Master Thesis Mathematical Sciences

Using class field theory to find function fields with many rational places

Utrecht University

Author:
Evie Roebroek

Supervisor:
dr. Valentijn Karemaker
Second Reader:
prof. dr. Gunther Cornelissen

March 2021

Abstract

In this thesis, two algorithms are proposed to find function fields with many rational places. These algorithms rely on the main theorem of class field theory, which tells us that there exists a functorial bijection between finite index subgroups of the idèle class group and finite extensions of a function field. Combining this with knowledge of the splitting behaviour of places in finite extensions gives one algorithm using unramified extensions and a second using ramified extensions. Running the first algorithm over genus 4 hyperelliptic function fields and the second over genus 2 hyperelliptic function fields, both over $\mathbb{F}_p$ with $3 \leq p \leq 13$ prime, gives 51 results that are improvements to the bounds currently stated on `manypoints.org`.

Acknowledgements

First and foremost, I would like to thank Valentijn Karemaker for guiding me through this process. She has been an amazing supervisor, both on a mathematical level and on a personal level. Writing a master's thesis during a pandemic was quite a challenging experience for me, and knowing that there was someone I could reach out to made this past year a lot better. Secondly, I would like to thank Gunther Cornelissen for his useful feedback as my second reader and his quick and elaborate answers to my questions while Valentijn was abroad.

I am also extremely grateful to Jeroen Sijsling and Stefano Marseglia for answering my (many) questions about the computational part of this thesis. Without their answers, I would probably still be stuck with a lot of frustration and no results. I would especially like to thank Jeroen for trusting me with his account on toby and allowing me to run my algorithm there. Moreover, I would like to thank Karl Rökeaus and Pavel Solomatin for answering my questions about their previous research.

One of the things that made this process a lot more fun were the coffee breaks with my fellow students, particularly Wilmer Smilde and Onno van Zomeren. Thank you for being there when I needed someone to talk to, to brainstorm, or just to laugh with. Lastly, I would like to thank Thijs, who has been my anchor through this all.

Contents

Introduction

An important open problem in arithmetic geometry is the following. Given an algebraic curve C over a finite field k, what is the maximal number of k-rational points that this curve can have? This question first sparked the interest of mathematicians almost a century ago, with Hasse proving a bound on the number of rational points of an elliptic curve in 1936 ([Has36]). Since then, many mathematicians have tried to answer this question, and considerable progress has been made over the years. However, for many cases, the answer is still unknown.

We will see that the number of rational points of a curve C is bounded above and below by the cardinality of the finite field and the genus of the curve. We will therefore denote by $N_g(q)$ the maximal number of rational points that a curve C with genus g over $\mathbb{F}_q$ can have. For each finite field $\mathbb{F}_q$ with $q \leq 100$ and genus $g \leq 50$, a list of the intervals in which this maximum can lie is published on `manypoints.org`. We see that for only a few combinations of g and q, $N_g(q)$ the answer is known, meaning that there no longer exists an interval in which the maximum can lay. The purpose of this thesis is to sharpen these intervals, thereby improving the currently best known bounds. We will call such an improvement of the current bounds a record.

Upper bounds on $N_g(q)$ are very difficult to improve, since one needs to show that for all curves of a certain genus over $\mathbb{F}_q$, this is the maximal number of points. On the other hand, to improve a lower bound M on $N_g(q)$, it suffices to find one curve that has at least $M+1$ rational points. This is what we will do in this thesis. We use an equivalence relation between curves with rational points and function field with rational places, so that we can use algebraic statements rather than geometric ones.

One option to find such records would be to simply check all possible function fields of a certain genus. However, a little investigation tells us that as soon as we reach function fields with genus larger than 5, we have not yet found a canonical embedding in projective space for all curves, meaning that we do not know how to construct all types of function fields. For each type of function fields that we do know, the amount of function fields of that type grows exponentially with the genus. Moreover, checking the number of rational places of a function field is quite a hard task, computationally speaking. We will therefore have to choose a more advanced path on our quest for new records.

In this thesis we use class field theory to find such a path. Class field theory gives an isomorphism between subgroups of the idèle class groups of a function field K and the Galois groups of finite abelian extensions of K. Knowledge of the Galois group will give us knowledge of the splitting behaviour of rational places, and therefore of the number of rational places of the extension field, as we will see in Chapter 1. Using this isomorphism, we can state the number of rational places of an extension field using only very little information. This enables us to quickly see which field extensions might give us new records, and which will not. We will illustrate a more elementary way to use this knowledge in Chapter 2, using unramified extensions, and a more advanced one in Chapter 5, using ramified extensions. Together, these algorithms provided 51 new records, and we believe that many more can be found when the advanced algorithm is applied to a wider range of function fields.

We will now give an overview of the material that will be covered in this thesis.
In Chapter 1, we will set up all necessary background information on function fields. We will start by introducing valuation theory, and see how the notion of an algebraic function field follows naturally. Once the basics of function fields are covered, we will start investigating extensions of function fields. As Galois extensions are essential to our construction, we will spend some time looking at the splitting behaviour of places under Galois extensions and briefly cover infinite Galois theory. We will then give a concise overview of the relation between the category of algebraic curves with rational points and that of algebraic function fields with rational places. We end our first chapter by introducing local fields and idèles, which will be of great importance when looking into class field theory in Chapter 4.

Once we know enough about function fields and their abelian extensions, we illustrate how we can use this knowledge to construct an algorithm that finds function fields with many rational places in Chapter 2. We will introduce one black box, Theorem 2.17, which tells us that there exists an isomorphism between the degree zero divisor class group of a function field and the Galois group of its maximal abelian extension in which one rational place splits completely. Combining this with the knowledge of field extensions from Chapter 1, we can create an algorithm that gives us unramified field extensions with many rational places. Applying this algorithm to genus four hyperelliptic function fields already gives us 26 records (see Table 1).

To prove the black box used in Chapter 2 and create an algorithm that uses ramified extensions to find new records, we need to learn more about group cohomology. The goal of Chapter 3 is to gain enough knowledge about (Tate) cohomology groups to develop the theory of class fields in Chapter 4. We will cover the general definitions of group cohomology, introduce Tate cohomology groups and look at subgroup maps. We finish this chapter by looking into cup products, which are crucial for class field theory.

Class field theory essentially consists of one important theorem, that gives an isomorphism between different cohomology groups, and some additional theorems that help us understand the structure of this isomorphism. In Chapter 4, we will work towards proving that there exists an isomorphism between finite index subgroups of the idèle class group of a function field, and the Galois groups of finite abelian extensions. To fully understand this theorem, we have to first cover abstract and local class field theory. At the end of this chapter we will have a thorough understanding of the relation between idèle class groups and Galois groups, which is exactly what we need for our last chapter.

We will start the final chapter of this thesis by proving the black box introduced in Chapter 2. We will then go through a similar process to construct an algorithm that finds function field with many rational places by looking at ramified extensions, which will give us 25 more records (see Table 2). We will finish this thesis by discussing some technicalities and limitations of this algorithm, as well as providing suggestions for future research.

1 Function Fields

The goal of this thesis is to find function fields with many rational points. In this chapter, we will set up all the preliminary information on function fields that will be needed to define an algorithm in the next chapter. We start with discrete valuations, as they induce valued fields. We will set up the theory of places, divisors, and define the genus of a function field. In the next chapter, we will construct function fields with many rational places by looking at abelian extensions of low genus function fields. It is therefore necessary and very informative to look into some theory of field extensions, both general extensions and Galois extensions. It is here that we will encounter Hurwitz' genus formula and Dedekind's different theorem, as well as some theorems that tell us more about the splitting behaviour in Galois extensions. We then explain the correspondence between curves with rational points and function field with rational places. We will set up the necessary definitions and tools, but refer the reader to other sources for the full proofs and background. Lastly, we will look into completions of global fields and define the idèle class group, which we will encounter again in Chapter 4. After those sections, we will have enough knowledge of function fields and their places to create an algorithm that uses unramified extensions to find new function fields with many places.

1.1 Valuations, places and divisors

In this section we will go through the basic concepts of function fields. We will define what a function field is and look at some of its properties. Although we are mainly interested in function fields over finite fields, the theory in this chapter holds for any perfect field k. We start with some basic definitions and facts about valuations and their maximal ideals, which we will call places. We will later see that rational points on curves correspond to rational places of function fields. Therefore, these places will play a key role in the rest of this thesis. We start by defining valuations and places in a general setting, which will be useful when we look at local fields in Section 1.5.

Definition 1.1. Let K be a field. A *discrete valuation* on K is a map $v : K^* \to \mathbb{Z}$ such that

1. v is a surjective homomorphism of additive groups (meaning $v(x \cdot y) = v(x) + v(y)$);
2. $v(x + y) \geq \min(v(x), v(y))$.

We set $v(0) = +\infty$ to extend this map to all of K.

Let K be a field and v a map satisfying the above conditions. We call the pair (K, v) a *valued field*.

Definition 1.2. Let (K, v) be a valued field. We define the following sets:

$$\mathcal{O}_K = \{x \in K \mid v(x) \geq 0\}, \qquad \mathfrak{p}_K = \{x \in K \mid v(x) > 0\}, \qquad U_K = \{x \in K \mid v(x) = 0\}.$$

Definition 1.3. A *discrete valuation ring* is a principal ideal domain with a unique nonzero prime ideal.

Proposition 1.4. *Let (K, v) be a valued field. Then $\mathcal{O}_K$ is a discrete valuation ring with unique prime ideal $\mathfrak{p}_K$.*

Proof. See [Ser13, Proposition 1.1.1]. □

We will now define the kind of valued fields that will be our main objects in this thesis.

Definition 1.5. Let k be a perfect field. An *algebraic function field* K/k of one variable over k is a finite algebraic extension of $k(x)$ where $x \in K$ is some element transcendental over k. A function field of the type $K = k(x)$ is called a *rational function field*.

Definition 1.6. Let K/k be an algebraic function field. The set

$$\widetilde{k} = \{z \in F \mid z \text{ is algebraic over } k\}$$

is the *field of constants* of K/k. If $k = \widetilde{k}$ then K is called the *full constant* field of K. From now on, when we write K/k we always mean that k is the full constant field of K.

Let us look at two examples of function fields.

1. Let k be $\mathbb{F}_7$, the finite field with 7 elements, and let $f \in k[x]$ be an irreducible polynomial of positive degree. Then the field $K = k(x)[y]/(y^2 - f)$ is an algebraic function field. It is a degree 2 extension of the rational function field $k(x)$ and has constant field k.

2. Let k again be the finite field $\mathbb{F}_7$. Then the extension $k(x)[\alpha]$ with α algebraic over k, such that $\alpha^2 + \alpha + 1 = 0$ is also an algebraic function field. This time we see that the constant field of the function field is no longer $\mathbb{F}_7$, but is now $\mathbb{F}_{49}$, as there are 7^2 elements of the form $a + b \cdot \alpha,\ a, b \in \mathbb{F}_7$ that are algebraic over k. We have thus again found a rational function field, but now over the constant field $\mathbb{F}_{49}$ rather than over $\mathbb{F}_7$.

In general, an algebraic function field can often be written as $k(x, y)$, where x is transcendental over k and $\varphi(y) = 0$ for some irreducible polynomial $\varphi(T) \in k(x)[T]$. Recall that when k is a perfect field, every irreducible polynomial over k is separable. We call the polynomial φ the defining equation of the function field.

For any algebraic function field K, there exist discrete valuations v. For example, for the rational function field $k(x)$, we have the following valuations.

1. For each monic irreducible polynomial $h(x) \in k(x)$, we have the finite valuation $v_{h(x)}$ which sends $z = \frac{f(x)}{g(x)} \in k(x)$ to $n_1 - n_2 \in \mathbb{Z}$ where n_1 is the maximal integer such that $h^{n_1} | f$ and n_2 the maximal integer such that $h^{n_2} | g$.

2. Moreover, there exists an infinite valuation v_∞ that sends an element $z = \frac{f(x)}{g(x)}$ to the integer $\deg(f(x)) - \deg(g(x))$.

Definition 1.7. Let K be an algebraic function field. We call the unique nonzero prime ideal of a valuation v of K a *place*. The valuation ring corresponding to the place $\mathfrak{p}$ is written as $\mathcal{O}_\mathfrak{p}$. An element $t \in \mathfrak{p}$ such that $\mathfrak{p} = t\mathcal{O}_\mathfrak{p}$ is called a *local parameter* or a *uniformizer* for $\mathfrak{p}$. We define the set of all places of K to be $\mathbb{P}_K$.

For a rational function field, this gives us the following places. For each monic irreducible polynomial $h(x) \in k(x)$ we have the finite place

$$\mathfrak{p}_{h(x)} = \{\frac{f(x)}{g(x)} \in k(x) \mid h(x) | f(x),\ h(x) \nmid g(x)\}$$

and moreover there is a unique infinite place

$$\mathfrak{p}_\infty = \{\frac{f(x)}{g(x)} \in k(x) \mid \deg(f(x)) < \deg(g(x))\}.$$

[Sti09, Theorem 1.2.2] tells us that those are the only places of a rational function field.

Definition 1.8. As a place $\mathfrak{p}$ is a maximal ideal, $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$ is a field. We define $\widetilde{K}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{p}$ to be the *residue class field* of $\mathfrak{p}$ and define the degree of the place $\mathfrak{p}$ to be $\deg(\mathfrak{p}) = [\widetilde{K}_\mathfrak{p} : k]$. A place of degree 1 is called a *rational place* of K. For $x \in \mathcal{O}_\mathfrak{p}$ we denote by $x(\mathfrak{p})$ the residue class of x in $\widetilde{K}_\mathfrak{p}$.

Proposition 1.9. *Let K be an algebraic function field and $\mathfrak{p}$ a place of K. Then the degree of $\mathfrak{p}$ is a finite integer.*

Proof. See [Sti09, Proposition 1.1.15]. □

Definition 1.10. Let $z \in K$ and $\mathfrak{p}$ a place of K. Then we say that $\mathfrak{p}$ is a zero of z is $v_\mathfrak{p}(z) > 0$ and that $\mathfrak{p}$ is a pole of z if $v_\mathfrak{p}(z) < 0$.

One might now wonder under which circumstances a function field has places, and how many places it has. The following proposition tells us that a function field always has at least two places.

Proposition 1.11. *Let K/k be a function field, and let $z \in K$ be transcendental over k (which is equivalent to $z \in K\backslash k$ as k is the full constant field of K). Then z has at least one and at most finitely many zeroes and poles.*

Proof. See [Sti09, Corollary 1.1.20 and 1.3.4] □

The next theorem tells us something about the independence of valuations. It is a very handy tool when working with algebraic function fields, and is often used in proofs in [Sti09]. For example, it can be used to show that every function field has in fact infinitely many places.

Theorem 1.12. *[Weak approximation theorem] Let K/k be a function field, $\mathfrak{p}_1, ..., \mathfrak{p}_n \in \mathbb{P}_K$ pairwise distinct places, $x_1, .., x_n \in K$, $r_1, .., r_n \in \mathbb{Z}$. Then there is an $x \in K$ such that $v_{\mathfrak{p}_i}(x - x_i) = r_i$ for all $1 \leq i \leq n$.*

Proof. See [Sti09, Theorem 1.3.1]. □

Corollary 1.13. *Every function field has infinitely many places.*

Proof. Suppose not, then by the weak approximation theorem there exists an element $x \in K$ such that $v_{\mathfrak{p}_i}(x) > 0$ for every place $\mathfrak{p}_i$. Since every element of k has no zeroes at all, we see that x must be transcendental over k. Now Proposition 1.11 gives a contradiction. □

We also have the following stronger version of Theorem 1.12, not surprisingly called the strong approximation theorem, which we will need in Chapter 5.

Theorem 1.14. *[Strong approximation theorem] Let K/k be a function field, A a proper non-empty subset of $\mathbb{P}_K$ and $\mathfrak{p}_1, ..., \mathfrak{p}_n \in A$ pairwise distinct places. Then for any given $x_1, .., x_n \in K$, and integers $r_1, .., r_n \in \mathbb{Z}$, there is an $x \in K$ such that*

$$v_{\mathfrak{p}_i}(x - x_i) = r_i \text{ for all } 1 \leq i \leq n, \qquad v_\mathfrak{p}(x) \geq 0 \text{ for all } \mathfrak{p} \in A\backslash\{\mathfrak{p}_1, ..\mathfrak{p}_n\}.$$

Proof. See [Ros02, Theorem 6.13]. □

Definition 1.15. Let K/k be a function field. Then the *divisor group* of K is defined as the additively written free abelian group generated by the places of K. The divisor group is denoted by $\mathrm{Div}(K)$ and its elements are called divisors. We write

$$D = \sum_{\mathfrak{p} \in \mathbb{P}_K} n_{\mathfrak{p}} \mathfrak{p} \text{ with } n_{\mathfrak{p}} \in \mathbb{Z} \text{ and } n_{\mathfrak{p}} = 0 \text{ for almost all places } \mathfrak{p}.$$

We define the sum of two divisors $D_1 = \sum n_{\mathfrak{p}} \mathfrak{p},\ D_2 = \sum m_{\mathfrak{p}} \mathfrak{p}$ to be

$$D_1 + D_2 := \sum (n_{\mathfrak{p}} + m_{\mathfrak{p}}) \mathfrak{p}.$$

We call the set of places for which $n_{\mathfrak{p}} \neq 0$ the *support* of D. If $D = 1 \cdot \mathfrak{p}$ then we say that D is a *prime divisor*.

The following gives a partial ordering on the group of divisors.

Definition 1.16. Let K be an algebraic function field and let $D_1 = \sum n_{\mathfrak{p}} \mathfrak{p},\ D_2 = \sum m_{\mathfrak{p}} \mathfrak{p}$ be two divisors of K. We say that $D_1 \geq D_2$ if $n_{\mathfrak{p}} \geq m_{\mathfrak{p}}$ for all places $\mathfrak{p}$ of K. Moreover, we say that D is *effective* if $D \geq 0$.

Definition 1.17. The degree of a divisor D is defined as $\sum n_{\mathfrak{p}} \cdot \deg(\mathfrak{p})$. The divisors of degree zero form a subgroup of the divisor group and are denoted by $\mathrm{Div}^0(K)$.

The following proposition follows from the fact that over a perfect field, the greatest common divisor of the degrees of the places is one.

Proposition 1.18. *The map* $\mathrm{Div}(K) \to \mathbb{Z}$*, sending each element* $\sum n_{\mathfrak{p}} \mathfrak{p}$ *to its degree* $\sum n_{\mathfrak{p}} \cdot \ \deg(\mathfrak{p})$ *is surjective.*

Proof. See [Ros02, p.242] □

Definition 1.19. Let K/k be a function field, then for any $x \in K$ we denote by (x) the divisor

$$(x) = \sum_{\mathfrak{p} \in \mathbb{P}_K} v_{\mathfrak{p}}(x) \mathfrak{p}.$$

We call such a divisor a *principal divisor*.

Proposition 1.20. *Any principal divisor has degree zero. Moreover, let* $(x)_0 = \sum \deg(\mathfrak{p}) \cdot \mathfrak{p}$ *with* $\mathfrak{p}$ *running over all zeroes of* x*, and* $(x)_\infty = \sum \deg(\mathfrak{q}) \cdot \mathfrak{q}$ *with* $\mathfrak{q}$ *running over all poles of* x*. Then*

$$\deg((x)_0) = \deg((x)_\infty) = [K : k(x)].$$

Proof. See [Sti09, Theorem 1.4.11]. □

Definition 1.21. The set $\mathrm{Princ}(K) = \{(x) \mid 0 \neq x \in K\}$ is called the *group of principal divisors*. As it is a subgroup of the group of all divisors, we define the *divisor class group* and the *degree zero divisor class group* to be the quotients

$$\mathrm{Cl}_K = \frac{\mathrm{Div}(K)}{\mathrm{Princ(K)}} \quad \text{and} \quad \mathrm{Cl}_K^0 = \frac{\mathrm{Div}^0(K)}{\mathrm{Princ(K)}}.$$

We write $D_1 \sim D_2$ when D_1 and D_2 are in the same equivalence class, meaning that $D_1 = D_2 + (x)$ for some $x \in K$. We denote the equivalence class of a divisor D by $[D]$.

Proposition 1.22. *Let K be an algebraic function field. Then Cl_K^0 is a finite group.*

Proof. See [Sti09, Proposition 5.1.3]. □

Definition 1.23. Let D be a divisor of the function field K/k, then we define

$$\mathcal{L}(D) = \{x \in K \mid (x) + D \geq 0\}.$$

We see that this is a k-vector space, as $v_\mathfrak{p}(x+y) = \min(v_\mathfrak{p}(x),\ v_\mathfrak{p}(y))$ whenever $v_\mathfrak{p}(x) \neq v_\mathfrak{p}(y)$ and $v_\mathfrak{p}(ax) = v_\mathfrak{p}(a) + v_\mathfrak{p}(x)$. The dimension of $\mathcal{L}(D)$ as a k-vector space is denoted by $l(D)$.

Proposition 1.24. *There exists a positive integer $\gamma \in \mathbb{N}$ such that for all divisors D of K we have that*

$$\deg(D) - l(D) \leq \gamma.$$

Proof. See [Sti09, Proposition 1.4.14]. □

This allows for the following definition.

Definition 1.25. The *genus* g of a function field K/k is defined as

$$g = \max\{\deg(D) - l(D) + 1 \mid D \in \mathrm{Div}(K)\}.$$

Proposition 1.26. *The genus of a function field K/k is a non-zero integer.*

Proof. Let $x \in k$, then x has no zeroes or poles. Therefore, the prime divisor $(x) = 0$ so $\deg((x)) = 0$. By Proposition 1.11 we see that there is no element $z \in K \backslash k$ such that $(z) + (x) \geq 0$. On the other hand, for every other constant $x' \in k$ it is true that $(x') + (x) \geq 0$ by Proposition 1.20. We thus see that $l((x)) = 1$, and so we have that $g \geq \deg((x)) - l((x)) + 1 = 0$. □

Proposition 1.27. *Let k be a finite field. Then the rational function field $k(x)/k$ has genus 0.*

Proof. See [Sti09, Example 1.4.18]. □

This tells us that any non-trivial function field has positive genus. In general, it can be very difficult to find the genus of a function field, especially for function fields with larger genera. We do have the following theorem, due to Riemann.

Theorem 1.28. *Let K be an algebraic function field of genus g. Then there exists an integer c, depending only on K, such that $l(A) = \deg(A) + 1 - g$ whenever $\deg(A) \geq c$.*

1.2 Algebraic extensions of function fields

The goal of this thesis is to create global function fields with many rational places. We will find these new function fields by looking at extensions of other function fields. In particular, we are interested in the splitting behaviour of places and the genus of the extension field. In what follows, we will assume k is a perfect field (which is true for any finite field) and moreover if we write K/k we assume k is the full constant field of K. When we say K'/k' is an algebraic extension of K/k we mean that $K \subseteq K'$ is an algebraic field extension and $k \subseteq k'$.

Definition 1.29. For an algebraic field extension K'/k' of K/k we use the following definitions.

1. We say K'/K is a *constant field extension* if $K' = Kk'$;
2. We say K'/K is a *geometric field extension* if $k' = k$;
3. We say K'/K is a *finite extension* if $[K' : K] < \infty$.

From this definition we see that any finite algebraic extension K'/k' of K/k can be seen as the compositum of a constant and a geometric extension. As these extensions behave quite differently, we will state some properties of constant extensions at the end of this section. By analyzing the behaviour of places in such extensions we will get one step closer to our goal.

Proposition 1.30. *Let K'/k' be an algebraic extension of K/k. Let $\mathfrak{p}$ be a place of K and $\mathfrak{q}$ a place of K'. The following three statements are equivalent.*

1. *$\mathfrak{p} \subseteq \mathfrak{q}$;*
2. *$\mathcal{O}_\mathfrak{p} \subseteq \mathcal{O}_\mathfrak{q}$;*
3. *there exists an integer $e \geq 1$ such that $v_\mathfrak{q}(x) = e \cdot v_\mathfrak{p}(x)$ for all $x \in K$.*

Proof. (i) $\rightarrow$ (ii). Assume $\mathfrak{p} \subseteq \mathfrak{q}$ but $\mathcal{O}_\mathfrak{p} \not\subseteq \mathcal{O}_\mathfrak{q}$. Then there exists a $x \in K$ with $v_\mathfrak{p}(x) \geq 0$ and $v_\mathfrak{q}(x) < 0$. Let t be a uniformizer for $\mathfrak{p}$ then $v_\mathfrak{p}(t) = 1$ and $\mathfrak{p} \subseteq \mathfrak{q}$ so $v_\mathfrak{q}(t) = r$ with $r \geq 1$. Then we see that

$$\begin{aligned} v_\mathfrak{p}(x^r t) &= r \cdot v_\mathfrak{p}(x) + v_\mathfrak{p}(t) \geq 1 \\ v_\mathfrak{q}(x^r t) &= r \cdot v_\mathfrak{q}(x) + v_\mathfrak{q}(t) \leq r \cdot -1 + r = 0. \end{aligned}$$

We thus see that this implies $\mathfrak{p} \not\subseteq \mathfrak{q}$ which is in contradiction with (i).

(ii) $\rightarrow$ (iii). We start by noting that if $u \in K$ such that $v_\mathfrak{p}(u) = 0$, we also have that $v_\mathfrak{q}(u) = 0$. Namely, if $v_\mathfrak{p}(u) = 0$ then $v_\mathfrak{p}(u^{-1}) = 0$ so both $u, u^{-1} \in \mathcal{O}_\mathfrak{p} \subseteq \mathcal{O}_\mathfrak{q}$, and thus $v_\mathfrak{q}(u) = 0$. We use this as follows. Choose a uniformizer $t \in K$ and set $v_\mathfrak{q}(t) = e$. Since $\mathfrak{p} \subseteq \mathfrak{q}$ we see that $e \geq 1$. Let $x \in K$ nonzero and set $v_\mathfrak{p}(x) = r$. Then $v_\mathfrak{p}(t^{-r}x) = 0$ and

$$v_\mathfrak{q}(x) = v_\mathfrak{q}(t^{-r}x) + v_\mathfrak{q}(t^r) = 0 + r v_\mathfrak{q}(t) = v_\mathfrak{p}(x) \cdot e.$$

(iii) $\rightarrow$ (i). If $v_\mathfrak{p}(x) \geq 1$ then we see that $v_\mathfrak{q}(x) \geq e \cdot 1 \geq 1$ and therefore that $\mathfrak{p} \subseteq \mathfrak{q}$. $\square$

Definition 1.31. If the statements in Proposition 1.30 hold, we say that $\mathfrak{q} \in \mathbb{P}_{K'}$ lies over $\mathfrak{p} \in \mathbb{P}_K$ (and write $\mathfrak{q}|\mathfrak{p}$). $\mathfrak{p}$ is also called the *restriction* of $\mathfrak{q}$ to K.

The following is an immediate corollary of Proposition 1.30.

Corollary 1.32. *Let K'/K be an algebraic extension, and let $\mathfrak{q}|\mathfrak{p}$. Then*

$$\mathfrak{p} = \mathfrak{q} \cap K, \quad \mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{q} \cap K.$$

Proof. Proposition 1.30 tells us that $\mathfrak{p} \subseteq \mathfrak{q}$ and moreover that $v_\mathfrak{q}(x) = e \cdot v_\mathfrak{p}(x)$ for all $x \in K$. Therefore we see that $\mathfrak{p} = \{x \in K \mid v_\mathfrak{p}(x) > 0\}$ consists exactly of the elements of K such that $v_\mathfrak{q}(x) > 0$. From this it follows that $\mathfrak{p} = \mathfrak{q} \cap K$ and analogously $\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{q} \cap K$. $\square$

Proposition 1.33. *Let K'/K be an algebraic extension, and let $\mathfrak{q}|\mathfrak{p}$. Then the residue class field $\widetilde{K}_\mathfrak{p}$ is a subfield of $\widetilde{K}'_\mathfrak{q}$.*

Proof. We see from Proposition 1.32 that $\mathcal{O}_\mathfrak{p} \subseteq \mathcal{O}_\mathfrak{q}$. We define a map from $\mathcal{O}_\mathfrak{p}/\mathfrak{p} \to \mathcal{O}_\mathfrak{q}/\mathfrak{q}$ by sending the class of x modulo $\mathfrak{p}$ to the class of x modulo $\mathfrak{q}$. This is well-defined, since if two elements $x, y \in \mathcal{O}_\mathfrak{p}$ are in the same class modulo $\mathfrak{p}$, then since $\mathfrak{p} \subseteq \mathfrak{q}$ they are definitely in the same class modulo $\mathfrak{q}$. Moreover, this map is injective since if x, y are not in the same class modulo $\mathfrak{p}$, they cannot be in the same class modulo $\mathfrak{q}$ since $\mathfrak{q} \cap K$ is all of $\mathfrak{p}$. From this it follows that $\widetilde{K}_\mathfrak{p}$ is a subfield of $\widetilde{K}'_\mathfrak{q}$. □

Definition 1.34. The integer e such that $v_\mathfrak{q}(x) = e \cdot v_\mathfrak{p}(x)$ is called the *ramification index* of $\mathfrak{q}$ over $\mathfrak{p}$ and is denoted by $e(\mathfrak{q}|\mathfrak{p})$. If $e(\mathfrak{q}|\mathfrak{p}) > 1$ we say that $\mathfrak{q}$ is ramified (over $\mathfrak{p}$), if not $\mathfrak{q}$ is *unramified* (over $\mathfrak{p}$). We define $f(\mathfrak{q}|\mathfrak{p}) = [\widetilde{K}'_\mathfrak{q} : \widetilde{K}_\mathfrak{p}]$ to be the *residue degree* or *relative degree* of $\mathfrak{q}$ over $\mathfrak{p}$. We say that a place $\mathfrak{p}$ splits completely in K'/K if there are exactly $[K' : K]$ places above $\mathfrak{p}$.

The residue degree tells us how much the constant field extends locally as we have the following equality:

$$f(\mathfrak{q}|\mathfrak{p}) = [\widetilde{K}'_\mathfrak{q} : \widetilde{K}_\mathfrak{p}] = \frac{[\widetilde{K}'_\mathfrak{q} : k']}{[\widetilde{K}_\mathfrak{p} : k]} \cdot [k' : k] = \frac{\deg(\mathfrak{q})}{\deg(\mathfrak{p})} \cdot [k' : k].$$

Moreover, we have the following important theorem, which tells us how ramification index and residue degree are related.

