mathfrak{m}_K \arrow[d, "\alpha"] & K^* \arrow[d, "{(-,L/K)}"] \\ I \arrow[r] & G \end{tikzcd}$$

Hence in the tamely ramified case, a character χ of G induces not only a character $\chi_K : K^* \to \mathbb{C}^*$, but also a character $\chi_k : k^* \to \mathbb{C}^*$ of the multiplicative group of the residue field, which makes the following diagram commute.

$$\begin{tikzcd} k^* \arrow[r, "\alpha"] \arrow[dr, "\chi_k"'] & I \arrow[d, "\chi|_I"] \\ & \mathbb{C}^* \end{tikzcd}$$

We end this subsection by proving a preliminary result that will be needed later, in Subsection 4.5.3.

Throughout the rest of this chapter, for any $n \in \mathbb{Z}$ and any cyclic group H, we write n as a shorthand notation for the group endomorphism $x \mapsto x^n$ of H. Furthermore, for any subgroup $H' \leq H$, we write $i_{H',H}$ or simply i for the inclusion $H' \hookrightarrow H$.

Proposition 4.2.3. *Let L/K be a tamely ramified abelian Galois extension of local fields. Let l/k denote the corresponding extension of residue fields. Let G denote the Galois group, I the inertia group of L/K. Let χ denote the (non-modular) character $I \to l^*$ afforded by $\mathfrak{m}_L/\mathfrak{m}_L^2$ as a* *one-dimensional l-representation of I. Furthermore, let $\alpha : k^* \to I$ be the surjective homomorphism from local class field theory, and let $t := \frac{|k^*|}{|I|}$. The following diagram commutes:*

$$\begin{tikzcd} k^* \arrow[r, "\alpha"] \arrow[d, "t"'] & I \arrow[d, "\chi"] \\ k^* \arrow[r, "i"'] & l^* \end{tikzcd}$$

The following lemma will later be used to reduce Proposition 4.2.3 to the case where L is the field $K(F(1))$ of π-th division points over K.

Lemma 4.2.4. *Let M/K be a tamely ramified abelian extension of local fields, and let L be an intermediate field that is Galois over K. Write $e(M/L) := |I(M/L)|$ for the ramification index of M/L. Furthermore, write m for the residue field of M, $\chi_{M/K}$ for the character $I(M/K) \to m^*$ afforded by the action of the inertia group $I(M/K)$ on $\mathfrak{m}_M/\mathfrak{m}_M^2$, and $\chi_{L/K}$ for the character $I(L/K) \to m^*$ afforded by the action of the inertia group $I(L/K)$ on $\mathfrak{m}_L/\mathfrak{m}_L^2$ The following diagram commutes:*

$$\begin{tikzcd} k^* \arrow[r, "\alpha_{M/K}"] \arrow[d, equal] & I(M/K) \arrow[r, "\chi_{M/K}"] \arrow[d] & m^* \arrow[r, "e(M/L)"] & m^* \\ k^* \arrow[r, "\alpha_{L/K}"'] & I(L/K) \arrow[rr, "\chi_{L/K}"'] & & l^* \arrow[u, "i"'] \end{tikzcd} \tag{4.2}$$

In particular, if Proposition 4.2.3 holds for M/K, then it also holds for L/K. The converse is true if M/K is unramified.

Proof. The square commutes by functoriality of local class field theory (see Theorem 5.8 in [Ne]). The commutativity of the rectangle follows from the fact that if π_M is a prime element for M and π_L is a prime element in L, then

$$\pi_L = u\pi_M^{e(L/K)}$$

for some unit $u \in \mathcal{O}_M^*$.

Assume now that Proposition 4.2.3 holds for the extension M/K. This means that we have

$$\chi_{M/K} \circ \alpha_{M/K} = i_{k^*,m^*} \circ \left(-\frac{|k^*|}{e(M/K)} \right). \tag{4.3}$$

Hence we have

$$
\begin{aligned}
& i_{l^*,m^*} \circ \chi_{L/K} \circ \alpha_{L/K} \\
&\quad = e(M/L) \circ \chi_{M/K} \circ \alpha_{M/K} && \text{since Diagram (4.2) commutes} \\
&\quad = e(M/L) \circ\ i_{k^*,m^*} \circ \Big(-\frac{|k^*|}{e(M/K)} \Big) && \text{by Formula (4.3)} \\
&\quad = i_{k^*,m^*}\ \circ e(M/L) \circ \Big(-\frac{|k^*|}{e(M/K)} \Big) \\
&\quad = i_{k^*,m^*} \circ\ \Big(-\frac{|k^*|}{e(L/K)} \Big)
\end{aligned}
$$

It follows that

$$\chi_{L/K} \circ \alpha_{L/K} = i_{k^*,l^*} \circ \Big(-\frac{|k^*|}{e(L/K)} \Big),$$

so Proposition 4.2.3 holds for L/K.

For the last part of the lemma, assume that M/L is unramified and that Proposition 4.2.3 holds for L/K. This means that we have

$$\chi_{L/K} \circ \alpha_{L/K} = i_{k^*,l^*} \circ \Big(-\frac{|k^*|}{e(L/K)} \Big). \tag{4.4}$$

Since M/L is unramified, we have $e(M/L) = 1$, so the map named $e(M/L)$ in Diagram (4.2) is the identity, and we have $e(M/K) = e(L/K)$. Hence we have

$$
\begin{aligned}
& \chi_{M/K} \circ \alpha_{M/K} \\
&\quad = i_{l^*,m^*} \circ \chi_{L/K} \circ \alpha_{L/K} && \text{since Diagram (4.2) commutes} \\
&\quad = i_{l^*,m^*}\ \circ\ i_{k^*,l^*} \circ\ \Big(-\frac{|k^*|}{e(L/K)} \Big) && \text{by Formula (4.4)} \\
&\quad = i_{k^*,m^*} \circ\ \Big(-\frac{|k^*|}{e(M/K)} \Big),
\end{aligned}
$$

and so Proposition 4.2.3 holds for M/K. □

In the proof of Proposition 4.2.3, we will use a little *Lubin-Tate theory*, which may be viewed as a generalization of the theory of cyclotomic fields. We first give a brief explanation of this theory, following §§4 and 5 of Chapter V in [Ne].

Let $\mathcal{O}$ be a ring.

Definition 4.2.5. A *formal group* over $\mathcal{O}$ is a formal power series $F(X,Y) \in \mathcal{O}[[X,Y]]$ having the following properties:

(i) $F(X,Y) \equiv X+Y \mod \text{degree } 2$.

(ii) $F(X,Y) = F(Y,X)$ ("commutativity").

(iii) $F(X,F(Y,Z)) = F(F(X,Y),Z)$ ("associativity").

Definition 4.2.6. Let F be a formal group over $\mathcal{O}$. An *endomorphism* of F is a power series $f(X) = a_1X + a_2X^2 + \ldots \in \mathcal{O}[[X]]$, such that

$$f(F(X,Y)) = F(f(X), f(Y)).$$

Proposition 4.2.7. *The endomorphisms of a formal group F form a ring $\mathrm{End}_{\mathcal{O}}(F)$, where addition and multiplication are given by*

$$(f +_F g)(X) := F(f(X), g(X))$$

and

$$(f \circ g)(X) = f(g(X)).$$

Definition 4.2.8. A *formal $\mathcal{O}$-module* is a formal group F over $\mathcal{O}$ together with a ring homomorphism

$$\mathcal{O} \to \mathrm{End}_{\mathcal{O}}(F), \quad a \mapsto [a]_F(X),$$

such that

$$[a]_F(X) \equiv aX \mod \text{degree } 2.$$

Let now K be a local field, and let $\mathcal{O} = \mathcal{O}_K$ be the ring of integers in K. Let q be the order of the residue field and let π be a prime element.

Definition 4.2.9. A *Lubin-Tate module* over $\mathcal{O}_K$ with respect to the prime element π is a formal $\mathcal{O}_K$-module such that

$$[\pi]_F(X) \equiv X^q \mod \pi.$$

Let now $\bar{K}$ be an algebraic closure of K. Then the valuation of K has a continuation on $\bar{K}$. Let $\mathcal{O}_{\bar{K}}$ be the corresponding valuation ring, $\mathfrak{m}_{\bar{K}}$ its maximal ideal.

Proposition 4.2.10. *Let F be a formal $\mathcal{O}_K$-module. Then the set $\mathfrak{m}_{\bar{K}}$ with the operations*

$$x +_F y := F(x,y)]$$

and

$$a \cdot x := [a]_F(x)$$

is an $\mathcal{O}_K$-module in the usual sense.

Let F be a Lubin-Tate module with respect to a prime element π. For every $n \in \mathbb{N}$, define the group of π^n-th *division points* to be

$$F(n) := \{\lambda \in \mathfrak{m}_{\bar{K}} | \pi^n \cdot \lambda = 0\} = \ker([\pi^n]_F).$$

This is a subset of $\mathfrak{m}_{\bar{K}}$ and hence of $\bar{K}$. By adjoining all π^n-th division points to K, we obtain an algebraic field extension $K(F(n))$ of K, the *field of π^n-th division points*, for every n. These extensions are sometimes also called *Lubin-Tate extensions* of K. They depend on the prime element π, but once π is fixed, they do not depend on the choice of F. It follows immediately from the definition that we have $F(n) \subseteq F(n+1)$ for all n and hence $K(F(n)) \subseteq K(F(n+1))$ for all n.

Proof of Proposition 4.2.3. Fix a prime π of K and a Lubin-Tate module F with respect to that prime. The generalized Kronecker-Weber theorem (Corollary 5.7 in [Ne]) yields that there exists an $n \in \mathbb{N}$ such that we have a tower of fields

$$K \leq L \leq K^{ur}K(F(n)), \tag{4.5}$$

where K^{ur} denotes the maximal unramified extension of K and $K(F(n))$ denotes the field of π^n-th division points (see above). By Theorem V.5.4 in [Ne], $K(F(n))/K$ is a totally ramified abelian extension of degree $q^{n-1}(q-1)$, where $q = \#k$. Hence for any $n > 1$, the ramification index of $K(F(n))$ over K is

$$e(K(F(n))/K) = [K(F(n)) : K] = q^{n-1}(q-1) = q^{n-1}e(K(F(1))/K),$$

which is a p-power times the ramification index of $K(F(1))/K$. It follows that any tamely ramified extension that is contained in $K(F(n))$ for some

$n \in \mathbb{N}$ is already contained in $K(F(1))$. Since L/K was assumed tamely ramified, this means that (4.5) is true for $n = 1$, i.e. we have

$$K \leq L \leq K^{ur}K(F(1)).$$

Consider the following diagram of fields and subfields:

$$\begin{tikzcd}[column sep=small]
& K^{ur}K(F(1)) \arrow[dl, dash] \arrow[dr, dash] & \\
K^{ur} \arrow[dr, dash] & & K(F(1)) \arrow[dl, dash] \\
& K &
\end{tikzcd}$$

Suppose that Proposition 4.2.3 holds for $K(F(1))/K$. Since $K^{ur}K(F(1))/K(F(1))$ is unramified, Lemma 4.2.4 yields that Proposition 4.2.3 also holds for $K^{ur}K(F(1))/K$. Applying Lemma 4.2.4 once again, we see that Proposition 4.2.3 also holds for L/K. Hence it suffices to show Proposition 4.2.3 for the extension $K(F(1))/K$.

Assume from now on that $L = K(F(1))$. Let λ be a π-th division point, i.e. an element of $F(1)$. Then by Theorem V.5.4 in [Ne], λ is a prime element for L.

Let now u be a unit in the ring of integers of K, i.e. $u \in \mathcal{O}_K^*$. Then by Theorem V.5.5 in [Ne], we have

$$(u, L/K)(\lambda) = [u^{-1}]_F(\lambda)$$

and by definition of the Lubin-Tate module structure (Definitions V.4.4 and V.4.5 in [Ne]), we have

$$[u^{-1}]_F(\lambda) \equiv u^{-1}\lambda \mod (\lambda^2).$$

So $(u, L/K) \in I(L/K)$ acts on the "cotangent space" $\mathfrak{m}_L/\mathfrak{m}_L^2 = (\lambda)/(\lambda^2)$ by multiplication with (the class in l^* of) u^{-1}. Hence the following diagram commutes:

$$\begin{tikzcd}
k^* \arrow[r, "\alpha"] \arrow[d, "i"'] & I \arrow[d, "\chi"] \\
l^* \arrow[r, "-1"'] & l^*
\end{tikzcd}$$

Since L/K is totally ramified of degree $q-1$ (see above), we have $|I(L/K)| = q-1$ and hence $-1 = -\frac{|k^*|}{|I(L/K)|}$, which proves Proposition 4.2.3. □

4.2.3 Modular characters

Most of the material in this subsection is taken from [CR] and [Ne]. In particular, the definition of modular characters that we give below can be found in [CR] as Definition 21.26.