Theorem 1.35 (Fundamental equality)**.** *Let K'/k' be a finite extension of K/k. Let $\mathfrak{p}$ be a place of K, and let $\mathfrak{q}_1, ..., \mathfrak{q}_m$ be all the places of K' lying over $\mathfrak{p}$. Then*

$$\sum_{i=1}^{m} e(\mathfrak{q}_i|\mathfrak{p}) \cdot f(\mathfrak{q}_i|\mathfrak{p}) = [K' : K].$$

The fundamental equality tells us several things. First of all, we see that there is at least one and at most $[K' : K]$ places lying above each place $\mathfrak{p}$ of K. Moreover, we see that when the places $\mathfrak{q}_i$ above a place $\mathfrak{p}$ have high ramification index or high residue degree, there can only be a small number of places above $\mathfrak{p}$. We will later see that this equality becomes even more useful in Galois extensions, since then the ramification indices and residue degrees of all places $\mathfrak{q}_i$ above a place $\mathfrak{p}$ are equal.

When looking at field extensions, we are not only interested in the splitting behaviour of places, but also in the behaviour of the genus. We will now build the foundation for Hurwitz' genus formula, which gives us the genus of a finite separable extension K'/k' in terms of the genus of the function field K/k and the ramification behaviour. We will first state some general properties of automorphisms of field extensions, that will be needed multiple times. In the next subsection we will look into Galois extensions, which is when the following properties will be extremely important.

Proposition 1.36. *Let K'/K be an algebraic extension of function fields, $\mathfrak{p} \in \mathbb{P}_K$ and $\mathfrak{q} \in \mathbb{P}_{K'}$ lying over $\mathfrak{p}$. Let $\mathrm{Aut}(K'/K)$ denote the automorphism group of K'/K, which is the set of all automorphisms of K' where the elements of K stay fixed, and let σ be an element of the automorphism group of K'/K. Then we have that $\sigma(\mathfrak{q}) = \{\sigma(x) \mid x \in \mathfrak{q}\}$ is a place of K' such that:*

1. $\sigma(\mathfrak{q})|\mathfrak{p}$;
2. $v_{\sigma(\mathfrak{q})}(y) = v_{\mathfrak{q}}(\sigma^{-1}(y))$ *for all* $y \in K'$;
3. $e(\sigma(\mathfrak{q})|\mathfrak{p}) = e(\mathfrak{q}|\mathfrak{p}),\ f(\sigma(\mathfrak{q})|\mathfrak{p}) = f(\mathfrak{q}|\mathfrak{p})$.

Proof. (i). We want to show $\mathfrak{p} \subseteq \sigma(\mathfrak{q})$. Since $\sigma(\mathfrak{q}) = \{\sigma(x) \mid x \in \mathfrak{q}\}$ we see that if $\mathfrak{p} \subseteq \mathfrak{q}$ then $\sigma(\mathfrak{p}) \subseteq \sigma(\mathfrak{q})$ but since $\sigma(\mathfrak{p}) = \mathfrak{p}$ by definition of the automorphism group this proves our case.

(ii). Let $y \in K'$ nonzero, then there exists $z \in K'$ such that $\sigma(z) = y$. Let t be a uniformizer for $\mathfrak{q}$, then $z = t^n \cdot u$ for some u with $v_{\mathfrak{q}}(u) = 0$. $v_{\mathfrak{q}}(u) = 0$ implies that $u \in \mathcal{O}_q \backslash \mathfrak{q}$, which means that $\sigma(u) \in \mathcal{O}_{\sigma(\mathfrak{q})} \backslash \sigma(\mathfrak{q})$. From this it follows that $v_{\sigma(\mathfrak{q})}(u) = 0$ and thus that $v_{\sigma(\mathfrak{q})}(y) = v_{\sigma(\mathfrak{q})}(\sigma(z)) = v_{\sigma(\mathfrak{q})}(\sigma(t^n)) = n = v_{\mathfrak{q}}(z) = v_{\mathfrak{q}}(\sigma^{-1}(y))$.

(iii). Choose a uniformizer t of $\mathfrak{p}$. Then we see that

$$e(\sigma(\mathfrak{q})|\mathfrak{p}) = v_{\sigma(\mathfrak{q})}(t) = v_{\mathfrak{q}}(\sigma^{-1}(t)) = v_{\mathfrak{q}}(t) = e(\mathfrak{q}|\mathfrak{p}).$$

An automorphism σ of K'/K induces an isomorphism of the residue class field $\widetilde{K}'_{\mathfrak{q}}$ onto $\widetilde{K}'_{\sigma(\mathfrak{q})}$ given by $\sigma(z + \mathfrak{q}) = \sigma(z) + \sigma(\mathfrak{q})$. Since this is the identity on $\widetilde{K}_{\mathfrak{p}}$ we have that $[\widetilde{K}'_{\mathfrak{q}} : \widetilde{K}_{\mathfrak{p}}] = [\widetilde{K}'_{\sigma(\mathfrak{q})} : \widetilde{K}_{\mathfrak{p}}]$ and thus that $f(\mathfrak{q}|\mathfrak{p}) = f(\sigma(\mathfrak{q})|\mathfrak{p})$. □

We will now define two maps that send elements of an extension field K' to elements of the ground field K.

Definition 1.37. Let K'/K be a finite extension, choose an algebraic closure Ω of K in which K' lies. Denote by $\sigma_1, ...\sigma_n$ the embeddings of K' into Ω, meaning the field homomorphisms $\sigma : K' \to \Omega$ such that $\sigma(a) = a$ for all $a \in K$. Then the *norm map* and the *trace map* are respectively given by

$$N_{K'/K}(x) = \prod_{i=1}^{n} \sigma_i(x), \qquad \mathrm{Tr}_{K'/K}(x) = \sum_{i=1}^{n} \sigma_i(x).$$

Definition 1.38. For $\mathfrak{p} \in \mathbb{P}_K$, let $\mathcal{O}'_{\mathfrak{p}}$ be the integral closure of $\mathcal{O}_{\mathfrak{p}}$ in K'. We then define

$$C_{\mathfrak{p}} = \{z \in K' \mid \mathrm{Tr}_{K'/K}(z \cdot \mathcal{O}'_{\mathfrak{p}}) \subseteq \mathcal{O}_{\mathfrak{p}}\}$$

to be the *complementary module* over $\mathfrak{p}$.

Proposition 1.39. *With the above notation we have the following.*

1. $C_{\mathfrak{p}}$ *is an* $\mathcal{O}'_{\mathfrak{p}}$*-module;*
2. *There exists an element* $t \in K'$*, depending on the place* $\mathfrak{p}$*, such that* $C_{\mathfrak{p}} = t \cdot \mathcal{O}'_{\mathfrak{p}}$;
3. *If* $C_{\mathfrak{p}} = t \cdot \mathcal{O}'_{\mathfrak{p}}$ *then* $v_{\mathfrak{q}}(t) \leq 0$ *for all* $\mathfrak{q}|\mathfrak{p}$ *and* $C_{\mathfrak{p}} = \mathcal{O}'_{\mathfrak{p}}$ *for almost all places* $\mathfrak{p} \in \mathbb{P}_K$.

Proof. See [Sti09, Proposition 3.4.2]. □

Definition 1.40. Let K'/K be a field extension, $\mathfrak{p}$ a place of K and $\mathcal{O}'_{\mathfrak{p}}$ as defined above. Let $C_{\mathfrak{p}} = t \cdot \mathcal{O}'_{\mathfrak{p}}$, then we define for every $\mathfrak{q}|\mathfrak{p}$ the *different exponent* of $\mathfrak{q}$ over $\mathfrak{p}$ by $d(\mathfrak{q}|\mathfrak{p}) = -v_{\mathfrak{q}}(t)$. Moreover, we define the *different* of K'/K to be

$$\mathrm{Diff}(K'/K) = \sum_{\mathfrak{p} \in \mathbb{P}_K} \sum_{\mathfrak{q}|\mathfrak{p}} d(\mathfrak{q}|\mathfrak{p}) \cdot \mathfrak{q}.$$

Theorem 1.41 (Hurwitz' genus formula)**.** *Let K/k be an algebraic function field of genus g and let K'/K be a finite separable extension. Let k' be the full constant field of K' and g' the genus of K'/k'. Then*

$$2g' - 2 = \frac{[K' : K]}{[k' : k]}(2g - 2) + \deg(\mathrm{Diff}(K'/K)).$$

Proof. See [Sti09, Theorem 3.4.13]. □

As the different plays an important role in Hurwitz' genus formula, it can be very useful to know a bit more about it. For the original definition, one needs to have information about all the places of K and their splitting behaviour. Fortunately, Dedekind came up with a very handy theorem.

Theorem 1.42 (Dedekind's different theorem)**.** *Let K'/K be a finite separable extension, $\mathfrak{q}$ a place of K' lying above $\mathfrak{p} \in \mathbb{P}_K$. Then we have that:*

1. *$d(\mathfrak{q}|\mathfrak{p}) \geq e(\mathfrak{q}|\mathfrak{p}) - 1$;*
2. *$d(\mathfrak{q}|\mathfrak{p}) = e(\mathfrak{q}|\mathfrak{p}) - 1 \iff e(\mathfrak{q}|\mathfrak{p})$ is not divisible by $\mathrm{char}(k)$.*

Proof. See [Sti09, Theorem 3.5.1]. □

This yields the following corollary.

Corollary 1.43. *Let K'/K be a finite separable extension of function fields having the same constant field. Let g be the genus of K, g' the genus of K'. Then $g \leq g'$.*

Proof. By Dedekind's different theorem we have that $d(\mathfrak{q}|\mathfrak{p}) \geq 0$ for all places $\mathfrak{p} \in \mathbb{P}_K$, and therefore that $\deg(\mathrm{Diff}(K'/K)) \geq 0$. Plugging this in the Hurwitz' genus formula then gives the desired result. □

One can apply Hurwitz' genus formula to find the following result.

Theorem 1.44. *Let K be a function field over a finite field k with cardinality $\neq 2$, given as a finite extension of the rational function field $k(x)$ by $y^2 - f(x)$, where $f(x)$ is some polynomial in $k(x)$ of degree $2n + 1$ or $2n + 2$. Then K has genus n.*

Proof. We start by noting that K is a degree 2 extension of the rational field $k(x)$. Moreover, $k(x)$ has genus 0 by Proposition 1.27. Therefore, Hurwitz' genus formula yields

$$2g' - 2 = 2(0 - 2) + \deg(\mathrm{Diff}(K/k(x)).$$

Now since $K/k(x)$ is a degree 2 field extension, we know that the ramification index of all places can be at most two. Dedekind's different theorem tells us that $d(\mathfrak{q}|\mathfrak{p}) = e(\mathfrak{q}|\mathfrak{p})-1 \iff e(\mathfrak{q}|\mathfrak{p})$ is not divisible by the characteristic of k. This means that for hyperelliptic function fields, the different consists of the sum of the ramified places.

Function fields of degree $2n + 1$ are called imaginary hyperelliptic function fields, since they have one place at infinity, and function fields of degree $2n + 2$ are called real hyperelliptic function fields, as they have two places at infinity. When looking at an imaginary hyperelliptic function field as an extension of a rational function field, we thus see that the place at infinity $\mathfrak{p}_\infty$ of $k(x)$ ramifies in the extension. On the other hand, for a real hyperelliptic function field we see that the place at infinity of $k(x)$ splits. From this it follows

that when the degree of f is $2n+1$, we see that the ramified places consist of all the places $(x-x_i)$, and the ramified place at infinity. When the degree of the polynomial f is $2n+2$, we see that the only ramified places are those of the form $(x-x_i)$ with x_i a root of $f(x)$ (see also [Sti09, Proposition 6.2.3.c]). In both cases all places have ramification index 2, so we see that the degree of the different is $2n+2$. Therefore we have that

$$g' = -1 + \frac{1}{2}\deg(\mathrm{Diff}(K/k(x))) = -1 + \frac{2n+2}{2} = n.$$

□

We will now state some properties of constant field extensions. As all field extensions can be split up in a constant and non-constant part, knowledge about how constant field extensions behave is needed when talking about general algebraic field extensions.

Proposition 1.45. *In a constant field extension $K' = Kk'$ the following hold:*

1. *k' is the full constant field of K';*
2. *K'/K is unramified;*
3. *K'/k' has the same genus as K/k;*
4. *The residue class field is of a place $\mathfrak{q}$ of K' is $\widetilde{K}'_{\mathfrak{q}} = \widetilde{K}_{\mathfrak{p}}k'$.*

Theorem 1.46. *Let K be a function field over $k = \mathbb{F}_q$ and let K_n denote the constant field extensions $K\mathbb{F}_{q^n}/\mathbb{F}_{q^n}$. Then we have that $\mathfrak{p}$ splits into $\gcd(n, \deg_K(\mathfrak{p}))$ places in K_n. Moreover, we have for every place $\mathfrak{q}_i|\mathfrak{p}$ that*

$$\deg_{K_n}(\mathfrak{q}_i) = \frac{\deg_K(\mathfrak{p})}{\gcd(n, \deg_K(\mathfrak{p}))} \quad \text{and} \quad f(\mathfrak{q}_i|\mathfrak{p}) = \frac{n}{\gcd(n, \deg_K(\mathfrak{p}))}.$$

Proof. See [Ros02, Theorem 8.13]. □

The above theorem tells us that rational places in the ground field stay rational in the extension field, as $\deg_K(\mathfrak{p}) = 1$ in that case. Therefore, each rational place in the ground field contributes exactly one rational place in the extension field, as these places stay inert. Moreover, we see that the only other places that become rational places in the extension field are those of degree dividing n. We thus have the following.

Proposition 1.47. *Let K be a function field over $k = \mathbb{F}_q$ and let K_n denote the constant field extension $K\mathbb{F}_{q^n}/\mathbb{F}_{q^n}$. Denote by $B_r(K)$ the number of places of degree r of the function field K. Then the number of rational places of the field extension K_n/K is $\sum_{d|n} d \cdot B_d(K)$.*

1.3 Galois extensions

In this subsection we will look at special properties of Galois extensions.

Definition 1.48. Let L/K be a finite algebraic extension of function fields. Then we say that L/K is *Galois* if the automorphism group of L/K consists of exactly $[L:K]$ elements.

The following theorem tells us why Galois extensions are easier to work with than general extensions.

Theorem 1.49 (Main theorem of Galois theory for finite extensions)**.** *Let K'/K be a finite Galois extension. Then the maps*

$$M \mapsto H := \mathrm{Aut}(K'/M) \text{ and } H \mapsto M := K'^H$$

yield an inclusion-reversing bijection between subfields $K \subseteq M \subseteq K'$ and subgroups H of the Galois group. The extension K'/M is always Galois, and the extension M/K is Galois if and only if H is a normal subgroup of G. Then $\mathrm{Gal}(M/K) \cong G/H$.

Proof. See [Sza09, Theorem 1.2.5]. □

This inclusion-reversing bijection will be of great importance for our algorithm in the next chapter. It tells us that looking at subgroups of the Galois group is equivalent to looking at subfields of a Galois extension. The goal of our algorithm is to find field extensions with many rational places. We will do that by first constructing a very large field extension, and then look at its subextensions. In the rest of this section we will investigate some properties of the behaviour of those intermediate extensions. This will lead to a key theorem (Theorem 1.55) that is one of the building blocks of our algorithm.

Theorem 1.50. *Let K'/k' be a Galois extension of K/k and $\mathfrak{q}_1, \mathfrak{q}_2 \in \mathbb{P}_{K'}$ above $\mathfrak{p}$. Then there is some $\sigma \in \mathrm{Gal}(K'/K)$ such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$, i.e. the Galois group acts transitively on the places above $\mathfrak{p}$.*

Proof. We start by noting that by Proposition 1.30 for two places $\mathfrak{q}_1, \mathfrak{q}_2$ over $\mathfrak{p}$ we have that for all $x \in K$,

$$v_{\mathfrak{q}_1}(x) = 0 \iff v_{\mathfrak{p}}(x) = 0 \iff v_{\mathfrak{q}_2}(x) = 0.$$

Denote by G the Galois group of K'/K and note that the norm map of an extension K'/K sends $x \in K'$ to $\prod_{\sigma \in G} \sigma(x) \in K$. Assume there is no $\sigma \in G$ such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$. By the weak approximation theorem, there exists an element $z \in K'$ such that $v_{\mathfrak{q}_2}(z) = 1$ and $v_{\mathfrak{q}_i}(z) = 0$ for all places $\mathfrak{q}_i$ over $\mathfrak{p}$, $\mathfrak{q}_i \neq \mathfrak{q}_2$. This gives us:

$$v_{\mathfrak{q}_1}(N_{K'/K}(z)) = v_{\mathfrak{q}_1}(\prod_{\sigma \in G} \sigma(z)) = \sum_{\sigma \in G} v_{\mathfrak{q}_1}(\sigma(z)) = \sum_{\sigma \in G} v_{\sigma^{-1}(\mathfrak{q}_1)}(z) = \sum_{\sigma \in G} 0 = 0,$$

since there is no $\sigma \in G$ such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$. On the other hand, we have that

$$v_{\mathfrak{q}_1}(N_{K'/K}(z)) = v_{\mathfrak{q}_1}(\prod_{\sigma \in G} \sigma(z)) = \sum_{\sigma \in G} v_{\mathfrak{q}_1}(\sigma(z)) \geq 1,$$

which is in contradiction with the fact that $v_{\mathfrak{q}_1}(x) = 0 \iff v_{\mathfrak{q}_2}(x) = 0$. □

Corollary 1.51. *Let $\mathfrak{q}_1, ..., \mathfrak{q}_n$ be all the places above $\mathfrak{p} \in \mathbb{P}_K$. Then*

1. $e(\mathfrak{q}_i|\mathfrak{p}) = e(\mathfrak{q}_j|\mathfrak{p}) = e(\mathfrak{p})$;
2. $f(\mathfrak{q}_i|\mathfrak{p}) = f(\mathfrak{q}_j|\mathfrak{p}) = f(\mathfrak{p})$;
3. $e(\mathfrak{p}) \cdot f(\mathfrak{p}) \cdot n = [K' : K]$;
4. $d(\mathfrak{q}_i|\mathfrak{p}) = d(\mathfrak{q}_j|\mathfrak{p}) = d(\mathfrak{p})$.

Proof. The first three statements are an immediate corollary of the above theorem and Proposition 1.36. For the last statement, see [Sti09, Corollary 3.7.2]. □

We thus see that in a Galois extension, a place ramifies or splits at all places lying above it in the same way. Therefore, if we know the splitting behaviour of one place above $\mathfrak{p}$, we know this about all the places above it. This will be a very important feature of Galois extensions and allows us to define the sets in the following definition. From now on we will assume K'/K is a Galois extension with Galois group $G = \mathrm{Gal}(K'/K)$ and that $\mathfrak{q}$ is a place of K' lying above $\mathfrak{p} \in \mathbb{P}_K$.

Definition 1.52. We define the following groups

$$G_Z(\mathfrak{q}|\mathfrak{p}) = \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}, \quad G_T(\mathfrak{q}|\mathfrak{p}) = \{\sigma \in G \mid v_{\mathfrak{q}}(\sigma z - z) > 0 \ \forall z \in \mathcal{O}_{\mathfrak{q}}\}.$$

$G_Z(\mathfrak{q}|\mathfrak{p})$ is called the *decomposition group* of $\mathfrak{q}$ over $\mathfrak{p}$ and $G_T(\mathfrak{q}|\mathfrak{p})$ is called the *inertia group* of $\mathfrak{q}$ over $\mathfrak{p}$. The fixed field $Z = Z(\mathfrak{q}|\mathfrak{p})$ of $G_Z(\mathfrak{q}|\mathfrak{p})$ is called the *decomposition field*, and the fixed field $T = T(\mathfrak{q}|\mathfrak{p})$ of $G_T(\mathfrak{q}|\mathfrak{p})$ is called the *inertia field*. Note that $G_T(\mathfrak{q}|\mathfrak{p}) \subseteq G_Z(\mathfrak{q}|\mathfrak{p})$.

Theorem 1.53. *Let K'/K be a Galois extension of function fields and let $\mathfrak{p}$ be a place of K, $\mathfrak{q}$ be a place of K' lying above $\mathfrak{p}$. Then*

(a) $G_Z(\mathfrak{q}|\mathfrak{p})$ has order $e(\mathfrak{q}|\mathfrak{p}) \cdot f(\mathfrak{q}|\mathfrak{p})$;

(b) The inertia group $G_T(\mathfrak{q}|\mathfrak{p})$ is a normal subgroup of $G_Z(\mathfrak{q}|\mathfrak{p})$ of order $e(\mathfrak{q}|\mathfrak{p})$;

(c) $\widetilde{K}'_{\mathfrak{q}}/\widetilde{K}_{\mathfrak{p}}$ is a Galois extension. Moreover, $\mathrm{Gal}(\widetilde{K}'_{\mathfrak{q}}/\widetilde{K}_{\mathfrak{p}}) \cong G_Z(\mathfrak{q}|\mathfrak{p})/G_T(\mathfrak{q}|\mathfrak{p})$.

Proof. (a). We use that the Galois group G of K'/K acts transitively on the places above $\mathfrak{p}$. Choose one place $\mathfrak{q}$ above $\mathfrak{p}$ and permutations $\sigma_1, ..., \sigma_r$ such that the $\sigma_i(\mathfrak{q})$ cover exactly all of the r places above $\mathfrak{p}$. The set of σ_i then forms a complete coset of the representatives of G/G_Z. We can see this by noting that $\sigma(\mathfrak{q})$ is also a place lying above $\mathfrak{p}$, and G_Z consists exactly of those permutations that leave $\mathfrak{q}$ fixed. Therefore we have that

$$[K' : K] = |\mathrm{Gal}(K'/K)| = r \cdot |G_Z|$$

and by the fundamental equality (Proposition 1.35) we get the statement of (a).

(b) +(c). Let $\sigma \in G_Z(\mathfrak{q}|\mathfrak{p})$, and $x, y \in \mathcal{O}_{\mathfrak{q}}$ with $\overline{x} = \overline{y} \in \widetilde{K}'_{\mathfrak{q}}$. Then we see that

$$x - y \in \mathfrak{q} \text{ so } \sigma(x) - \sigma(y) = \sigma(x - y) \in \sigma(\mathfrak{q}) = \mathfrak{q} \text{ and therefore } \sigma(x) + \mathfrak{q} = \sigma(y) + \mathfrak{q}.$$

We thus have a well-defined homomorphism from $G_Z(\mathfrak{q}|\mathfrak{p})$ to the automorphism group of $\widetilde{K}'_{\mathfrak{q}}/\widetilde{K}_{\mathfrak{p}}$. Moreover, we see that the kernel of this map is $G_T(\mathfrak{q}|\mathfrak{p})$ since

$$G_T(\mathfrak{q}|\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(K'/K) \mid \sigma(x) = x \text{ for all } x \in \mathcal{O}_{\mathfrak{q}}\}.$$

Since the kernel of a group homomorphism is a normal subgroup, this shows the first part of (b). Now we claim that this map is surjective and that $\widetilde{K}'_{\mathfrak{q}}/\widetilde{K}_{\mathfrak{p}}$ is Galois, see [Sti09, Theorem 3.8.2]. (Note that since k is perfect, $\widetilde{K}'_{\mathfrak{q}}/\widetilde{K}_{\mathfrak{p}}$ is separable, say $\widetilde{K}'_{\mathfrak{q}} = \widetilde{K}_{\mathfrak{p}}(\overline{u})$, so showing $\widetilde{K}'_{\mathfrak{q}}/\widetilde{K}_{\mathfrak{p}}$ is Galois means showing that $\widetilde{K}'_{\mathfrak{q}}$ is the splitting field of the minimal polynomial of $\overline{u}$.) From these two claims it follow that the Galois group of $\widetilde{K}'_{\mathfrak{q}}/\widetilde{K}_{\mathfrak{p}}$ is indeed $G_Z(\mathfrak{q}|\mathfrak{p})/G_T(\mathfrak{q}|\mathfrak{p})$. Moreover, we see that

$$\begin{aligned} f(\mathfrak{q}|\mathfrak{p}) = [\widetilde{K}'_{\mathfrak{q}} : \widetilde{K}_{\mathfrak{p}}] &= |\mathrm{Gal}(\widetilde{K}'_{\mathfrak{q}}/\widetilde{K}_{\mathfrak{p}})| \\ &= |G_Z(\mathfrak{q}|\mathfrak{p})|/|G_T(\mathfrak{q}|\mathfrak{p})| \\ &= (e(\mathfrak{q}|\mathfrak{p}) \cdot f(\mathfrak{q}|\mathfrak{p}))/|G_T(\mathfrak{q}|\mathfrak{p})| \end{aligned}$$

and thus that $|G_T(\mathfrak{q}|\mathfrak{p})| = e(\mathfrak{q}|\mathfrak{p})$. □

Theorem 1.54. *Let K'/K be a Galois extension of function fields and let $\mathfrak{p}$ be a place of K, $\mathfrak{q}$ be a place of K' lying above $\mathfrak{p}$. Let $\mathfrak{p}_Z$ denote the restriction of $\mathfrak{q}$ to Z, $\mathfrak{p}_T$ the restriction of $\mathfrak{q}$ to T. Then we have the following field extensions and relations:*

$$\begin{array}{cc} K' & \mathfrak{q} \\ | & | \\ T & \mathfrak{p}_T \\ | & | \\ Z & \mathfrak{p}_Z \\ | & | \\ K & \mathfrak{p} \end{array}$$

(i) $e(\mathfrak{q}|\mathfrak{p}_T) = e(\mathfrak{q}|\mathfrak{p}) = [K' : T], \quad f(\mathfrak{q}|\mathfrak{p}_T) = 1;$

(ii) $e(\mathfrak{p}_T|\mathfrak{p}_Z) = 1, \quad f(\mathfrak{p}_T|\mathfrak{p}_Z) = f(\mathfrak{q}|\mathfrak{p}) = [T : Z];$

(iii) $e(\mathfrak{p}_Z|\mathfrak{p}) = f(\mathfrak{p}_Z|\mathfrak{p}) = 1.$

Proof. It follows from $\{\mathrm{id}\} \subseteq G_T \subseteq G_Z \subseteq G$ that $K \subseteq Z \subseteq T \subseteq K'$.

(iii) Note that since Z is the fixed field of $G_Z(\mathfrak{q}|\mathfrak{p})$, this means that $\mathrm{Gal}(K'/Z) = G_Z(\mathfrak{q}|\mathfrak{p})$ consists exactly of those permutations that leave $\mathfrak{q}$ fixed, therefore $G_Z(\mathfrak{q}|\mathfrak{p}_Z) = G_Z(\mathfrak{q}|\mathfrak{p})$. Applying Theorem 1.54 (a) to both decomposition groups gives us

$$e(\mathfrak{q}|\mathfrak{p}_Z) \cdot f(\mathfrak{q}|\mathfrak{p}_Z) = e(\mathfrak{q}|\mathfrak{p}) \cdot f(\mathfrak{q}|\mathfrak{p})$$

and therefore $e(\mathfrak{q}|\mathfrak{p}_Z) = e(\mathfrak{q}|\mathfrak{p}),\ f(\mathfrak{q}|\mathfrak{p}_Z) = f(\mathfrak{q}|\mathfrak{p})$. This leads us to conclude that $e(\mathfrak{p}_Z|\mathfrak{p}) = f(\mathfrak{p}_Z|\mathfrak{p}) = 1$, which is the third statement. Since the Galois group acts transitively on the places above $\mathfrak{p}_Z$ and we have $\mathrm{Gal}(K'/Z) = G_Z(\mathfrak{q}|\mathfrak{p})$, we see that there is only one place $\mathfrak{q}$ over $\mathfrak{p}_Z$ since all elements of the Galois group send $\mathfrak{q}$ to itself.

(i) Note that we have $G_T(\mathfrak{q}|\mathfrak{p}) = G_T(\mathfrak{q}|\mathfrak{p}_T)$ by definition. Moreover, we defined $f(\mathfrak{q}|\mathfrak{p}) = [\widetilde{K}'_{\mathfrak{q}} : \widetilde{K}_{\mathfrak{p}}]$ so combining Theorem 1.54 (c) with (a) tells us that $|G_T(\mathfrak{q}|\mathfrak{p})| = e(\mathfrak{q}|\mathfrak{p}) = e(\mathfrak{q}|\mathfrak{p}_T)$ where the last equality follows from applying the above to K'/T. As $\mathrm{Gal}(K'/T) = G_T(\mathfrak{q}|\mathfrak{p}_T)$ we can now conclude that $[K' : T] = e(\mathfrak{q}|\mathfrak{p}) = e(\mathfrak{q}|\mathfrak{p}_T)$ and therefore $f(\mathfrak{q}|\mathfrak{p}_T) = 1$.

(ii) This follows immediately from the fact that

$$e(\mathfrak{q}|\mathfrak{p}) = e(\mathfrak{q}|\mathfrak{p}_T) \cdot e(\mathfrak{p}_T|\mathfrak{p}_Z) \cdot e(\mathfrak{p}_Z|\mathfrak{p})$$

and similarly for $f(\mathfrak{q}|\mathfrak{p})$. Combining this with the above results gives us $e(\mathfrak{p}_T|\mathfrak{p}_Z) = 1$ and $f(\mathfrak{p}_T|\mathfrak{p}_Z) = f(\mathfrak{q}|\mathfrak{p}) = [\mathfrak{p}_T : \mathfrak{p}_Z]$. □

The above theorem tells us that ramification happens in the extension K'/T, places stay inert in T/Z, and they split in Z/K. Moreover, as a direct corollary of the above theorem and the fundamental equality we see that the number of places $\mathfrak{q} \in \mathbb{P}_{K'}$ lying above a place $\mathfrak{p}$ of K is exactly $[Z : K]$.

Theorem 1.55. *Consider a Galois extension K'/K of algebraic function fields, $\mathfrak{p} \in \mathbb{P}_K$ and $\mathfrak{q}|\mathfrak{p}$. For $K \subseteq M \subseteq K'$ let $\mathfrak{p}_M = \mathfrak{q} \cap M$. Then:*

(a) $M \subseteq Z(\mathfrak{q}|\mathfrak{p}) \iff e(\mathfrak{p}_M|\mathfrak{p}) = f(\mathfrak{p}_M|\mathfrak{p}) = 1$, *so $\mathfrak{p}$ splits completely in M;*

(b) $M \supseteq Z(\mathfrak{q}|\mathfrak{p}) \iff \mathfrak{q}$ *is the only place lying above $\mathfrak{p}_M$;*

(c) $M \subseteq T(\mathfrak{q}|\mathfrak{p}) \iff e(\mathfrak{p}_M|\mathfrak{p}) = 1$;

(d) $M \supseteq T(\mathfrak{q}|\mathfrak{p}) \iff \mathfrak{p}_M$ *is totally ramified in* K'/M.

Proof. All implications $\implies$ are a direct corollary of the above theorem. We prove the inverse implications below.

(a). Note that as $e(\mathfrak{p}_M|\mathfrak{p}) = f(\mathfrak{p}_M|\mathfrak{p}) = 1$, we see that $e(\mathfrak{q}|\mathfrak{p}_M) = e(\mathfrak{q}|\mathfrak{p})$ and $f(\mathfrak{q}|\mathfrak{p}_M) = f(\mathfrak{q}|\mathfrak{p})$. Therefore, (a) of Theorem 1.53 tells us that $|G_Z(\mathfrak{q}|\mathfrak{p}_M)| = |G_Z(\mathfrak{q}|\mathfrak{p})|$. By definition we have that $G_Z(\mathfrak{q}|\mathfrak{p}_M) \subseteq G_Z(\mathfrak{q}|\mathfrak{p})$ so we see that the two decomposition groups are equal. This is possible only if M is a subset of the fixed field of $G_Z(\mathfrak{q}|\mathfrak{p})$, and thus we have that $M \subseteq Z(\mathfrak{q}|\mathfrak{p})$.

(b). When $\mathfrak{q}$ is the only place lying above $\mathfrak{p}_M$ we see that $G_Z(\mathfrak{q}|\mathfrak{p}_M) = \mathrm{Gal}(K'/M)$, since all elements of the Galois group send $\mathfrak{q}$ to itself. On the other hand we have that $G_Z(\mathfrak{q}|\mathfrak{p}_M) \subseteq G_Z(\mathfrak{q}|\mathfrak{p})$. Looking at their fixed fields gives

$$M = (K')^{\mathrm{Gal}(K'/M)} = (K')^{G_Z(\mathfrak{q}|\mathfrak{p}_M)} \supseteq (K')^{G_Z(\mathfrak{q}|\mathfrak{p})} = Z.$$

(c). We know that $G_T(\mathfrak{q}|\mathfrak{p})$ has order $e(\mathfrak{q}|\mathfrak{p})$ by Theorem 1.53. If $e(\mathfrak{p}_M|\mathfrak{p}) = 1$ this means that $G_T(\mathfrak{p}_M|\mathfrak{p})$ has order 1 and thus that $G_T(\mathfrak{q}|\mathfrak{p}) = G_T(\mathfrak{q}|\mathfrak{p}_M)$. From this it follows that M is fixed by all of $G_T(\mathfrak{q}|\mathfrak{p})$ and thus that $M \subseteq T$.

(d).When $\mathfrak{q}$ is totally ramified in K'/M we see that $e(\mathfrak{q}|\mathfrak{p}_M) = [K' : M]$. Since $G_T(\mathfrak{q}|\mathfrak{p}_M)$ has order $e(\mathfrak{q}|\mathfrak{p}_M)$ we have $|G_T(\mathfrak{q}|\mathfrak{p}_M)| = |\mathrm{Gal}(K'/M)|$. On the other hand we have that $G_T(\mathfrak{q}|\mathfrak{p}_M) \subseteq G_T(\mathfrak{q}|\mathfrak{p})$. Looking at their fixed fields gives

$$M = (K')^{\mathrm{Gal}(K'/M)} = (K')^{G_T(\mathfrak{q}|\mathfrak{p}_M)} \supseteq (K')^{G_T(\mathfrak{q}|\mathfrak{p})} = T.$$

□

When looking at class formations in Chapter 4, we will also encounter some infinite Galois groups. We will therefore briefly state the main theorem of infinite Galois theory here. For proofs of the statements below, see [Sza09, Chapter 1.3]. Before we can do that, we will need a few definitions.

Definition 1.56. An *inverse system of groups* $(G_\alpha, \phi_{\alpha\beta})$ consists of

1. A partially ordered set $(\Lambda, \leq)$ such that for all $\alpha, \beta \in \Lambda$ there is some $\gamma \in \Lambda$ such that $\alpha \leq \gamma,\ \beta \leq \gamma$;
2. For each $\alpha \in \Lambda$ a group G_α;
3. For each $\alpha \leq \beta$ a homomorphism $\phi_{\alpha\beta} : G_\beta \to G_\alpha$ such that we have $\phi_{\alpha\gamma} = \phi_{\alpha\beta} \circ \phi_{\beta\gamma}$ for all $\alpha \leq \beta \leq \gamma$.

The *inverse limit* of this system is defined as the subgroup of the direct product $\prod G_\alpha$ consisting of sequences (g_α) such that $\phi_{\alpha\beta}(g_\beta) = g_\alpha$ for all $\alpha \leq \beta$.

We call the inverse limit of a system of finite groups a *profinite group*. The most well-known example is the following. Let us look at the partially ordered set $(\mathbb{N}, \leq)$ where $m \leq n$ if and only if m divides n. We know that for all $m, n \in \mathbb{N}$ there is an element $\gamma \in \mathbb{N}$, namely mn such that $m \leq \gamma, n \leq \gamma$. For each $n \in \mathbb{N}$ we set $G_n = \mathbb{Z}/n\mathbb{Z}$, and the homomorphism

$$\phi_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \quad \frac{a}{n} \mapsto \frac{n}{m} \cdot \frac{a}{n} = \frac{a}{m}$$

satisfies the requirements.

The inverse limit of this inverse system is then denoted by $\hat{\mathbb{Z}}$ and is also called the set of *profinite integers*. It occurs in field extensions as the Galois group of the maximal constant extension of a function field over a finite field $\mathbb{F}_q$, since for each positive integer n there exists a constant field extension of degree n, which gives a Galois group of $\mathbb{Z}/n\mathbb{Z}$. Running over all these constant extensions then gives a Galois group of $\hat{\mathbb{Z}}$.

Proposition 1.57. *Let L/K be a possibly infinite Galois extension of fields. The Galois groups of finite Galois subextensions of L/K together with the canonical surjective homomorphisms $\phi_{MN} : \mathrm{Gal}(M/K) \to \mathrm{Gal}(N/K)$ whenever M/N is a Galois extension form an inverse system. Their inverse limit is isomorphic to $\mathrm{Gal}(L/K)$, which means $\mathrm{Gal}(L/K)$ is a profinite group.*

We endow profinite groups with a natural topology as follows. If G is the inverse limit of a system of finite groups $(G_\alpha, \phi_{\alpha\beta})$ then give the groups G_α the discrete topology, and their product the product topology. We can then give $G \subseteq \prod G_\alpha$ the subspace topology and see that the natural projection maps $G \to G_\alpha$ are continuous. Moreover, their kernels form a basis of open neighbourhoods of 1 in G.

Proposition 1.58. *Let $(G_\alpha, \phi_{\alpha\beta})$ be an inverse system of groups equipped with the discrete topology. Then the inverse limit G is a closed topological subgroup of the product $\prod G_\alpha$.*

Theorem 1.59 (Main theorem for infinite Galois theory)**.** *Let M be a subextension of the Galois group L/K. Then $\mathrm{Gal}(L/M)$ is a closed subgroup of $\mathrm{Gal}(L/K)$ and the maps*

$$M \mapsto H = \mathrm{Gal}(L/M) \qquad H \mapsto M = L^H$$

yield an inclusion-reversing bijection between subfields $K \subseteq M \subseteq L$ and closed subgroups $H \subseteq G$. A subextension M/K is Galois if and only if $\mathrm{Gal}(L/M)$ is normal in $\mathrm{Gal}(L/K)$. In that case there is a natural isomorphism $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$.

1.4 Equivalence between curves and function fields

The following section is based on Chapter 4 of [Sza09]. All proofs and more background information can be found there. The goal of this section is to state an anti-equivalence of categories between a certain set of curves and algebraic function fields. This result allows us to transfer between the terms "field with many rational places" and "curves with many rational points" whenever we want. Since a large part of the literature is written in terms of algebraic varieties and schemes, it is important to see that these are essentially the same objects. As we want to use this equivalence for a finite field k, we cannot use the definitions of affine and projective curves as zero sets of polynomials. In [Har13] they cover the same material for algebraically closed field, which is where we refer the reader who would like some more intuition behind the correspondence that we will set up now.

Definition 1.60. Let X be a topological space. A *presheaf* of rings $\mathcal{F}$ on X is a rule that associates with each non-empty open subset $U \subseteq X$ a ring $\mathcal{F}(U)$ an each inclusion of open sets $V \subseteq U$ a homomorphism $\rho_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$. Here the maps ρ_{UU} are the identity maps and $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$ whenever $W \subseteq V \subseteq U$. The elements of $\mathcal{F}(U)$ are called the *sections* of $\mathcal{F}$ over U.

Definition 1.61. A morphism of presheaves $\Phi : \mathcal{F} \to \mathcal{G}$ is a collection of homomorphisms $\Phi_U : \mathcal{F}(U) \to \mathcal{G}(U)$ such that for each inclusion $V \subseteq U$ the following diagram commutes.

$$\begin{array}{ccc} \mathcal{F}(V) & \xrightarrow{\Phi_V} & \mathcal{G}(V) \\ \downarrow{\scriptstyle \rho^{\mathcal{F}}_{UV}} & & \downarrow{\scriptstyle \rho^{\mathcal{G}}_{UV}} \\ \mathcal{F}(U) & \xrightarrow{\Phi_U} & \mathcal{G}(U) \end{array}$$

Definition 1.62. A presheaf $\mathcal{F}$ is a *sheaf* if for any non-empty open set U and covering $\{U_i \mid i \in I\}$ by non-empty open sets, it satisfies the following two axioms.

1. If two sections $s, t \in \mathcal{F}(U)$ satisfy $s|_{U_i} = t|_{U_i}$ for all $i \in I$, then $s = t$;
2. Given a system of sections $\{s_i \in \mathcal{F}(U_i) \mid i \in I\}$ such that $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$ whenever $U_i \cap U_j \neq \emptyset$, then there exists a unique section $s \in \mathcal{F}(U)$ such that $s|_{U_i} = s_i$ for all $i \in I$.

A morphism of sheaves is just a morphism of presheaves.

Definition 1.63. A *ringed space* is a pair $(X, \mathcal{F})$ in which X is a topological space, and $\mathcal{F}$ is a sheaf of rings on X.

We can now define an integral affine curve over an arbitrary field k. Let A be a finitely generated integral domain of transcendence degree 1 over k. By Noether's normalization lemma, in such an integral domain, every prime ideal is maximal. We associate to such an integral domain A a topological space X as follows. As a set, X is the set of prime ideals of A. The open subsets are X itself and those that do not contain a given ideal $I \subset A$. All non-empty open subsets contain the prime ideal (0), which is called the generic point of X. The other points of X come from maximal ideals and are closed as one point subsets, which is why we call them closed points. We see that the open subsets in X are exactly the subsets whose complement is a finite set of closed points.

Definition 1.64. For a point $P \in X$ we define the *local ring* $\mathcal{O}_{X,P}$ as the localization of A at P, denoted by A_P. Note that we have $\mathcal{O}_{X,(0)} = K(X)$, the field of fractions of A which we call the function field of X. For an open subset $U \subseteq X$ we define

$$\mathcal{O}_X(U) = \bigcap_{P \in U} \mathcal{O}_{X,P}.$$

Proposition 1.65. *The above construction defines a sheaf of rings on X. Moreover, we have that $A = \mathcal{O}_X(X)$.*

Definition 1.66. We define an *integral affine curve* over k to be a ringed space $(X, \mathcal{O}_X)$ defined above. We write $X = \mathrm{Spec}(A)$ to say that X is the curve defined by the set A.

Definition 1.67. A morphism $(Y, \mathcal{G}) \to (X, \mathcal{F})$ of ringed spaces is a pair $(\phi, \phi^{\#})$ with $\phi : Y \to X$ a continuous map and $\phi^{\#} : \mathcal{F} \to \phi_* \mathcal{G}$ a morphism of sheaves. $\phi_* \mathcal{G}$ is the sheaf on X defined by $\phi_* \mathcal{G}(U) = \mathcal{G}(\phi^{-1}(U))$ for all open $U \subseteq X$.

Proposition 1.68. *Let $X = \mathrm{Spec}(A)$, $Y = \mathrm{Spec}(B)$ be two affine curves. Then any morphism $\phi : X \to Y$ induces a ring homomorphism $\phi^{\#}_X : A \to B$ given by $\mathcal{O}(X) \to (\phi_* \mathcal{O}_Y(X)) = \mathcal{O}(Y)$. Moreover, for every homomorphism $\rho : A \to B$ there exists a unique morphism $\mathrm{Spec}(\rho) : Y \to X$ such that $(\mathrm{Spec}(\rho))^{\#}_X : \mathcal{O}(X) \to \mathcal{O}(Y)$ equals ρ.*

Proposition 1.69. *The following maps induce mutually inverse contravariant functors between the category of finitely generated integral domains of transcendence degree one over a field k, and that of integral affine curves over k.*

$$A \mapsto \mathrm{Spec}(A),\ \rho \mapsto \mathrm{Spec}(\rho) \text{ and } X \mapsto \mathcal{O}(X),\ \phi \mapsto \phi_X^{\#}.$$

Definition 1.70. An integral affine curve X is called *normal* if all its local rings are integrally closed.

Definition 1.71. Let $\phi : Y \to X$ be a morphism of integral affine curves. We say ϕ is *finite* if $\mathcal{O}(Y)$ becomes a finitely generated $\mathcal{O}(X)$-module via the map $\phi_X^{\#}$.

Note that a finite morphism is always surjective. Therefore, if $\phi : Y \to X$ is a finite morphism of integral affine curves, then we see that there is a corresponding injective homomorphism $\mathcal{O}(Y) \to \mathcal{O}(X)$. This gives an inclusion $\phi^* : K(X) \to K(Y)$. We can now state the first result of this subsection.

Theorem 1.72. *Let X be an integral normal affine curve. Then the rule $Y \to K(Y)$, $\phi \mapsto \phi^*$ induces an anti-equivalence between the category of normal integral affine curves with finite morphisms $\phi : Y \to X$ and that of finite field extensions of the function field $K(X)$.*

We would like to find such an anti-equivalence for all algebraic function fields of degree 1, rather than just those for which an affine curve exists that has that field as its function field. We will therefore define a larger set of curves, whose function fields are in fact all global function fields. This will tell us that for every algebraic function field, there is at least one curve that has that field as its function field. This will later enable us to transfer all of our records for function fields with many rational places immediately to the context of curves, which means that they can be uploaded on `manypoints.org`.

Definition 1.73. Let k be a field and K/k be a finitely generated field extension of transcendence degree 1. Let X^K be the set of discrete valuation rings with fraction field K containing k. We endow X^K with the topology in which the proper closed subsets are all finite sets. We define a sheaf of rings on X^K by $\mathcal{O}^K(U) = \cap_{P \in U} P$ for any open subset $U \subseteq X^K$. Then $(X^K, \mathcal{O}^K)$ is a ringed space, and we call it an *integral proper normal curve* over k with function field K.

It can be shown that proper normal curves come from projective curves in the same way that affine open subsets come from affine curves (see [Sza09, Remark 4.4.4]).

Proposition 1.74. *We call an open subset U of an integral proper curve affine if $\mathcal{O}^K(U)$ is a finitely generated k-algebra. The category of integral affine normal curves is equivalent to that of affine open subsets of integral proper normal curves.*

Definition 1.75. A morphism $\phi : Y \to X$ of proper normal curves is *finite* if for all affine open subsets $U \subseteq X$ the preimage $\phi^{-1}(U) \subseteq Y$ is affine and moreover $\phi_* \mathcal{O}(U)$ is a finitely generated $\mathcal{O}(U)$-module.

Proposition 1.76. *A morphism of proper normal curves is surjective if and only if it is finite.*

We can now state the equivalence that we have been looking for.

Theorem 1.77. *The map that sends an integral proper normal curve over k to its function field induces an anti-equivalence between the category of integral proper normal curves with finite surjective morphisms, and that of finitely generated field extensions of k having transcendence degree 1.*

The above theorem tells us that for every finitely generated field extension of k of transcendence degree 1 (so for every algebraic function field) there exists a unique integral proper normal curve over k that has that field as its function field. As integral proper normal curves can be seen as projective curves (see for example [Har13, Proposition II.6.7]), we can thus always find a projective curve that has our desired function field. Moreover, we have seen that the points of a normal integral proper curve are the discrete valuation rings with fraction field K containing k.

Theorem 1.78. *Let X be a proper normal curve and K be its function field. Then the anti-equivalence of categories induces a one-to-one correspondence between the k-rational points of X and the rational places of K.*

Proof. See [Sti09, B.12] □

From this theorem we see that talking about curves with many rational points is indeed equivalent to talking about function fields with many rational places. The main benefit of function fields is that we do not have to consider smoothness; for example, every hyperelliptic function field corresponds uniquely to a proper normal curve, which in fact corresponds again to a smooth projective hyperelliptic curve. For more information on hyperelliptic curves, see [Liu02, Chapter 7.4.3].

1.5 Completions, local fields and adèles

Now that we have defined algebraic function fields and looked at their properties in field extensions, it is time to introduce another type of field. Algebraic function fields will be the main player of this thesis, and together with algebraic number fields, they form the category of global fields. There is another category of fields, which is (not surprisingly) called local fields. When discussing class field theory in Chapter 4, we will see that we need to know a bit about local fields before we can look into global class field theory. We therefore quickly introduce the terminology of local fields here, which will help us a lot when looking into local and global class field theory. This section is based on [Ser13], all proofs and more background information can be found there.

We start with a valued field (K, v) where we do not request any properties of K. First, we will define an extension of K which we call its completion. The motivation for this extension is the following.

Definition 1.79. We say that for elements $x_i \in K$ the sequence $x_1, x_2, ...$ is *convergent* with respect to the valuation v if there exists an element $x \in K$ such that for any $N \in \mathbb{N}$ there exists an integer n_0 such that $v(x_n - x) > N$ for all $n \geq n_0$.
We say that a sequence $x_1, x_2, ...$ is *Cauchy* if for any $N \in \mathbb{N}$ there exists an integer n_0 such that $v(x_n - x_m) > N$ whenever $n, m \geq n_0$.

Any convergent sequence is Cauchy, but not every Cauchy sequence is convergent. This motivates the following definition.

Definition 1.80. A valued field (K, v) is called *complete* if any Cauchy sequence of elements of K is convergent with respect to the valuation v.

When the field we work with is not yet complete, which is the case for the global fields we will consider, we can create a unique field extension that is complete.

Definition 1.81. Let (K, v_K) be a valued field. A *completion* of K is a field extension K' with a discrete valuation $v_{K'}$ such that:

1. v_K is the restriction of $v_{K'}$ to K;
2. K' is complete with respect to $v_{K'}$.

Proposition 1.82. *For any valued field (K, v) there exists a completion (K', v') and it is unique up to isomorphism. Moreover, if (K, v) is a complete valued field, then v has a unique extension to any algebraic extension field L/K and there exists an integer e such that $v'(x) = e \cdot v(x)$ for all $x \in K$.*

Proposition 1.83. *Let (K, v) be a valued field, and let $\hat{K}$ be its completion with respect to v. Then K lies dense in $\hat{K}$.*

Proposition 1.84. *If K is a complete field and L/K is a finite extension, then L is a complete field with the extended valuation.*

Definition 1.85. We say that a field K is a *local field* if it is complete and its residue field $\mathcal{O}_K/\mathfrak{p}_K$ is finite.

Proposition 1.86. *There are three types of local fields.*

1. *Both $\mathbb{R}$ and $\mathbb{C}$ are local fields, as they are complete with respect to the Euclidean valuation. These are the Archimedian local fields.*
2. *Let p be a prime number and denote by v_p the valuation on the integers such that $v_p(x) = n$ if $p^n | x$, $p^{n-1} \nmid x$. We can extend this valuation to $\mathbb{Q}$ by setting $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$. The completion of $\mathbb{Q}$ with respect to this valuation is denoted by $\mathbb{Q}_p$ and this field is called the field of p-adic numbers. Any finite extension of a field of p-adic numbers is a local field. These are the non-Archimedean local fields of characteristic zero.*
3. *Let $k = \mathbb{F}_p$ be a finite field of prime cardinality and let $K = \mathbb{F}_p(t)$ be a rational function field. Then the completion of K with respect to one of the places of K is of the form $\mathbb{F}_p((t))$, which is its formal Laurent series. Any finite extension of a field of the form $\mathbb{F}_p((t))$ is a local field. These are the non-Archimedean local field of positive characteristic.*

The following theorem tells us why we are interested in local fields.

Theorem 1.87. *Let k be finite field, let K be a global function field over k, and v a discrete valuation of K with maximal ideal $\mathfrak{p}$. Then the completion of K with respect to the valuation $v_\mathfrak{p}$ is a local field, which we denote by $K_\mathfrak{p}$. It is a finite extension of a formal Laurent series of the form $\mathbb{F}_q((t))$.*

Proof. See [Lor07, Chapter 25, Theorem 2]. □

Proposition 1.88. *Let K a global field, and $\mathfrak{p}$ a place of K. Let L/K an abelian extension, and denote by $\mathfrak{q}$ a place of L above $\mathfrak{p}$. Then the Galois group of $L_\mathfrak{q}/K_\mathfrak{p}$ is exactly the decomposition group $G_Z(\mathfrak{q}|\mathfrak{p})$.*

Proof. We start by noting that for any $\sigma \in \mathrm{Gal}(L/K)$ and any element $x \in L^*$ we have that $v_{\mathfrak{q}}(x) = v_{\sigma(\mathfrak{q})}(\sigma(x))$ (see [Sti09, Lemma 3.5.2]). Therefore σ induces an isomorphism from $L_{\mathfrak{q}}$ to $L_{\sigma(\mathfrak{q})}$. Whenever $\sigma \in G_Z(\mathfrak{q}|\mathfrak{p})$ we know that $\sigma(\mathfrak{q}) = \mathfrak{q}$ and σ thus induces an automorphism $\sigma_{\mathfrak{q}}$ of $L_{\mathfrak{q}}$. Moreover, $\sigma_{\mathfrak{q}}$ is the identity on K, and therefore also on $K_{\mathfrak{p}}$ (as K lies dense in $K_{\mathfrak{p}}$). We thus see that $\sigma_{\mathfrak{q}} \in \mathrm{Aut}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$. This means that there exists a group homomorphism $\eta : G_Z(\mathfrak{q}|\mathfrak{p}) \to \mathrm{Aut}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ and we see that this map is injective.

All that is left to prove now is that η is surjective. We do so by showing that $|G_Z(\mathfrak{q}|\mathfrak{p})| = |\mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})|$. Set $r = [\mathrm{Gal}(L/K) : G_Z(\mathfrak{q}|\mathfrak{p})]$; then we know that there are exactly r places of L that lie above $\mathfrak{p}$. We denote them by $\mathfrak{q}_1, ..., \mathfrak{q}_r$. Then we have that

$$|\mathrm{Gal}(L/K)| = r \cdot |G_Z(\mathfrak{q}|\mathfrak{p})| = \sum_{i=1}^{r} |G_Z(\mathfrak{q}_i|\mathfrak{p})| \leq \sum_{i=1}^{r} [L_{\mathfrak{q}_i} : K_{\mathfrak{p}}] = [L : K] = |\mathrm{Gal}(L/K)|.$$

We see that $|G_Z(\mathfrak{q}_i|\mathfrak{p})| = [L_{\mathfrak{q}_i} : K_{\mathfrak{p}}]$ and thus that the above map is indeed an isomorphism. □

Corollary 1.89. *Let L/K be an abelian extension of function fields. Let $\mathfrak{p}$ be a place of K and let $\mathfrak{q}$ be a place of L lying above $\mathfrak{p}$. Then $L_{\mathfrak{q}}/K_{\mathfrak{p}}$ has cyclic Galois group.*

One of the great benefits of local fields is that they have only one prime ideal. Studying a local field then gives us a lot of information about this prime ideal. When studying extensions of global fields in Chapter 4, it will therefore be very useful to look at the behaviour of each place individually. We can do that by studying the following object.

Definition 1.90. We define the *adèle ring* to be

$$A_K = \{(a_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p} \in \mathbb{P}_K} K_{\mathfrak{p}} \mid v_{\mathfrak{p}}(a_{\mathfrak{p}}) \geq 0 \text{ for all but finitely many } \mathfrak{p} \in \mathbb{P}_K\}.$$

The units of the adèle ring are the *idèles*, defined as

$$J_K = \{(a_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p} \in \mathbb{P}_K} K_{\mathfrak{p}} \mid v_{\mathfrak{p}}(a_{\mathfrak{p}}) = 0 \text{ for all but finitely many } \mathfrak{p} \in \mathbb{P}_K\}.$$

As each element $a \in K$ has $v_{\mathfrak{p}}(a) = 0$ for all but finitely many $\mathfrak{p}$, we see that K can be viewed as a subring of J_K embedded diagonally. The idèles corresponding to elements of K are called the *principal idèles*. Therefore, the following object is well-defined.

Definition 1.91. Let K be an algebraic function field, and J_K its ring of idèles. Then we define $C_K = J_K/K$ to be the *idèle class group*.

This idèle class group will be one of the main objects throughout this thesis. We will see in Chapter 4 that there exists an injective homomorphism from the idèle class group to the Galois group of the maximal abelian extension of a function field K. This homomorphism, together with a relation between the divisor class group and the idèle class group, will be the foundation of the algorithm that we use in Chapter 5.

2 Unramified Extensions

In this chapter, we will construct an algorithm that finds many new records using unramified extensions. We will first look at some upper bounds on the maximal number of rational places, as we wish to come as close to those upper bounds as possible. We will then create a map that sends each divisor to an element of the Galois group. When we restrict this map, this gives us an isomorphism between the degree zero divisor class group and the Galois group of the maximal abelian extension in which one place splits completely. Although we can only prove this theorem in Chapter 5, we will see here how it can be used to find extension fields with many rational places.

2.1 Upper bounds on the number of rational places

In this section, we will give an overview of upper bounds that are relevant for our research. Roughly speaking, two kinds of upper bounds can be found in the literature (see [Ser20] for an extensive overview). First, there are explicit upper bounds, which give a direct relation between the genus g, the cardinality of the finite field q, and the number of rational points of a curve/rational places of a function field with those parameters, which we denote by $N_g(q)$. These are the kind of bounds that we will consider in this section. The other kind of upper bounds are those that give an asymptotic relation between g and q on the one hand, and $N_g(q)$ on the other, when g (or sometimes q) goes to infinity. Most of the time, these are denoted in terms of $A_g(q) = \frac{N_g(q)}{g}$ for $g \to \infty$. Since we are interested in curves with genus up to 50, these are not very relevant for our research, and we will focus on the explicit bounds.

We will consider three different bounds. First of all, we will look into the Hasse-Weil bound and the Serre bound, as the Serre bound is an improvement of the Hasse-Weil bound. When looking at the entries of `manypoints.org`, we see that this bound is very effective when looking at entries where g is small, up to about half the size of q. After a description of this bound, we will continue with the Ihara bound. This bound is very effective when the genus is roughly equal to the size of the finite field, say $\frac{1}{2}q \leq g \leq 2q$. Lastly, we treat the Oesterlé bound, which is most effective when the genus is larger than the size of the finite field. Together, these three bounds account for the majority of the upper bounds for finite fields of prime cardinality 3-13, which is our playing field. All proofs and more background information, as well as other bounds, can be found in [Ser20] and [Voi05].

We start with the Hasse-Weil bound, perhaps the most famous of these bounds.

Theorem 2.1 (Hasse-Weil bound)**.** *Let K be a function field over $\mathbb{F}_q$ with genus g. Denote by $N_g(q)$ the number of rational places of K. Then we have the following bound:*

$$|N_g(q) - (q+1)| \leq 2gq^{1/2}.$$

This bound gives both an upper and a lower bound for the number of rational places of a function field. We see that when g and q get larger, the range in which the maximum number of places can lie grows quite fast, especially when g grows. This is why this bound is most effective when g is small in terms of q.
The following, slightly improved, version of this bound is due to Serre [Ser83].

Theorem 2.2 (Serre's bound)**.** *Let K be a function field over $\mathbb{F}_q$ with genus g. Denote by $N_g(q)$ the number of rational places of K. Then we have the following bound:*

$$|N_g(q) - (q+1)| \leq 2\lfloor gq^{1/2} \rfloor.$$

We see that in practice this can decrease the upper bound of $N_g(q)$ by one rational place. Although that might not seem revolutionary, for low genera and small finite fields many of the gaps between the highest number of rational places found and the lowest theoretical bound are only one or two places. Moreover, this bound (denoted by Hasse-Weil-Serre on `manypoints.org`) is the best bound found yet for many combinations of g and q. For larger primes, say $p > 30$, this bound is actually responsible for almost all upper bounds known for $g \leq \frac{q}{2}$ over $\mathbb{F}_p$.

The next bound that we will consider is the Ihara bound, first published in [Iha82].

Theorem 2.3 (Ihara bound)**.** *Let K be a function field over $\mathbb{F}_q$ with genus g. Denote by $N_g(q)$ the number of rational places of K. Then we have the following bound:*

$$N_g(q) \leq \frac{1}{2}\sqrt{(8q+1)g^2 + (4q^2-4q)g} - (g - 2q - 2).$$

Proposition 2.4. *The Ihara bound is stronger than the Hasse-Weil upper bound when*

$$g > \frac{\sqrt{q}(\sqrt{q}-1)}{2}.$$

Proof. We see that the Ihara bound is stronger than the Hasse-Weil upper bound whenever

$$2gq^{1/2} + q + 1 > \frac{1}{2}\sqrt{(8q+1)g^2 + (4q^2-4q)g} - (g - 2q - 2)$$

Squaring on both sides and using some algebra gives us the following inequalities

$$\begin{aligned}
g^2(4q^{1/2}+1)^2 &> (8q+1)g^2 + (4q^2-4q)g \ ; \\
g((4q^{1/2}+1)^2 - 8q - 1) &> (4q^2-4q) \ ; \\
g &> \frac{4q^2-4q}{(4q^{1/2}+1)^2 - 8q - 1} \ ; \\
g &> \frac{q^2-q}{2q+2q^{1/2}} \ ; \\
g &> \frac{\sqrt{q}(\sqrt{q}-1)}{2} \ .
\end{aligned}$$

We thus see that the Ihara bound is stronger than the Hasse-Weil upper bound whenever $g > \frac{\sqrt{q}(\sqrt{q}-1)}{2}$. □

We thus see that whenever g is about half as large as q, the Ihara bound is better than the Hasse-Weil bound. When we get to even larger genera, the Ihara bound will be superseded by the following bound. See [Ser20, p. VI.3] for more background on the Oesterlé bound.

Theorem 2.5 (Oesterlé bound)**.** *Let K be a function field of genus g over $\mathbb{F}_q$ with $N+1$ rational places. Let m be the integer such that $\sqrt{q}^m < N \leq \sqrt{q}^{m+1}$ and let*

$$u = \frac{\sqrt{q}^{m+1} - N}{N\sqrt{q} - \sqrt{q}^m} \in [0, 1).$$

Denote by θ_0 the unique solution in $[\frac{\pi}{m+1}, \frac{\pi}{m})$ of

$$\cos\left(\frac{m+1}{2}\theta_0\right) + u\cos\left(\frac{m-1}{2}\theta_0\right) = 0.$$

Then

$$g \geq \frac{(N-1)\sqrt{q}\cos(\theta_0) + q - N}{q+1-2\sqrt{2}\cos(\theta_0)}.$$

This bound gives us a minimum value for the genus whenever a curve has at least a certain amount of rational places. This way, we can also deduce a maximum number of rational places for each pair (g, q). In practice, not many function fields have been found that reach this bound, but it is still the best generally applicable upper bound whenever $g \geq 2q$.