In classical representation theory, one usually only considers group representations over fields of characteristic zero. This ensures, for example, that two representations have the same composition factors (which, in this setting, is equivalent to the representations being isomorphic) if and only if their characters coincide. Here the *character* afforded by a representation V at a group element σ is the sum of the eigenvalues of σ on V, or equivalently, the trace of a matrix representing σ with respect to some basis of the vector space V. If we were to use the same definition for representations over fields of positive characteristic, this important result would fail (see §17B in [CR] for examples). To work round this problem, Brauer came up with the notion of *modular characters*, nowadays frequently called *Brauer characters*. They are defined as follows.

Let k be a field of characteristic $p>0$, let m denote the exponent of G (the least common multiple of the orders of elements of G) and let m' denote its p-regular part, i.e. $m = p^a m'$ where $(m',p)=1$. Let k_0 be the prime field of k, and let $k_1 := k_0(\tilde{\zeta}) \subseteq k(\tilde{\zeta})$, where $\tilde{\zeta}$ is a primitive m'-th root of unity over k. Then there exists a discrete valuation ring R with maximal ideal $\mathfrak{p}$, such that the quotient field K of R has characteristic zero and the residue field $R/\mathfrak{p}$ is k_1. A triple (K,R,k_1) with these properties is called a *p-modular system.*

Example 4.2.11. If k_1 is perfect (which it will be in our applications), then a p-modular system (K,R,k_1) can be constructed as follows. Let W be the ring of *Witt vectors* over k_1, which is defined in Exercise II.4.2 in [Ne], and let $F(W)$ be the field of fractions of $W(k_1)$. Then by Exercise II.4.6 in [Ne], $(F(W),W,k_1)$ is a p-modular system.

Example 4.2.12. The triple $(\mathbb{Q}_p,\mathbb{Z}_p,\mathbb{F}_p)$ is a p-modular system. More generally, if k is any finite field of characteristic p, then the field k_1 constructed above is a finite algebraic extension of the prime field $\mathbb{F}_p$, and a p-modular system for it will involve some algebraic extension K of $\mathbb{Q}_p$ and some integral extension R of $\mathbb{Z}_p$.

If (K, R, k_1) is a p-modular system, then R contains an m'-th root of unity ζ such that $\bar{\zeta} = \tilde{\zeta}$ in $R/\mathfrak{p} = k_1$. This is essentially due to Hensel's Lemma (II.4.6 in [Ne]). We denote the groups of m'-th roots of unity in k_1 and K by $\mu_{k_1,m'}$, $\mu_{K,m'}$ respectively. Reduction mod $\mathfrak{p}$ defines an isomorphism $\mu_{K,m'} \to \mu_{k_1,m'}$. Its inverse is called the *Teichmüller character* and will be denoted T in the following.

Let now V be a k-representation of G, and let σ be an element of G of order l, where $(l,p) = 1$. Then σ acts on V as an endomorphism whose eigenvalues are all l-th roots of unity over k. Since $l|m'$, they are also m'-th roots of unity and hence are contained in $\mu_{k_1,m'}$. So we can define

$$\mathrm{Trace}(\sigma|V) := \sum_{i=1}^{\dim V} T(\lambda_i) \in K, \tag{4.6}$$

where the λ_i are the eigenvalues of σ. The map

$$\mathrm{Trace}(-|V) : G_{\mathrm{reg}} \to K$$

is called the *modular character* or *Brauer character* of V. Here G_{reg} denotes the set of elements of G whose order is coprime to p.

As one can see, modular characters take values in the field K, a field of characteristic zero. If we start off with a finite field k, then as stated in Example 4.2.12 above, K is a finite algebraic extension of $\mathbb{Q}_p$. One can therefore consider K as a subset of an algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, so that the modular characters take values "in $\bar{\mathbb{Q}}_p$".

It is easy to check that modular characters are well-defined on the Grothendieck group $K_0(G,k)$.

If k is of characteristic zero, then we can take $K := k, f := \mathrm{id}$ to obtain the classical definition of the character of a representation. It turns out that (4.6) is a "good" definition, in the sense that many results from classical representation theory can be generalized to this setting. In particular, two $k[G]$-modules have the same composition factors if and only if their Brauer characters coincide (see Corollary 17.10 in [CR]).

A *virtual Brauer character* relative to k is a $\mathbb{Z}$-linear combination of Brauer characters of $k[G]$-modules. The set of virtual Brauer characters carries a ring structure (as a subset of $\mathrm{Maps}(G_{\mathrm{reg}}, \bar{\mathbb{Q}}_p)$). It will be denoted $R_{G,k}$ or simply R_G in the following. The subring generated by the characters of *projective* $k[G]$-modules will be denoted $P_{G,k}$ or simply P_G. By Proposition 17.14 in [CR], the map

$$K_0(G,k) \to R_G, \quad [V] \mapsto \mathrm{Trace}(-|V)$$

is an isomorphism of rings and restricts to an isomorphism

$$K_0(k[G]) \to P_G.$$

Just as in classical representation theory, one has a *character pairing*

$$\langle -, - \rangle : R_G \times R_G \to \mathbb{Z}$$

defined by

$$\langle \chi, \psi \rangle := \frac{1}{|G|} \sum_{g \in G_{\mathrm{reg}}} \chi(g)\psi(g^{-1}).$$

(cf. (18.18) in [CR]).
Now if V is any k-representation of G and if $\chi_V = \mathrm{Trace}(-|V)$ is the corresponding character, then we have

$$[V] = \sum_W \langle \chi_V, \chi_W \rangle [W] \tag{4.7}$$

in $K_0(G,k)$, where the sum runs over the irreducible $k[G]$-modules W and χ_W denotes the Brauer character corresponding to W. This is a consequence of Theorem 18.23 in [CR].
There are two important homomorphisms between Grothendieck groups that we will need in this chapter. The first one is the Cartan homomorphism

$$c : K_0(k[G]) \hookrightarrow K_0(G,k),$$

which we have already seen in Chapter 2. The second one is the homomorphism

$$e : K_0(k[G]) \to K_0(G,K)$$

constructed as follows (see [CR], Theorem (18.2) and the subsequent paragraphs, up to Formula (18.3)):

Let (K, R, k) be a p-modular system. Let $\bar{P}$ be a projective $k[G]$-module. Then there is a unique $R[G]$-module P such that $\bar{P} \cong P \otimes_R k$. Let now

$$e(P) := P \otimes_R K.$$

If K is sufficiently large with respect to G, then the homomorphism $e : K_0(k[G]) \to K_0(G, K)$ is injective, and it induces an injective homomorphism

$$P_{G,k} \hookrightarrow R_{G,K} = R_{G,\bar{K}}$$

which is compatible with the character pairing on both sides.

4.3 Artin L-functions and epsilon constants

The purpose of this section is to introduce Artin L-functions and epsilon constants and state some of their properties. The presentation given here is based on Deligne's work [De3], where the epsilon constants are defined via their properties and in particular via a functional equation, namely the local functional equation from Tate's thesis.

4.3.1 Tate's local functional equation

In this subsection, we attempt to give an outline of the first part of Tate's thesis. For a more detailed explanation, we refer the reader to the unbeatably clear and beautiful presentation in Tate's original work [Ta] and the summary in Lang's book [La].

Let p be a prime, and let K be a p-adic number field, i.e. a local field of characteristic zero, with ring of integers $\mathcal{O}_K$ and maximal ideal $\mathfrak{m}_K$. Let $q := |\mathcal{O}_K/\mathfrak{m}_K|$. Let $|\ |_p$ denote the p-adic absolute value on K.

For every element $y \in K$, Tate defines a distinguished additive character from K to $\mathbb{C}^*$ by the assignment

$$x \mapsto e^{2\pi i \Lambda(xy)},$$

where Λ is an additive continuous map from K into the reals mod 1 satisfying certain extra conditions (cf. [Ta], proof of Lemma 2.2.1 on p. 309).

Let dx be the uniquely determined Haar measure on K that satisfies

$$\int_{\mathcal{O}_K} dx = |\mathcal{O}_K/\mathfrak{d}|^{-\frac{1}{2}}, \tag{4.8}$$

where $\mathfrak{d}$ denotes the *absolute different* of K, i.e. the *different* of the field extension $K/\mathbb{Q}_p$ (see Definition III.2.1 in [Ne]).

We can now define the *Fourier transform* $\hat{f}$ of an absolutely integrable function $f \in L_1(K)$ as follows:

$$\hat{f}(y) := \int_K f(x)e^{-2\pi i\Lambda(xy)}dx.$$

Let d^*a be the "multiplicative" Haar measure on K^* defined by

$$d^*a := \frac{q}{(q-1)\,|a|_p}da \tag{4.9}$$

We view K^* as a topological group in the usual way, i.e. such that the unit groups $U^{(s)} = 1 + \mathfrak{m}_K^s$ form a basis for the neighbourhoods of $1 \in K^*$. Let $c : K^* \to \mathbb{C}^*$ be a continuous homomorphism of topological groups. We will call such a homomorphism a *quasi-character*. Then we can write $c(a) = \chi(a)|a|^\sigma$ for some *character* (i.e. some continuous homomorphism of absolute value 1) χ of K^* and some $\sigma \in \mathbb{R}$. Assume for the moment that the "exponent" σ is greater than 0. Furthermore, let $f : K \to \mathbb{C}$ be a function satisfying the following two conditions:

1. Both f and its Fourier transform $\hat{f}$ are continuous and in $L_1(K)$.

2. Both $f(a)|a|^\sigma$ and $\hat{f}(a)|a|^\sigma$ (as functions of $a \in K^*$) are in $L_1(K^*)$.

Then we define the *zeta function* $\zeta(f,c)$ as follows:

$$\zeta(f,c) := \int_{K^*} f(a)c(a)\,d^*a.$$

The following result appears in Tate's thesis [Ta] as Theorem 2.4.1.

Theorem 4.3.1 (Tate's local functional equation). *The zeta function $\zeta(f,c)$ is analytic on the domain of all quasi-characters of the form $c(a) = \chi(a)|a|^\sigma$ with $\sigma > 0$. It has an analytic continuation to the domain* *of all quasi-characters (with arbitrary $\sigma \in \mathbb{R}$) given by a functional equation of the type*

$$\zeta(f, c) = \rho(c)\zeta(\hat{f}, \hat{c}),$$

where $\hat{c}$ denotes the quasi-character given by $\hat{c}(a) := |a|_p c^{-1}(a)$.
The factor $\rho(c)$, which is independent of the function f, is a meromorphic function of quasi-characters defined in the domain $0 < \sigma < 1$ by the functional equation itself, and for all quasi-characters by analytic continuation.

4.3.2 A more general version of Tate's local functional equation

Deligne [De3] quotes a slightly more general version of Theorem 4.3.1.
Let K be a local field of arbitrary characteristic with ring of integers $\mathcal{O}_K$, maximal ideal $\mathfrak{m}_K$, valuation v_K and prime element π_K. Let $q := |\mathcal{O}_K/\mathfrak{m}_K|$. Let $|\,|$ be the absolute value corresponding to the valuation of K, i.e.

$$|a| = q^{-v_K(a)}.$$

Let $\psi : K \to \mathbb{C}^*$ be an additive character, let dx be a Haar measure on K and let $c : K^* \to \mathbb{C}^*$ be a quasi-character. Define the multiplicative measure d^*a, dependent of the additive measure dx, by formula (4.9).
We define $l(c) \in \mathbb{C} \cup \{\infty\}$ as follows:

$$\begin{array}{lcll} l(c) & := & 1 & \text{if } c|_{\mathcal{O}_K^*} \not\equiv 1, \\ l(c) & := & \frac{1}{1-c(\pi_K)} & \text{if } c|_{\mathcal{O}_K^*} \equiv 1. \end{array} \tag{4.10}$$

Furthermore, we define $\hat{c}(a) := |a|c^{-1}(a)$ as before. Let f be a function having the properties 1. and 2. from the previous subsection. We define the *Fourier transform* of f to be

$$\hat{f}(y) := \int_K f(x)\psi(xy)\,dx.$$

Theorem 4.3.2. *In the above situation, we have*

$$\frac{\int_{K^*} \hat{f}(a)\hat{c}(a)\,d^*a}{l(\hat{c})} = E(c, \psi, dx)\frac{\int_{K^*} f(a)c(a)\,d^*a}{l(c)} \tag{4.11}$$

with a factor $E(c, \psi, dx)$ *independent of* f.