2.2 The Artin map

In this section, we will construct a map from the group of divisors of a global function field K to the Galois group of a finite abelian unramified extension L/K. This map will eventually induce an isomorphism between the degree zero part of the class group and the Galois group of the maximal unramified extension of K in which one rational place splits completely over K. It is this isomorphism that we will use to create extensions with many rational places.

Let L/K be a finite Galois extension of global function fields. Let $\mathfrak{p}$ be a place of K that does not ramify in L, i.e. $\mathfrak{p}$ has decomposition $\mathfrak{p} = \mathfrak{q}_1 \cdot ... \cdot \mathfrak{q}_r$. Recall from Definition 1.52 that the decomposition group of $\mathfrak{q}_i$ is the stabilizer group of $\mathfrak{q}_i$, i.e.

$$G_Z(\mathfrak{q}_i|\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{q}_i) = \mathfrak{q}_i\}.$$

Lemma 2.6. *Let L/K be a finite Galois extension of global function fields. The decomposition group of an unramified place is a cyclic group.*

Proof. We know from Theorem 1.53.3 that $\mathrm{Gal}(\widetilde{K}'_{\mathfrak{q}}/\widetilde{K}_{\mathfrak{p}}) \cong G_Z(\mathfrak{q}|\mathfrak{p})/G_T(\mathfrak{q}|\mathfrak{p})$. For unramified places, we have that $G_T(\mathfrak{q}|\mathfrak{p}) = \{\mathrm{id}\}$ and thus that $\mathrm{Gal}(\widetilde{K}'_{\mathfrak{q}}/\widetilde{K}_{\mathfrak{p}}) \cong G_Z(\mathfrak{q}|\mathfrak{p})$. Since $\widetilde{K}'_{\mathfrak{q}}/\widetilde{K}_{\mathfrak{p}}$ is a finite extension of finite fields, it has a cyclic Galois group, which means $G_Z(\mathfrak{q}|\mathfrak{p})$ is cyclic. □

Lemma 2.6 tells us that the decomposition group is cyclic, and therefore has a well-defined generator. This allows us to define the following.

Definition 2.7. Let L/K be a finite Galois extension of global function fields, and let $\mathfrak{q}_i$ be a place of L that lies above an unramified place $\mathfrak{p}$ of K. Choose a generator of the decomposition group $D(\mathfrak{q}_i)$ and denote this by $(\frac{L|K}{\mathfrak{q}_i})$. We call this the *Artin symbol* of $\mathfrak{q}_i$ in L/K.

It turns out that we can simplify this definition when we are considering only abelian extensions.

Proposition 2.8. *Let L/K be a finite Galois extension and let $\mathfrak{p}$ be an unramified place of K. Then the Artin symbols of all places $\mathfrak{q}_i$ above $\mathfrak{p}$ are conjugate. Moreover, when L/K is abelian, the Artin symbols are all equal and we can define the Artin symbol of a place $\mathfrak{p}$ of K, which is denoted by $(\frac{L|K}{\mathfrak{p}})$.*

Proof. Let $\mathfrak{q}_i, \mathfrak{q}_j$ be two distinct places of L above $\mathfrak{p}$. Since the Galois group acts transitively on the places above $\mathfrak{p}$, there always exists a permutation $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{q}_i) = \mathfrak{q}_j$. Now for any $\tau \in \mathrm{Gal}(L/K)$ we have that

$$\tau(\sigma(\mathfrak{q}_i)) = \sigma(\mathfrak{q}_i) \iff (\tau\sigma - \sigma)\mathfrak{q}_i = 0 \iff (\sigma^{-1}\tau\sigma - id)\mathfrak{q}_i = 0$$

and therefore that $\tau \in D(\mathfrak{q}_j) = D(\sigma(\mathfrak{q}_i))$ if and only if $\tau \in \sigma D(\mathfrak{q}_i)\sigma^{-1}$. □

This enables us to create a map from the group of divisors to the Galois group of an abelian extension.

Definition 2.9. Let L/K be a finite unramified abelian extension of global function fields. The Artin symbol induces a map from the divisor group of K to the Galois group of L/K as follows. Let $\mathrm{Div}(K)$ be the divisor group of L/K. Then the Artin map can be defined as:

$$\left(\frac{L|K}{\cdot}\right) : \mathrm{Div}(K) \to \mathrm{Gal}(L/K);$$
$$\sum_{\mathfrak{p}\in\mathbb{P}_K} n_{\mathfrak{p}}\mathfrak{p} \mapsto \prod_{\mathfrak{p}\in\mathbb{P}_K} \left(\frac{L|K}{\mathfrak{p}}\right)^{n_{\mathfrak{p}}}.$$

which is well-defined because the support of any divisor is finite.

We will now show that this Artin map is surjective for every finite abelian extension of global function fields L/K.

Proposition 2.10. *Let L/K be a finite abelian unramified extension of global function fields. Then for any place $\mathfrak{p} \in \mathbb{P}_K$ we have that $\left(\frac{L|K}{\mathfrak{p}}\right) = 1$ if and only if $\mathfrak{p}$ splits completely in L.*

Proof. Let $\mathfrak{p}$ be a place of K that splits completely in L. Then we see that none of the non-trivial elements of the Galois group send a place $\mathfrak{q}_i \in \mathbb{P}_L$ to itself, as there are exactly as many elements in the Galois group as there are places above $\mathfrak{p}$ and the Galois group acts transitively. This means that the decomposition group of the places $\mathfrak{q}_i$ above $\mathfrak{p}$ consist only of the identity element. As the Artin symbol is the generator of the decomposition group, a place that splits completely is sent to the identity element by the Artin map.

On the other hand, if the Artin map sends a place to the identity element, that means that the decomposition group of that place consists only of the identity element. Proposition 2.8 tells us that the Artin symbol of all places $\mathfrak{q}_i$ above $\mathfrak{p}$ are equal. Therefore, by definition of the decomposition group, this means that no non-trivial element of the Galois group sends the places above $\mathfrak{p}$ to themselves. Therefore there must be $|\mathrm{Gal}(L/K)| = |L : K|$ places above $\mathfrak{p}$, which implies that $\mathfrak{p}$ splits completely in L. □

In order to show that the Artin map is surjective, we need an auxiliary lemma that is a corollary of Chebotarev's density theorem. We will first state this theorem.

Theorem 2.11 (Chebotarev's density Theorem)**.** *Let L/K be a finite Galois extension of function fields, and let $G = \mathrm{Gal}(L/K)$. Let C be a conjugacy class in G and denote by*

S_K the set of places in K which are unramified in L. Denote by $|\widetilde{K}_\mathfrak{p}|$ the cardinality of the residue class field of K at $\mathfrak{p}$. We define the Dirichlet density of a subset M of S_K to be

$$\delta(M) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in M} |\widetilde{K}_\mathfrak{p}|^{-s}}{\sum_{\mathfrak{p} \in S_K} |\widetilde{K}_\mathfrak{p}|^{-s}}.$$

Then we have that

$$\delta\left(\{\mathfrak{p} \in S_K \mid \left(\frac{L|K}{\mathfrak{p}}\right) \in C\}\right) = \frac{\#C}{\#G}.$$

Proof. See [Ros02, Theorem 9.13 A]. □

The auxiliary lemma is the following.

Lemma 2.12. *Let L/K be a finite abelian extension. If all places $\mathfrak{p} \in \mathbb{P}_K$ split completely in L then $K = L$.*

Proof. We see that if all places $\mathfrak{p} \in \mathbb{P}_K$ split completely in L then we have that the Artin symbol of every place $\mathfrak{p} \in \mathbb{P}_K$ is equal to the identity. This means that

$$\frac{1}{\#G} = \delta\left(\{\mathfrak{p} \in S_K \mid \left(\frac{L|K}{\mathfrak{p}}\right) \in \{\mathrm{id}\}\}\right) = 1$$

from which it follows that $G = \{\mathrm{id}\}$ and thus that $L = K$. □

Theorem 2.13. *Let L/K be a finite abelian extension of function fields. Then the Artin map is surjective.*

Proof. Let H be the image of the Artin map, and let F be the fixed field of L by H. Then it suffices to show that $F = K$ in order to prove that the Artin map is surjective.

Let $D \in \mathrm{Div}(K)$. Then since F is the fixed field of H, we see that $\left(\frac{F|K}{D}\right) = 1$. In particular, if we take D to be a divisor consisting of one place $\mathfrak{p}$, then we see by Proposition 2.10 that this is possible if and only if $\mathfrak{p}$ splits completely. Thus we see that all divisors consisting of one place in $\mathrm{Div}(K)$ split completely in F. Therefore by Lemma 2.12 we see that this implies that $[F : K] = 1$ and thus our result is proven. □

Let us look at how we can use the Artin map to create unramified field extensions with many rational places.

Proposition 2.14. *Let K be a global function field and let L/K be an unramified finite purely geometric abelian extension. Then any rational place in L lies above a place of K that is also rational. Moreover, a rational place $\mathfrak{p}$ of K only has rational places lying above it, if $\mathfrak{p}$ splits completely in L.*

Proof. Let L/K be a finite unramified abelian extension, let $\mathfrak{p}$ be a place of K and let $\mathfrak{q}_1, ..\mathfrak{q}_m$ be the places lying above $\mathfrak{p}$. Then we know from Theorem 1.35 that we have

$$\sum_{i=1}^{m} e(\mathfrak{q}_i|\mathfrak{p}) \cdot f(\mathfrak{q}_i|\mathfrak{p}) = [L : K].$$

Now since L/K is Galois, we see that the ramification and inertia indices of all places $\mathfrak{q}_i$ above a place $\mathfrak{p}$ are equal, so we have $e(\mathfrak{q}_i|\mathfrak{p}) = e(\mathfrak{p}), f(\mathfrak{q}_i|\mathfrak{p}) = f(\mathfrak{p})$. Since L/K is unramified

we know that $e(\mathfrak{p}) = 1$, which means that $m \cdot f(\mathfrak{p}) = [L : K]$. Now, by definition we have that

$$f(\mathfrak{p}) = [\widetilde{L}_{\mathfrak{q}_i} : \widetilde{K}_{\mathfrak{p}}] = \frac{\deg(\mathfrak{q}_i)}{\deg(\mathfrak{p})} \cdot [k' : k]$$

where k' is the constant field of L. Now, as L/K is a purely geometric extension, we see that $[k' :' k] = 1$ and thus that $f(\mathfrak{p}) \cdot \deg(\mathfrak{p}) = \deg(\mathfrak{q}_i)$. From this it follows that $\deg(\mathfrak{q}_i) = 1$ if and only if both $f(\mathfrak{p}) = 1$ and $\deg(\mathfrak{p}) = 1$, which concludes our proof. □

We see from Proposition 2.14 that the only way to create unramified field extensions with many rational places, is to make sure that many of the rational places of the ground field split completely. We will therefore look into a special kind of field extensions, namely those in which at least one rational place splits completely. We will need the following definition.

Definition 2.15. Let K be a global function field, and let $\mathfrak{o}$ be a rational place of K. Then we denote by $K^{\mathfrak{o}}$ the maximal unramified extension of K such that the rational place $\mathfrak{o}$ splits completely.

Proposition 2.16. *The field extension $K^{\mathfrak{o}}/K$ is a completely geometric extension.*

Proof. When we demand that a rational place $\mathfrak{o}$ splits completely in an extension L/K, we see that this means that $f(\mathfrak{o}_i|\mathfrak{o}) = 1$ for all places $\mathfrak{o}_i$ lying above $\mathfrak{o}$. Moreover, Theorem 1.35 tells us that

$$f(\mathfrak{q}_i|\mathfrak{p}) = \frac{\deg(\mathfrak{q}_i)}{\deg(\mathfrak{p})} \cdot [k' : k]$$

where k' is the constant field of L. When $\deg(\mathfrak{p}) = 1$, that means that $f(\mathfrak{q}_i|\mathfrak{p}) = \deg(\mathfrak{q}_i) \cdot [k' : k]$. Now since we require $\mathfrak{o}$ to split completely, that means $f(\mathfrak{o}_i|\mathfrak{o}) = 1$ in the extension $K^{\mathfrak{o}}/K$. Therefore, we see that there is no constant field extension, and $K^{\mathfrak{o}}/K$ is thus a fully geometric extension. □

We will now define the Artin map on the degree zero divisor class. Fix a place of degree one in K, call that place $\mathfrak{o}$. Then we see that every divisor of degree 0 can be written as the sum of divisors of the form $\mathfrak{p} - \deg(\mathfrak{p})\mathfrak{o}$. We thus see that those divisors form a basis of the group Cl_K^0.

Theorem 2.17. *Let K be a global function field. Then the map $\varphi_{\mathfrak{o}}$ sending*

$$\mathrm{Cl}_K^0 \to \mathrm{Gal}(K^{\mathfrak{o}}/K), \quad [\mathfrak{p} - \deg(\mathfrak{p})\mathfrak{o}] \mapsto \left(\frac{K^{\mathfrak{o}}|K}{\mathfrak{p}}\right)$$

is an isomorphism.

Let us try to create some intuition behind this map, as this map will be the foundation of our algorithm. First of all, we see that the domain of this map is Cl_K^0 instead of $\mathrm{Div}(K)$. We can go from $\mathrm{Div}(K)$ to $\mathrm{Div}^0(K)$ by mapping each divisor

$$D = \sum m_{\mathfrak{p}}\mathfrak{p} \mapsto D' = \sum m_{\mathfrak{p}}\mathfrak{p} - (\sum m_{\mathfrak{p}})\mathfrak{o}.$$

This way, each divisor D is mapped to $D - \deg(D)\mathfrak{o}$. Taking the quotient with the group of principal divisors (which always have degree zero) then gives a map $\phi : \mathrm{Div}(K) \to \mathrm{Cl}_K^0$ such that if we denote the Artin map from Definition 2.9 by $\varphi_{L/K}$, we have $\varphi_{L/K} = \varphi_{\mathfrak{o}} \circ \phi$.

Recall that the Galois group of the maximal constant extension of a function field K is isomorphic to $\hat{\mathbb{Z}}$, the group of profinite integers. The Galois group of the maximal unramified abelian extension of K will then be of the form $G_0 \times \hat{\mathbb{Z}}$, where G_0 is the Galois group of the maximal geometric extension of K. The fact that $K^{\mathfrak{o}}/K$ is a purely geometric extension tells us that the Galois group of $K^{\mathfrak{o}}/K$ is a subgroup of G_0. On the other hand, we know that $\mathrm{Div}(K)/\mathbb{Z} \cong \mathrm{Div}^0(K)$, which is for example induced by the degree map. Therefore, it seems reasonable that when the image of the Artin map is the Galois group of a purely geometric extension, a quotient by $\mathbb{Z}$ can be taken on the preimage of the Artin map. In Chapter 5 , after treating cohomology and abstract class field theory, we will be able to fully prove this isomorphism. For now, let us look at how we can apply it to find unramified field extensions that have many rational places.

Recall that for an algebraic extension L/K we denote by $Z(\mathfrak{q}_i|\mathfrak{p})$ the fixed field of L under $G_Z(\mathfrak{q}_i|\mathfrak{p})$. Theorem 1.55 tells us that for any intermediate field $K \subseteq M \subseteq L$ and $\mathfrak{p}$ a place of K, we have that

$$M \subseteq Z(\mathfrak{q}_i|\mathfrak{p}) \iff \mathfrak{p} \text{ splits completely in } M/K.$$

This will be the foundation of our algorithm. We are looking for extensions with a high number of rational places, and we have seen that the only way to create rational places in extensions is to have rational places in the ground field that split completely. In our algorithm, we will thus try to find as many of those extensions as possible. In the rest of this section, we will investigate some properties of intermediate extensions $K \subseteq L \subseteq K^{\mathfrak{o}}$. The goal is to find out which requirements we need to put on those intermediate field in order for them to have many rational places.

Definition 2.18. Let K be a global function field and let $\mathfrak{o}$ be a rational place of K. Let G be a subgroup of Cl_K^0. Since Cl_K^0 is an abelian group, we see that G is a normal subgroup. Denote by $\mathcal{G}$ the corresponding subgroup under the isomorphism of Theorem 2.17 in $\mathrm{Gal}(K^{\mathfrak{o}}/K)$, which is again a normal subgroup. We denote by $(K^{\mathfrak{o}})^{\mathcal{G}}$ the intermediate extension of K consisting of those elements of $K^{\mathfrak{o}}$ that are fixed under the action of $\mathcal{G}$.

Note that the Galois group of $(K^{\mathfrak{o}})^{\mathcal{G}}/K$ is isomorphic to $\mathrm{Gal}(K^{\mathfrak{o}}/K)/\mathcal{G}$.

Proposition 2.19. *Let K be a global function field of genus g, and $\mathfrak{o}$ a rational place of K. Let G be a subgroup of Cl_K^0 of index d. Then the genus of the extension $(K^{\mathfrak{o}})^{\mathcal{G}}$ is equal to*

$$g' = d \cdot (g-1) + 1.$$

Proof. Hurwitz' genus formula 1.41 tells us that for an extension K'/K we have

$$2g' - 2 = \frac{[K' : K]}{[k' : k]}(2g-2) + \deg(\mathrm{Diff}(K'/K)).$$

Moreover, we know from Dedekind's different theorem (Theorem 1.42) that in an unramified extension (so when $e(\mathfrak{q}_i|\mathfrak{p}) = 1$ for all places $\mathfrak{p}$ of K), the degree of the different is zero. This leads to

$$g' = \frac{[(K^{\mathfrak{o}})^{\mathcal{G}} : K]}{[k' : k]}(g-1) + 1.$$

Because $K^{\mathfrak{o}}$ is a purely geometric extension, we have that $[k' : k] = 1$ and see that $\frac{[(K^{\mathfrak{o}})^{\mathcal{G}}:K]}{[k':k]}$ is equal to $[(K^{\mathfrak{o}})^{\mathcal{G}} : K]$. Now as G is a subgroup of index d in Cl_K^0, we know

that $\mathcal{G}$ has index d in $\mathrm{Gal}(K^{\mathfrak{o}}/K)$. From this, we see that $[(K^{\mathfrak{o}})^{\mathcal{G}} : K] = d$ and we get $g' = d \cdot (g-1) + 1$. □

Proposition 2.20. *A place $\mathfrak{p}$ splits completely in $(K^{\mathfrak{o}})^{\mathcal{G}}/K$ if and only if $[\mathfrak{p} - \deg(\mathfrak{p})\mathfrak{o}] \in G$.*

Proof. Assume $\mathfrak{p}$ splits completely. We know by Proposition 2.10 that a place $\mathfrak{p}$ splits completely if and only if its Artin symbol satisfies $(\frac{(K^{\mathfrak{o}})^{\mathcal{G}}|K}{\mathfrak{p}}) = \mathrm{id}$. As the Galois group of $(K^{\mathfrak{o}})^{\mathcal{G}}/K$ is equal to $\mathrm{Gal}(K^{\mathfrak{o}}/K)/\mathcal{G}$, that means that the Artin symbol of $\mathfrak{p}$ is an element of $\mathcal{G}$. Now the Artin map sends $[\mathfrak{p} - \deg(\mathfrak{p})\mathfrak{o}] \mapsto (\frac{(K^{\mathfrak{o}})^{\mathcal{G}}|K}{\mathfrak{p}})$, and if the Artin symbol of $\mathfrak{p}$ is an element of $\mathcal{G}$, we conclude that $[\mathfrak{p} - \deg(\mathfrak{p})\mathfrak{o}]$ must be an element of G. For the reverse implication we can use the same arguments. If $[\mathfrak{p} - \deg(\mathfrak{p})\mathfrak{o}] \in G$ then we know that $(\frac{(K^{\mathfrak{o}})^{\mathcal{G}}|K}{\mathfrak{p}}) \in \mathcal{G}$, which is the Galois group of $K^{\mathfrak{o}}/(K^{\mathfrak{o}})^{\mathcal{G}}$. We therefore see that $[\mathfrak{p} - \deg(\mathfrak{p})\mathfrak{o}]$ is mapped to the identity in $\mathrm{Gal}((K^{\mathfrak{o}})^{\mathcal{G}}/K)$ by the Artin map, and can use Proposition 2.10 to conclude that $\mathfrak{p}$ splits completely. □

We can use this proposition to determine the number of rational places of a field extension that is formed by taking subgroups of the degree zero class group, and then applying the Artin map.

Proposition 2.21. *Let K be a global function field of genus g, and $\mathfrak{o}$ a rational place of K. Let G be a subgroup of Cl_K^0 of index d and let $\mathcal{G}$ be the corresponding subgroup of $\mathrm{Gal}(K^{\mathfrak{o}}/K)$. Denote the set of rational places of K by $\{\mathfrak{p}_i\}$. Then the number of rational places of $(K^{\mathfrak{o}})^{\mathcal{G}}$ is equal to*

$$d \cdot |G \cap \{[\mathfrak{p}_i - \mathfrak{o}]\}|.$$

Proof. We know from Proposition 2.14 that every rational place of $(K^{\mathfrak{o}})^{\mathcal{G}}$ lies above a rational place $\mathfrak{p}$ of K. Moreover, in an unramified extension the only way a rational place in the ground field can stay rational in the extension field is if it splits completely. Proposition 2.20 tells us that a rational place $\mathfrak{p}$ of K splits completely if and only if $[\mathfrak{p} - \mathfrak{o}] \in G$. For each rational place of the ground field that splits completely, there will be $[(K^{\mathfrak{o}})^{\mathcal{G}} : K] = d$ rational places in the extension field. This concludes our proof. □

We will see in Chapter 5 that when looking at ramified extensions, both of these formulas will be a bit more complicated. This is the main reason why we treat unramified extensions first. We will now see how we can use this theory to find function fields with many rational places.

2.3 Construction of the algorithm

The goal of the algorithm we will construct in this section is to find for each genus $g' \leq 50$ and small finite field $\mathbb{F}_q$ with $5 \leq q \leq 13$ prime, a function field over $\mathbb{F}_q$ with genus g' and a high number of rational places, preferably higher than the number of rational places known on `manypoints.org`. A naive way to find these records is to create a list of all function fields over $\mathbb{F}_q$ with genus g, and then check for each of those function fields how many rational places they have. Unfortunately, in practice this is not at all feasible for multiple reasons. First of all, the number of function fields for a given genus grows exponentially with the genus, so there are way too many possible function fields for genus > 4. For example, considering only hyperelliptic function fields (which are only a small subset of all possible function fields) gives about q^{2g+1} possible function fields of a given genus g. Moreover it

takes an enormous amount of memory to store the defining equations for all those function fields. Even more important is the fact that checking the number of rational places of a function field of large genus can easily take several minutes in MAGMA [BCP97]. We are therefore looking for a way around this direct computation. This is what we will propose here.

Let K be a global function field. We have seen that the Artin map sends the degree zero part of the class group of K to the Galois group of the maximal unramified extension of K in which one fixed rational place $\mathfrak{o}$ splits completely. By taking a subgroup $\mathcal{G}$ of index d in this Galois group and looking for the subfield of $K^{\mathfrak{o}}$ that is fixed under that subgroup, we get unramified field extensions of K. By Theorem 2.17, we know that there exists a subgroup G of the degree zero class group such that $\mathrm{Cl}_K^0/G \cong \mathrm{Gal}((K^{\mathfrak{o}})^{\mathcal{G}}/K)$. Moreover, Proposition 2.19 and Theorem 2.21 determine the genus of this extension and its number of rational places. This way we know for all function fields that can be constructed as an unramified field extension of a lower genus function field how many rational places they have, given that we have enough information on the ground field.

We will now write down in words how the algorithm works. In the appendix one can see the algorithm for unramified extensions for genus 4 curves over $\mathbb{F}_5$. We start by creating a list of all suitable function fields of a certain genus g over $\mathbb{F}_q$. We do this using the following steps. First, we make a list of all possible coefficients of the type of polynomial that we are interested in. For example, when looking at hyperelliptic function fields of genus 2 over $\mathbb{F}_7$, we can make a list of all possible coefficients of a monic degree 5 polynomial (which gives 7^5 items) and a similar list for monic degree 6 polynomials (giving 7^6 items). We then filter this list so that we only get separable or only irreducible polynomials, and add those polynomials to another list. Lastly, we choose to filter these polynomials based on how many rational places their corresponding function fields have.

Once we have the set of polynomials we can start finding field extensions. We start by creating a set `Results` that consists of at least 50 entries that are all zero. We want our algorithm to manipulate that set, meaning that each time that it finds a field extension of genus x with N rational points, the algorithm checks the x-th entry of the set `Results`. If that entry is less than N, it overwrites the x-th entry of the set `Results`. Since we want our algorithm to not only give the number of places, but also the corresponding ground field, subgroup G of Cl_K^0 and the place $\mathfrak{o}$ that needs to split completely, we also have a set we call `set` in which this information is stored. Whenever the x-th entry of `Results` is overwritten, the x-th entry of `set` is also automatically overwritten. This way, when the algorithm ends, we know exactly which field extension corresponds to our record.

In order to find out how many rational point each function field has, we do the following. Starting with a polynomial from our set of irreducible polynomials with many places (denoted by `polmanyplaces`), we compute its class field and the subgroups of the degree zero class field. For each of those subgroups G, we compute the index. If the index is less than 50 for genus 2 ground fields, or 25 for genus 3 ground fields, or 17 for genus 4 ground fields, we continue. By bounding the index like this we make sure that all our field extensions have genus less than 50, which speeds up our algorithm. For each rational place $\mathfrak{o}$ we compute the number of elements in the set $\{[\mathfrak{p}_i - \mathfrak{o}]\} \cap G$, where $\mathfrak{p}_i$ ranges over the rational places of K. By Propositions 2.19 and 2.21, this gives us the genus and the number of rational

places of this field extension. If this number of places is higher than we have found in the current computation, the sets `Results` and `set` are overwritten. Either way, the algorithm then proceeds to the extension in which the next rational place splits completely. This way it goes through all subsets of Cl_K^0 of bounded index, and once that is done it can go onto the next function field.

There are still some limitations to this approach. First of all, for genus larger than 3 it is not feasible to let this algorithm run over all function fields of this genus. We will therefore focus on hyperelliptic function fields only for this thesis, most of the time only allowing imaginary hyperelliptic curves. This means working only with degree $2g+1$ polynomials, which means only a fraction of $\frac{1}{q+1}$ of the input set. We see that almost all optimal function fields that are found in previous papers using these methods for finite fields of cardinality at least 7 came from imaginary hyperelliptic curves, with one exception in [Rök12]. We therefore think this is a reasonable reduction. For even larger finite fields, the input set has to be narrowed down even further. We can do this by letting the algorithm run only over polynomials that have a fixed coefficient in front of certain terms of the polynomial or by only looking at irreducible polynomials instead of all separable ones.

Moreover, we will set a lower bound on the number of rational places that a function field needs to have in order to consider its extensions. We see in Theorem 2.21 that the number of rational places of a field extension is $d \cdot |\{[\mathfrak{p}_i - \mathfrak{o}]\} \cap G|$. This means that when a function field has only 2 rational places, the field extension can have at most $2d$ rational places, whereas the genus of the field extension is $g' = d \cdot (g-1) + 1$. Looking at the current records we see that a function field with 2 rational points will never be able to have a field extension that is a new record. For each function field, the running time of the algorithm depends on the degree of the defining polynomial and the cardinality of the finite field that it is defined over. Depending on this running time, one has to choose a bound for the number of rational places that a function field needs to have in order to be considered potentially successful. A lower bounds means longer running time, but also a higher probability to actually find all records that can be found this way.

This way, we reach only a small subset of all function fields of genus four or higher. However, until now a similar algorithm has only been carried out for genus two and three in [Rök12] and [Sol15], and over finite fields of cardinality seven or more there has not been much research apart from the papers mentioned above and a few papers looking at fibre products of two Kummer covers, see for example [ÖTY13]. We therefore expected that reaching a small subset of large genus function fields can already give us many new records.

The run time depends mostly on the number of function fields that one wants to consider, and the number of rational places that they have. The number of hyperelliptic function fields grows roughly as q^{2g+1}, with q the cardinality of the finite field and g the genus of the ground field. When looking at the entries for low genus function fields over $\mathbb{F}_5$ up to $\mathbb{F}_{13}$ at `manypoints.org` we see that the maximum number of places grows roughly linearly with q. Therefore, the total run time can be estimated to grow as q^{2g+2} which shows that the computations slow down extremely fast when moving to higher genus ground fields.

2.4 Results

We first list an overview of the new records that we found. In order for a lower bound to appear on `manypoints.org` it needs to satisfy the following minimum. Let $U_g(q)$ be the upper bound stated, then the lower bound needs to be at least $\frac{U_g(q)-q-1}{\sqrt{2}} + q + 1$. For example, the best known upper bound for $q = 11,\ g = 22$ is 114. This means that for a function field of genus 22 over $\mathbb{F}_{11}$ to be considered, it needs to have at least $\frac{114-12}{\sqrt{2}} + 12 \leq 85$ rational places.

We denote in the table by "previous bound" the current bound on `manypoints.org`. The fact that the previous bound for $q = 11,\ g = 22$ is ... - 114 means that the best known upper bound is 114 and that no function field has yet been found with this g and q that has at least 85 rational places. The function field that we found has 91 rational places, which means that it can be entered in `manypoints.org` as a new record.

finite field	**genus**	**number of rational places**	**previous bound**
$\mathbb{F}_5$	34	77	76 - 83
$\mathbb{F}_7$	16	55	54 - 63
$\mathbb{F}_7$	28	81	72 - 95
$\mathbb{F}_7$	31	90	... - 103
$\mathbb{F}_7$	34	99	... - 111
$\mathbb{F}_7$	37	108	... - 119
$\mathbb{F}_7$	43	112	... - 135
$\mathbb{F}_7$	46	120	... - 142
$\mathbb{F}_7$	49	128	114 - 150
$\mathbb{F}_{11}$	16	75	... - 89
$\mathbb{F}_{11}$	22	91	... - 114
$\mathbb{F}_{11}$	25	104	96 - 127
$\mathbb{F}_{11}$	31	120	... - 149
$\mathbb{F}_{11}$	34	121	... - 160
$\mathbb{F}_{11}$	37	132	... - 171
$\mathbb{F}_{11}$	40	143	... - 181
$\mathbb{F}_{11}$	43	168	... - 192
$\mathbb{F}_{11}$	46	165	... - 203
$\mathbb{F}_{11}$	49	176	... - 213
$\mathbb{F}_{13}$	25	112	... - 142
$\mathbb{F}_{13}$	28	117	... - 156
$\mathbb{F}_{13}$	31	130	... - 170
$\mathbb{F}_{13}$	34	143	... - 183
$\mathbb{F}_{13}$	37	156	144 - 195
$\mathbb{F}_{13}$	40	156	... - 207
$\mathbb{F}_{13}$	49	192	... - 243

Table 1: Records found using the unramified algorithm

We have found these records by letting the algorithm run over the following sets.

1. Hyperelliptic function fields of genus 4 over $\mathbb{F}_3$: all monic separable degree 9 and 10 polynomials with at least 5 rational places (no new records).

2. Hyperelliptic function fields of genus 4 over $\mathbb{F}_5$: all monic separable degree 9 and 10 polynomials with at least 8 rational places.

3. Hyperelliptic function fields of genus 4 over $\mathbb{F}_7$: all monic irreducible degree 9 polynomials with at least 10 rational places.

4. Hyperelliptic function fields of genus 4 over $\mathbb{F}_{11}$: all monic irreducible degree 9 polynomials for which the coefficient of x^8 is always 1 with at least 14 rational places.

5. Hyperelliptic function fields of genus 4 over $\mathbb{F}_{11}$: all monic separable degree 9 polynomials of the form $x^9 + x^8 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ where a_0 is either 0, 1 or 2 and the corresponding function fields has at least 14 rational places.

6. Hyperelliptic function fields of genus 4 over $\mathbb{F}_{13}$: a subset of the set of monic irreducible degree 9 polynomials for which the coefficients of x^8 is always 1 with at least 16 rational places. I managed to let this algorithm run over $588 \cdot 13^5$ polynomials. This is about 2 percent of all degree 9 polynomials with coefficients in $\mathbb{F}_{13}$ so it is reasonable to say that more records can be found using this algorithm when running over the entire set.

7. Hyperelliptic function fields of genus 4 over $\mathbb{F}_{13}$: all monic separable degree 9 polynomials of the form $x^9 + x^8 + x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ with $a_i \in \mathbb{F}_{13}$ with at least 16 rational places.

We will now state the information needed to verify the results above and show how to actually verify this result. The first record that we found is the following.

$\mathbb{F}_5$	$g = 34,\ N = 77$
polynomial	$y^2 + 4 * x^9 + 3 * x^5 + x^4 + 4 * x^3 + 4$
subgroup	$\mathbb{Z}/175\mathbb{Z}$
o	$(1/x, 1/x^5 * y)$

We can verify this record as follows. First, we create the function field that corresponds to this polynomial. We then define the set of rational places, the class group of this function field and the set of subgroups of the degree zero class group. We obtain the degree zero class group by eliminating the last generator of the class group, as the last generator always corresponds to a factor $\mathbb{Z}$.

```
k:=GF(5);
R<x>:=PolynomialRing(k);
P<y>:=PolynomialRing(R);
L<y>:=FunctionField(y^2+4*x^9+3*x^5+x^4+4*x^3+4);
pl1:=Places(L,1);

C,f,g:=ClassGroup(L);
l:=Ngens(C);
G:=Generators(C);
GG:=Exclude(G, C.l);
C0:=sub< C | GG>;
CC:=Subgroups(C0);
C;
```

```
Abelian Group isomorphic to Z/1925 + Z
Defined on 2 generators
Relations:
1925*C.1 = 0
```

When printing the places of degree 1 and the subgroups of the degree zero class group, the first place that MAGMA gives us is always the infinite place. In this case, we thus have that $\mathfrak{o}$ corresponds to the first place. The subgroup we consider here is the fourth that MAGMA prints in the list `CC`.

```
CC[4]`subgroup;
```

```
Abelian Group isomorphic to Z/175
Defined on 1 generator in supergroup C0:
$.1 = 11*C0.1
Relations:
175*$.1 = 0
```

We see that this subgroup has order 175, and that the degree zero part of the class group has order 1925. This means that the subgroup we consider has index 11 in the class group.

```
for i in [1..#pl1] do
    DD:= g(pl1[i]-pl1[1]);
    if DD in CC[4]`subgroup then
        print i;
    end if;
end for;
```

```
1
2
3
6
7
10
11
```

This output tells us that there are 7 places in the set $\{[\mathfrak{p}_i - \mathfrak{o}]\} \cap G$. We have seen that we are working with a subgroup of index 11, which means that Theorem 2.21 tells us that this extension has $11 \cdot 7 = 77$ places, which is an improvement of the old lower bound.

The other records can be verified in a similar way using the information in the appendix.

3 Cohomology

The goal of this chapter is to set up the language and theorems that will be needed to construct class fields in the next chapter. We will therefore not give a complete overview of Galois cohomology, but only state what will be needed. We start with the definition of cohomology groups, using complexes and projective resolutions. We will look into the most intuitive resolution, called the standard resolution of $\mathbb{Z}$. This enables us to create homology groups in a similar way without spending too much time on the details. We will then define Tate cohomology groups, which have the advantage that there is no need for a distinction between cohomology and homology groups. We proceed by investigating the relation between different cohomology groups, defining the restriction, corestriction and inflation maps and their connection. The last tool that we need in order to understand class field theory is the cup product. This construction relates Tate cohomology groups of different degrees, which will be extremely useful for our purposes. At the end of this chapter we will have enough knowledge of Galois cohomology to understand abstract class field theory, which will bring us one step closer to constructing curves over finite fields with many rational points. This chapter roughly follows Chapter 3 of [GS17] except for the part on Tate cohomology.

3.1 Group cohomology

We start this section by quickly recalling some facts about groups and modules.

Definition 3.1. Let G be a group. A *G-module* is an abelian group A with a left action by G such that for any $a, b \in A,\ g \in G$ we have that $g(a+b) = ga + gb$.

Definition 3.2. We say that a G-module M is trivial whenever G acts trivially on M, meaning that G sends any element of M to itself.

Definition 3.3. For two G modules A and B, we denote by $\mathrm{Hom}_G(A, B)$ the set of G-module homomorphisms, which are morphisms of abelian groups compatible with the G-action. $\mathrm{Hom}_G(A, B)$ is itself again an abelian group under the natural addition of homomorphisms. We denote by A^G the subgroup of G-invariant elements in a G-module A.

The goal of this subsection is to define cohomology groups. These groups tell something about the group actions of G on a given G-module A. More specifically, we are looking for the following.

Proposition 3.4. *Let G be any group and A, B be G-modules. We will define abelian groups $H^i(G, A)$ such that:*

1. *$H^0(G, A) = A^G$ for all G-modules A;*
2. *For all G-homomorphisms $A \to B$ there exist canonical maps $H^i(G, A) \to H^i(G, B)$ for all $i \geq 0$;*
3. *Given a short exact sequence $0 \to A \to B \to C \to 0$ of G-modules, there exists an infinitely long exact sequence of abelian groups, starting from $H^0(G, A)$*

$$... \to H^i(G, A) \to H^i(G, B) \to H^i(G, C) \to H^{i+1}(G, A) \to ...$$

We will now work towards setting up the necessary tools in order to create these groups. Note that for every group G, we have the ring $\mathbb{Z}[G]$ whose ring structure follows immediately from the multiplicative structure of G; 0 is defined as the empty sum, 1 as the identity element of G, and we have

$$\sum a_g g + \sum b_g g = \sum (a_g + b_g) g \text{ and } \sum a_{g_1} g_1 \cdot \sum b_{g_2} g_2 = \sum_{g_1 \in G} \sum_{g_2 \in G} a_{g_1} b_{g_2} g_1 g_2.$$

Lemma 3.5. *Let G be a group. Then every G-module can be seen as a $\mathbb{Z}[G]$-module.*

Proof. The group ring $\mathbb{Z}[G]$ contains all elements of the form $\sum a_g g$ with $a_g \in \mathbb{Z}$, $g \in G$ and $a_g = 0$ for almost all $g \in G$. Now we see that every G-module A can be seen as a $\mathbb{Z}[G]$-module by noting that from $g(a+b) = ga + gb$ for all $a, b \in A, g \in G$ it follows that A is left and right associative and has a unique identity. □

Definition 3.6. Let R be a ring, and A be an R-module. A *(cohomological) complex* $A^\bullet$ of R-modules is a sequence of R-module homomorphisms

$$\ldots \xrightarrow{d^{i-1}} A^i \xrightarrow{d^i} A^{i+1} \xrightarrow{d^{i+1}} A^{i+2} \xrightarrow{d^{i+2}} \ldots$$

for all $i \in \mathbb{Z}$ such that $d^{i+1} \circ d^i = 0$ for all i.

Note that a cohomological complex is not necessarily an exact sequence, it only says that $\mathrm{Im}(d^i) \subseteq \ker(d^{i+1})$, not that they are equal. We introduce the following notation.

Definition 3.7. $\mathcal{Z}^i(A^\bullet) := \ker(d^i)$, $\mathcal{B}^i(A^\bullet) := \mathrm{Im}(d^{i-1})$, $\mathcal{H}^i(A^\bullet) := \mathcal{Z}^i(A^\bullet)/\mathcal{B}^i(A^\bullet)$

We now see that a complex is an exact sequence precisely when $\mathcal{H}^i(A^\bullet) = 0$ for all $i \in \mathbb{Z}$.

Definition 3.8. A morphism of complexes $\phi : A^\bullet \to B^\bullet$ is a collection of morphisms $\phi^i : A^i \to B^i$ such the following diagrams commute for all i.

$$\begin{array}{ccc} A^i & \xrightarrow{d_A^i} & A^{i+1} \\ {\scriptstyle \phi^i}\downarrow & & \downarrow{\scriptstyle \phi^{i+1}} \\ B^i & \xrightarrow{d_B^i} & B^{i+1} \end{array}$$

A short exact sequence of complexes is a sequence $0 \to A^\bullet \to B^\bullet \to C^\bullet \to 0$ such that the sequences $0 \to A^i \to B^i \to C^i \to 0$ are exact for all $i \in \mathbb{Z}$.

Note that any morphism of complexes $A^\bullet \to B^\bullet$ gives rise to maps $\mathcal{H}^i(A^\bullet) \to \mathcal{H}^i(B^\bullet)$. The following lemma is a very important tool in (co)homological algebra.

Lemma 3.9 (Snake Lemma)**.** *Given a commutative diagram of G-modules,*

$$\begin{array}{ccccccc} & & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & & \end{array}$$

with exact rows, there is an exact sequence

$$\ker(\alpha) \to \ker(\beta) \to \ker(\gamma) \to \mathrm{coker}(\alpha) \to \mathrm{coker}(\beta) \to \mathrm{coker}(\gamma).$$

Proposition 3.10. *Let $0 \to A^\bullet \to B^\bullet \to C^\bullet \to 0$ be a short exact sequence of complexes of R-modules. Then there exists a long exact sequence*

$$0 \to \mathcal{H}^0(A^\bullet) \to \mathcal{H}^0(B^\bullet) \to \mathcal{H}^0(C^\bullet) \to \mathcal{H}^1(A^\bullet) \to \mathcal{H}^1(B^\bullet) \to ...$$

where the map $\mathcal{H}^i(C^\bullet) \to \mathcal{H}^{i+1}(A^\bullet)$ is denoted by δ^i and called the boundary map.

Proof. The short exact sequence of complexes gives us the following commutative diagram of G-modules.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^i & \longrightarrow & B^i & \longrightarrow & C^i & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_A^i} & & \downarrow{\scriptstyle d_B^i} & & \downarrow{\scriptstyle d_C^i} & & \\ 0 & \longrightarrow & A^{i+1} & \longrightarrow & B^{i+1} & \longrightarrow & C^{i+1} & \longrightarrow & 0 \end{array} \tag{1}$$

The fact that

$$... \xrightarrow{d^{i-1}} A^i \xrightarrow{d^i} A^{i+1} \xrightarrow{d^{i+1}} A^{i+2} \xrightarrow{d^{i+2}} ...$$

is a complex means that $\mathcal{B}^i(A^\bullet) = \mathrm{Im}(d^{i-1}) \subseteq \ker(d^i)$ and moreover that $\mathrm{Im}(d^i) \subseteq \ker(d^{i+1}) = \mathcal{Z}^{i+1}(A^\bullet)$. We thus see that d_A^i induces a map $A^i/\mathcal{B}^i(A^\bullet) \to \mathcal{Z}^{i+1}(A^\bullet)$ and therefore the above commutative diagram (1) can be written as

$$\begin{array}{ccccccccc} & & A^i/\mathcal{B}^i(A^\bullet) & \longrightarrow & B^i/\mathcal{B}^i(B^\bullet) & \longrightarrow & C^i/\mathcal{B}^i(C^\bullet) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_A^i} & & \downarrow{\scriptstyle d_B^i} & & \downarrow{\scriptstyle d_C^i} & & \\ 0 & \longrightarrow & \mathcal{Z}^{i+1}(A^\bullet) & \longrightarrow & \mathcal{Z}^{i+1}(B^\bullet) & \longrightarrow & \mathcal{Z}^{i+1}(C^\bullet) & & \end{array}$$

Now note that $\ker(d_A^i)$ is exactly $\mathcal{Z}^i(A^\bullet)/\mathcal{B}^i(A^\bullet)$ and that $\mathrm{coker}(d_A^i)$ is equal to $\mathcal{Z}^{i+1}(A^\bullet)/\mathcal{B}^{i+1}(A^\bullet)$. We thus see that the snake lemma gives us an exact sequence

$$\mathcal{H}^i(A^\bullet) \to \mathcal{H}^i(B^\bullet) \to \mathcal{H}^i(C^\bullet) \to \mathcal{H}^{i+1}(A^\bullet) \to \mathcal{H}^{i+1}(B^\bullet) \to \mathcal{H}^{i+1}(C^\bullet).$$

Note that $\mathcal{H}^0(A^\bullet) \to \mathcal{H}^0(B^\bullet)$ is injective since $\mathcal{H}^0(A^\bullet) = A^G,\ \mathcal{H}^0(B^\bullet) = B^G$ and $0 \to A \to B \to C \to 0$ is exact. This gives us the first term of the long exact sequence. Putting these sequences together for all $i \in \mathbb{Z}_{\geq 0}$ gives the proof of this proposition. □

Definition 3.11. A *projective R-module* is a module P such that for every surjection $\alpha : A \to B$ of R-modules, the natural map $\mathrm{Hom}(P, A) \to \mathrm{Hom}(P, B)$ sending λ to $\alpha \circ \lambda$ is surjective.

The following lemma provides us with a set of projective R-modules.

Lemma 3.12. *R itself is projective and consequently, every free R-module is projective.*

Proof. Let $f : R \to B$ be a homomorphism, and $\alpha : A \to B$ a surjection. Choose an element a_0 in A such that $\alpha(a_0) = f(1)$. Then by the properties of a ring homomorphism we see that the map sending $R \to A,\ 1 \mapsto a_0$ satisfies $\lambda \circ \alpha = f$ and thus that R is a projective R-module. Now, if both P_1 and P_2 are projective R-modules, it follows from compatibility of Hom-groups with direct sums in the first variable that $P_1 \otimes P_2$ is also a projective module, which completes the proof. □

For each R-module A there exist projective resolutions, which are infinite exact sequences $... \to P_2 \to P_1 \to P_0 \to A \to 0$ with P_i projective. We denote the map $P_{i+1} \to P_i$ by p_{i+1}. Using the definitions and tools stated above, we can now construct the groups that fulfill the requirements from Proposition 3.4.

Definition 3.13. Let G be a group and A be a G-module. Take a projective resolution $P_\bullet = (... \to P_2 \to P_1 \to P_0)$ of the trivial G-module $\mathbb{Z}$. Consider the sequence $\mathrm{Hom}_G(P_\bullet, A)$ defined by

$$\mathrm{Hom}_G(P_0, A) \to \mathrm{Hom}_G(P_1, A) \to \mathrm{Hom}_G(P_2, A) \to ...$$

where the maps $\mathrm{Hom}_G(P_i, A) \to \mathrm{Hom}_G(P_{i+1}, A)$ are defined by $\lambda \mapsto \lambda \circ p_{i+1}$. Because $P_\bullet$ is a complex of G-modules we see that $\mathrm{Hom}_G(P_\bullet, A)$ is a complex of abelian groups. We write $\mathrm{Hom}_G(P_i, A)$ for the i-th term. We then define the *i-th cohomology group* to be

$$H^i(G, A) := \mathcal{H}^i(\mathrm{Hom}_G(P_\bullet, A)) \text{ for } i \geq 0.$$

Theorem 3.14. *Every commutative diagram of short exact sequence of G-modules*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

induces a corresponding commutative diagram of long exact sequences of cohomology groups

$$\begin{array}{ccccccccccc} H^{i-1}(G,C) & \longrightarrow & H^i(G,A) & \longrightarrow & H^i(G,B) & \longrightarrow & H^i(G,C) & \longrightarrow & H^{i+1}(G,A) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H^{i-1}(G,C') & \longrightarrow & H^i(G,A') & \longrightarrow & H^i(G,B') & \longrightarrow & H^i(G,C') & \longrightarrow & H^{i+1}(G,A') \end{array}$$

Theorem 3.15. *The groups $H^i(G, A)$ defined above are independent of the projective resolution $P_\bullet$ chosen, and they satisfy the requirements 1-3 from the beginning of this subsection.*

Proof. See [GS17, Proposition 3.1.9]. □

3.2 The standard resolution

We will now consider an explicit projective resolution that will give us some more intuition for cohomology groups and hopefully make them a little less abstract. Since Theorem 3.15 tells us that the cohomology groups $H^i(G, A)$ are independent of the chosen projective resolution, we will work with an intuitive resolution. Lemma 3.12 tells us that any free R-module is projective, so it makes sense to choose a free resolution of which we can easily prove that it is exact.

Definition 3.16. Let G be a group. Then the *standard resolution* of $\mathbb{Z}$ by G-modules is the sequence

$$... \xrightarrow{\delta^{n+1}} \mathbb{Z}[G^{n+1}] \xrightarrow{\delta^n} \mathbb{Z}[G^n] \xrightarrow{\delta^{n-1}} ... \xrightarrow{\delta^2} \mathbb{Z}[G^2] \xrightarrow{\delta^1} \mathbb{Z}[G] \xrightarrow{\delta^0} \mathbb{Z} \longrightarrow 0 \quad (2)$$

where the boundary maps are given by $\delta^n(g_0, ..., g_n) := \sum_{i=0}^{n} (-1)^i (g_0, ..., g_{i-1}, g_{i+1}, ...g_n)$ and the map δ^0 sends each $g \in G$ to 1. Note that δ^0 can be extended to the augmentation map $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$, sending $\sum a_g g \to \sum a_g$, which we will encounter a few more times.

Lemma 3.17. *The standard resolution of $\mathbb{Z}$ by G-modules is exact.*

Proof sketch. We need to show that $\mathrm{Im}(\delta^{i+1}) = \ker(\delta^i)$. Writing out $\delta^i \circ \delta^{i+1}$ show us that $\delta^i \circ \delta^{i+1} = 0$ for all i because of the factor $(-1)^i$ in the definition of δ^n. Denote for each integer m by $\chi(m)$ its residue class modulo 2. Then we have that

$$\delta^n(\sigma_0, ..., \sigma_n) = (\chi(1)\sigma_1 - \chi(n-0)\sigma_0, \chi(2)\sigma_2 - \chi(n-1)\sigma_1, ..., \chi(n)\sigma_n - \chi(n-(n-1))\sigma_{n-1}).$$

Then $\delta^{n-1} \circ \delta^n$ has as j-th entry

$$\chi(j)(\chi(j+1)\sigma_{j+1} - \chi(n-j)\sigma_j) - \chi(n-1-j)(\chi(j)\sigma_j - \chi(n-(j-1))\sigma_{j-1}),$$

which is equal to zero. We thus have that $\mathrm{Im}(\delta^{i+1}) \subseteq \ker(\delta^i)$. To show the other inclusion we need an auxiliary map h^i, sending $\mathbb{Z}[G^{i+1}] \to \mathbb{Z}[G^{i+2}]$ by sending $(g_0, ...g_i) \mapsto (1, g_0, ..., g_i)$. Writing out these maps gives that $\delta^{i+1} \circ h^i + h^{i-1} \circ \delta^i = \mathrm{id}_{\mathbb{Z}[G^{i+1}]}$. Now from this it follows that $\ker(\delta^i) \subseteq \mathrm{Im}(\delta^{i+1})$ and thus that the standard resolution is exact. □

Since every free $\mathbb{Z}$-module is projective, we see that the standard resolution of $\mathbb{Z}$ by G-modules is indeed a projective resolution, and we can use Definition 3.13 to create the corresponding cohomology groups. We can now give an alternative definition of cohomology groups.

Definition 3.18. Let G be a group and A be a G-module. The standard resolution of $\mathbb{Z}$ by G-modules (2) induces an exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \xrightarrow{d^1} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^2], A) \xrightarrow{d^2} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^3], A) \xrightarrow{d^3} ...$$

Here the maps d^i are the maps that send $\lambda \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^i], A)$ to $\lambda \circ \delta^i \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}], A)$. Since the resolution (2) is exact, we know that $\mathrm{Im}(d^{i-1}) \subseteq \ker(d^i)$ and we can define the cohomology group $H^i(G, A)$ as $\ker(d^i)/\mathrm{Im}(d^{i-1})$.

In order to look at some explicit calculations of cohomology groups, we need a slightly modified resolution. This is called the inhomogeneous cochain resolution, and it looks at the modules $\mathbb{Z}[G]$ a bit differently. Consider the elements $[g_1, ..., g_i] := (1, g_1, g_1g_2, ..., g_1g_2...g_i)$ for any $g_1, g_2, ..., g_i \in G$. They form a basis of $\mathbb{Z}[G^{i+1}]$ as a free $\mathbb{Z}[G]$-module. The maps δ^i act on this basis by sending

$$[g_1, ..., g_i] \mapsto g_1[g_2, ..., g_i] + \sum_{j=1}^{i} (-1)^j [g_1, ..., g_j g_{j+1}, ..., g_i] + (-1)^{i+1}[g_1, ..., g_{i-1}].$$

We then see that the map $d^{i-1} : \mathrm{Hom}_G(\mathbb{Z}[G^{i-1}], A) \to \mathrm{Hom}_G(\mathbb{Z}[G^i], A)$ sends

$$f(g_1, ..., g_{i-1}) \mapsto g_1 f(g_2, ..., g_i) + \sum_{j=1}^{i} (-1)^j f(g_1, ..., g_j g_{j+1}, ..., g_i) + (-1)^{i+1} f(g_1, ..., g_{i-1}).$$

Using this, we can recompute the first two cohomology groups. We see that d^0 sends

$$\mathrm{Hom}_G(\mathbb{Z}, A) \cong A \to \mathrm{Hom}_G(\mathbb{Z}[G], A), \quad a \mapsto a(g) := ga - a,$$

and therefore that the kernel of d^0 consists of exactly those $a \in A$ that are stable under the G-action on A. In that case we would have that $ga = a$ for all $g \in G$ and thus that $ga - a = 0$ for all $g \in G$. We thus have that $\ker(d^0) = A^G$. Since the image of the map

$0 \to \mathbb{Z}$ is exactly $\{0\}$, we see that $H^0(G,A) = \ker(d^0)/\mathrm{Im}(d^{-1}) = \ker(d^0) = A^G$.

Note that the image of d^0 can be written as

$$\{f : G \to A \mid \exists\ a \in A :\ f(g) = ga - a\ \forall\ g \in G\}.$$

The map d^1 sends

$$\mathrm{Hom}_G(\mathbb{Z}[G], A) \cong A \to \mathrm{Hom}_G(\mathbb{Z}[G^2], A) \quad f(g) \mapsto f(g,h) := gf(h) - f(gh) + f(g).$$

From this we see that $\ker(d^1) = \{f : G \to A \mid f(gh) = gf(h) + f(g) \text{ for all } g, h \in G\}$ and we can use that to prove the following proposition.

Proposition 3.19. *Let G be a group, and A be a trivial G-module. Then $H^1(G,A) \cong \mathrm{Hom}(\mathbb{Z}[G], A)$.*

Proof. From the above we see that when A is a trivial G-module, that means that $\mathrm{Im}(d^0)$ is trivial: if $f : g \mapsto ga - a$ then f sends all of G to 0 and thus is the zero map itself. By definition, every morphism $f : G \to A$ has $f(gh) = f(g) + f(h)$, and since G acts trivially on A we see that this means that every morphism $f : \mathbb{Z}[G] \to A$ belongs to $\ker(d^1)$. Combining these results gives that $H^1(G,A) = \ker(d^1)/\mathrm{Im}(d^0) = \mathrm{Hom}_G(\mathbb{Z}[G], A)$. □

The construction we used above to get cohomology groups out of the standard resolution for $\mathbb{Z}$ can also be used to create homology groups $H_i(G,A)$. We will stick to a few definitions on homology groups. One of the reasons to bring them up here is to motivate the definition of Tate cohomology: when using that definition there is no difference between homology and cohomology groups. Moreover, for our main theorem (Theorem 4.17) some knowledge of some homology groups (especially the group $H_1(G,A)$) will be needed.

We construct the homology groups $H_i(G,A)$ by again using the standard resolution (2). Instead of applying the contravariant functor $\mathrm{Hom}_{\mathbb{Z}[G]}(\bullet, A)$ to the resolution, we will now apply the covariant functor $\bullet \otimes_{\mathbb{Z}[G]} A$ to get a chain complex of $\mathbb{Z}$-modules

$$\ldots \xrightarrow{d_3} \mathbb{Z}[G^3] \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_2} \mathbb{Z}[G^2] \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_1} \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \longrightarrow 0,$$

where the maps d_n are defined by sending

$$(g_0, \ldots, g_n) \otimes a \in \mathbb{Z}[G^{n+1}] \otimes_{\mathbb{Z}[G]} A \qquad \text{to} \qquad \delta^n(g_0, \ldots, g_n) \otimes a \in \mathbb{Z}[G^n] \otimes_{\mathbb{Z}[G]} A,$$

where δ^n is the map defined in the standard resolution of $\mathbb{Z}$. In order for this to also work for non-commutative groups, we need to view $\mathbb{Z}[G^n]$ as right G-modules instead of left G-modules. We can now define homology groups analogous to Definition 3.18.

Definition 3.20. We define the *homology groups* $H_i(G,A)$ as $\ker(d_i)/\mathrm{Im}(d_{i+1})$ where the maps d_i are induced by the standard resolution of $\mathbb{Z}$ by setting $d_i = \delta^i \otimes \mathrm{id}$. Again, this group is well-defined since $\mathrm{Im}(d_{i+1}) \subseteq \ker(d_i)$ by exactness of (2).

Analogously to cohomology group, short exact sequences of G-modules induce long exact sequences of homology groups.

Theorem 3.21. *Every short exact sequence of G-modules $0 \to A \to B \to C \to 0$ induces a long exact sequence of homology groups*

$$\ldots \to H_1(G,C) \to H_0(G,A) \to H_0(G,B) \to H_0(G,C) \to 0$$

and any commutative diagram of short exact sequences of G-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

induces a corresponding commutative diagram of long exact sequences of homology groups

$$\begin{array}{ccccccccccc} \ldots & \longrightarrow & H_{i-1}(G,C) & \longrightarrow & H_i(G,A) & \longrightarrow & H_i(G,B) & \longrightarrow & H_i(G,C) & \longrightarrow & \ldots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \ldots & \longrightarrow & H_{i-1}(G,C') & \longrightarrow & H_i(G,A') & \longrightarrow & H_i(G,B') & \longrightarrow & H_i(G,C') & \longrightarrow & \ldots \end{array}$$

Definition 3.22. Let G be a group. Recall from Definition 3.16 that the *augmentation map* $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$ is the ring homomorphism sending $\sum_g a_g g \mapsto \sum_g a_g$. We define the *augmentation ideal* I_G to be the kernel of the augmentation map. I_G is a free $\mathbb{Z}$-module with basis $\{g-1 \ : \ g \in G\}$.

Definition 3.23. For a G-module A we define the group of *co-invariants* to be $A_G := A/I_G A$. It is the largest trivial G-module that is a quotient of A.

Note that I_G is exactly the annihilator of the $\mathbb{Z}[G]$-module $\mathbb{Z}$. We thus have that $\mathbb{Z} \otimes_{\mathbb{Z}[G]} A \cong A/I_G A = A_G$. On the other hand, $\mathbb{Z} \otimes_{\mathbb{Z}[G]} A$ is precisely $H_0(G,A)$. We thus have that

$$H_0(G,A) = A_G \qquad \text{and} \qquad H^0(G,A) = A^G.$$

3.3 Tate cohomology

We are now ready to define cohomology groups. As stated before, one of the main advantages of Tate cohomology groups is that there is no distinction between homology and cohomology groups. Moreover, we will see that a short exact sequence of G-modules induces a long exact sequence of G-modules that is infinitely long on both sides (Theorem 3.26). First, we need the following definition.

Lemma 3.24. *Let A be a G-module and $N_G : A \to A$ be the norm map, sending a to $N_G a = \sum_{g \in G}(ga)$. Then $I_G A \subseteq \ker(N_G)$ and $\mathrm{Im}(N_G) \subseteq A^G$. Thus N_G induces a morphism N_G^* from $A_G \to A^G$ of trivial G-modules.*

We will now define Tate cohomology groups. We will see that the only difference between the cohomology and homology groups defined in the previous subsections and the Tate groups is what happens around the degree 0 groups.

Definition 3.25. Let A be a G-module of a finite group G. Then the *Tate homology and cohomology groups* are defined as follows.

$$\hat{H}^n(G,A) := \begin{cases} \mathrm{coker}(N_G^*) = \frac{A^G}{N_G A} & \text{for } n = 0; \\ H^n(G,A) & \text{for } n > 0; \end{cases} \quad \hat{H}_n(G,A) := \begin{cases} \ker(N_G^*) = \frac{\ker(N_G)}{I_G \cdot A} & \text{for } n = 0; \\ H_n(G,A) & \text{for } n > 0. \end{cases}$$

Moreover, each Tate homology group can be seen as a Tate cohomology group and vice versa by

$$\hat{H}^{-n}(G,A) := \hat{H}_{n-1}(G,A) \qquad \text{and} \qquad \hat{H}_{-n}(G,A) := \hat{H}^{n-1}(G,A).$$

We will now see that these Tate cohomology group give a stronger version of the property described in Proposition 3.4.3 and Theorem 3.21.

Theorem 3.26. *Let G be a finite group. Every short exact sequence of G-modules*

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

induces a infinitely long exact sequence of Tate (co)homology groups

$$... \to \hat{H}^n(G,A) \to \hat{H}^n(G,B) \to \hat{H}^n(G,C) \to \hat{H}^{n+1}(G,A) \to \hat{H}^{n+1}(G,B) \to ...$$

Note that this sequence is infinitely long in both directions, as opposed to the sequences stated in Theorems 3.10 and 3.21. Moreover, commutative diagrams of short exact sequences of G-modules induce commutative diagrams of long exact sequences of Tate (co)homology groups.