4.3.3 A functional equation of global quasi-characters

Let now K be a global field. An *adèle* of K is a family

$$a = (a_{\mathfrak{p}})$$

of elements $a_{\mathfrak{p}} \in K_{\mathfrak{p}}$, where $\mathfrak{p}$ runs over all places of K and $a_{\mathfrak{p}}$ is an integer in $K_{\mathfrak{p}}$ for almost all $\mathfrak{p}$. The adèles form a ring (with respect to pointwise addition and multiplication), which we denote $\mathbb{A}_K$.
The *group of idèles* of K is the group of units $\mathbb{A}_K^*$ of $\mathbb{A}_K$. It consists of exactly those families $(a_{\mathfrak{p}})$ where $a_{\mathfrak{p}}$ is a unit in the local ring $\mathcal{O}_{\mathfrak{p}}$ for almost all $\mathfrak{p}$. (Cf. [Ne], beginning of §VI.1.)
We view $\mathbb{A}_K^*$ as a topological group in the usual way. Let c be a quasi-character of $\mathbb{A}_K^*$. For every finite place $\mathfrak{p}$ of K, let $c_{\mathfrak{p}}$ denote its restriction to $K_{\mathfrak{p}}^*$:

$$c_{\mathfrak{p}}(a_{\mathfrak{p}}) = c\,\big(\,(1, \ldots, a_{\mathfrak{p}}, \ldots, 1)\,\big) \text{ for } a_{\mathfrak{p}} \in K_{\mathfrak{p}}^*.$$

Then for every $\mathfrak{p}$, $c_{\mathfrak{p}}$ is a quasi-character of $K_{\mathfrak{p}}^*$. We define the global l-function by

$$l(c) := \prod_{\mathfrak{p}} l(c_{\mathfrak{p}}),$$

where the local l-function $l(c_{\mathfrak{p}})$ is defined by (4.10).
Let now ψ be a nontrivial additive character of $\mathbb{A}_K$, and for every place $\mathfrak{p}$, let $\psi_{\mathfrak{p}}$ be the restriction of ψ to $K_{\mathfrak{p}}$:

$$\psi_{\mathfrak{p}}(a_{\mathfrak{p}}) = \psi\,\big(\,(1, \ldots, a_{\mathfrak{p}}, \ldots, 1)\,\big) \text{ for } a_{\mathfrak{p}} \in K_{\mathfrak{p}}.$$

For each finite place $\mathfrak{p}$ of K, let $dx_{\mathfrak{p}}$ be a Haar measure on $K_{\mathfrak{p}}$. We assume these measures are chosen in such a way that

$$\int_{\mathcal{O}_{\mathfrak{p}}} dx_{\mathfrak{p}} = 1 \text{ for almost all } \mathfrak{p}.$$

Then one can define a measure on the ring of adèles $\mathbb{A}_K$ by a Fubini type construction that is due to Tate (cf. [Ta], Section 3.3). By Theorem 3.3.1

in [Ta], the measure constructed in this way satisfies the equation

$$\int_{\mathbb{A}_K} dx = \prod_{\mathfrak{p}} \int_{\mathcal{O}_{\mathfrak{p}}} dx_{\mathfrak{p}}$$

and may therefore be denoted $dx = \prod_{\mathfrak{p}} dx_{\mathfrak{p}}$.
Suppose that the local measures $dx_{\mathfrak{p}}$ are chosen in such a way that

$$\int_{\mathbb{A}_K} dx = 1.$$

Define ([De3] (3.11.3))

$$E(c, \psi, dx) := \prod_{\mathfrak{p}} E(c_{\mathfrak{p}}, \psi_{\mathfrak{p}}, dx_{\mathfrak{p}}),$$

where the local constants $E(c_{\mathfrak{p}}, \psi_{\mathfrak{p}}, dx_{\mathfrak{p}})$ are defined by the local functional equation (4.11).
Since the $dx_{\mathfrak{p}}$ were chosen in such a way that $\int_{\mathcal{O}_{\mathfrak{p}}} = 1$ for almost all $\mathfrak{p}$, (3.11.3) in [De3] yields that almost all factors in the product are equal to 1.

Proposition 4.3.3 ([De3] (3.11.3)). *$E(c, \psi, dx)$ is independent of the choice of ψ and of the decomposition $dx = \prod_{\mathfrak{p}} dx_{\mathfrak{p}}$, so that we can write*

$$E(c) := E(c, \psi, dx).$$

We have the functional equation

$$l(c) = E(c)l(\hat{c}),$$

where $\hat{c}(a) := |a|c^{-1}(a)$ and $|a| := \prod_{\mathfrak{p}} |a|_{\mathfrak{p}}$ for any adèle $a = (a_{\mathfrak{p}})_{\mathfrak{p}}$.

4.3.4 The local L-function and local epsilon constant of a higher dimensional representation

Let L/K be a finite Galois extension of local fields, in the sense of Definition 4.2.1. Let G be the Galois group and I the inertia group of L/K. Let l/k denote the corresponding extension of residue class fields, and let $q := |k|$. Let V be a complex representation of G. Then we define the local L-function of V as follows, where t is a complex variable.

$$L(V,t) := \det(1 - \mathcal{F}t|V^I)^{-1}, \tag{4.12}$$

where $\mathcal{F} \in G$ is a *geometric Frobenius*, i.e. the *inverse* of an automorphism inducing the map $x \mapsto x^q$ on the residue field of L. Furthermore, we put

$$l(V) := L(V,1).$$

When we are talking about *L-functions*, then we always write down the variables, i.e. we write $L(V,t)$ and $l(V)$ rather than L, l, which should avoid confusion with the notations L, l for a local field and its residue class field.

Remark 4.3.4. Suppose V is one-dimensional, and let χ be the character afforded by V. Let χ_K denote the multiplicative character of K^* that χ induces via local class field theory. Let l/k denote the extension of residue class fields for L/K. One can show that the norm residue symbol $(-, L/K) : K^* \to \mathrm{Gal}(L/K)$ composed with the projection $\mathrm{Gal}(L/K) \to \mathrm{Gal}(l/k)$ must map a prime element π_K of K to either the Frobenius of l/k or the geometric Frobenius (see [De3] (2.3) and [Wei]). Deligne normalizes the norm residue symbol in such a way that the prime elements correspond to the *geometric* Frobenius. With this choice, we obtain

$$\begin{aligned} l(V) &= 1 && \text{if } \chi|_I \not\equiv 1, \text{ i.e. if } \chi_K|_{\mathcal{O}_K^*} \not\equiv 1 \\ l(V) &= \tfrac{1}{1-\chi_K(\pi_K)} && \text{if } \chi|_I \equiv 1, \text{ i.e. if } \chi_K|_{\mathcal{O}_K^*} \equiv 1 \end{aligned}$$

Hence in this case, $l(V) = l(\chi_K)$ where the latter l-function is defined by Formula (4.10). In other words, the definition (4.10) of the local l-function of quasi-characters is compatible with the definition (4.12) of the local l-function of a representation.

Proposition 4.3.5 ([De3] (3.8.1) and (3.8.2)). *(a) For any short exact sequence*

$$0 \to V' \to V \to V'' \to 0$$

of complex representations of G, we have

$$l(V) = l(V')l(V'').$$

(b) Let $H \leq G$, $H = \mathrm{Gal}(L/L')$ for some intermediate field L', and let W be a complex representation of H. Then we have

$$l(\mathrm{Ind}_H^G(W)) = l(W),$$

where the first l-function is taken with respect to the extension L/K and the second l-function with respect to the extension L/L'.

(c) *Let H, L' as in part (b), let $\sigma \in G$, $H^\sigma := \sigma^{-1}H\sigma$, $H^\sigma = \mathrm{Gal}(L/L'')$ for some intermediate field L''. Let W^σ denote the vector space W with the action of H^σ given by*

$$\sigma^{-1}h\sigma.w := h.w \text{ for all } h \in H, w \in W.$$

Then we have

$$l(W^\sigma) = l(W),$$

where the first l-function is taken with respect to the extension L/L'' and the second l-function with respect to the extension L/L'.

Proof. Parts (a) and (b) are (3.8.1) and (3.8.2) in [De3]. For part (c), we consider

$$l(W) = \det\left(1 - \mathcal{F}|W^{I(L/L')} \right)$$

and

$$l(W^\sigma) = \det\left(1 - \mathcal{F}| \left(W^\sigma \right)^{I(L/L'')}\right).$$

It is easy to show that

$$\left(W^\sigma \right)^{I(L/L'')} = \sigma^{-1}.(W^{I(L/L')}) \le W.$$

It is then easy to check that the eigenvalues of $\mathcal{F}$ on $W^{I(L/L')}$ are the same as those on $(W^\sigma)^{I(L/L'')}$, so the determinant of $1 - \mathcal{F}$ on both spaces is the same. The assertion follows. □

Theorem 4.3.6 (cf. Theorem 4.1 in [De3]). *There is a unique function ε, satisfying 1.-4. below, which assigns a number $\varepsilon(V, \psi, dx) \in \mathbb{C}^*$ to any isomorphism class of sextuples $(L/K, \psi, dx, V, \rho)$ consisting of an extension of local fields L/K, a nontrivial additive character $\psi : K \to \mathbb{C}^*$, a Haar measure dx on K, a finite dimensional complex vector space V and a representation $\rho : G := \mathrm{Gal}(L/K) \to GL(V)$.*

1. *For any short exact sequence*

$$0 \to V' \to V \to V'' \to 0$$

of complex representations of G, *we have*

$$\varepsilon(V,\psi,dx)=\varepsilon(V',\psi,dx)\varepsilon(V'',\psi,dx).$$

Hence ε *is well-defined on* virtual complex representations *of* G, *i.e. on elements of the Grothendieck group* $K_0(\mathbb{C}[G])$.

2. *For any* $a\in\mathbb{R}$, *we have*

$$\varepsilon(V,\psi,adx)=a^{\dim V}\varepsilon(V,\psi,dx).$$

In particular, if V *is a virtual representation of dimension zero, then* $\varepsilon(V,\psi,dx)=:\varepsilon(V,\psi)$ *is independent of* dx.

3. *Let* $H\le G$, $H=\mathrm{Gal}(L/L')$ *for some intermediate field* L', *and let* W *be a virtual representation of dimension zero of* H, *i.e.* W *is an element of* $K_0(\mathbb{C}[G])$ *that is mapped to zero under the homomorphism* $K_0(\mathbb{C}[G])\to\mathbb{Z}$, $[M]\mapsto\dim_{\mathbb{C}}M$. *Then we have*

$$\varepsilon(W,\psi)=\varepsilon(\mathrm{Ind}_H^G(W),\psi\circ\mathrm{Tr}_{L/K}).$$

4. *If* $\dim V=1$ *and* $\chi: G\to\mathbb{C}^*$ *is the character afforded by* V, *then we have*

$$\varepsilon(V,\psi,dx)=E(\chi_K,\psi,dx).$$

Here χ_K *denotes the multiplicative character* $K^*\to\mathbb{C}^*$ *that* χ *induces via local class field theory, and* $E(\chi_K,\psi,dx)$ *denotes the constant from the local functional equation (4.11).*

4.3.5 The global L-function of a higher-dimensional representation – and its functional equation

Let L/K be a finite Galois extension of global fields, of group G. Let V be a finite dimensional complex representation of G. For every place $\mathfrak{p}$ of K, we define

$$V_{\mathfrak{p}}:=\mathrm{Res}^G_{G_{\mathfrak{p}}}(V),$$

where $G_{\mathfrak{p}}=\mathrm{Gal}(L_{\mathfrak{p}}/K_{\mathfrak{p}})$ is the decomposition group at an arbitrary but fixed place lying over $\mathfrak{p}$, and $L_{\mathfrak{p}}$ is the completion of L at that place. Furthermore, we write $I_{\mathfrak{p}}$ for the inertia group of $L_{\mathfrak{p}}/K_{\mathfrak{p}}$ and $\mathcal{F}(\mathfrak{p})$ for a geometric Frobenius of $L_{\mathfrak{p}}/K_{\mathfrak{p}}$. The global L-function is then defined as follows: ([De3] (5.11.1), [Ch])

$$L(V,t) := \prod_{\mathfrak{p}} L(V_{\mathfrak{p}},t) = \prod_{\mathfrak{p}} \det(1 - \mathcal{F}(\mathfrak{p})t^{[k_{\mathfrak{p}}:\mathbb{F}_p]}|V_{\mathfrak{p}}^{I_{\mathfrak{p}}})^{-1} \tag{4.13}$$

Note that $L(V,t)$ does not depend on the choice of a "place lying over $\mathfrak{p}$"! Furthermore, we put

$$l(V) := L(V,1). \tag{4.14}$$

Lemma 4.3.7. *(a) For any short exact sequence*

$$0 \to V' \to V \to V'' \to 0$$

of complex representations of G, we have

$$l(V) = l(V')l(V'').$$

(b) Suppose now that L, K are function fields in one variable over a finite field $\mathbb{F}_q$. Let $H \leq G$, $H = \mathrm{Gal}(L/L')$ for some intermediate field L', and let W be a complex representation of H. Then we have

$$l(\mathrm{Ind}_H^G(W)) = l(W),$$

where the first l-function is taken with respect to the extension L/K and the second l-function with respect to the extension L/L'.

Proof. (a) Part (a) follows readily from the definition and Proposition 4.3.5 (a).

(b) Let X be a nonsingular projective curve over $\mathbb{F}_q$ with function field L, and let $Y := X/G$, with function field K. By definition (Formulae (4.13) and (4.14)), $l(\mathrm{Ind}_H^G(W))$ is equal to a product of local l-functions as follows:

$$l(\mathrm{Ind}_H^G(W)) = \prod_{\mathfrak{p}\text{ place of K}} l\left(\mathrm{Res}^G_{G_{\mathfrak{p}}}(\mathrm{Ind}_H^G(W))\right) = \prod_{R\in|Y|} l\left(\mathrm{Res}^G_{G_{\tilde{R}}}(\mathrm{Ind}_H^G(W))\right),$$

where for any $R \in Y$, $\tilde{R}$ denotes an arbitrary but fixed preimage of R on X.