Proof. First, note that it suffices to prove exactness at the terms $\hat{H}^0(G,\bullet)$ and $\hat{H}_0(G,\bullet)$ since all other terms are equal to what we have proved before. Therefore, we consider the following diagram.

$$\begin{array}{ccccccccc} H_1(C,G) & \xrightarrow{\delta_0} & A_G & \xrightarrow{\alpha_0} & B_G & \xrightarrow{\beta_0} & C_G & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_G^*} & & \downarrow{\scriptstyle N_G^*} & & \downarrow{\scriptstyle N_G^*} & & \\ 0 & \longrightarrow & A^G & \xrightarrow{\alpha^0} & B^G & \xrightarrow{\beta^0} & C^G & \xrightarrow{\delta^0} & H^1(A,G). \end{array} \tag{3}$$

Note that the upper row is just the regular homology exact sequence and the lower row is the cohomology exact sequence, since $A_G = H_0(G,A)$ and $A^G = H^0(G,A)$. We see that this diagram commutes, so we can apply the snake lemma (Lemma 3.9) to it. This then gives the following exact sequence:

$$\begin{array}{ccccccc} \hat{H}_0(G,A) & \xrightarrow{\hat{\alpha}_0} & \hat{H}_0(G,B) & \xrightarrow{\hat{\beta}_0} & \hat{H}_0(G,C) & \to & \\ & & & \overset{\delta}{\searrow} & & & \\ \to \hat{H}^0(G,A) & \xrightarrow{\hat{\alpha}^0} & \hat{H}^0(G,B) & \xrightarrow{\hat{\beta}^0} & \hat{H}^0(G,C). & & \end{array}$$

In order to reach our goal we need to show that both $\mathrm{Im}(\hat{\delta}_0) = \ker(\alpha_0)$, where $\hat{\delta}_0 : \hat{H}_1(G,C) \to \hat{H}_0(G,A)$, and $\mathrm{Im}(\hat{\beta}^0) = \ker(\hat{\delta}^0)$, where $\hat{\delta}^0 : \hat{H}^0(G,C) \to \hat{H}^1(G,A)$. For the first equality, note that since α^0 is injective. This follows from (3), as we have that $\ker(\alpha_0) \subseteq A_G$ is sent to zero by N_G^*. Thus $\ker(\alpha_0) \subseteq \ker(N_G^*)$ and since $\hat{H}_0(G,A) = \ker(N_G^*)$ we see that $\ker(\alpha_0) = \ker(\hat{\alpha}_0)$.

For the second equality, note that from the commutative diagram (3) we see that β_0 is surjective, thus $\mathrm{Im}(N_G^*) \subseteq \mathrm{Im}(\beta^0)$. Since $\hat{H}^0(G,C) = C^G/\mathrm{Im}(N_G^*)$ we have that

$$\mathrm{Im}(\hat{\beta}^0) = \mathrm{Im}(\beta^0)/\mathrm{Im}(N_G^*) = \ker(\delta)^0/\mathrm{Im}(N_G^*) = \ker(\hat{\delta}^0).$$

We thus see that the sequence is exact at all places and we have proven the theorem. □

Proposition 3.27. *Let G a finite group and let A a free $\mathbb{Z}[G]$-module. Then $\hat{H}^n(G,A) = 0$ for all $n \in \mathbb{Z}$.*

Proof. See [Bro12, Section VI.8]. □

Proposition 3.28. *Let G be a finite group of order p^n for some prime p and A a G-module. Then if*

$$\hat{H}^i(G,A) = \hat{H}^{i+1}(G,A) = 0$$

for some integer i, then $\hat{H}^j(G,A) = 0$ for all $j \in \mathbb{Z}$.

Proof. See [Bro12, Theorem VI.8.5]. □

We will now dive into the case where G is a cyclic group of finite order. Recall from Definition 3.22 that the augmentation ideal I_G is a free $\mathbb{Z}[G]$-module generated by $\{g-1 \mid g \in G\}$. Denote by g_0 a generator of G. Then any element $g \in G$ is some power of g_0 and $g-1 = g_0^j - 1$ can then be written as some product of $g_0 - 1$ times an element of $\mathbb{Z}[G]$. We may thus conclude that the augmentation ideal I_G is principal and generated by $g_0 - 1$ in the ring $\mathbb{Z}[G]$. For any G-module A we then get the following projective resolution:

$$\ldots \xrightarrow{g_0-1} \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g_0-1} \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g_0-1} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0, \qquad (4)$$

which we call the free resolution. This is an exact sequence since the augmentation ideal I_G is exactly equal to the principal ideal $(g_0 - 1)$, so we have that $\mathrm{Im}(N_G^*) = \ker(g_0 - 1)$. Since G is cyclic, $\mathbb{Z}[G]$ is an abelian group so left and right $\mathbb{Z}[G]$-modules can be treated equally. We can view the homology group $\mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A$ as a G-module via $g(h \otimes a) = gh \otimes a = h \otimes ga$ and the cohomology group $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A)$ as a G-module via $(g\varphi)(h) = \varphi(gh)$. This gives us the following theorem.

Theorem 3.29. *Let G be a finite cyclic group with generator g and let A be a G-module. For all $n \in \mathbb{Z}$ we have the following isomorphisms.*

$$\hat{H}^{2n}(G,A) \cong \hat{H}_{2n-1}(G,A) \cong \hat{H}^0(G,A) \text{ and } \hat{H}_{2n}(G,A) \cong \hat{H}^{2n-1}(G,A) \cong \hat{H}_0(G,A).$$

Proof. We have canonical G-module isomorphism:

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \to A, \quad \varphi \mapsto \varphi(1) \text{ and } A \to \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A, \quad a \mapsto 1 \otimes a.$$

We can see that these morphisms are isomorphisms by noting that $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A)$ and $\mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A$ as G-modules, as described above. We have the free resolution (4). Applying the contravariant functor $\mathrm{Hom}_{\mathbb{Z}[G]}(\bullet, A)$ to this, we get

$$0 \longrightarrow A \xrightarrow{g-1} A \xrightarrow{N_G} A \xrightarrow{g-1} A \xrightarrow{N_G} \ldots \ .$$

Similarly tensoring with the covariant functor $\bullet \otimes_{\mathbb{Z}[G]} A$ gives

$$\ldots \xrightarrow{g-1} A \xrightarrow{N_G} A \xrightarrow{g-1} A \xrightarrow{N_G} A \xrightarrow{g-1} A \longrightarrow 0.$$

We can now use this to compute $H^n(G,A)$ and $H_n(G,A)$. We know that $\ker(g-1) = A_G$ so we see that

$$H^{2n}(G,A) \cong H_{2n-1}(G,A) = \ker(g-1)/\mathrm{Im}(N_G) = \mathrm{coker}(N_G^*) = \hat{H}^0(G,A).$$

Analogously we see

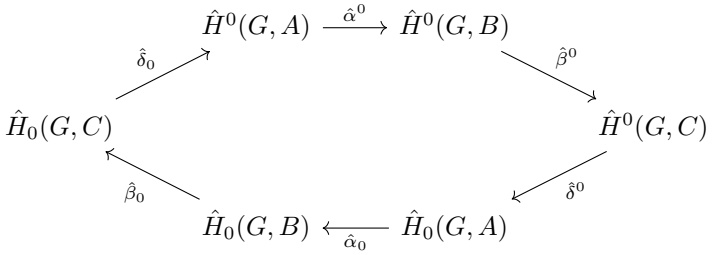
$$H_{2n}(G,A) \cong H^{2n-1}(G,A) = \ker(N_G)/\mathrm{Im}(g-1) = \ker(N_G^*) = \hat{H}_0(G,A),$$

which gives the desired result.

□

From the above theorem, we see that when G is a finite cyclic group, all Tate (co)homology groups are determined by $\hat{H}_0(G,A)$ and $\hat{H}^0(G,A)$. This fact will be extremely useful in the rest of this chapter and will be one of the key insights needed for the fundamental theorem of abstract class field theory. We have the following corollary.

Corollary 3.30. *Let G a finite cyclic group. Given an exact sequence of G-modules $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$, we have a corresponding exact hexagon*



3.4 Maps for subgroups

The goal of this subsection is to construct a number of maps that relate the cohomology groups of a group G with those of a subgroup H of G. There are three maps that we will cover here, called restriction (sending $H^i(G,A)$ to $H^i(H,A)$) corestriction (going in the opposite direction) and inflation (sending $H^i(G/H, A^H)$ to $H^i(G,A)$). We will then look at some relations between those maps, that will give us useful properties of cohomology groups. We will first state these maps for regular cohomology and homology groups, and then prove that they extend to maps of Tate cohomology groups. For the first part, we will follow [GS17].

We start with the following definition that will help us define the desired maps. When we say that G acts canonically on $\mathbb{Z}[G]$ we mean that $g \cdot (\sum n_i g_i) = \sum n_i (g \cdot g_i)$ where $g \cdot g_i$ is the group action of G.

Definition 3.31. Let H be a subgroup of G and A an H-module. Then $\mathbb{Z}[G]$ with canonical G-action is an H-module too, which allows the following definition.

$$M_H^G(A) := \mathrm{Hom}_H(\mathbb{Z}[G], A)$$

where the action of an element $\sigma \in G$ on an H-homomorphism $\phi : \mathbb{Z}[G] \to A$ is given by $\sigma\phi(g) = \phi(\sigma g)$ for $g \in \mathbb{Z}[G]$. Note that $M_H^G(A)$ is a G-module, since this G-action is well-defined.

Lemma 3.32. *Let M be any G-module. Then using the definitions above there exists a canonical isomorphism*

$$\mathrm{Hom}_G(M, M_H^G(A)) \to \mathrm{Hom}_H(M, A)$$

sending a G-homomorphism $m \mapsto \phi_m$ on the left to the H-homomorphism $m \mapsto \phi_m(1)$ on the right.

Lemma 3.33 (Shapiro's lemma)**.** *Let H be a subgroup of G and let A be an H-module. Then for all $i \geq 0$ we have*

$$H^i(G, M_H^G(A)) \cong H^i(H, A).$$

We now have enough tools to define the restriction and corestriction maps.

Definition 3.34. Let G be a group, A be a G-module, H be a subgroup of G. Then there are natural maps of G-modules

$$A \cong \mathrm{Hom}_G(\mathbb{Z}[G], A) \to \mathrm{Hom}_H(\mathbb{Z}[G], A) = M_H^G(A),$$

where the first isomorphism is given by mapping $a \in A$ to the unique G-homomorphism sending $1 \mapsto a$ and the second by noting that any G-homomorphism can be seen as an H-homomorphism. Taking cohomology and applying Shapiro's lemma then gives a map

$$\mathrm{Res} : H^i(G, A) \to H^i(H, A)$$

for all $i \geq 0$, called the *restriction map.*

Note that when applying the restriction map for $i = 0$ we get the natural inclusion $A^G \subseteq A^H$. There is also a map in the opposite direction when H is a subgroup of finite index.

Definition 3.35. Let H be a subgroup of G of finite index n and let A be a G-module. Let $\rho_1, ..., \rho_n$ be a system of left coset representatives of H in G. Given an H-homomorphism $\phi : \mathbb{Z}[G] \to A$, define a new map $\mathbb{Z}[G] \to A$ by

$$\phi_H^G : x \mapsto \sum_{j=1}^{n} \rho_j \phi(\rho_j^{-1} x).$$

This map does not depend on the choice of ρ_j and also is a G-homomorphism because for $\sigma \in G$ we get that $\phi_H^G(\sigma x) = \sigma(\phi_H^G(x))$. We have thus constructed a well-defined map

$$\mathrm{Hom}_H(\mathbb{Z}[G], A) \to \mathrm{Hom}_G(\mathbb{Z}[G], A), \quad \phi \mapsto \phi_H^G.$$

Again by taking cohomology and using Shapiro's lemma this gives us a map

$$\mathrm{Cor} : H^i(H, A) \to H^i(G, A)$$

for all $i \geq 0$, which we call the *corestriction map.*

Proposition 3.36. *Let G be a group, H be a subgroup of finite index n and A be a G-module. Then the composite maps*

$$\mathrm{Cor} \circ \mathrm{Res} : H^i(G, A) \to H^i(G, A)$$

are given by multiplication by n for all $i \geq 0$.

Theorem 3.37. *The restriction and corestriction maps defined above extend to maps of Tate cohomology groups. Consequently, Proposition 3.36 also holds for Tate cohomology groups.*

Proof. Note that we only need to prove this for the groups $\hat{H}^0(G, A)$ and $\hat{H}_0(G, A)$ since all other groups are equal. We will start with the restriction map.

On H^0, the restriction map is given by the inclusion map, since it sends $H^0(G, A) = A^G$ to $H^0(H, A) = A^H$. In order to prove that this gives a well-defined map from

$$\hat{H}^0(G, A) = A^G / N_G A \qquad \text{to} \qquad \hat{H}^0(H, A) = A^H / N_H A$$

we need to show that the restriction map on H^0 sends $N_G A$ to $N_H A$. This follows immediately from the definition: let $a \in N_G A$, then for some $b \in A$ we have

$$a = \sum_{g \in G} gb = \sum_{h \in H} h \sum_{s_i \in G/H} s_i b = \sum_{h \in H} hc \in N_H A$$

where $c \in A$ since A is a G-module and all $s \in G/H$ are elements of G. We thus see that $\mathrm{Res} : H^0(G, A) \to H^0(H, A)$ induces a map $\mathrm{Res} : \hat{H}^0(G, A) \to \hat{H}^0(H, A)$.

On H_0 we have that the restriction map is given by

$$H_0(G, A) \to H_0(H, A),\ a + I_G A \mapsto N_{G/H}^{-1} a + I_H A \ \text{ where } \ N_{G/H}^{-1} : a \to \sum_{s \in G/H} s^{-1} a.$$

The map $N_{G/H}^{-1}$ is independent of the choice of coset representatives $s \in G/H$ since

$$((gh)^{-1} - g^{-1})a = (h^{-1} - 1)g^{-1} a \in I_H A.$$

Since $H_0(G, A) = A/I_G A$ and $\hat{H}_0(G, A) = \ker(N_G)/I_G A$ we need to show that the restriction map on H_0 maps $\ker(N_G) + I_G A$ to $\ker(N_H) + I_H A$. Let $a \in \ker(N_G)$. Then $a + I_G A$ is mapped to $\sum_{s \in G/H} s^{-1} a + I_H A$ and

$$N_H(\sum_{s \in G/H} s^{-1} a) = \sum_{h \in H} \sum_{s \in G/H} s^{-1} a = \sum_{g \in G} a = 0.$$

We thus see that $a \in \ker(N_G)$ is mapped to $\ker(N_H) + I_H A$ and we may conclude that $\mathrm{Res} : H_0(G, A) \to H_0(H, A)$ induces a map $\mathrm{Res} : \hat{H}_0(G, A) \to \hat{H}_0(H, A)$.

For the corestriction maps we proceed analogously. The map $\mathrm{Cor} : H^0(H, A) \to H^0(G, A)$ sends $a \in A^H$ to $N_{G/H} a$ in A^G. In order to show that this induces a map sending $\hat{H}^0(H, A) \to \hat{H}^0(G, A)$ we need to show that $N_H A$ is sent to $N_G A$. We see that for such $a \in N_H A$ we have that

$$a \mapsto N_{G/H} a = \sum_{s \in G/H} sa = \sum_{s \in G/H} s \sum_{h \in H} hb = \sum_{g \in G} b \in N_G A$$

for some $b \in A$. We may thus conclude that $\mathrm{Cor} : H^0(H, A) \to H^0(G, A)$ induces a well-defined map $\mathrm{Cor} : \hat{H}^0(H, A) \to \hat{H}^0(G, A)$.

Finally we need to check the corestriction map on H_0. We see that $\mathrm{Cor} : H_0(H, A) \to H_0(G, A)$ sends $A/I_H A$ to $A/I_G A$ and since $I_H A \subseteq I_G A$ this is just the quotient map. Now we see that $\ker(N_H) \subseteq \ker(N_G)$ since if

$$\sum_{h \in H} ha = 0 \text{ then } \sum_{g \in G} ga = \sum_{s \in G/H} s \sum_{h \in H} ha = \sum_{s \in G/H} 0 = 0.$$

We thus conclude that $\mathrm{Cor} : H_0(H, A) \to H_0(G, A)$ induces a map $\mathrm{Cor} : \hat{H}_0(H, A) \to \hat{H}_0(G, A)$ of Tate cohomology groups, which finishes our proof. □

The last of the three maps that we want to define here is the following.

Definition 3.38. Let G be a group and H be a normal subgroup. Then A^H is again a G-module and H acts trivially on it, so A^H is a G/H-module. Take a projective resolution $P_\bullet$ of $\mathbb{Z}$ as a trivial G-module and a projective resolution $A_\bullet$ of $\mathbb{Z}$ as a trivial G/H-module. There exists a morphism $P_\bullet \to Q_\bullet$ of complexes of G-modules, which leads to maps $\mathrm{Hom}_{G/H}(Q_\bullet, A^H) \to \mathrm{Hom}_G(P_\bullet, A^H)$. Taking cohomology and composing with the natural map $A^H \to A$ we get the *inflation map* for all $i \geq 0$,

$$\mathrm{Inf} : H^i(G/H, A^H) \to H^i(G, A).$$

The following proposition tells us a bit more about the relation between the inflation map and the restriction map. This sequence is therefore called the inflation-restriction exact sequence.

Proposition 3.39. *Let G be a group, H a normal subgroup and A a G-module. There is a natural map $\tau : H^1(H, A)^{G/H} \to H^2(G/H, A^H)$ fitting into the exact sequence*

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^1(G, A) \xrightarrow{\mathrm{Res}} H^1(H, A)^{G/H}$$

$$\xrightarrow{\tau} H^2(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^2(G, A).$$

Proof. See [GS17, Proposition 3.3.14]. □

Moreover, we have the following higher degree inflation-restriction sequence, that we will need when proving the axioms of class field theory.

Proposition 3.40. *Again, let G be a group, H a normal subgroup, A a G-module, and $i > 1$ an integer. Assume that the groups $H^j(H, A)$ are trivial for $a \leq j \leq i-1$. Then there is a natural map $\tau_{i,A} : H^i(H, A)^{G/H} \to H^{i+1}(G/H, A^H)$ fitting into the exact sequence*

$$0 \longrightarrow H^i(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^i(G, A) \xrightarrow{\mathrm{Res}} H^i(H, A)^{G/H}$$

$$\xrightarrow{\tau_{i,A}} H^{i+1}(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^{i+1}(G, A).$$

Proof. See [GS17, Proposition 3.3.17]. □

Since the inflation-restriction sequences only involve cohomology groups of positive degree, replacing the cohomology groups by Tate cohomology groups makes no difference. Proving the following statement goes analogously to the proof for restriction and corestriction maps.

Proposition 3.41. *The inflation map of (co)homology groups induces an inflation map of Tate (co)homology groups with the same properties.*

3.5 Cup products

The last cohomological technique that we will need to state the main theorem in the next chapter is that of a cup product. A cup product will give a map from the Tate cohomology groups of two G-modules A and B to the Tate cohomology group of $A \otimes B$. It is exactly this construction that will enable us to state the map needed in the main theorem of class field theory (Theorem 4.17). We will follow [GS17] in our construction.

Let $A^\bullet$ and $B^\bullet$ be two complexes of abelian groups. We then define the tensor product $T^\bullet = A^\bullet \otimes B^\bullet$ by considering the following double complex.

$$\begin{array}{ccccccc}
 & & \vdots & & \vdots & & \vdots \\
 & & \uparrow & & \uparrow & & \uparrow \\
\dots & \longrightarrow & A^{i-1} \otimes B^{j+1} & \xrightarrow{\delta^h_{i-1,j+1}} & A^i \otimes B^{j+1} & \xrightarrow{\delta^h_{i,j+1}} & A^{i+1} \otimes B^{j+1} \longrightarrow \dots \\
 & & \delta^v_{i-1,j} \uparrow & & \delta^v_{i,j} \uparrow & & \delta^v_{i+1,j} \uparrow \\
\dots & \longrightarrow & A^{i-1} \otimes B^{j} & \xrightarrow{\delta^h_{i-1,j}} & A^i \otimes B^{j} & \xrightarrow{\delta^h_{i,j}} & A^{i+1} \otimes B^{j} \longrightarrow \dots \\
 & & \delta^v_{i-1,j-1} \uparrow & & \delta^v_{i,j-1} \uparrow & & \delta^v_{i+1,j-1} \uparrow \\
\dots & \longrightarrow & A^{i-1} \otimes B^{j-1} & \xrightarrow{\delta^h_{i-1,j-1}} & A^i \otimes B^{j-1} & \xrightarrow{\delta^h_{i1,j-1}} & A^{i+1} \otimes B^{j-1} \longrightarrow \dots \\
 & & \uparrow & & \uparrow & & \uparrow \\
 & & \vdots & & \vdots & & \vdots
\end{array}$$

The horizontal maps $\delta^h_{i,j}$ are given by $\delta^i_A \otimes \mathrm{id}$ and the vertical maps $\delta^v_{i,j}$ by $\mathrm{id} \otimes (-1)^i \delta^j_B$, with δ^i as defined in Definition 3.16. The squares are then anticommutative, meaning that $\delta^h_{i,j+1} \circ \delta^v_{i,j} = -\delta^v_{i+1,j} \circ \delta^h_{i,j}$. The total complex associated with this double complex, denoted by $T^\bullet$, has n-th component

$$T^n = \bigoplus_{i+j=n} A^i \otimes B^j$$

with maps $\delta^n : T^n \to T^{n+1}$, where δ^n acts on $A^i \otimes B^j$ as $\delta^h_{i,j} + \delta^v_{i,j}$. Since the squares above are anticommutative, we see that $\delta^{n+1} \circ \delta^n = 0$ which means that $T^\bullet$ is indeed a complex.

Definition 3.42. Let $A^\bullet, B^\bullet$ be two complexes. Then we define $A^\bullet \otimes B^\bullet$ to be the complex $T^\bullet$ as described above.

Let C, D be two G-modules and $A^\bullet, B^\bullet$ two complexes. Consider the complexes $\mathrm{Hom}(A^\bullet, C)$ and $\mathrm{Hom}(B^\bullet, D)$ whose degree-i terms are $\mathrm{Hom}(A^{-i}, C)$ and $\mathrm{Hom}(B^{-i}, D)$, and where the δ maps are those induced by the complexes $A^\bullet$ and $B^\bullet$. The goal is now to construct a product operation

$$\mathcal{H}^i(\mathrm{Hom}(A^\bullet, C)) \otimes \mathcal{H}^j(\mathrm{Hom}(B^\bullet, D)) \to \mathcal{H}^{i+j}(\mathrm{Hom}(A^\bullet \otimes B^\bullet, C \otimes D)).$$

where the notation $\mathcal{H}^i(X)$ is that of Definition 3.7. We will do so as follows.

Definition 3.43. Let $\alpha : A^{-i} \to C$ and $\beta : B^{-j} \to D$ where $i + j = n$. Then $\alpha \otimes \beta$ is a homomorphism $A^{-i} \otimes B^{-j} \to C \otimes D$, and therefore defines a degree $i + j$ term in $\mathrm{Hom}(A^\bullet \otimes B^\bullet, C \otimes D)$ via the diagonal embedding

$$\mathrm{Hom}(A^{-i} \otimes B^{-j}, C \otimes D) \to \mathrm{Hom}(\bigoplus_{k+l=i+j} A^{-k} \otimes B^{-l}, C \otimes D).$$

Whenever $\alpha \in \mathcal{Z}^i(\mathrm{Hom}(A^\bullet, C))$ and $\beta \in \mathcal{Z}^j(\mathrm{Hom}(B^\bullet, D))$ we see that

$$\alpha \otimes \beta \in \mathcal{Z}^{i+j}(\mathrm{Hom}(A^\bullet \otimes B^\bullet, C \otimes D)),$$

and similarly for $\mathcal{B}^i, \mathcal{B}^j$, which concludes the construction of this map.

The following proposition will be necessary to create a product of cohomology groups of different G-modules.

Proposition 3.44. *Let G be a group and let $P_\bullet$ be a complex of G-modules which is a projective resolution of the trivial G-module $\mathbb{Z}$. Then $P_\bullet \otimes P_\bullet$ is a projective resolution of the trivial $\mathbb{Z}[G \times G]$-module $\mathbb{Z}$.*

Proof. See [GS17, Proposition 3.4.3] □

Definition 3.45. Let A, B be G-modules, let $P_\bullet$ a projective resolution of the trivial G-module $\mathbb{Z}$. Using the above construction with $A^\bullet = B^\bullet = P_\bullet$ we get

$$H^i(\mathrm{Hom}(P_\bullet, A)) \times H^i(\mathrm{Hom}(P_\bullet, B)) \to H^{i+j}(\mathrm{Hom}(P_\bullet \otimes P_\bullet, A \otimes B)).$$

By Proposition 3.44 we know that $P_\bullet \otimes P_\bullet$ is a projective resolution of $\mathbb{Z}$ as a $G \times G$-module, so by taking Tate cohomology we get

$$\hat{H}^i(G, A) \times \hat{H}^j(G, B) \to \hat{H}^{i+j}(G \times G, A \otimes B).$$

Using the fact that we can embed G diagonally into $G \times G$, we can see G as a subgroup of $G \times G$, which gives us a restriction map sending $\hat{H}^{i+j}(G \times G, A \otimes B)$ to $\hat{H}^{i+j}(G, A \otimes B)$. Composing these two maps gives us the desired map, which we call the *cup product* and denote by

$$\cup : \hat{H}^j(G, A) \times \hat{H}^j(G, B) \to \hat{H}^{i+j}(G, A \otimes B)$$

Proposition 3.46. *Suppose G is a finite group. Then the cup product*

$$\cup : \hat{H}^i(G, A) \times \hat{H}^j(G, B) \to \hat{H}^{i+j}(G, A \otimes B)$$

has the following properties for all $i, j \in \mathbb{Z}$ and G-modules A, B:

1. *The homomorphisms are functorial in A and B, meaning that for a morphism $A \to A'$ of G-modules, the corresponding diagram commutes, and similarly in the second variable.*
2. *When $i = j = 0$, the homomorphism is just the natural map $A^G \otimes B^G \to (A \otimes B)^G$.*
3. *Suppose that $0 \to A' \to A \to A'' \to 0$ is exact and so is $0 \to A' \otimes B \to A \otimes B \to A'' \otimes B \to 0$ (which is true for for example flat modules). Then $(\delta a'') \cup b = \delta(a'' \cup b)$ for all $a'' \in \hat{H}^p(G, A'')$ and $b \in \hat{H}^q(G, B)$, where δ is the connecting homomorphism as defined in Proposition 3.10.*
4. *Suppose that $0 \to B' \to B \to B'' \to 0$ is exact and so is $0 \to A \otimes B' \to A \otimes B \to A \otimes B'' \to 0$. Then $a \cup (\delta b'') = (-1)^p \delta(a \cup b'')$ for all $a \in \hat{H}^p(G, A)$ and $b \in \hat{H}^q(G, B'')$.*

Proof. For the first two items, see [GS17, Remark 3.4.6] and for the last two see [GS17, Proposition 3.4.8] . □

The last property of cup products that we will need is the following.

Proposition 3.47. *Given a morphism of G-modules $A \otimes B \to C$, we get pairings*

$$\hat{H}^i(G, A) \times \hat{H}^j(G, B) \to \hat{H}^{i+j}(G, C)$$

for all i and j, by composing the cup-product with the natural map $\hat{H}^{i+j}(G, A \otimes B) \to \hat{H}^{i+j}(G, C)$.

As an example of a place where we will encounter cup products, we will state the following theorem. It essentially tells us the same as Theorem 3.29, but uses cup products to create the isomorphisms between Tate cohomology groups of different degrees.

Let G be a finite cyclic group of order n. We start by looking at the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Taking cohomology gives a connecting homomorphism $\hat{H}^r(G, \mathbb{Q}/\mathbb{Z}) \to \hat{H}^{r+1}(G, \mathbb{Z})$. We denote by δ the map $\hat{H}^1(G, \mathbb{Q}/\mathbb{Z}) \to \hat{H}^2(G, \mathbb{Z})$. All groups $\hat{H}^r(G, \mathbb{Q})$ become trivial, as $\hat{H}^r(G, \mathbb{Q})$ is torsion whenever G is a finite group. Now since G is a cyclic group of order n, the only possible automorphism on $\mathbb{Q}$ is the identity automorphism, so $\hat{H}^r(G, \mathbb{Q})$ is trivial. This gives us an isomorphism $\delta : \mathrm{H}^1(G, \mathbb{Q}/\mathbb{Z}) \to \hat{H}^2(G, \mathbb{Z})$. On the other hand, we have that $\mathbb{Q}/\mathbb{Z}$ is a trivial G-module when G is a cyclic group, so Theorem 3.19 tells us that $\mathrm{H}^1(G, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$.

Definition 3.48. Let G be a finite group. We call an element χ of the group $\hat{G} = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong \hat{H}^1(G, \mathbb{Q}/\mathbb{Z})$ a character.

Theorem 3.49. *Let G be a finite cyclic group of order n and A a G-module, and φ a generator of G. Let $\chi : G \to \mathbb{Q}/\mathbb{Z}$ be the character of G such that $\chi(\varphi) = 1/n$. Then the cup product with $\delta\chi$ gives an isomorphism for all integers i:*

$$.. \cup \delta\chi : \hat{H}^i(G, A) \to \hat{H}^{i+2}(G, A), \quad a \mapsto a \cup \delta\chi.$$

Proof. See [AT68, Chapter 3, Theorem B]. □

We will see in Theorem 4.26 that this cup product will be very important if we want to know more about the isomorphisms induced by class field theory.

4 Class Field Theory

The goal of class field theory is to characterize all abelian extensions of a field k. It does so by first investigating the maximal abelian extension of a field, and then looking at all intermediate extensions $k \subseteq F \subseteq k^{ab}$. In this chapter, we will work towards proving that there exists an isomorphism between finite quotients of the idèle class group of a global field and the Galois group of finite abelian extensions. This isomorphism is in fact a special case of a more general isomorphism, which we will call the main theorem of abstract class field theory. We start by defining formations, which are the objects on which we will define abstract class field theory. We will impose a set of conditions on these formations, and then work towards proving an isomorphism of cohomology groups that is true for all formations that meet these conditions. This will be our abstract main isomorphism (Theorem 4.17), and we will analyze some of its properties.