For every $R \in |Y|$, let T_R be a system of representatives of the $H - G_{\tilde{R}}$-double cosets, i.e. T_R is such that G can be written as a disjoint union

$$G = \bigcup_{\tau \in T_R} H\tau G_{\tilde{R}}.$$

This means that the G-orbit of $\tilde{R} \in |X|$ is the disjoint union of the H-orbits of the points $\tau(\tilde{R})$, $\tau \in T_R$, i.e. we have a bijection between T_R and the closed points of the curve $Z := X/H$ which lie above R.

By Mackey's subgroup theorem (Theorem 10.13 in [CR]), we have

$$\begin{aligned}
\operatorname{Res}^G_{G_{\tilde{R}}}(\operatorname{Ind}^G_H(W)) &= \sum_{\tau \in T_R} \operatorname{Ind}^{G_{\tilde{R}}}_{H^\tau \cap G_{\tilde{R}}} \operatorname{Res}^{H^\tau}_{H^\tau \cap G_{\tilde{R}}}(W^\tau) \\
&= \sum_{\tau \in T_R} \left(\operatorname{Ind}^{G_{\tau(\tilde{R})}}_{H_{\tau(\tilde{R})}} \operatorname{Res}^H_{H_{\tau(\tilde{R})}}(W) \right)^\tau .
\end{aligned}$$

Hence we have

$$\begin{aligned}
l\left(\operatorname{Res}^G_{G_{\tilde{R}}}(\operatorname{Ind}^G_H(W)) \right) &= l\left(\sum_{\tau \in T_R} \left(\operatorname{Ind}^{G_{\tau(\tilde{R})}}_{H_{\tau(\tilde{R})}} \operatorname{Res}^H_{\tau(\tilde{R})}(W) \right)^\tau \right) \\
&= \prod_{\tau \in T_{\tilde{R}}} l\left(\left(\operatorname{Ind}^{G_{\tau(\tilde{R})}}_{H_{\tau(\tilde{R})}} \operatorname{Res}^H_{H_{\tau(\tilde{R})}}(W) \right)^\tau \right) \quad \text{by Proposition 4.3.5 (a)} \\
&= \prod_{\tau \in T_{\tilde{R}}} l\left(\operatorname{Ind}^{G_{\tau(\tilde{R})}}_{H_{\tau(\tilde{R})}} \operatorname{Res}^H_{H_{\tau(\tilde{R})}}(W) \right) \quad \text{by Proposition 4.3.5 (c).}
\end{aligned}$$

It follows that

$$\begin{aligned}
l(\operatorname{Ind}^G_H(W)) &= \prod_{R \in |Y|} l\left(\operatorname{Res}^G_{G_{\tilde{R}}}(\operatorname{Ind}^G_H(W)) \right) \\
&= \prod_{R \in |Y|} \prod_{\tau \in T_{\tilde{R}}} l\left(\operatorname{Ind}^{G_{\tau(\tilde{R})}}_{H_{\tau(\tilde{R})}} \operatorname{Res}^H_{H_{\tau(\tilde{R})}}(W) \right) \\
&= \prod_{Q \in |Z|} l\left(\operatorname{Ind}^{G_{\tilde{Q}}}_{H_{\tilde{Q}}} \operatorname{Res}^H_{H_{\tilde{Q}}}(W) \right) \\
&= \prod_{Q \in Z} l(\operatorname{Res}^H_{H_{\tilde{Q}}}(W)) \quad \text{by Proposition 4.3.5 (b)} \\
&= l(W).
\end{aligned}$$

□

Let $\psi = (\psi_\mathfrak{p})$, $dx = \prod_\mathfrak{p} dx_\mathfrak{p}$ as in Subsection 4.3.3. Then we define the global epsilon constants as follows. ([De3] (5.11.2))

$$\varepsilon(V, \psi, dx) := \prod_\mathfrak{p} \varepsilon(V_\mathfrak{p}, \psi_\mathfrak{p}, dx_\mathfrak{p}),$$

where $\varepsilon(V_\mathfrak{p}, \psi_\mathfrak{p}, dx_\mathfrak{p})$ are the local epsilon constants from Theorem 4.3.6.

Proposition 4.3.8. *$\varepsilon(V, \psi, dx)$ is independent of the choice of ψ and of the decomposition of dx, so that we can write*

$$\varepsilon(V) := \varepsilon(V, \psi, dx).$$

If L, K are of positive characteristic p, then we have the functional equation

$$L(V, 1) = \varepsilon(V) L(V^*, \frac{1}{p}), \tag{4.15}$$

where V^* denotes the contragredient of V.

This proposition follows from the proof of 5.11 in [De3]; in particular, the functional equation (4.15) is Formula (5.11.3) in [De3].

Remark 4.3.9. The functional equation (4.15) is part of the *Weil conjectures*, which are no longer conjectures – the proof of the most general case was completed by Deligne in [De1] and [De2] – and play a very important role in algebraic number theory. The Weil conjectures also state that the global epsilon constants are always algebraic numbers, i.e. that they lie in $\bar{\mathbb{Q}}^*$. For the special case where L/K is a cyclic extension, we will see this more explicitly in Subsection 4.5.1.

From the functional equation (4.15) and from Lemma 4.3.7, we easily deduce the following properties of the global epsilon constants.

Lemma 4.3.10. *(a) For a short exact sequence*

$$0 \to V' \to V \to V'' \to 0$$

of representations, we have

$$\varepsilon(V) = \varepsilon(V')\varepsilon(V'').$$

(b) For $H \leq G$, defining an intermediate field L', and V a virtual representation, we have

$$\varepsilon(\mathrm{Ind}_H^G(V)) = \varepsilon(V).$$

4.4 Chinburg's theorem

Let $\pi : X \to Y$ be a tamely ramified cover of nonsingular, geometrically irreducible projective curves over a finite field $\mathbb{F}_m$ of characteristic p, such that the corresponding extension of function fields, denoted L/K, is a Galois extension, of group G.

Definition 4.4.1. The equivariant Euler characteristic of the de Rham complex of X/Y is defined as

$$\psi(X/Y) := [H^0(X, \mathcal{O}_X)] - [H^1(X, \mathcal{O}_X)] \in K_0(G, \mathbb{F}_p).$$

By Theorem 2.4.10, we may view $\psi(X/Y)$ as an element of the Grothendieck group $K_0(\mathbb{F}_p[G])$ of projective $\mathbb{F}_p[G]$-modules.

Remark 4.4.2. In the literature, depending on the author, the notation $\psi(X/Y)$ can mean the Euler characteristic in $K_0(\mathbb{Z}[G])$, in $K_0(\mathbb{F}_p[G])$ (cf. [Ch]), or in $K_0(\mathbb{F}_m[G])$ (cf. [Er]).

In order to state Chinburg's formula for $\psi(X/Y)$, we first have to explain the "Hom description" of the Grothendieck group $K_0(\mathbb{F}_m[G])$.
For $k = \bar{\mathbb{Q}}$, $\mathbb{C}$, or $\bar{\mathbb{Q}}_p$, let $R_{G,K}$ denote the ring of virtual characters from G to K, i.e. the ring formed by linear combinations of characters afforded by K-representations of G.

Proposition 4.4.3 (Hom description). *Let W be the Witt ring of $\mathbb{F}_m$. Fix an embedding of W into $\bar{\mathbb{Q}}_p$, and let $F(W)$ be the fraction field of W. Let $\Omega_{F(W)} := \mathrm{Gal}(\bar{\mathbb{Q}}_p/F(W))$. Then there is an injective homomorphism*

$$\Delta : K_0(\mathbb{F}_m[G]) \hookrightarrow \mathrm{Hom}_{\Omega_{F(W)}}(R_{G,\bar{\mathbb{Q}}_p}, \bar{\mathbb{Q}}_p^*)$$

as follows:
Suppose $\bar{P}$ is a finitely generated projective $\mathbb{F}_m[G]$-module. Then $\bar{P}$ is isomorphic to P/pP for some finitely generated projective $W[G]$-module P. This follows from the Cartan-Brauer triangle (see §18 A in [CR], in particular Proposition 18.5).
Let now $\chi_{\bar{\mathbb{Q}}_p \otimes_W P}$ be the character of the $\bar{\mathbb{Q}}_p$-representation $\bar{\mathbb{Q}}_p \otimes_W P$. (The tensor product is defined via the embedding $W \to \bar{\mathbb{Q}}_p$ fixed earlier.) Note that $\bar{\mathbb{Q}}_p \otimes_W P$ is the image of $\bar{P}$ under the map e from the Cartan-Brauer triangle (see (18.3) in [CR] for the definition of e).

Write $\chi_{\bar{\mathbb{Q}}_p \otimes_W P}$ *as a sum of irreducible characters in* $R_{G,\bar{\mathbb{Q}}_p}$,

$$\chi_{\bar{\mathbb{Q}}_p \otimes_W P} = \sum_{\chi} m_\chi \chi. \tag{4.16}$$

then $\Delta(\bar{P})$ *is the element of* $\mathrm{Hom}_{\Omega_{F(W)}}(R_{G,\bar{\mathbb{Q}}_p}, \bar{\mathbb{Q}}_p^*)$ *given by*

$$\Delta(\bar{P})(\chi) = p^{-m_\chi}$$

for any irreducible character $\chi \in R_{G,\mathbb{Q}_p}$.

Proposition 4.4 in [Ch] shows that this construction does define a (uniquely determined) homomorphism Δ, which appears in his formula for the equivariant Euler characteristic.

We are now in position to explain Chinburg's formula. Throughout the rest of this whole chapter, we consider the algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ as a subset of $\mathbb{C}$ and fix an embedding $j_p : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$. We also write j_p for the induced map $R_{G,\bar{\mathbb{Q}}} \to R_{G,\bar{\mathbb{Q}}_p}$ of character rings. Since all p-adic virtual characters of G take values in $\bar{\mathbb{Q}}$, this map is an isomorphism. Similarly, the embedding $\bar{\mathbb{Q}} \to \mathbb{C}$ induces an isomorphism between $R_{G,\bar{\mathbb{Q}}}$ and $R_{G,\mathbb{C}}$.

$$\begin{tikzcd} & \mathbb{C} \\ \bar{\mathbb{Q}} \arrow[ur, "\subseteq"] \arrow[dr, "j_p"'] & \\ & \bar{\mathbb{Q}}_p \end{tikzcd} \qquad \begin{tikzcd} & R_{G,\mathbb{C}} \\ R_{G,\bar{\mathbb{Q}}} \arrow[ur, "\text{``$=$''}"] \arrow[dr, "j_p"'] & \\ & R_{G,\bar{\mathbb{Q}}_p} \end{tikzcd}$$

Theorem 4.4.4 (Theorem 5.2 in [Ch]). *Let* $\chi_V \in R_{G,\mathbb{C}}$ *be the character of the complex representation* V *of* G, *and let* V^* *be the dual (contragredient) of* V. *Let* $\Delta : K_0(\mathbb{F}_p[G]) \hookrightarrow \mathrm{Hom}_{\Omega_{F(W)}}(R_{G,\bar{\mathbb{Q}}_p}, \bar{\mathbb{Q}}_p^*)$ *be the injective homomorphism from Proposition 4.4.3 relative to the prime field* $\mathbb{F}_p$. *Let* $|\,|_p$ *be the extension of the standard absolute value on* $\mathbb{Q}_p$ *to* $\bar{\mathbb{Q}}_p$. *Then we have*

$$\Delta(\psi(X/Y))(j_p\chi_V) = |j_p\varepsilon(V^*)^{-1}|_p.$$

In particular, $|j_p(\varepsilon(V^*)^{-1}|_p$ *is an integral power of* p *and hence an element of* $\mathbb{Q}$.

Note that in order to formulate this theorem, it is crucial that the epsilon constants are algebraic numbers, so they lie in $\bar{\mathbb{Q}}$ and we can consider their image in $\bar{\mathbb{Q}}_p$ under the embedding j_p, to which we can then assign a p-adic value.

Next, we state Erez' reformulation of Chinburg's theorem.

Definition 4.4.5. For any $g \in G$, let

$$S(g) := -\sum_{\chi} v_p(j_p\varepsilon(\chi)) \cdot j_p(\chi(g)) \in \bar{\mathbb{Q}}_p,$$

where the sum is taken over all irreducible complex characters of G, and

$$C(g) := \mathrm{Trace}(g|\psi(X/Y)) \in \bar{\mathbb{Q}}_p,$$

where $\mathrm{Trace}(-,-)$ denotes the modular character defined in Subsection 4.2.3.

Theorem 4.4.6 (Theorem 2.1 in [Er]). *For any $g \in G$ of order prime to p, we have*

$$S(g) = C(g).$$

Lemma 4.4.7. *Theorem 4.4.6 and Theorem 4.4.4 are equivalent.*

Proof. Assume first that Theorem 4.4.4 holds for any complex representation V of G.

In analogy to Formula 4.16, we write

$$\mathrm{Trace}_{\mathbb{F}_m}(g|\psi(X/Y)) = \mathrm{Trace}_{\bar{\mathbb{Q}}_p}(g|e(\psi(X/Y)) = \sum_{\chi \text{ irred.}} m_\chi \chi(g), \qquad (4.17)$$

where χ runs over the irreducible $\bar{\mathbb{Q}}_p$-representations of G.

In the following calculation, χ runs first over the irreducible complex representations of G and then later over the irreducible $\mathbb{Q}_p$ representations of G. The map j_p fixed earlier maps these 1-1 to each other.

$$\begin{aligned}
S(g) &= -\sum_{\chi \text{ complex irr.}} v_p(j_p\varepsilon(j_p\chi))\chi(g) \\
&= -\sum_{\chi \text{ complex irr.}} \log_p(\Delta(\psi(X/Y))(j_p(\chi)))(j_p\chi)(g) \quad \text{by Theorem 4.4.4 for each } \chi \\
&= -\sum_{\chi \text{ p-adic irr.}} \log_p(\Delta(\psi(X/Y))(\chi))(\chi)(g) \\
&= -\sum_{\chi \text{ p-adic irr.}} \log_p(p^{-m_{j_p\chi}}) \cdot \chi(g) \qquad \text{by definition of } \Delta \\
&= \sum_{\chi \text{ p-adic irr.}} m_\chi \chi(g) \\
&= \mathrm{Trace}(g|\psi(X/Y)) \\
&= C(g)
\end{aligned}$$

Assume now that Theorem 4.4.6 is true, that is,

$$\sum_\chi v_p(j_p\varepsilon(j_p\chi))\chi(g) = \mathrm{Trace}(g|\psi(X/Y))$$

for all $g \in G_{\mathrm{reg}}$. With the notation (4.17) from above, we have the following, where all sums run over the irreducible complex characters:

$$\begin{aligned}
&-\sum_\chi v_p(j_p\varepsilon(j_p\chi)) \cdot (j_p\chi)(g) \\
&\quad = \mathrm{Trace}(g|\psi(X/Y)) \quad \text{by Theorem 4.4.6} \\
&\quad = \sum_\chi m_{j_p\chi} j_p\chi(g) \\
&\quad = -\sum_\chi \log_p(\Delta(\psi(X/Y))(j_p(\chi)))j_p\chi(g)
\end{aligned}$$

The first and last line are just the characters of two $\bar{\mathbb{Q}}_p$- representations of G. Since the above expression holds for any $g \in G_{\mathrm{reg}}$, the representations are equal, and by taking the character pairing with every irreducible character, we see that the coefficients are equal.

Hence we have

$$-v_p(\varepsilon(\chi)) = -\log_p(\Delta(\psi(X/Y))(j_p(\chi))),$$

and so

$$|\varepsilon(\chi))|_p = (\Delta(\psi(X/Y))(j_p(\chi)))$$

for any *irreducible* character χ. It follows from the proposition below that Theorem 4.4.4 then holds for *all* characters afforded by complex representations of G. □

Proposition 4.4.8. *To prove Theorem 4.4.4, it suffices to prove it for G cyclic and V irreducible.*

Proof. We use Artin's induction theorem (Theorem (15.4) in [CR]): Any character of a finite group can be written as a rational linear combination of characters induced from characters of cyclic subgroups, i.e.

$$\chi = \sum_{H \leq G \text{ cyclic}} m_H \operatorname{Ind}_H^G(\chi_H)$$

with coefficients $m_H \in \mathbb{Q}$.
Equivalently, there exists $d \in \mathbb{N}$ such that we can write

$$d \cdot \chi = \sum_{H \leq G \text{ cyclic}} n_H \operatorname{Ind}_H^G(\chi_H) \tag{4.18}$$

with *integer* coefficients $n_H \in \mathbb{Z}$.
Since induction commutes with direct sums and since every character is a $\mathbb{Z}$-linear combination of irreducible ones, we may assume that the χ_H are *irreducible* characters.
With the notation of Formula 4.18, we get

$$\begin{aligned}
\varepsilon(\chi)^d &= \varepsilon(d \cdot \chi) && \text{by property } (G1) \text{ from Lemma 4.3.10} \\
&= \varepsilon\Big(\sum_{H \leq G \text{ cyclic}} n_H \operatorname{Ind}_H^G(\chi_H) \Big) \\
&= \prod_{H \leq G \text{ cyclic}} \varepsilon(\operatorname{Ind}_H^G \chi_H)^{n_H} && \text{by property } (a) \text{ from Lemma 4.3.10} \\
&= \prod_{H \leq G \text{ cyclic}} \varepsilon(\chi_H)^{n_H} && \text{by property } (b) \text{ from Lemma 4.3.10.}
\end{aligned}$$

Hence the d-th power of the right-hand side of Chinburg's theorem can be written as follows:

$$|\varepsilon(\chi)^{-1}|_p^d = \prod_{H \leq G \text{ cyclic}} |\varepsilon(\chi_H)|_p^{-n_H}.$$

On the other hand, because $\Delta(\psi(X/Y))$ is a homomorphism, we have

$$\begin{aligned}
(\,\Delta(\psi(X/Y))(\chi)\,)^d &= \Delta(\psi(X/Y))(d \cdot \chi) \\
&= \Delta(\psi(X/Y))\,(\sum_{H \leq G \text{ cyclic}} n_H \operatorname{Ind}_H^G(\chi_H)\,) \\
&= \prod_{H \leq G \text{ cyclic}} \Big(\,\Delta(\psi(X/Y))\,(\operatorname{Ind}_H^G(\chi_H)\,)\Big)^{n_H} \\
&= \prod_{H \leq G \text{ cyclic}} (\,\Delta(\operatorname{Res}_H^G \psi(X/Y))(\chi_H)\,)^{n_H}
\end{aligned}$$

The last step is due Frobenius reciprocity; see also Proposition 4.7 in [Ch]. Assume now that Chinburg's theorem holds for cyclic groups. Then we have

$$\Delta(\operatorname{Res}_H^G \psi(X/Y))(\chi_H) = |\varepsilon(\chi_H)^{-1}|_p$$

for all cyclic subgroups H of G.

This together with the above calculation yields

$$(\,\Delta(\psi(X/Y))(\chi)\,)^d = \prod_{H \leq G \text{ cyclic}} |\varepsilon(\chi_H)|_p^{-n_H} = |\varepsilon(\chi)^{-1}|_p^d$$

Hence the d-the powers of both sides of Chinburg's theorem are equal. Since the p-adic absolute value $|\ |_p$ only takes values in the positive rational number $\mathbb{Q}^+$ (even when it is extended to $\bar{\mathbb{Q}}_p$), both sides are in $\mathbb{Q}$, it is uniquely determined by its d-th power. Hence we have

$$(\,\Delta(\psi(X/Y))(\chi)\,) = |\varepsilon(\chi)^{-1}|_p$$

and Theorem 4.4.4 holds. □

Remark 5.4 in [Ch] yields another useful reduction:

Lemma 4.4.9. *In order to prove Theorem 4.4.4 for nonsingular, geometrically irreducible projective curves over a finite field $\mathbb{F}_m$, it suffices to prove it for the case in which the underlying field is a prime field $\mathbb{F}_p$.*

Proof (Chinburg). Let p be the characteristic of $\mathbb{F}_m$. Let $\hat{X} \to \hat{Y}$ be the cover $X \to Y$ viewed as a cover of curves over $\mathbb{F}_p$ rather than over $\mathbb{F}_m$. Then we have

$$\psi(\hat{X}/\hat{Y}) = \psi(X/Y) \text{ in } K_0(\mathbb{F}_p[G]).$$

Let $a := [\mathbb{F}_m : \mathbb{F}_p]$, and let V ve a complex representation of G. Let $L(V,t)$ denote the Artin L-function associated to V and to the cover X/Y. Let $\hat{L}(V,t)$ be the Artin L-function associated to V and to the cover $\hat{X}/\hat{Y}$. One easily verifies that

$$L(V, t^a) = \hat{L}(V,t).$$

It follows that the corresponding epsilon constants are equal.
So if theorem 4.4.4 holds for the cover $\hat{X} \to \hat{Y}$, then it also holds for the cover $X \to Y$. $\square$

4.5 Proof of Theorem 4.4.6

In this section, we prove Theorem 4.4.6 for the case of curves over $\mathbb{F}_p$, and for a cyclic group G. By the reductions above, this is enough to prove both Theorem 4.4.4 and Theorem 4.4.6 in the general form quoted earlier.
As before, L, K denote the function fields of X, Y respectively, and $\mathfrak{p}$ usually denotes a place of K.
We choose local additive characters $\psi_\mathfrak{p} : K_\mathfrak{p} \to \mathbb{C}^*$ that satisfy the following conditions.

- For every ramified place $\mathfrak{p}$, we have $\psi_\mathfrak{p}|_{\mathfrak{m}_\mathfrak{p}} \equiv 1$, such that $\psi_\mathfrak{p}$ induces an additive character $\psi_{k_\mathfrak{p}}$ of the residue class field $k_\mathfrak{p}$. We require this induced character to be of the form

$$\psi_{k_\mathfrak{p}}(x) = \zeta_p^{\mathrm{Tr}(x)},$$

where $\zeta_p := e^{\frac{2\pi i}{p}}$ and $\mathrm{Tr}(x) = \mathrm{Trace}_{k_\mathfrak{p}/\mathbb{F}_p}(x)$.

- For every unramified place $\mathfrak{p}$, we have $\psi_\mathfrak{p}|_{\mathcal{O}_\mathfrak{p}} \equiv 1$.

These local characters can then be "glued together" to an additive character ψ of $\mathbb{A}_K$ via the assignment

$$\psi\left((a_\mathfrak{p})_\mathfrak{p} \right) := \prod_\mathfrak{p} \psi_\mathfrak{p}(a_\mathfrak{p}).$$

Since there are only finitely many ramified places and therefore only finitely many $\mathfrak{p}$ with $\psi_\mathfrak{p}(a_\mathfrak{p}) \neq 1$, the product is finite, so ψ is well-defined.
Now we choose local Haar measures $dx_\mathfrak{p}$ that satisfy

$$\int_{\mathcal{O}_\mathfrak{p}} dx_\mathfrak{p} = 1 \text{ for all places } \mathfrak{p}.$$

Furthermore, we write

$$\overline{dx}_\mathfrak{p} := q\, dx_\mathfrak{p},$$

where q is the number of elements in $k_\mathfrak{p}$. One easily checks that

$$\int_{\mathfrak{m}_\mathfrak{p}} \overline{dx}_\mathfrak{p} = 1$$

(see also [Wei]). Moreover, the measure

$$dx = \prod_\mathfrak{p} dx_\mathfrak{p}$$

on $\mathbb{A}_K$ satisfies

$$\int_{\mathbb{A}_K} dx = 1.$$

4.5.1 The left-hand side of Theorem 4.4.6 for $g \neq \mathrm{id}$

Assume that g is an element of G whose order is coprime to p, and that g is not the identity. By definition, we have

$$\begin{aligned} S(g) &= -\sum_\chi v_p(j_p\varepsilon(\chi)) \cdot j_p\chi(g) \\ &= -\sum_\chi v_p\left(j_p \prod_\mathfrak{p} \varepsilon(\chi_\mathfrak{p}, \psi_\mathfrak{p}, dx_\mathfrak{p}) \right) \cdot j_p\chi(g), \end{aligned}$$

where the sums run over the irreducible complex characters of G, the product in the second line runs over the finite places of $K = K(Y)$, and $\chi_{\mathfrak{p}}$ denotes the restriction of χ to $G_{\mathfrak{p}}$. (Cf. Subsection 4.3.5.)

If $\mathfrak{p}$ is an unramified place, then for any character χ, the restriction $\chi_{\mathfrak{p}}$ and the corresponding character $\chi_{K_{\mathfrak{p}}}$ of $K_{\mathfrak{p}}^*$ are "unramified" in the sense of Deligne (2.3 in [De3]). It then follows from Formula 5.9 in [De3] that

$$\varepsilon(\chi_{\mathfrak{p}}, \psi_{\mathfrak{p}}, dx_{\mathfrak{p}}) = 1.$$

For Formula 5.9 in [De3] to hold, we need that $\int_{\mathcal{O}_{\mathfrak{p}}} dx_{\mathfrak{p}} = 1$, which is true because of our choice of $dx_{\mathfrak{p}}$.

Hence only the ramified places contribute to the product above, so the formula remains true if $\mathfrak{p}$ runs only over the ramified places.

Let now $\mathfrak{p}$ be a ramified place. Let V be an irreducible representation of G, affording the character χ. We define the "twisted epsilon constant"

$$\varepsilon_0(\chi_{\mathfrak{p}}, \psi_{\mathfrak{p}}, dx_{\mathfrak{p}})$$

by

$$\varepsilon(\chi_{\mathfrak{p}}, \psi_{\mathfrak{p}}, dx_{\mathfrak{p}}) = \varepsilon_0(\chi_{\mathfrak{p}}, \psi_{\mathfrak{p}}, dx_{\mathfrak{p}}) \cdot \det(-\operatorname{Frob}(\mathfrak{p}), V_{\mathfrak{p}}^{I_{\mathfrak{p}}})^{-1},$$

using the same notations as in the definition of the Artin L-function, see Formula (4.13).