Once we know enough about the abstract isomorphism, we can start looking at specific formations. The goal is to get an isomorphism from the idèle class group to the Galois group of the maximal abelian extension of a global field. As idèles consist of infinite products of local fields, we will look at a formation of local fields first. We will show that this local formation satisfies the stated conditions and investigate what the main isomorphism looks like for local fields in Section 4.4. Finally, we will move on to a formation of global fields, where we do the same as for local fields. One of our final results will be Theorem 4.74, which tells us exactly how the Galois group of a finite abelian extension of function fields is related to the idèle class group of the ground field. We will spend quite some time on investigating what the map that induces the isomorphism looks like, since this will be crucial information for our algorithm in the next chapter.

4.1 Field formations

In this section, we will introduce formations, which are the objects for which we will define the main theorem in all generality. Formations can be seen as a generalization of the following situation.

Let k be any field and let Ω be the separable part of an algebraic closure. Let G be the Galois group of Ω/k, which can be infinite. Denote by Σ the set of all finite extensions of k in Ω. Then for each $F \in \Sigma$, denote by G_F the subgroup of G consisting of all automorphisms of G that are the identity on F. G can be made into a topological group by taking the family of subgroups $\{G_F\}_{F\in\Sigma}$ as a fundamental system of open neighbourhoods of the identity. This makes sense since all of these subgroups contain the identity. From Galois theory, we then know that every open subgroup of G is of the form G_F for some $F \in \Sigma$ (see Theorem 1.49).

Let A be a G-module, for example Ω^*. Then for each finite extension subgroup G_F we denote by F the fixed submodule of A under G_F, so $A_F = A^{G_F}$. When $A = \Omega^*$, we have that $A_F = F^*$. For two extensions F, K of k we know that $F \subseteq K$ if and only if $G_F \supseteq G_K$, and in that case K/F is an extension of degree $[K : F] = (G_F : G_K)$ with Galois group $G_{K/F} \cong G_F/G_K$. This enables us to think about cohomology groups $H^r(G_{K/F}, A_K)$, and those are exactly the groups that we are interested in. To understand those groups better, we will generalize the construction stated above.

Definition 4.1. A *formation* $\{G, \{G_F\}; A\}$ consists of:
(a) A group G together with a non-empty indexed family $\{G_F\}_{F\in\Sigma}$ of subgroups of G satisfying the following conditions:

1. Each member of the family $\{G_F\}$ is of finite index in G;
2. Each subgroup of G which contains a member of the family $\{G_F\}$ also belongs to the family;
3. The intersection of two members of $\{G_F\}$ also belongs to $\{G_F\}$;
4. Any conjugate in G of a member of $\{G_F\}$ also belongs to $\{G_F\}$;
5. The intersection of all members of $\{G_F\}$ is the identity: $\bigcap_{F\in\Sigma} G_F = 1$.

(b) A G-module A such that $A = \bigcup_{F\in\Sigma} A^{G_F}$, where A^{G_F} is the module fixed by G_F.

We see that the above example, with k a field, G the Galois group of its maximal abelian extension Ω over k, $\{G_F\}$ the Galois groups of the subfields $k \subseteq F \subseteq \Omega$ over k and $A = \Omega^*$ is indeed a formation. It will turn out to be exactly the formation that will be formed when talking about local class field theory. Unfortunately, this formation does does not help us towards our goal when applying it to global fields. The main reason behind this is that local fields have one prime ideal, and global fields have infinitely many prime ideals. Recall that the goal of class field theory is to gain knowledge about the abelian extensions of a field. As we have seen that the splitting behaviour of places largely determines a field extension (see Theorem 1.55), we will need to embed more information about all places in our formation. Therefore, we will construct another formation for global fields. This global formation will eventually give us the isomorphism stated in Theorem 2.17 and a more general isomorphism that we will use to create a ramified algorithm. Since the formations for local and global theory look quite different, it makes sense to first prove the theory of class fields for a very general set of formations. We will then prove that the formations that we are interested in satisfy the needed criteria, so that we can apply the theory of class fields to those formations. In order to talk about these general formations, we need a bit more terminology.

Definition 4.2. Let $\{G, \{G_F\}; A\}$ be a formation. Then we have the following terminology.

1. G is called the *Galois group* of the formation, A is called the formation module;
2. The indices F are referred to as *fields* (even when they do not resemble fields, rings or groups in the usual setting);
3. The submodules $A_F = A^{G_F}$ corresponding to a field F are called *levels* of the formation, and A_F is called the F-level;
4. If F, K are two fields such that $F \subseteq K$ (or similarly $G_F \supseteq G_K$), we say that F is a *subfield* of K;
5. When $F \subseteq K$ we say that K/F is a *layer* of the formation, where A_F is called the *ground level* and A_K is the *top level*;
6. The index $(G_F : G_K)$ is called the *degree* of the layer K/F and G_F/G_K is the Galois group of the layer;
7. If G_K is a normal subgroup of G_F we call the layer K/F *normal* and denote the Galois group by $G_{K/F}$. Similarly, we call the layer *abelian* or *cyclic* when the Galois group is abelian or cyclic.

We will not dive into the topological aspects of a formation, but whenever G' is called an *open subgroup* of G in the literature, that means that G' is of the form G_F for some $F \in \Sigma$. We see that for a normal layer,

$$A_F = A^{G_F} = (A^{G_K})^{G_F/G_K} = A_K^{G_{K/F}}$$

meaning that the ground level of a normal layer consists exactly of the elements in the top level that are left fixed by the Galois group of the layer.

Definition 4.3. By *cohomology groups of a normal layer* K/F we mean the groups

$$\hat{H}^i(K/F) = \hat{H}^i(G_{K/F}, A_K) = \hat{H}^i(G_F/G_K, A^{G_K}).$$

Note that when talking about cohomology groups in this section we will always talk about Tate cohomology groups, and denote them by $\hat{H}(G, A)$. Moreover, note that although G is infinite, the group $G_{K/F}$ is always finite since both F and K are finite extensions of k. We can therefore apply the theory from the previous chapter here.

The purpose of formations is to study cohomology groups of all layers. Putting all layers into one object tells us more about those layers, using the easier layers to get information about more difficult layers. Most properties of ordinary Galois theory carry over to formations. For example, we have the following.

Proposition 4.4. *Let K/F be a normal layer of the formation, and $G_{K/F}$ the corresponding Galois group. Then every subgroup of $G_{K/F}$ is of the form $G_{K/E}$ for some $F \subseteq E \subseteq K$.*

Proof. We know that $G_{K/F} = G_F/G_K$, so every subgroup of $G_{K/F}$ is of the form $G_K \subseteq H \subseteq G_F$. By property 2 of Definition 4.1 we then see that H is also a member of the family $\{G_F\}$, and thus that there is a field $F \subseteq E \subseteq K$ such that $H = G_E$. □

In order to get the most out of the theory, we want to narrow down the formations we work with a bit further. We will therefore state two axioms. Formations that satisfy both axioms are called *class formations*, which are the objects that we are interested in.

Axiom I. *Let $\{G, \{G_F\}; A\}$ be a formation. Then for any normal layer K/F, we have*

$$\hat{H}^1(K/F) = 0.$$

Definition 4.5. A formation that satisfies Axiom I is called a *field formation*.

We will see that this axiom is true whenever F and K are fields and A_K is the multiplicative group of K by Hilbert's Theorem 90 (Theorem 4.33). This motivates the name field formation. The following proposition tells us that to prove that a formation satisfies Axiom I, it is enough to prove it on the cyclic layers of prime degree.

Lemma 4.6. *Let (G, A) be a formation in which all inflation-restriction sequences*

$$\hat{H}^r(K/F) \xrightarrow{\text{Inf}} \hat{H}^r(L/F) \xrightarrow{\text{Res}} \hat{H}^r(L/K)$$

are exact for a certain positive integer r. Then in order to prove that a divisibility of the form

$$|\hat{H}^r(L/F)| \mid [L : F]^n$$

holds for all normal layers L/F, it is enough to show that it holds for all cyclic layers of prime degree.

Proof. See [AT68, Chapter XIV, Lemma 1]. □

Proposition 3.39 tells us that the inflation restriction sequence is exact for $r = 1$ for all normal layers. We can see Axiom I as a divisibility of the form $|\hat{H}^r(L/F)| \mid [L : F]^n$ for $n = 0$. We therefore have the following corollary.

Corollary 4.7. *Axiom I is equivalent to the following statement:*

$$\hat{H}^1(K/F) = 0 \text{ for every cyclic layer of prime degree } K/F.$$

4.2 The Brauer group and class formations

In the previous section we have defined field formations, which are formations that satisfy Axiom I. We will need to impose one more condition on our formations before they will be able to satisfy the main theorem of abstract class field theory. In this section, we define the objects needed for this second requirement, and set up different ways to prove that a formation satisfies Axiom II.

We know that when our formation is a field formation, $\hat{H}^1(K/F) = 0$ for any normal layer K/F. We thus see that the following is a direct corollary of Proposition 3.40, with $G = G_{L/F}$ and $H = G_{L/K}$, so that $G/H = G_{K/F}$.

Proposition 4.8. *Let $\{G, \{G_F\}; A\}$ be a field formation, and let $F \subseteq K \subseteq L$ with K/F and L/F normal. Then the following sequence is exact.*

$$0 \longrightarrow \hat{H}^2(K/F) \xrightarrow{\text{Inf}} \hat{H}^2(L/F) \xrightarrow{\text{Res}_{F,K}} \hat{H}^2(L/K).$$

When the sequence above is exact, that means that the inflation map $\hat{H}^2(K/F) \to \hat{H}^2(L/F)$ is injective, and thus that $\hat{H}^2(K/F)$ can be identified with its image in $\hat{H}^2(L/F)$ by seeing the inflation map as inclusion. Taking another extension, so $F \subseteq K \subseteq L \subseteq M$, by transitivity of inflation we can also see $\hat{H}^2(K/F)$ embedded directly in $\hat{H}^2(M/F)$. Taking the inverse limit gives the following construction.

Definition 4.9. We denote by $\hat{H}^2(*/F)$ the group $\varprojlim_K \hat{H}^2(K/F)$, which we call the *Brauer group* over F of the field formation $\{G, \{G_F\}; A\}$. It has the following properties:

1. For each normal layer K/F, the group $\hat{H}^2(K/F)$ is a subgroup of $\hat{H}^2(*/F)$;
2. If $F \subseteq K \subseteq L$ then the subgroup $\hat{H}^2(K/F)$ is contained in $\hat{H}^2(L/F)$ and the inclusion map is the inflation from K/F to L/F;
3. $\hat{H}^2(*/F)$ is the union of all the subgroups $\hat{H}^2(K/F)$ for normal layers K/F.

Proposition 4.10. *Let $F \subseteq E \subseteq K \subseteq L$ with K/F and L/F normal. Then the following diagram is commutative*

$$\begin{array}{ccc} \hat{H}^2(K/F) & \xrightarrow{\text{Inf}} & \hat{H}^2(L/F) \\ \downarrow{\scriptstyle \text{Res}} & & \downarrow{\scriptstyle \text{Res}} \\ \hat{H}^2(K/E) & \xrightarrow{\text{Inf}} & \hat{H}^2(L/E) \end{array}$$

For a further overview of how the inflation, restriction and corestriction maps work in the case of the Brauer group, see [AT68, Chapter XIV].

Axiom II. *For each field F, there is a given injective homomorphism* $\mathrm{inv}_F : \hat{H}^2(*/F) \to \mathbb{Q}/\mathbb{Z}$ *sending* $\alpha \mapsto \mathrm{inv}_F\ \alpha$ *such that:*

1. *If K/F is a normal layer of degree n, then* inv_F *maps* $\hat{H}^2(K/F)$ *onto the subgroup* $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$*;*
2. *For any layer E/F (not necessarily normal) of degree n we have* $\mathrm{inv}_E \mathrm{Res}_{F,E} = n{\cdot}\mathrm{inv}_F$.

Definition 4.11. A field formation that also satisfies Axiom II is called a *class formation.*

Definition 4.12. Let K/F be a normal layer of a class formation $\{G, \{G_F\}; A\}$. Then Axiom II tells us that $\hat{H}^2(K/F)$ is mapped onto $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. We call the element $\alpha \in \hat{H}^2(K/F)$ that is mapped to $\frac{1}{n}$ the *fundamental class*, and since inv_F is an isomorphism, this also means that the fundamental class is the canonical generator of $\hat{H}^2(K/F)$.

As the requirements of Axiom II might come a little out of the blue, we will try to give a little preview of why this is a reasonable thing to ask. In the next section, we will prove that for any class formation and every normal layer K/F, there exists an isomorphism from $\hat{H}^q(G_{K/F}, \mathbb{Z})$ to $\hat{H}^{q+2}(G_{K/F}, A_K)$. One of the steps in proving this is showing that there is a bijective map from $\hat{H}^0(G_{K/F}, \mathbb{Z})$ to $\hat{H}^2(G_{K/F}, A_K)$. Whenever a formation satisfies Axiom II, we know that $\hat{H}^2(K/F)$ is isomorphic through the inv_F map with $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. We will see that $\hat{H}^0(G_{K/F}, \mathbb{Z})$ is also a cyclic group of degree n, which will then lead to a bijective map. Moreover, the inv_F map will tell us more about which elements of $\hat{H}^0(G_{K/F}, \mathbb{Z})$ are sent to a certain element of $\hat{H}^2(G_{K/F}, A_K)$ by this isomorphism, which will be very important when setting up the algorithm in Chapter 5.

In practice, it turns out that Axiom II can be quite hard to prove. We therefore propose three different statements that are easier to prove and together imply both Axiom I and Axiom II. The first two statements are known as the first and second inequality, and the third is a weaker form of Axiom II. Historically, the first statement was $h_2(K/F) \geq [K : F]$, from which the name "inequality" follows.

Definition 4.13 (First Inequality)**.** Let $\{G, \{G_F\}; A\}$ be a field formation. We denote by h_r the order of the cohomology group $\hat{H}^r$. Then we say that a field formation satisfies the first inequality if for all normal layers we have:

$$h_2(K/F) = [K : F] \cdot h_1(K/F).$$

Definition 4.14 (Second Inequality)**.** Let $\{G, \{G_F\}; A\}$ be a field formation. Then we say that a field formation satisfies the second inequality if for all normal layers K/F we have

$$h_2(K/F) \leq [K : F].$$

By Lemma 4.6 we again see that it suffices to prove these equalities for all normal layers of prime degree. When looking at global fields, we will prove that $h_2(K/F) \mid [K : F]$ which leads to the same conclusion.

We see that proving both the first and the second inequality gives that $h_1(K/F) \leq 1$ and since $h_r(K/F)$ is a positive integer, we see that $h_1(K/F) = 1$. On the other hand, it turns out that the second inequality together with the axiom below implies Axiom II.

Axiom II'. *For each field F, there exists a subgroup $\overline{H}^2(*/F)$ of the Brauer group $\hat{H}^2(*/F)$ and an injective homomorphism $\overline{\text{inv}}_F$ of this subgroup to $\mathbb{Q}/\mathbb{Z}$ such that:*

1. *For any layer E/F we have that* $\text{Res}_{F,E}\ \overline{H}^2(*/F) \subseteq \overline{H}^2(*/E)$ *and*
$$\overline{\text{inv}}_E\ \text{Res}_{F,E}\ (\alpha) = [E:F]\ \overline{\text{inv}}_F\ (\alpha)$$
for all $\alpha \in \overline{H}^2(*/F)$;
2. *If there exists a layer E/F of degree n then $\overline{H}^2(*/F)$ contains a subgroup which is cyclic of order n.*

Theorem 4.15. *Let $\{G, \{G_F\}; A\}$ be a field formation. If this field formation satisfies the second inequality and Axiom II', then it satisfies Axiom II.*

Proof. Let K/F be a normal layer of the field formation of degree n. Then we want to show that $\hat{H}^2(K/F)$ is contained in $\overline{H}^2(*/F)$ and moreover that $\overline{\text{inv}}_F$ maps $\hat{H}^2(K/F)$ onto $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. We know from Axiom II' that there exists a subgroup T of $\overline{H}^2(*/F)$ which is cyclic of degree n. From Axiom II'.1 we then see that

$$\overline{\text{inv}}_K\ \text{Res}_{K,F}\ T = n\ \overline{\text{inv}}_F\ T = \overline{\text{inv}}_F\ n \cdot T = \overline{\text{inv}}_F\ \text{id} = 0$$

where $n \cdot T = \text{id}$ since T is cyclic of degree n. Since $\overline{\text{inv}}_F$ is an isomorphism that means that $\text{Res}_{K,F}\ T = \text{id}$. By the higher degree inflation-restriction sequence of Proposition 3.40

$$0 \to \hat{H}^2(K/F) \xrightarrow{\text{Inf}_{K,*}} \hat{H}^2(*/F) \xrightarrow{\text{Res}_{F,K}} \hat{H}^2(*/K)$$

we see that $\text{Res}_{K,F}\ T = \text{id}$ implies that $T \subseteq \hat{H}^2(K/F)$. On the other hand, by the second inequality we have that the order of $\hat{H}^2(K/F)$ is less than or equal to n, and since the order of T is n, we see that $\hat{H}^2(K/F) = T$. We may now conclude that for every normal layer we have $\hat{H}^2(K/F) \subseteq \overline{H}^2(*/F)$. Since $\overline{\text{inv}}_F$ is an isomorphism and T is a cyclic group of degree n, we see that $\overline{\text{inv}}_F$ must map T to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$, since that is the only cyclic subgroup of degree n of $\mathbb{Q}/\mathbb{Z}$. This concludes our proof. □

4.3 Abstract class field theory

We will now work towards defining Theorem 4.17, which is the main theorem of abstract class field theory. Applying this theorem to the global class formation will lead to the main tool in our algorithm. Whenever we give only a proof sketch, the full proof is available in [AT68, Chapter XIV].

Let K/F be a normal layer in a class formation, with Galois group of order n. We then have the following cup product:

$$\hat{H}^2(G_{K/F}, A_K) \times \hat{H}^q(G_{K/F}, \mathbb{Z}) \to \hat{H}^{q+2}(G_{K/F}, A_K \otimes \mathbb{Z}).$$

Fixing the first part of the cup product to be the fundamental class of the layer, denoted by α, we get for each integer q a map $\hat{H}^q(G_{K/F}, \mathbb{Z}) \to \hat{H}^{q+2}(G_{K/F}, A_K \otimes \mathbb{Z})$.

Note that the natural pairing $A_K \times \mathbb{Z} \to A_K,\ (a, x) \mapsto a\overline{x}$ where $\overline{x} = x \mod n$ is G-bilinear. By the universal property of the tensor product it thus corresponds to a G-linear module homomorphism $A_K \otimes \mathbb{Z} \to A_K$.

Definition 4.16. The map that we get by applying Proposition 3.47 to the pairing described above is

$$\alpha_q : \hat{H}^q(G_{K/F}, \mathbb{Z}) \to \hat{H}^{q+2}(G_{K/F}, A_K), \quad \zeta \mapsto \alpha \cup \zeta$$

for any variable element $\zeta \in \hat{H}^q(G_{K/F}, \mathbb{Z})$.

We will now state the main theorem of abstract class field theory.

Theorem 4.17 (Main theorem of abstract class field theory)**.** *Let K/F be a normal layer in a class formation. Then the maps α_q defined above are isomorphisms for all $q \in \mathbb{Z}$:*

$$\alpha_q : \hat{H}^q(G_{K/F}, \mathbb{Z}) \xrightarrow{\sim} \hat{H}^{q+2}(G_{K/F}, A_K) = \hat{H}^{q+2}(K/F).$$

Before we can prove this theorem, we need the following proposition.

Proposition 4.18. *Let G be a finite group, and $A \times B \to C$ be a G-pairing of G-modules. Let $\alpha \in \hat{H}^p(G, A)$. Then for each $q \in \mathbb{Z}$ and each subgroup $S \subseteq G$, the cup product with the restriction of α to S gives a homomorphism*

$$\alpha_{q,S} : \hat{H}^q(S, B) \to \hat{H}^{p+q}(S, C).$$

Suppose that for some integer q_0 the map $\alpha_{q_0-1,S}$ is surjective, $\alpha_{q_0,S}$ is bijective and $\alpha_{q_0+1,S}$ injective for every subgroup S of G. Then the maps $\alpha_{q,S}$ are bijective for all $q \in \mathbb{Z}$ and $S \subseteq G$.

Proof sketch. Using a technique called dimension shifting (see [Bro12, Chapter III.7]) we can reduce the proof to the case $p = 0$. One can create an exact sequence

$$0 \to B \to C' \to D$$

where $C' = C \otimes \overline{C}$ such that B injects into C', and D is an induced module that makes the sequence exact. Then taking cohomology gives

$$\ldots \longrightarrow \hat{H}^{q_0-1}(S, B) \longrightarrow \hat{H}^{q_0-1}(S, C) \longrightarrow \hat{H}^{q_0-1}(S, D) \longrightarrow \hat{H}^{q_0}(S, B) \longrightarrow$$

$$\hat{H}^{q_0}(S, C) \longrightarrow \hat{H}^{q_0}(S, D) \longrightarrow \hat{H}^{q_0+1}(S, B) \longrightarrow \hat{H}^{q_0+1}(S, C) \longrightarrow \ldots$$

Now, since $\alpha_{q_0-1,S}$ is surjective, $\alpha_{q_0,S}$ is bijective and $\alpha_{q_0+1,S}$ injective, we see that both $\hat{H}^{q_0-1}(S, D)$ and $\hat{H}^{q_0}(S, D)$ are zero. By a generalized version of Proposition 3.28 this means that $\hat{H}^n(S, D) = 0$ for all $n \in \mathbb{Z}$ and $S \subseteq G$. Therefore, we see that the maps $\alpha_{q,S}$ are bijective for all q and all S. □

Proof of Theorem 4.17. We know from Proposition 4.4 that every open subgroup S of $G_{K/F}$ is of the form $G_{K/F'}$ for some $F \subseteq F' \subseteq K$. Moreover, if the fundamental class of K/F is denoted by α, then the fundamental class of K/F' is $\alpha' := \mathrm{Res}_{F,F'}\, \alpha$. We denote by α'_q the map

$$\hat{H}^q(G_{K/F'}, \mathbb{Z}) \to \hat{H}^{q+2}(G_{K/F'}, A_K), \quad \zeta \mapsto \alpha' \cup \zeta.$$

Using the Proposition 4.18, we see that proving that α'_{q_0-1} is surjective, α'_{q_0} is bijective and α'_{q_0+1} injective gives the desired result.

Since $\{G, \{G_F\}; A\}$ is a class formation, we see by Axiom I that $\hat{H}^1(K/F) = 0$ for all normal layers K/F. Therefore we can conclude that α'_{q_0-1} is surjective, since it maps $\hat{H}^{-1}(G_{K/F'}, \mathbb{Z}) \to \hat{H}^1(K/F)$. Also, since $\mathbb{Z}$ is a trivial G-module, Proposition 3.19 tells us that $\hat{H}^1(G_{K/F'}, \mathbb{Z}) = 0$. Therefore α'_{q_0+1} is injective by definition.

Showing that $\alpha'_{q_0} : \hat{H}^0(G_{K/F'}, \mathbb{Z}) \to \hat{H}^2(G_{K/F'}, A_K)$ is bijective is where Axiom II is needed. Axiom II demands that for every normal layer, the group $\hat{H}^2(K/F')$ is cyclic of degree n' and has generator α'. Moreover, we have that $\hat{H}^0(G_{K/F'}, \mathbb{Z}) = \frac{\mathbb{Z}^G}{N_G(\mathbb{Z})} = \mathbb{Z}/n'\mathbb{Z}$ by Definition 3.25. By definition of the map α'_0 we see that the generator of $\hat{H}^0(G_{K/F'}, \mathbb{Z})$, is sent to α', which is the generator of $\hat{H}^2(K/F')$. We can thus use the above proposition to conclude that

$$\alpha_q : \hat{H}^q(G_{K/F}, \mathbb{Z}) \cong \hat{H}^{q+2}(G_{K/F}, A_K) = \hat{H}^{q+2}(K/F)$$

is indeed an isomorphism for all $q \in \mathbb{Z}$. □

We will now look at a particularly interesting case of this theorem, namely the case where $q = -2$. We will see that in that case, the main theorem induces for each normal layer K/F a surjective homomorphism from the G-module A_F to the Galois group $G_{K/F}$. We quickly recall the definition of the norm map, which we will need to describe the kernel of this homomorphism.

Definition 4.19. Let K/F be a layer in a formation, and let $G_{K/F} = G_F/G_K$ be the corresponding group. Then we define the *norm map* to be

$$N_{K/F} : K \to F, \quad x \mapsto \prod_{g \in G_{K/F}} g(x),$$

and we call the index $(F : N_{K/F}K)$ the *norm index*.

For $q = -2$, Theorem 4.17 gives a map from $\hat{H}^{-2}(G_{K/F}, \mathbb{Z})$ to $\hat{H}^0(K/F)$. By definition of Tate cohomology groups, we know that

$$\hat{H}^0(K/F) \cong A_F/N_{K/F}A_K.$$

For $\hat{H}^{-2}(G_{K/F}, \mathbb{Z})$, we have the following isomorphism.

Theorem 4.20. *Let K/F be a normal layer in the class formation with abelian group G. Then we have*

$$\hat{H}^{-2}(G_{K/F}, \mathbb{Z}) \cong G_{K/F}.$$

In order to prove this, one needs to combine the following two lemmas.

Lemma 4.21. *For an abelian group G, we have that $\hat{H}^{-2}(G, \mathbb{Z}) \cong \frac{I_G}{I_G^2}$.*

Proof. We know that the augmentation map $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$ has kernel $I_G = \langle \sigma - 1 \mid \sigma \in G \rangle$ and is surjective. We therefore have the exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0.$$

Since $\mathbb{Z}[G]$ is itself a free $\mathbb{Z}[G]$-module, we know by Proposition 3.27 that it has trivial cohomology. Taking cohomology then gives

$$... \longrightarrow 0 \longrightarrow \hat{H}^r(G,\mathbb{Z}) \xrightarrow{\delta} \hat{H}^{r+1}(G,I_G) \longrightarrow 0 \longrightarrow ...$$

We thus see that δ gives an isomorphism $\hat{H}^r(G,\mathbb{Z}) \cong \hat{H}^{r+1}(G,I_G)$. Taking $r=-2$ then gives us an isomorphism $\hat{H}^{-2}(G,\mathbb{Z}) \cong \hat{H}^{-1}(G,I_G)$.

On the other hand, we have by definition of Tate cohomology that $\hat{H}^{-1}(G,A) = \hat{H}_0(G,A) = \ker(N_G^*) = \frac{\ker(N_G)}{I_G \cdot A}$ where N_G is the map from $A \to A$, sending $a \mapsto \sum_{g\in G} ga$. Taking $A = I_G$ we see that all of I_G is mapped to the kernel by N_G, which gives us $\ker(N_G^*) = \frac{I_G}{I_G^2}$.

We thus have that $\hat{H}^{-2}(G,\mathbb{Z}) \cong \hat{H}^{-1}(G,I_G) \cong \frac{I_G}{I_G^2}$ which finishes the proof. □

Lemma 4.22. *Let G be an abelian group. Then $G \cong \frac{I_G}{I_G^2}$.*

Proof. We claim that the following map is an isomorphism:

$$G \to I_G/I_G^2, \quad \sigma \mapsto (\sigma - 1)\cdot I_G^2.$$

We know that I_G is generated by $\langle \sigma - 1 \mid \sigma \in G\rangle$ as a $\mathbb{Z}$-module. From the identity $(s-1)(t-1) = (st-1)-(s-1)-(t-1)$ we see that $I_G/I_G^2 \cong \{\sigma - 1 \mid \sigma \in G\}$ and therefore the proposed map is the desired isomorphism. □

Combining Theorem 4.17 and 4.20 with the definition of Tate cohomology groups gives us the following result. This will be the main result that we use in the next chapter.

Theorem 4.23. *Let K/F be a normal layer in a class formation with abelian group G. The map α_{-2} gives an isomorphism*

$$\omega_{K/F} : A_F/N_{K/F}A_K \cong \hat{H}^0(K/F) \cong \hat{H}^{-2}(G_{K/F},\mathbb{Z}) \cong G_{K/F}.$$

Definition 4.24. We call the isomorphism $\omega_{K/F} : A_F/N_{K/F}A_K \cong G_{K/F}$ the *reciprocity law isomorphism.* One can also see the above isomorphism as a homomorphism from A_F to $G_{K/F}$ with kernel $N_{K/F}A_K$. This homomorphism is called the *norm-residue map* and the image of $a \in A_F$ is denoted by $(a, K/F)$.

Definition 4.25. Let K/F be a normal layer and let a be an element of A_F. Then we denote by $\overline{a}$ the corresponding element in $\hat{H}^0(K/F) = A_F/N_{K/F}A_K$.

We see that an element $a \in A_F$ is sent to $\sigma \in \mathrm{G}_{K/F}$ if and only if $\overline{a} = \alpha \cup \zeta_\sigma$, where α is the fundamental class of the layer K/F and ζ_σ is the class in $\hat{H}^{-2}(G_{K/F},\mathbb{Z})$ that corresponds to $\sigma \in G_{K/F}$. The following theorem tells us a bit more about where the norm-residue map maps each element. It shows that knowledge of the inv_F map is very important when using the norm-residue map.

Theorem 4.26. *Let $a \in A_F$ and $\sigma \in G_{K/F}$. Denote by $\overline{a}$ the class of a in $\hat{H}^0(K/F)$ and let $\cup\, \delta\chi$ be the map sending $\hat{H}^p(G,A) \to \hat{H}^{p+2}(G,A)$ as defined in Theorem 3.49. Then a is sent to σ by the norm-residue map if and only if*

$$\mathrm{inv}_F(\overline{a} \cup \delta\chi) = \chi(\sigma)$$

for all characters $\chi \in \hat{H}^1(G,\mathbb{Q}/\mathbb{Z})$.

Proof. See [AT68, Chapter XIV, Proposition 6]. □

Definition 4.27. For any extension K/F (not necessarily abelian), we call a subgroup of A_F of the form $N_{K/F}A_K$ a *norm subgroup* of A_F .

The following lemma explains why there is no loss of generality when only considering abelian extensions in what follows.

Lemma 4.28. *The norm group of an arbitrary extension E/F (not necessarily abelian) is the same as that of its maximal abelian subextension M/F, so we have that*

$$N_{E/F}A_E = N_{M/F}A_M.$$

Proof. See [AT68, Chapter XIV, Theorem 7]. □

The following statements will tell us how towers of normal field extensions behave under the reciprocity law.