The p-adic valuations of $\varepsilon(\chi_{\mathfrak{p}}, \psi_{\mathfrak{p}}, dx_{\mathfrak{p}})$ and $\varepsilon_0(\chi_{\mathfrak{p}}, \psi_{\mathfrak{p}}, dx_{\mathfrak{p}})$ are the same. Indeed, since the determinant term is a product of $f_{\mathfrak{p}}$-th roots of unity, it has valuation zero.

Hence the left-hand side of Theorem 4.4.6 becomes

$$\begin{aligned} S(g) &= -\sum_{\chi} v_p \Big(\prod_{\mathfrak{p} \text{ ramified}} j_p \varepsilon(\chi_{\mathfrak{p}}, \psi_{\mathfrak{p}}, dx_{\mathfrak{p}}) \Big) \cdot j_p \chi(g) \\ &= -\sum_{\chi} \sum_{\mathfrak{p} \text{ ramified}} v_p \Big(j_p \varepsilon(\chi_{\mathfrak{p}}, \psi_{\mathfrak{p}}, dx_{\mathfrak{p}}) \Big) \cdot j_p \chi(g) \\ &= -\sum_{\chi} \sum_{\mathfrak{p} \text{ ramified}} v_p \Big(j_p \varepsilon_0(\chi_{\mathfrak{p}}, \psi_{\mathfrak{p}}, dx_{\mathfrak{p}}) \Big) \cdot j_p \chi(g). \end{aligned}$$

In [De3], Deligne expresses the twisted epsilon constants as a Gauss sum. We explain the terms in this Gauss sum before stating it.

Local class field theory yields, for every place $\mathfrak{p}$ of $K(Y)$, a surjective homomorphism

$$\alpha : k_{\mathfrak{p}}^* = \mathcal{O}_{\mathfrak{p}}^*/\mathfrak{m}_{\mathfrak{p}} \to I_{\mathfrak{p}}$$

(see Subsection 4.2.2). The existence of the surjective homomorphism α implies that $\# k_{\mathfrak{p}}^*$ is divisible by $e_{\mathfrak{p}}$.
As explained in Subsection 4.2.2, if χ is a character of G or $G_{\mathfrak{p}}$, then χ defines a character $\chi_{k_{\mathfrak{p}}}$ of $k_{\mathfrak{p}}^*$ making the following diagram commute:

$$\begin{tikzcd} k_{\mathfrak{p}}^* \arrow[r, "\alpha"] \arrow[dr, dashed, "\chi_{k_{\mathfrak{p}}}"'] & I_{\mathfrak{p}} \arrow[d, "\chi|_{I_{\mathfrak{p}}}"] \\ & \mathbb{C}^* \end{tikzcd}$$

The character $\chi_{k_{\mathfrak{p}}}$ only depends on the restriction of χ to $I_{\mathfrak{p}}$, and thus is trivial if this restriction is.
Recall that we had chosen the local additive characters $\psi_{\mathfrak{p}} : K \to \mathbb{C}^*$ in such a way that $\psi_{\mathfrak{p}}|_{\mathfrak{m}_{\mathfrak{p}}} \equiv 0$ for every place $\mathfrak{p}$ of K. Hence for every $\mathfrak{p}$, we have an additive character $\psi_{k_{\mathfrak{p}}} : k_{\mathfrak{p}} \to \mathbb{C}^*$ making the following diagram commute.

$$\begin{tikzcd} \mathcal{O}_{\mathfrak{p}} \arrow[r, "\psi_{\mathfrak{p}}|_{\mathcal{O}_{\mathfrak{p}}}"] \arrow[d] & \mathbb{C}^* \\ k_{\mathfrak{p}} \arrow[ur, dashed, "\psi_{k_{\mathfrak{p}}}"'] & \end{tikzcd}$$

By (5.10) in [De3], the twisted epsilon constant defined above can be written as a Gauss sum as follows:

$$\varepsilon_0(\chi_{\mathfrak{p}}, \psi_{\mathfrak{p}}, \overline{dx}_{\mathfrak{p}}) = \tau(\chi_{k_{\mathfrak{p}}}) := \sum_{x \in k_{\mathfrak{p}}^*} \chi_{k_{\mathfrak{p}}}^{-1}(x) \cdot \psi_{k_{\mathfrak{p}}}(x). \tag{4.19}$$

(With Deligne's notation, this Gauss sum would be denoted $-\tau(\chi_{k_{\mathfrak{p}}}, \psi_{k_{\mathfrak{p}}})$.)
In this formula, we have used the measure $\overline{dx}_{\mathfrak{p}}$ rather than the measure $dx_{\mathfrak{p}}$, because (5.10) in [De3] requires the measure to be normalized in such a way that the volume of the maximal ideal is equal to 1. Now since $\overline{dx}_{\mathfrak{p}} = q\, dx_{\mathfrak{p}}$, the second property of the local epsilon constants (cf.

Theorem 4.3.6) yields that

$$\begin{aligned}\varepsilon_0(\chi_\mathfrak{p}, \psi_\mathfrak{p}, dx_\mathfrak{p}) &= \varepsilon_0(\chi_\mathfrak{p}, \psi_\mathfrak{p}, \frac{1}{q}\overline{dx}_\mathfrak{p}) \\ &= \frac{1}{q}\,\varepsilon_0(\chi_\mathfrak{p}, \psi_\mathfrak{p}, \overline{dx}_\mathfrak{p}) \\ &= \frac{1}{q}\,\tau(\chi_{k_\mathfrak{p}}).\end{aligned}$$

It follows that

$$v_p(\varepsilon_0(\chi_\mathfrak{p}, \psi_\mathfrak{p}, dx_\mathfrak{p})) = -[k_\mathfrak{p} : \mathbb{F}_p] + v_p(\tau(\chi_{k_\mathfrak{p}})).$$

Remark 4.5.1. Since the Gauss sum in Formula (4.19) is a sum of products of roots of unity, it is an algebraic number. Hence Formula (4.19) shows that the local epsilon constants at ramified places are algebraic numbers. As seen above, they are equal to 1 at the unramified places, so the product

$$\varepsilon(\chi) = \prod_\mathfrak{p} \varepsilon(\chi_\mathfrak{p})$$

is an algebraic number, too. The fact that both the global and local epsilon constants are algebraic numbers means that "taking the p-adic valuation of their image under j_p" always makes sense, a fact that we have already been using above.

For the left-hand side of Theorem 4.4.6, we can now write

$$\begin{aligned}S(g) &= -\sum_\chi \sum_{\mathfrak{p}\text{ ramified}} \left(-[k_\mathfrak{p} : \mathbb{F}_p] + v_p\left(j_p\tau(\chi_{k_\mathfrak{p}}) \right)\right) \cdot j_p\chi(g) \\ &= \sum_\chi \sum_\mathfrak{p} [k_\mathfrak{p} : \mathbb{F}_p] \cdot j_p\chi(g) - \sum_\chi \sum_\mathfrak{p} v_p\left(j_p\tau(\chi_{k_\mathfrak{p}}) \right) \cdot j_p\chi(g) \\ &= \sum_\mathfrak{p} [k_\mathfrak{p} : \mathbb{F}_p] j_p \left(\sum_\chi \chi(g) \right) - \sum_\chi \sum_\mathfrak{p} v_p\left(j_p\tau(\chi_{k_\mathfrak{p}}) \right) \cdot j_p\chi(g) \\ &= \sum_\mathfrak{p} [k_\mathfrak{p} : \mathbb{F}_p] j_p \left(\mathrm{Trace}(g|\mathbb{C}[G]) \right) - \sum_\chi \sum_\mathfrak{p} v_p\left(j_p\tau(\chi_{k_\mathfrak{p}}) \right) \cdot j_p\chi(g) \\ &= -\sum_\chi \sum_\mathfrak{p} v_p\left(j_p\tau(\chi_{k_\mathfrak{p}}) \right) \cdot j_p\chi(g),\end{aligned}$$

Here we have used that g is not the identity, and hence $\mathrm{Trace}(g|\mathbb{C}[G]) = 0$.
Theorem 27 in [Fr] gives a formula for the p-adic valuation of the Gauss sums $\tau(\chi_{k_\mathfrak{p}})$, which we will now explain. The same result can be found in [La], see Theorem IV.3.9 on p. 94 in [La] and the lemma on p. 96 in [La].
Let q be the order of $k_\mathfrak{p}$. For any $h \in \{0, \ldots, q-2\}$, let $s(h)$ denote the sum of the p-adic digits of h. For any $x \in \mathbb{Q}$, let $\{x\}$ denote the fractional part of x, i.e. $\{x\} \in \mathbb{Q}$, $0 \leq \{x\} < 1$ and $x \equiv \{x\} \mod \mathbb{Z}$. For any $h \in \{0, \ldots, q-2\}$, define a rational number $r(h)$ as follows:

$$r(h) := \sum_{j=1}^{[k_\mathfrak{p}:\mathbb{F}_p]} \left\{ \frac{p^j h}{q-1} \right\}.$$

Finally, we define the integer $f_{\chi,\mathfrak{p}} \in \{0, \ldots, q-2\}$ as follows.
The character values of $\chi_{k_\mathfrak{p}} : k_\mathfrak{p} \to \mathbb{C}^*$ are $(q-1)$-st roots of unity in $\bar{\mathbb{Q}}$, and the embedding $j_p : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$ maps them to $(q-1)$-st roots of unity in $\bar{\mathbb{Q}}_p$. Writing $\mu_{K,q-1}$ for the group of $(q-1)$-st roots of unity in any field K, we obtain the following commutative diagram:

$$\begin{tikzcd}
k_\mathfrak{p}^* \arrow[r, "\chi_{k_\mathfrak{p}}"] \arrow[d, equal] & \bar{\mathbb{Q}}^* \arrow[r, "j_p"] & \bar{\mathbb{Q}}_p^* \\
k_\mathfrak{p}^* \arrow[r, "\chi_{k_\mathfrak{p}}"] & \mu_{\bar{\mathbb{Q}},q-1} \arrow[r, "j_p"] \arrow[u] & \mu_{\bar{\mathbb{Q}}_p,q-1} \arrow[u]
\end{tikzcd}$$

Let now $M \subseteq \bar{\mathbb{Q}}_p$ be a p-adic number field with residue field $\mathbb{F}_q$. Then M contains all $(q-1)$-st roots of unity; in other words, we have $\mu_{\bar{\mathbb{Q}}_p,q-1} = \mu_{M,q-1}$. As seen in Subsection 4.2.3, "reduction modulo $\mathfrak{m}_M$" defines an isomorphism (the inverse of the *Teichmüller character*) $T^{-1} : \mu_{M,q-1} \to \mu_{\mathbb{F}_q,q-1} = \mathbb{F}_q^*$. Write c for the homomorphism $k_\mathfrak{p} \to \mathbb{F}_q^*$ making the following diagram commute:

$$\begin{tikzcd}
k_\mathfrak{p}^* \arrow[r, "\chi_{k_\mathfrak{p}}"] \arrow[rrd, dashed, "c"'] & \mu_{\bar{\mathbb{Q}}} \arrow[r, "j_p"] & \mu_{\bar{\mathbb{Q}}_p,q-1} = \mu_{M,q-1} \arrow[d, "T^{-1}"] \\
& & \mathbb{F}_q^*
\end{tikzcd}$$

If we now identify $k_\mathfrak{p}$ with $\mathbb{F}_q$, then c can be viewed as an automorphism of the group $\mathbb{F}_q^*$. Since $\mathbb{F}_q^*$ is a cyclic group, this means that there exists a unique $f = f_{\chi,\mathfrak{p}} \in \{0, \ldots, q-2\}$ such that $c(x) = x^{-f}$ for all $x \in \mathbb{F}_q^*$. In other words, there exists a unique $f = f_{\chi,\mathfrak{p}}$ such that the following diagram commutes.

$$\begin{tikzcd}
k_{\mathfrak{p}}^* \arrow[r, "\chi_{k_{\mathfrak{p}}}"] \arrow[d, "\cong"'] & \mu_{\bar{\mathbb{Q}}} \arrow[r, "j_p"] & \mu_M \arrow[d, "T^{-1}"] \\
\mathbb{F}_q^* \arrow[rr, dashed, "x \mapsto x^{-f}"'] & & \mathbb{F}_q^*
\end{tikzcd}$$

We are now in position to state the expressions for the p-adic valuation of the Gauss sum given in [Fr] and [La]):

$$v_p\left(j_p\tau(\chi_{k_{\mathfrak{p}}}) \right) = r(f_{\chi,\mathfrak{p}}) = s(f_{\chi,\mathfrak{p}}) \cdot \frac{1}{p-1} \tag{4.20}$$

This also shows that the quantities $s(f_{\chi,\mathfrak{p}})$ and $r(f_{\chi,\mathfrak{p}})$ appearing in this formula do not depend on the choice of the identification $k_{\mathfrak{p}} \cong \mathbb{F}_q$.

Using the first part of Formula (4.20) (we will not need the second part), we can write

$$S(g) = -\sum_{\chi}\sum_{\mathfrak{p}} r(f_{\chi,\mathfrak{p}}) \cdot j_p\chi(g). \tag{4.21}$$

4.5.2 The right-hand side of Theorem 4.4.6 for $g \neq \mathrm{id}$

We now consider the right-hand side of Theorem 4.4.6, again in the case where $g \neq \mathrm{id}$. Since $\mathrm{Trace}(g|\mathbb{F}_p[G]) = 0$, the equivariant Hurwitz formula (Formula (2.16) in Theorem 2.4.11) yields that

$$-C(g) = -\,\mathrm{Trace}(g|\chi(G, X, \mathcal{O}_X)) = \mathrm{Trace}(g|N_{G,X}).$$

Recall that $N_{G,X}$ denotes the *ramification module*, defined by Formula (2.15) in Theorem 2.4.11, which is a projective module encoding the ramification of the cover $\pi : X \to Y$.

By Formula (4.7) and by the relations between the various character rings developped earlier, we have

$$\mathrm{Trace}(-|N_{G,X}) = \sum_{\chi \in \mathrm{Hom}(G, \bar{\mathbb{Q}}_p^*)} \langle \chi, \mathrm{Trace}(-|N_{G,X}) \rangle \cdot \chi.$$

Here we have used that G is cyclic and $\bar{\mathbb{Q}}_p$ is algebraically closed, so that the irreducible (modular) characters from G to $\bar{\mathbb{Q}}_p$ are just the homomorphisms from G to $\bar{\mathbb{Q}}_p^*$.
Let n denote the order of G. Using the definition of $N_{G,X}$ (Formula (2.15) in Theorem 2.4.11), we obtain

$$\begin{aligned}
-C(g) &= \mathrm{Trace}(g|N_{G,X}) \\
&= \sum_{\chi\in\mathrm{Hom}(G,\bar{\mathbb{Q}}_p^*)} \langle\chi, \mathrm{Trace}(-|N_{G,X})\rangle\,\chi(g) \\
&= \sum_{\chi}\frac{1}{n}\sum_{P\in|X|}\sum_{d=1}^{e_P-1} d\cdot\langle\chi, \mathrm{Trace}\left(\,-|\,\mathrm{Ind}_{I_P}^G(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}\,\right)\rangle\chi(g) \\
&= \sum_{\chi}\frac{1}{n}\sum_{P\in|X|}\sum_{d=1}^{e_P-1} d\cdot\langle\chi|_{I_P}, \mathrm{Trace}\left(\,-|(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d}\,\right)\rangle\chi(g).
\end{aligned}$$

The last step in this calculation is due to Frobenius reciprocity. Up to the penultimate line, $\langle -,-\rangle$ denotes the pairing of modular characters of $\mathbb{F}_p[G]$-modules; in the last line, it denotes the pairing of modular characters of $\mathbb{F}_p[I_P]$-modules. $\mathrm{Trace}(-|-)$ denotes modular characters of $\mathbb{F}_p[G]$-modules and $\mathbb{F}_p[I_P]$-modules, respectively.
By Lemma 2.4.14, every closed point R on Y has exactly $\frac{n}{e_{\tilde{R}}f_{\tilde{R}}}$ preimages on X, where $\tilde{R}$ denotes an arbitrary but fixed preimage. We can thus rewrite the above as follows.

$$-C(g) = \sum_{\chi}\sum_{R\in|Y|}\frac{1}{e_{\tilde{R}}f_{\tilde{R}}}\sum_{d=1}^{e_{\tilde{R}}-1} d\cdot\langle\chi|_{I_{\tilde{R}}}, \mathrm{Trace}\left(\,-|(\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes d}\,\right)\rangle\chi(g). \quad (4.22)$$

Let now P be a closed point on X. Our next aim is to compute the modular characters $\mathrm{Trace}(-|(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d})$ $(d = 1,\ldots,e_P)$. Let χ_P denote the "naive" character $\chi_P : I_P \to k(P)^*$, defined by

$$\sigma.x = \chi_P(\sigma)\cdot x \quad \text{for all } x\in\mathfrak{m}_P/\mathfrak{m}_P^2, \sigma\in G.$$

Furthermore, let $R := \pi(P)$ denote the image of P on Y. As explained in Subsection 4.2.2, local class field theory gives a surjective homomorphism

$$\alpha : I_P \to k(R)^*,$$

so $k(R)$ contains the e_P-th roots of unity. Hence χ_P factors through $k(R)^*$:

$$\begin{tikzcd} I_P \arrow[r, "\chi_P"] \arrow[dr, dashed, "\chi_R"'] & k(P)^* \\ & k(R)^* \arrow[u, "\subseteq"'] \end{tikzcd}$$

The character

$$\chi_R : I_P \to k(R)^*$$

which makes the above diagram commute determines a one-dimensional $k(R)$-representation of I_P, which we denote $V_{P,1}$. There obviously is an isomorphism of $k(R)[I_P]$-modules

$$\mathfrak{m}_P/\mathfrak{m}_P^2 \cong \bigoplus^{f_P} V_{P,1}.$$

For any $d \in \{1, \ldots, e_P - 1\}$, the character $\chi_P^d : I_P \to k(P)^*$ also factors through $k(R)^*$, defining a $k(R)$-module $V_{P,d}$, and we have

$$(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d} \cong \bigoplus^{f_P} V_{P,d}.$$

We will now compute the modular character of $V_{P,d}$ viewed as an $\mathbb{F}_p$-vector space. To this end, we note that the eigenvalues (and their multiplicities) of a group element σ on $V_{P,d}$ viewed as an $\mathbb{F}_p$-vector space are equal to the eigenvalues of $\sigma \otimes \mathrm{id}$ on the tensor product $V_{P,d} \otimes_{\mathbb{F}_p} k(R)$ viewed as a $k(R)$-vector space. The latter space is described by the following lemma.

Lemma 4.5.2. *For* $d = 1, \ldots, e_P - 1$, *we have*

$$V_{P,d} \otimes_{\mathbb{F}_p} k(R) \cong \bigoplus_{i=1}^{[k(R):\mathbb{F}_p]} V_{P,d}^{\otimes p^i}$$

as $k(R)[I_P]$*-modules.*

Proof. We define a homomorphism of $k(R)$-vector spaces

$$\varphi : k(R) \otimes_{\mathbb{F}_p} k(R) \to \bigoplus_{\sigma \in \mathrm{Gal}(k(R)/\mathbb{F}_p)} k(R) = \bigoplus_{i=1}^{[k(R):\mathbb{F}_p]} k(R),$$

$$a \otimes b \mapsto (\sigma(a) \cdot b)_{\sigma \in \mathrm{Gal}(k(R)/\mathbb{F}_p)} = (a^{p^i} \cdot b)_{i=1,\dots,[k(R):k]}$$

This is an isomorphism of $k(R)$-vector spaces, by the Galois descent lemma. We now define a homomorphism of $k(R)$-vector spaces

$$\tilde{\varphi} : V_{P,d} \otimes_{\mathbb{F}_p} k(R) \to \bigoplus_{i=1}^{[k(R):\mathbb{F}_p]} V_{P,d}^{\otimes p^i},$$

$$v \otimes b \mapsto (v^{\otimes p^i} \cdot b)_{i=1,\dots,[k(R):\mathbb{F}_p]}$$

Since $V_{P,d}$ is one-dimensional over $k(R)$, it follows from the bijectivity of φ that $\tilde{\varphi}$ also is an isomorphism of vector spaces over $k(R)$. It is compatible with the action of I_P on both sides, since the following diagram commutes for every $\sigma \in I_P$, $v \in V_{P,d}$ and $b \in k(R)$.

$$\begin{tikzcd}
v \otimes b \arrow[r, mapsto] \arrow[d, mapsto, "\sigma\otimes\mathrm{id}"'] & (v^{\otimes p^i} \cdot b)_i \arrow[d, mapsto, "(\sigma,\dots,\sigma)"] \\
\sigma(v) \otimes b \arrow[r, mapsto] & \left(\sigma(v)^{\otimes p^i} \cdot b \right)_i
\end{tikzcd}$$

□

We now define a character $\tilde{\chi}_P : I_P \to \bar{\mathbb{Q}}_p^*$ as follows. We identify $k(R)$ with $\mathbb{F}_q$, where $q = \#k(R)$, and write T for the Teichmüller character $k(R)^* \to \bar{\mathbb{Q}}_p^*$ (cf. Subsection 4.2.3). Let $\tilde{\chi}_P$ denote the composition

$$\begin{tikzcd}
I_P \arrow[r, "\chi_R"] \arrow[rr, bend right, "\tilde{\chi}_P"'] & k(R)^* \arrow[r, "T"] & \bar{\mathbb{Q}}_p^*
\end{tikzcd}$$

Then by the above considerations, in particular by Lemma 4.5.2, we have for $d = \{1, \dots, e_P - 1\}$:

$$\mathrm{Trace}\left(-|(\mathfrak{m}_P/\mathfrak{m}_P^2)^{\otimes d} \right) = \sum_{i=1}^{[k(R):\mathbb{F}_p]} f_P \, \tilde{\chi}_P^{dp^i}.$$

We can now plug this into Formula (4.22) and obtain

$$
\begin{aligned}
-C(g) &= \sum_{\chi} \sum_{R\in|Y|} \frac{1}{e_{\tilde{R}} f_{\tilde{R}}} \sum_{d=1}^{e_{\tilde{R}}-1} d \cdot \langle j_p \chi|_{I_{\tilde{R}}}, \mathrm{Trace}(-|\mathfrak{m}_{\tilde{R}}/\mathfrak{m}_{\tilde{R}}^2)^{\otimes d} \rangle \chi(g) \\
&= \sum_{\chi} \sum_{R\in|Y|} \frac{1}{e_{\tilde{R}} f_{\tilde{R}}} \sum_{d=1}^{e_{\tilde{R}}-1} d \cdot \langle j_p \chi|_{I_{\tilde{R}}}, \sum_{i=1}^{[k(R):\mathbb{F}_p]} f_{\tilde{R}} \tilde{\chi}_{\tilde{R}}^{dp^i} \rangle \chi(g) \\
&= \sum_{\chi} \sum_{R\in|Y|} \frac{1}{e_{\tilde{R}} f_{\tilde{R}}} \sum_{d=1}^{e_{\tilde{R}}-1} f_{\tilde{R}}\, d \sum_{i=1}^{[k(R):\mathbb{F}_p]} \cdot \langle \chi|_{I_{\tilde{R}}}, \tilde{\chi}_{\tilde{R}}^{dp^i} \rangle \chi(g) \\
&= \sum_{\chi} \sum_{R\in|Y|} \sum_{d=1}^{e_{\tilde{R}}-1} \frac{d}{e_{\tilde{R}}} \sum_{i=1}^{[k(R):\mathbb{F}_p]} \cdot \langle \chi|_{I_{\tilde{R}}}, \tilde{\chi}_{\tilde{R}}^{dp^i} \rangle \chi(g).
\end{aligned}
$$

By Proposition 2.3.14, for every $P \in |X|$, χ_P generates the character group $\mathrm{Hom}(I_P, k(P)^*)$. Therefore $\tilde{\chi}_P$ generates the character group $\mathrm{Hom}(I_P, \bar{\mathbb{Q}}_p^*)$. So for each $\chi \in \mathrm{Hom}(G, \bar{\mathbb{Q}}_p^*)$, there is exactly one $d' = d'(\chi, P) \in \{0, \ldots, e_P - 1\}$ for which the scalar product $\langle \chi|_{I_P}, \tilde{\chi}_P^{d'} \rangle$ is equal to 1; for all other values of d' in the range from 0 to $e_P -'1$, the scalar product is equal to zero. Hence the scalar product $\langle \chi|_{I_P}, \tilde{\chi}_P^{dp^i} \rangle$ is equal to 1 if $dp^i \equiv d'(\chi, P) \bmod e_P$, and 0 otherwise. If we define

$$
\mathcal{I}(d, P) := \{\, i \in \{1, \ldots, [k(R) : \mathbb{F}_p]\} \,:\, dp^i \equiv d'(\chi, P) \mod e_P \,\},
$$

then we can write

$$
-C(g) = \sum_{\chi} \sum_{R\in|Y|} \sum_{d=1}^{e_{\tilde{R}}-1} \frac{d}{e_{\tilde{R}}} |\mathcal{I}(d, \tilde{R})| \cdot \chi(g). \tag{4.23}
$$

4.5.3 Completion of the proof for $g \neq \mathrm{id}$

Let $\chi : G \to \mathbb{C}^*$ be an irreducible character, let P be a closed point on X, and let $\mathfrak{p}$ be the place of $K = K(Y)$ corresponding to the image of P in Y, which we will denote R. As defined in the previous subsection, let $d' = d'(\chi, P) \in \{1, \ldots, e_P - 1\}$ such that $\chi|_{I_P} = \tilde{\chi}_P^{d'}$. We identify $k_{\mathfrak{p}}$ with $\mathbb{F}_q$, for $q := \#k_{\mathfrak{p}}$, and write T for the Teichmüller character $k_{\mathfrak{p}}^* \to \bar{\mathbb{Q}}_p^*$.

Proposition 4.2.3 implies that both triangles in the following diagram commute,

$$\begin{tikzcd} k_{\mathfrak{p}}^* \arrow[r, "\alpha"] \arrow[d, "\frac{d'(q-1)}{e_P}"'] & I_P \arrow[d, "\tilde{\chi}_P^{d'}"] \arrow[dl] \\ k_{\mathfrak{p}}^* \arrow[r, "T"'] & \bar{\mathbb{Q}}_p^* \end{tikzcd}$$

Here the diagonal arrow represents the character $\chi_R^{d'}$, where χ_R is defined as in the previous subsection.

Recall that in Subsection 4.5.1, we had defined $f_{\chi,\mathfrak{p}} \in \{0,\ldots,q-1\}$ in such a way that the following diagram commutes:

$$\begin{tikzcd} k_{\mathfrak{p}}^* \arrow[r, "\alpha"] \arrow[d, "f_{\chi,\mathfrak{p}}"'] \arrow[dr] & I_P \arrow[d, "\chi|_{I_P}"] \\ k_{\mathfrak{p}}^* \arrow[r, "T"'] & \bar{\mathbb{Q}}_p^* \end{tikzcd}$$

Here the diagonal arrow represents the character $\chi_{k_{\mathfrak{p}}}$. Given that $\chi|_{I_P} = \tilde{\chi}_P^{d'}$, it follows from the commutativity of these diagrams that the assignments $x \mapsto x^{\frac{d'(q-1)}{e_P}}$ and $x \mapsto x^{f_{\chi,\mathfrak{p}}}$ define the same automorphism of $k_{\mathfrak{p}}^*$. Since the automorphism group of $k_{\mathfrak{p}}^*$ is cyclic of order $q-1$, we conclude that

$$f_{\chi,\mathfrak{p}} \equiv \frac{d'(q-1)}{e_P} \mod (q-1).$$

Thus we have

$$r(f_{\chi,\mathfrak{p}}) \stackrel{\text{def.}}{=} \sum_{j=1}^{[k(R):\mathbb{F}_p]} \left\{ \frac{p^j f_{\chi,\mathfrak{p}}}{q-1} \right\} = \sum_{j=1}^{[k(R):\mathbb{F}_p]} \left\{ \frac{d'p^j}{e_P} \right\}. \tag{4.24}$$

For $d \in \{1,\ldots,e_P-1\}$ define

$$\mathcal{J}(d,P) := \left\{ j \in \{1,\ldots,[k(R):\mathbb{F}_p]\} \,:\, d'p^j \equiv d \mod e_P \right\}$$

and, as at the end of Subsection 4.5.2,

$$\mathcal{I}(d,P) := \left\{ i \in \{1,\ldots,[k(R):\mathbb{F}_p]\} \,:\, d' \equiv dp^i \mod e_P \right\}.$$

Lemma 4.5.3. *The two index sets have the same cardinality,*

$$|\mathcal{I}(d,P)| = |\mathcal{J}(d,P)|.$$

Proof. Let $i \in \{1,\ldots,[k(R):k]\}$, and let $j := [k(R):\mathbb{F}_p] - i$. Then i lies in $\mathcal{I}(d,P)$ if and only if j lies in $\mathcal{J}(d,P)$. Here is a short proof of this fact:

$$\begin{aligned}
i \in \mathcal{I}(d,P) &\Leftrightarrow d' \equiv dp^i && \mod e_P \\
&\Leftrightarrow d'\,p^j \equiv dp^{i+j} && \mod e_P && \text{because } (p,e_P)=1 \\
&\Leftrightarrow d'\,p^j \equiv d && \mod e_P && \text{because } p^{i+j} = q \equiv 1 \mod e_P \\
&\Leftrightarrow j \in \mathcal{J}(d,P).
\end{aligned}$$

It follows that $\mathcal{I}(d,P)$ and $\mathcal{J}(d,P)$ have the same cardinality. $\square$

We can now prove Theorem 4.4.6. We have

$$\begin{aligned}
S(g) &= -\sum_{\chi}\sum_{\mathfrak{p}} r(f_{\chi,\mathfrak{p}})\cdot\chi(g) && \text{by Formula (4.21)} \\
&= -\sum_{\chi}\sum_{R\in|Y|}\sum_{j=1}^{[k(R):\mathbb{F}_p]} \left\{ \frac{d'p^j}{e_{\tilde{R}}} \right\}\cdot\chi(g) && \text{by Formula (4.24)} \\
&= -\sum_{\chi}\sum_{R\in|Y|}\sum_{d=1}^{e_{\tilde{R}}-1} \frac{d}{e_{\tilde{R}}}\,|\mathcal{J}(d,\tilde{R})|\cdot\chi(g) \\
&= -\sum_{\chi}\sum_{R\in|Y|}\sum_{d=1}^{e_{\tilde{R}}-1} \frac{d}{e_{\tilde{R}}}\,|\mathcal{I}(d,\tilde{R})|\cdot\chi(g) && \text{by Lemma 4.5.3} \\
&= C(g) && \text{by Formula (4.23).}
\end{aligned}$$

Hence $S(g) = C(g)$ as required.

4.5.4 Proof of Theorem 4.4.6 for $g = \mathrm{id}$

In the case where $g = \mathrm{id}$, we have $\chi(g) = 1$ for any irreducible character χ. Hence we have

$$\begin{aligned}
S(\mathrm{id}) &= -\sum_{\chi} v_p(j_p\varepsilon(\chi)) \cdot j_p\chi(\mathrm{id}) \\
&= -\sum_{\chi} v_p(j_p\varepsilon(\chi)) \\
&= -v_p(j_p \prod_{\chi} \varepsilon(\chi)) \\
&= -v_p(j_p\varepsilon(\sum_{\chi} \chi)) && \text{by Lemma 4.3.10} \\
&= -v_p(j_p\varepsilon(\mathbb{C}[G])) \\
&= -v_p(j_p\varepsilon(\mathrm{Ind}_1^G(\mathbb{C}))) \\
&= -v_p(j_p\varepsilon(\mathbb{C})) && \text{by Lemma 4.3.10}
\end{aligned}$$

In order to compute the epsilon constant of the trivial representation $\mathbb{C}$, note that the L-function $L(X, \mathbb{C}, t)$ with respect to the trivial group $\{1\}$ is the same as the *non-equivariant Zeta function* $Z(X, t)$ as defined by Milne:

$$L(X, \mathbb{C}, t) = \prod_{P \in |X|} (1 - t^{[k(P):\mathbb{F}_p]})^{-1} = Z(X, t)$$

(cf. proof of Theorem 12.4 in [Mi]). The (non-equivariant) Weil conjectures yield that $Z(Y, t)$ satisfies the functional equation

$$Z(X, \frac{1}{pt}) = \pm p^{e_X/2} t^{e_X} Z(X, t),$$

where $e_X = 2g_X - 2$ is the topological Euler characteristic of X (cf. (W3) at the beginning of §VI.12 in [Mi], or Section 2a in [Er]).
Setting $t := 1$ and comparing with the functional equation (4.15), we obtain

$$\varepsilon(\mathbb{C}) = \pm p^{e_X/2}$$

and thus

$$S(\mathrm{id}) = -v_p(\varepsilon(\mathbb{C})) = -\frac{e_X}{2} = 1 - g_X.$$

It is then easy to check that $\mathrm{Trace}(\mathrm{id}\,|V) = \dim_{\mathbb{F}_p}(V)$ for any $\mathbb{F}_p[G]$-module V. Hence we have

$$\begin{aligned} C(\mathrm{id}) &= \mathrm{Trace}(g|\psi(X/Y)) \\ &= \dim_{\mathbb{F}_p}(H^0(X, \mathcal{O}_X)) - \dim_{\mathbb{F}_p}(H^1(X, \mathcal{O}_X)) \\ &= 1 - g_X \\ &= S(\mathrm{id}) \end{aligned}$$

as required.

Bibliography

[Bo] N. BORNE, *Une formule de Riemann-Roch équivariante pour les courbes*, thesis, Univ. Bordeaux I, 2000. Available online at `http://tel.archives-ouvertes.fr/tel-00001272/en/`

[Ch] T. CHINBURG, *Galois structure of de Rham cohomology of tame covers of schemes*, Ann. of Math. **139** (1994), 443-490

[CR] C.W. CURTIS, I. REINER, *Methods of Representation Theory*, Wiley, New York 1981

[CW] C. CHEVALLEY, A. WEIL, *Über das Verhalten der Integrale erster Gattung bei Automorphismen des Funktionenkörpers*, Hamb. Abh. **10** (1934), 358-361

[De1] P.DELIGNE, *La conjecture de Weil: I.*, Publications Mathématiques de l'IHÉS, Vol. **43** (1974), 273-307

[De2] P.DELIGNE, *La conjecture de Weil: II.*, Publications Mathématiques de l'IHÉS, Vol. **52** (1980), 137-252

[De3] P. DELIGNE, *Les constantes des équations fonctionelles des fonctions L*, in: P. Deligne, W. Kuyk (eds.), *Modular functions of one variable II*, Springer lecture notes in Math., Vol. **349**, Springer, Berlin Heidelberg New York (1973), 501-597

[EL] G. ELLINGSRUD, K. LØNSTED, *An equivariant Lefschetz formula for finite reductive groups*, Math. Ann. **251** (1980), 253-261

[Er] B. EREZ, *Geometric trends in Galois module theory*, in: "Galois Representations in Arithmetic Algebraic Geometry", edited by A.J. Scholl and R.L. Taylor, Cambridge 1998

[Fi] H. FISCHBACHER-WEITZ, *Equivariant Riemann-Roch theorems for curves over perfect fields*, diploma thesis, Karlsruhe 2007

[FK] H. FISCHBACHER-WEITZ, B. KÖCK, *Equivariant Riemann-Roch theorems for curves over perfect fields*, preprint, 2007. Available online at `http://xxx.soton.ac.uk/abs/math/0701257`

[Fr] A. FRÖHLICH, *Galois Module Structure of Algebraic Integers*, Erg. der Math., 3. Folge, Vol. **1**, Springer, Heidelberg/ New York/ Tokyo, 1983

[Fu] W. FULTON, *Intersection Theory*, Springer, Berlin/ Heidelberg 1984

[Ha] R. HARTSHORNE, *Algebraic Geometry*, Springer, New York 1977

[Has] H. HASSE, *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper*, J. Reine Angew. Math. **172** (1934), 37-54. Also in: H. Hasse, *Mathematische Abhandlungen*, edited by H.W. Leopoldt and P. Roquette, de Gruyter, Berlin 1975

[HKS] F. HALTER-KOCH, J. KLINGEN, H. STICHTENOTH, *Artin'sche L-Funktionen*, notes on a seminar held at the Universität Essen in the academic year 1975/76, Essen 1976

[HvLP] HOHOLDT/ VAN LINDT/ PELLIKAAN, *Algebraic Geometry Codes*, in: Handbook of Coding Theory, Huffman/Pless (Editors), Elsevier, New York 1998

[JK] D. JOYNER, A. KSIR, *Modular representations on some Riemann-Roch spaces of modular curves X(N)*, preprint, 2005. Available online at `http://xxx.soton.ac.uk/abs/math/0502586`

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

[Kö1] B. KÖCK, *Computing the equivariant Euler characteristic of Zariski and étale sheaves on curves*, Homology Homotopy Appl. **7**, No.3 (2005), 83-98

[Kö2] B. Köck, *Galois structure of Zariski cohomology for weakly ramified covers of curves*, American Journal of Mathematics **126** (2004), 1085-1107

[Ku1] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, Boston 1985

[Ku2] E. Kunz, *Kähler differentials*, Vieweg, Wiesbaden 1986

[La] S. Lang, *Algebraic Number Theory*, Springer, New York 1994

[Mi] J.S. Milne, *Etale cohomology*, Princeton Univeristy Press, Princeton 1942

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

[Ne] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin/ Heidelberg 1992

[Se1] J.-P. Serre, *Corps locaux*, Publications de l'Institut de Mathématique de l'Université de Nancago, Vol. VIII, Hermann, Paris 1962

[Se2] J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, Paris 1978

[St] H. Stichtenoth, *Algebraic function fields and codes*, Springer, Berlin/ Heidelberg 1993

[Ta] J.T. Tate, *Fourier Analysis in Number Fields and Hecke's Zeta-Functions*, thesis, Princeton 1950. In: J.W.S. Cassels, A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, London/ New York 1967

[Tay] M. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. **63** (1981), 41-79

[We] A. Weil, *Number of solutions of equations over finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497-508

[Wei] R. WEISSAUER, *Skript zur Vorlesung Zahlentheorie*, lecture notes, Heidelberg 2007. Available online at `www.mathi.uni-heidelberg.de/~weissaue/vorlesungsskripte/Zahlentheorie.pdf`

[Wes] S. WESEMEYER, *On the Automorphism Group of Various Goppa Codes*, IEEE Trans. Inform. Theory **44**, No. 2 (March 1998), 630-643