Proposition 4.29. *Let $F \subseteq E \subseteq K$ be normal extensions and let $a \in A_F$. Then we have*

$$a \in N_{E/F}A_E \iff (a, K/F) \in G_{K/E}.$$

Proof. If $a \in N_{E/F}A_E$, that means that there exists $b \in A_E$ such that $a = N_{E/F}b$. We have the following commutative diagram:

$$\begin{array}{ccc} A_F & \xleftarrow{N_{E/F}} & A_E \\ \downarrow{\scriptstyle (a,K/F)} & & \downarrow{\scriptstyle (a,K/E)} \\ G_{K/F} & \xleftarrow{inclusion} & G_{K/E} \end{array}$$

From this we see that $(a, K/F) = (b, K/E)$ and $(b, K/E) \in G_{K/E}$ so $(a, K/F) \in G_{K/E}$.

To show the reverse implication, we note that A_E is mapped to $G_{K/E}$ surjectively, so there must be a $b \in A_E$ such that if $(a, K/E) \in G_{K/E}$ then $(a, K/F) = (b, K/E)$. Using the fact that the kernel of the norm-residue map $A_F \to G_{K/F}$ is $N_{K/F}A_K$, we see that there must exist $c \in A_K$ such that $a = N_{E/F}b \cdot N_{K/F}c = N_{E/F}(b \cdot N_{K/E}c)$, which proves the proposition. □

In the next chapter, we will create function fields with many rational places by looking at finite abelian extensions. Those extensions will present themselves as intermediate extensions $K \subseteq M \subseteq K^{\mathrm{ab}}$. The following theorem gives us more information about those intermediate fields. It tells us that they are well-behaved when looking at inclusions of subfields and the composita. These properties will make it possible to apply abstract class field theory to find fields with many rational places.

Theorem 4.30. *Let $\{G, \{G_F\}; A\}$ be a class formation, and let $\{M_i\}$ be the set of all abelian extensions of a field F. Then there is a one-to-one correspondence between the set $\{M_i\}$ and the set of all norm subgroups of A_F such that:*

1. $M_1 \subseteq M_2 \iff N_{M_1/F}A_{M_1} \supseteq N_{M_2/F}A_{M_2}$;
2. $N_{M_1M_2/F}A_{M_1M_2} = (N_{M_1/F}A_{M_1}) \cup (N_{M_2/F}A_{M_2})$;

3. $[M : F] = (A_F : N_{M/F}A_M)$ *for any* $M \in \{M_i\}$.

Proof. We know that the homomorphism $A_F \to G_{M/F},\ a \mapsto (a, M/F)$ is surjective. Therefore, the subgroups of $G_{M/F}$ are in one-to-one correspondence with their preimages in A_F. Moreover, since the kernel of the norm-residue map is $N_{M/F}A_M$, we see that these preimages are subgroups of A_F containing $N_{M/F}A_M$. Proposition 4.29 shows that the inverse image of $G_{M/F}$ is exactly $N_{M/F}A_M$.

Assume now that there exist two abelian extensions M_1, M_2 such that $F \subseteq M_1, M_2, \subseteq K$ and such that $N_{M_1/F}A_{M_1} = N_{M_2/F}A_{M_2}$. Then by Proposition 4.29 we see that their images under the norm-residue map $(a, K/F)$ would be the same. We thus have that $G_{K/M_1} = G_{K/M_2}$ and therefore that $M_1 = K^{G_{K/M_1}} = K^{G_{K/M_2}} = M_2$ which concludes the proof of the first statement. The three properties all follow from the one-to-one correspondence. □

In the next two sections, we will investigate local and global class field theory. Global class field theory is what we will need to find function fields with many rational places. The reason why we also cover local class field theory lies in the set up of the local and global formation.

Definition 4.31. Let k be a local field, let Ω be its algebraic closure. Denote by G the Galois group of Ω/k. We will call the formation $\{G, \{G_F\}, \Omega^*\}$, where $\{G_F\}$ is the set of all closed subgroups of G (see Theorem 1.59), the *local formation*.

Definition 4.32. Let F be a global field, and let G be the Galois group of F^{ab}/F, and denote by C_F the idèle class group of F. We will call the formation $\{G, \{G_K\}; C_K\}$, where $\{G_K\}$ is the set of all closed subgroups of G, the *global formation*.

Since an idèle is an element of the infinite product of local fields, we will cover local class field theory first.

4.4 Local class field theory

The goal of this section is to show that the local formation defined in Definition 4.31 is indeed a class formation. We will first show that it is a field formation, meaning that it satisfies Axiom I (see Corollary 4.34). We will then work towards a statement that gives a relation between the ramification degrees of towers of local field extensions. Using this, we then prove the second inequality for local formations in Proposition 4.45. Lastly, we will show that the local formation satisfies Axiom II' in Theorem 4.46, so that we can conclude that the local formation is indeed a class formation.

First, we fix some notation. Let k be a local field, meaning that it is complete under a discrete valuation and has finite residue field. Denote by $\mathfrak{p}$ the unique maximal ideal of k and by $\mathcal{O}_k$ the ring of integers of k. We recall that the local formation is the set $\{G, \{G_K\}, \Omega^*\}$, where $\{G_K\}$ is the set of closed subgroups of G. By the main theorem of infinite Galois theory (Theorem 1.59) we see that for a finite Galois extension K/k, the submodule corresponding to G_K is just K^*. For an extension K/k we denote by $\mathfrak{q}$ the maximal ideal of K and by $\mathcal{O}_K$ the ring of integers of K.

We start by showing that the local formation is a field formation, which is a direct corollary of Hilbert's 90th theorem.

Theorem 4.33 (Hilbert 90)**.** *Let F, K be fields and let K/F be a finite Galois extension with Galois group G. Then*

$$\hat{H}^1(G, K^*) = 0.$$

Corollary 4.34. *The local formation satisfies Axiom I.*

Proof. Let K/F be a normal layer in the formation. Proving that the local formation satisfies Axiom I means showing that $\hat{H}^1(K/F) = 0$. But we have that $\hat{H}^1(K/F) = \hat{H}^1(G_{K/F}, K^*)$ which is zero by Hilbert 90. □

In Chapter 2, we constructed function fields with many rational places by looking at intermediate extensions of a function field K and its maximal abelian unramified extension in which one rational place splits completely. In Chapter 5, we will do something similar, but we will then look at intermediate extensions of K and the maximal abelian extension that is ramified only at certain places and in which one rational place splits completely. Controlling this ramification behaviour is then an important step of the construction. The reason why we treat this material now, instead of after proving that the local formation is a class formation, is that once we have established this result, it is easier to prove the second inequality than doing that from scratch. We start with the following definitions.

Definition 4.35. We define

$$V_i = \{\sigma \in G \mid \sigma\alpha \equiv \alpha \mod \mathfrak{q}^{i+1} \text{ for all } \alpha \in \mathcal{O}_K\}$$

to be the *i-th ramification group* of K/k. Note that we have $G = V_{-1} \supseteq V_0 \supseteq V_1 \supseteq \ldots$.

In accordance with Definition 1.52, V_0 is the inertia group, and its fixed field T is again the maximal unramified subfield of K.

Definition 4.36. We define

$$U_k^{(i)} = \{x \in U_k \mid x \equiv 1 \mod \mathfrak{p}^i\}.$$

Here $U_k^{(0)}$ is the group of units and $U_k^{(-1)} = k^*$. Note that $k^* = U_k^{(-1)} \supseteq U_k^{(0)} \supseteq U_k^{(1)} \supseteq \ldots$

Let K/k be a field extension of local fields with Galois group G, let H be a subgroup of G and let E be the fixed field of K under H, so $k \subseteq E \subseteq K$. We denote the ramification groups of E/k by $\overline{V}_i$ and those of K/E by $\widetilde{V}_i$. We have a simple result for the groups $\widetilde{V}_i$.

Lemma 4.37. *Let K/k be a normal extension with Galois group G, and E an intermediate extension which is the field fixed under H. Then $\widetilde{V}_i = V_i \cap H$.*

Unfortunately, for the ramification groups $\overline{V}_i$ of E/k the result is less straightforward. It turns out that the ramification groups of E/k are in fact the groups V_iH/H, but that we do not have that $\overline{V}_i = V_iH/H$. We will now set up some theory that will help us understand this correspondence. We are looking for a function that will tell us for each subfield $k \subseteq E \subseteq K$, which group V_i of K/k corresponds to which ramification group $\overline{V}_j = V_iH/H$ of E/k. Denote by $i(\sigma)$ the highest index of a ramification group containing σ, meaning that $\sigma \in V_{i(\sigma)}$ but $\sigma \notin V_{i(\sigma)+1}$. We then see that for subextensions $k \subseteq E \subseteq K$ we have the following.

Lemma 4.38. *Let E/k be a normal extension, where E is the fixed field of K under H. If $\sigma H \cap V_i$ is non-empty for some $i \geq 0$, then*

$$\bar{i}(\overline{\sigma}) + 1 = \sum_{j=0}^{l(\sigma)} \frac{1}{(\widetilde{V}_0 : \widetilde{V}_j)}$$

where $l(\sigma)$ is the largest integer j such that $\sigma H \cap V_j$ is non-empty.

Proof. See [AT68, Chapter XI, Lemma 2]. □

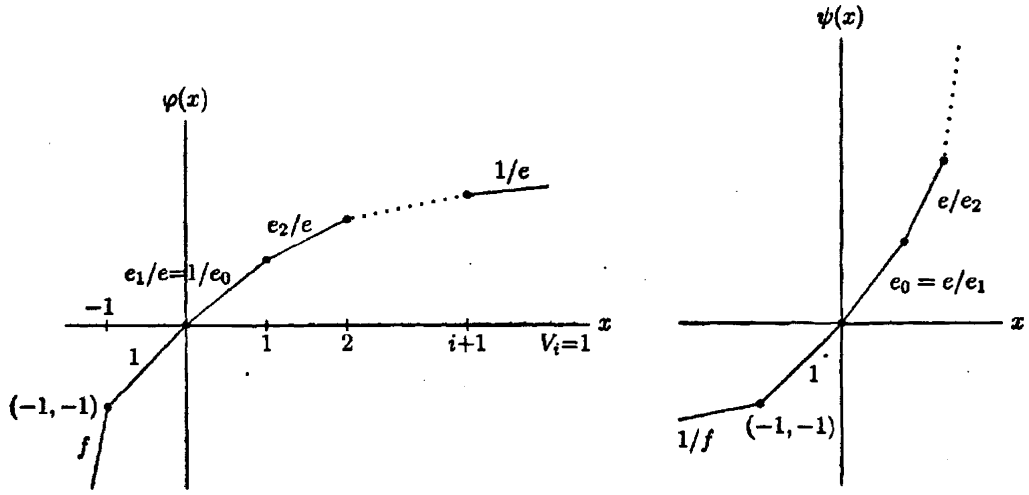
This lemma motivates the following definition.

Definition 4.39. Let K/k be a normal extension. We define for $x \geq 0$ the function $\varphi_{K/k}$ such that

$$\varphi_{K/k} = \int_0^x \frac{1}{(V_0 : V_t)} dt$$

where $V_x = V_{[x]}$ whenever x is not an integer. Moreover, we extend φ to all of $\mathbb{R}$ by setting $(V_0 : V_x) = (V_x : V_0)^{-1}$ for $x \leq 0$.

The function $\varphi(x)$ and its inverse $\psi(x)$ are graphed below (see [AT68, Chapter XI]).



Proposition 4.40. *Let K/k be a normal extension and $\varphi = \varphi_{K/k}$ as defined above. Then*

1. *$\varphi(x)$ is continuous, strictly monotone increasing, convex and satisfies $\varphi(0) = 0$;*
2. *$\varphi(x)$ has left and right derivatives everywhere, denoted by φ'_l and φ'_r. At any integer we have $\varphi'_l = \frac{1}{(V_0:V_i)}$ and $\varphi'_r = \frac{1}{(V_0:V_{i+1})}$; otherwise $\varphi'_l(x) = \varphi'_r(x) = \frac{1}{(V_0:V_x)}$;*
3. *$\varphi'(-\infty) = f$ and $\varphi'(+\infty) = 1/e$;*
4. *$\varphi(x)$ has a well-defined inverse (because of the previous statements), which we denote by $\psi(x)$;*
5. *$\psi(x)$ is continuous, strictly monotone increasing, convex and satisfies $\psi(0) = 0$;*

6. *$\psi(x)$ has left and right derivatives everywhere, denoted by ψ'_l and ψ'_r, which are both integers for any $x > -1$;*

7. *$\psi'(-\infty) = 1/f$ and $\psi'(+\infty) = e$.*

Theorem 4.41 (Hasse-Arf)**.** *Let K/k be a normal extension. If $V_i \neq V_{i+1}$, then $\varphi(i)$ is an integer. Moreover, if $V_i = V_{i+1}$ then $\varphi(i)$ is not an integer.*

We can now state which ramification group of K/k corresponds to which ramification group of E/k, through the following theorem.

Theorem 4.42. *Let $k \subseteq E \subseteq K$ with K/k, E/k both normal, and E fixed under H. Then the ramification groups of K/k and E/k are related as follows. Let $\overline{V}_i$ be a ramification group of E/k, then this group is equal to $V_{\varphi_{K/E}(i)}H/H$, where $V_{\varphi_{K/E}(i)}$ is the $\varphi_{K/E}(i)$-th ramification group of K/k.*

Proof. See [AT68, Chapter XI, Theorem 6]. □

Once we have established that the local formation is indeed a class formation, the following theorem will tell us how the ramification groups behave in the field extensions.

Theorem 4.43. *Let k be a local field, and let K/k be a finite abelian extension. Then $U_k^{(i)} \subseteq N_{K/k}K$ if and only if $V_{\psi(i)} = 1$.*

Proof. See [AT68, Chapter XI, Theorem 11]. □

We will now work towards proving the second inequality for the local formation.

Theorem 4.44. *Let K/F be a normal extension. For any integer $i \geq -1$ we have*

1. *$N_{K/F}U_K^{(\psi(i))} \subseteq U_F^{(i)}$ and $N_{K/F}U_K^{(\psi(i)+1)} \subseteq U_F^{(i+1)}$;*

2. *$(U_F^{(i)} : U_F^{(i+1)}N_{K/F}U_K^{(\psi(i))}) \leq \frac{\psi'_r(i)}{\psi'_l(i)}$;*

3. *There is an integer s such that $U_F^{(s)} \subseteq N_{K/F}K$.*

Proof. See [AT68, Chapter XI, Theorem 9]. □

Proposition 4.45. *The second inequality holds for the local formation.*

Proof. From Theorem 4.44.3 we see that we may write the norm index of a normal layer K/F as a finite product

$$(F : N_{K/F}K) = \prod_{i=-1}^{s} (U_F^{(i)}N_{K/F}K : U_F^{(i+1)}N_{K/F}K). \tag{5}$$

Moreover, after some calculations we get that

$$\begin{aligned}(U_F^{(i)}N_{K/F}K : U_F^{(i+1)}N_{K/F}K) \cdot (U_F^{(i)} \cap N_{K/F}K : U_F^{(i+1)}N_{K/F}U_K^{(\psi(i))} \cap N_{K/F}K) \\ = (U_F^{(i)} : U_F^{(i+1)}N_{K/F}U_K^{(\psi(i))}).\end{aligned} \tag{6}$$

Combining (5) and (6) with Theorem 4.44.2 gives:

$$(F : N_{K/F}K) \leq \prod_{i=-1}^{s} \frac{\psi_r'(i)}{\psi_l'(i)} = \frac{1}{\psi_l'(-1)} \cdot \prod_{i=0}^{s} \frac{\psi_r'(i-1)}{\psi_l'(i)} \cdot \psi_r'(+\infty) \leq \frac{1}{1/f} \cdot e = e \cdot f = n$$

since $\psi_r'(i-1) \leq \psi_l'(i)$ (see the graph of $\psi(x)$). Note that for a cyclic extension K/F we have that $\hat{H}^2(K/F) \cong \hat{H}^0(K/F) = F/N_{K/F}K$ and thus that $h_2(K/F) = (F : N_{K/F}K)$. From this it follows that we have $h_2(K/F) \leq [K : F]$ for all cyclic layers of prime degree, and therefore we can say that the second inequality holds. □

The last thing we need to show in order to prove that the local formation is a class formation, is that Axiom II' holds. We will now construct a map that can be extended to the invariant map needed for Axiom II'.

Let K/F be a finite extension of local fields and let U_K be the set of all elements of K that have valuation 0. We then have an exact sequence

$$0 \to U_K \to K^* \to \mathbb{Z} \to 0$$

where the latter map is the valuation map corresponding to the local field K. We claim that in this formation $\hat{H}^r(G_{K/F}, U_K) = 0$ for all $r \in \mathbb{Z}$ (this follows from the fact that the Herbrand quotient $h_{2/1}(U_K) = 1$, see [AT68, Chapter 4]) so taking cohomology gives an isomorphism $v : \hat{H}^r(G_{K/F}, K^*) \cong \hat{H}^r(G_{K/F}, \mathbb{Z})$. On the other hand, we have the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Here we claim that $\hat{H}^r(G_{K/F}, \mathbb{Q}) = 0$ since $G_{K/F}$ is cyclic of finite degree n and multiplying by any integer is an automorphism of $\mathbb{Q}$. As $\hat{H}^r(G, M)$ is torsion whenever G is a finite group, we see that $\hat{H}^r(G_{K/F}, \mathbb{Q})$ can only consist of the identity automorphism of $\mathbb{Q}$. Taking cohomology then tells us that the connecting map gives an isomorphism

$$\delta : \hat{H}^{r-1}(G_{K/F}, \mathbb{Q}/\mathbb{Z}) \cong \hat{H}^r(G_{K/F}, \mathbb{Z}).$$

Combining the two isomorphisms v and δ for $r = 2$ then gives

$$\hat{H}^2(G_{K/F}, K^*) \cong \hat{H}^2(G_{K/F}, \mathbb{Z}) \cong \hat{H}^1(G_{K/F}, \mathbb{Q}/\mathbb{Z}).$$

Now since $\mathbb{Q}/\mathbb{Z}$ is a trivial G-module, we have by Proposition 3.19 that $\hat{H}^1(G_{K/F}, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(G_{K/F}, \mathbb{Q}/\mathbb{Z})$. Since $G_{K/F}$ is cyclic (see Corollary 1.89), we see that this is isomorphic to $\frac{1}{|G_{K/F}|}\mathbb{Z}/\mathbb{Z}$. Combining all the above we thus see that

$$\hat{H}^2(G_{K/F}, K^*) \cong \frac{1}{|G_{K/F}|}\mathbb{Z}/\mathbb{Z}. \tag{7}$$

Theorem 4.46. *The map defined in (7) can be extended to a map $\hat{H}^2(G_k^{unr}, k_{unr}^*) \to \mathbb{Q}/\mathbb{Z}$ that satisfies the conditions of Axiom II'. From this it follows that the local formation is indeed a class formation.*

Proof. Let K/F be the extension described above and let L/K be another unramified extension. Let $H = \mathrm{Gal}(L/F) \supseteq \mathrm{Gal}(K/F)$. Then the following diagram is commutative:

$$\begin{array}{ccc} \hat{H}^2(H, L^*) & \xrightarrow{\text{inv}_{L/F}} & \frac{1}{|H|}\mathbb{Z}/\mathbb{Z} \\ {\scriptstyle \text{Inf}}\uparrow & & \uparrow \\ \hat{H}^2(G, K^*) & \xrightarrow{\text{inv}_{K/F}} & \frac{1}{|G|}\mathbb{Z}/\mathbb{Z} \end{array}$$

From this we see that the individual maps of the form (7) all fit in a larger invariant map

$$\text{inv}_k : \hat{H}^2(G_k^{unr}, k_{unr}^*) \to \mathbb{Q}/\mathbb{Z}. \tag{8}$$

This map is surjective, and therefore an isomorphism, since for every integer n there exists an unramified extension of k of degree n.

We will now show that this map satisfies the conditions of Axiom II'. First of all, we see that the second condition is satisfied by definition of the map, since for every layer of degree n there is a subgroup of $\hat{H}^2(G_k^{unr}, k_{unr}^*)$ that will be mapped onto $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$, so this subgroup is cyclic of order n.

Let L/K be an unramified layer of the local formation. Recall that for an element $a \in K^*$ we denote by $\overline{a}$ the corresponding element in $\hat{H}^0(L/K) = K^*/N_{L/K}L^*$ (see Definition 4.25). Theorem 3.49 tells us that if we denote by χ the character of G such that $\chi(\varphi) = 1/n$, then any element c of $\hat{H}^2(G_{L/K}, L^*)$ can be written as $\overline{a} \cup \delta\chi$ with $\overline{a} \in \hat{H}^0(G_{L/K}, L^*) = K^*/N_{L/K}L^*$ by definition of Tate cohomology groups. For such an element $\overline{a} \cup \delta\chi$ we see that

$$\text{inv}_{L/K}(\overline{a} \cup \delta\chi) = \chi^{v_L(a)}(\varphi) = \chi(\varphi^{v_L(a)}) = \chi(\varphi^{v_K(a)}) \tag{9}$$

where $v_L(a) = v_K(a)$ since L/K is unramified.

Let us now look at any layer E/F (not necessarily unramified) in the formation. Note that we have that $v_E(a) = e \cdot v_F(a)$ for any $a \in F$, where e is the ramification index. Moreover, if K/F is an unramified extension, then there exists a map from $G_{KE/E} \to G_{K/F}$, sending $\varphi_{KE/E}$ to $\varphi_{K/F}^f$, where f is the residue class degree. Now, (9) tells us that

$$\begin{aligned} \overline{\text{inv}}_E \ \text{Res}_{F,E}\ c &= \chi((\varphi_{KE/E})^{v_E(\text{Res}_{F,E}(a))}) \\ &= \chi((\varphi_{K/F}^f)^{e \cdot v_F(a)}) \\ &= \chi((\varphi_{K/F})^{e \cdot f \cdot v_F(a)}) \\ &= [E:F] \cdot \chi((\varphi_{K/F})^{v_F(a)}) \\ &= [E:F] \cdot \overline{\text{inv}}\ c \end{aligned}$$

for all $c \in \overline{H}^2(*/F)$, which is exactly the second condition of Axiom II'. □

Definition 4.47. The invariant map defined above, sending $\hat{H}^2(*/K) \to \mathbb{Q}/\mathbb{Z}$ is called the *local invariant map*, and denoted by inv_K or $\text{inv}_\mathfrak{p}$, when $\mathfrak{p}$ is the unique maximal ideal of the local field K.

Now that we have proved that the local formation is indeed a class formation, we can apply the main theorem of class field theory on it. This gives us the following result.

Theorem 4.48. *Let k be a local field, and let K/k be a finite abelian extension. Let φ be the generator of* $\text{Gal}(K/k)$*. Then the local norm-residue map*

$$\theta_{K/k} : k^* \to \text{Gal}(K/k),\ a \mapsto (a, K/k)$$

is surjective with kernel $N_{K/k}K^*$ and has the following properties:

1. *If K/k is an unramified extension, then $(a, K/k) = \varphi^{v_k(a)}$ for all $a \in k^*$;*

2. *$\theta_{K/k}$ maps the i-th unit group $U_k^{(i)}$ onto the ramification group $V_{\psi(i)}(K/k)$ for all integers $i \geq 0$.*

Proof. Surjectivity and the fact that the kernel is $N_{K/k}K^*$ follows from Theorem 4.23.

1. This follows almost immediately from Theorem 4.26. We have that $a \in k^*$ is sent to $\sigma \in G_{K/k}$ if and only if

$$\mathrm{inv}_k(\overline{a} \cup \delta\chi) = \chi(\sigma)$$

for all $\chi \in \mathrm{Hom}(G_{K/k}, \mathbb{Q}/\mathbb{Z})$. We know that for an unramified extension K/k, we have that

$$\mathrm{inv}_k(\overline{a} \cup \delta\chi) = \mathrm{inv}_{K/k}(\overline{a} \cup \delta\chi) = \chi(\varphi^{v_k(a)})$$

and therefore that $\theta_{K/k}$ sends $a \in k^*$ to $\varphi^{v_k(a)} \in G_{K/k}$.

2. Theorem 4.43 tells us that $U_k^{(i)} \subseteq N_{K/k}K = \ker(\theta_{K/k})$ if and only if $V_{\psi(i)} = 1$. Denote by Ω again the maximal abelian extension of k, and by $\theta_{\Omega/k}$ the norm-residue map into $\mathrm{Gal}(\Omega/k)$. Then we have that

$$\begin{aligned} K \text{ is left fixed by } V_{\psi(i)}(\Omega/k) &\iff \\ V_{\psi(i)}(K/k) = 1 &\iff \\ U_k^{(i)} \subseteq N_{K/k}K &\iff \\ \theta_{\Omega/k}(U_k^{(i)}) \text{ leaves } K \text{ fixed.} & \end{aligned}$$

From this we see that $\theta_{\Omega/k}(U_k^{(i)})$ lies dense in $V_{\psi(i)}(\Omega/k)$. Since the multiplicative groups of units $U_k^{(i)}$ are compact, it follows that $\theta_{K/k}(U_k^{(i)}) = V_{\psi(i)}(K/k)$ (see [Ser13, Chapter XV.2]). □

4.5 Global class field theory

The goal of this section is to prove that the global formation (Definition 4.32) is indeed a class formation, and to see how the isomorphism from Theorem 4.17 works in the case of global fields. To prove that the global formation is a class formation, we will start by proving the first and second inequality for this formation, from which Axiom I follows. We will then spend most of our time on proving that Axiom II holds for the global formation, since this is where we gain most intuition on the global norm-residue map. We start by illustrating what the cohomology groups of the global formation look like. Recall that

$$C_K = J_K/K^*, \quad J_K = \{(a_\mathfrak{q})_\mathfrak{q} \in \prod_{\mathfrak{q} \in \mathbb{P}_K} K_\mathfrak{q}^* \mid v_\mathfrak{q}(a_\mathfrak{q}) = 0 \text{ for all but finitely many } \mathfrak{q} \in \mathbb{P}_K\}.$$

The Galois group $G_{K/F}$ acts on $\prod_{\mathfrak{q}|\mathfrak{p}} K_\mathfrak{q}^*$ by permuting the factors. Let $\sigma \in G_{K/F}$. Then we see that σ acts on the local field $K_\mathfrak{q}$ by sending $K_\mathfrak{q}$ to $K_{\sigma(\mathfrak{q})}$, $x \mapsto \sigma(x)$. Since $K_\mathfrak{q}$ is a local field, knowing how a group acts on its maximal ideal is enough to know how it acts on the entire field. [CF10, Section VII.1] tells us that

$$\sigma : (a_\mathfrak{q})_\mathfrak{q} \mapsto (\sigma(a_{\sigma^{-1}(\mathfrak{q})}))_\mathfrak{q}.$$

Proposition 4.49. *Let K/F be a normal extension and let $G = G_{K/F}$ be the Galois group. Let $\mathfrak{p}$ be a place of F and $\mathfrak{q}$ a place of K lying above $\mathfrak{p}$, and denote by $G_\mathfrak{q}$ the decomposition group $G_Z(\mathfrak{q}|\mathfrak{p})$. Denote by $U_{K_\mathfrak{q}}$ group of units of $K_\mathfrak{q}$. Then we have isomorphisms*

$$\hat{H}^r(G_{K/F}, \prod_{\mathfrak{q}|\mathfrak{p}} K_\mathfrak{q}^*) \cong \hat{H}^r(G_\mathfrak{q}, K_\mathfrak{q}^*), \qquad \hat{H}^r(G_{K/F}, \prod_{\mathfrak{q}|\mathfrak{p}} U_{K_\mathfrak{q}}^*) \cong \hat{H}^r(G_\mathfrak{q}, U_{K_\mathfrak{q}}^*).$$

Proof. We use Shapiro's lemma (Lemma 3.33) to prove this. Recall that the Galois group of $K_\mathfrak{q}/F_\mathfrak{p}$ is the decomposition group $G_\mathfrak{q} = G_Z(\mathfrak{q}|\mathfrak{p}) = \{\sigma \in G_{K/F} \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$. Now, we see that

$$M_{G_\mathfrak{q}}^G(K_\mathfrak{q}^*) = \mathrm{Hom}_{G_\mathfrak{q}}(\mathbb{Z}[G], K_\mathfrak{q}) \cong \prod_{\mathfrak{q}|\mathfrak{p}} K_\mathfrak{q}^*,$$

where the latter isomorphism follows from the fact that $G = G_{K/F}$ acts transitively on the places above $\mathfrak{p}$. Now Shapiro's lemma tells us that $\hat{H}^i(G, M_{G_\mathfrak{q}}^G(A)) \cong \hat{H}^i(G_\mathfrak{q}, A)$, so we see that

$$\hat{H}^i(G, \prod_{\mathfrak{q}|\mathfrak{p}} K_\mathfrak{q}^*) \cong \hat{H}^i(G, M_{G_\mathfrak{q}}^G(A)) \cong \hat{H}^i(G_\mathfrak{q}, K_\mathfrak{q}^*).$$

The second isomorphism follows analogously. □

From now on, we fix the following notation. Let K/F be a normal layer of the global formation. Recall that for $a \in J_F$ we denote by $\overline{a}$ its class in $\hat{H}^0(G_{K/F}, J_K) = J_F/N_{K/F}J_K$ by Definition 4.25. We will denote the local components of $a \in J_F$ by $a_\mathfrak{p} \in F_\mathfrak{p}^*$ and denote by $\overline{a}_\mathfrak{p}$ its class in $\hat{H}^0(G_{K_\mathfrak{p}/F_\mathfrak{p}}, K_\mathfrak{p}^*) = F_\mathfrak{p}^*/N_{K/F}K_\mathfrak{p}^*$.

For a class $c \in \hat{H}^2(G_{K/F}, J_K)$ we denote by $\overline{c}$ its class in $\hat{H}^2(G_{K/F}, C_K)$. We denote by $c_\mathfrak{p}$ the local class in $\hat{H}^2(G_{K_\mathfrak{p}/F_\mathfrak{p}}, K_\mathfrak{p}^*)$. We say that $a \in J_F$ corresponds to $c \in \hat{H}^2(G_{K/F}, J_K)$ if $c = \overline{a} \cup \delta\chi$.

Definition 4.50. Let $\{G, \{G_F\}; A\}$ be a formation and denote by $h_i(G, A)$ the order of $\hat{H}^i(G, A)$. We define the *Herbrand quotient* $h_{2/1}(G, A)$ to be the quotient $\frac{h_2(G,A)}{h_1(G,A)}$.

We will now state three properties of the index $h_{2/1}$ that will be needed to prove the first inequality.

Proposition 4.51. *Let $\{G, \{G_F\}; A\}$ be formation and denote by $h_{2/1}(A)$ the Herbrand quotient of (G, A).*

1. *The index $h_{2/1}$ is multiplicative, meaning that if A is an abelian group and A_0 is a subgroup invariant under G we have that*

$$h_{2/1}(A) = h_{2/1}(A/A_0) \cdot h_{2/1}(A_0);$$

2. *If A_0 is a finite group, then $h_{2/1}(A_0) = 0$;*

3. *If $A \cong \mathbb{Z}$ and G operates trivially on A, then $h_{2/1}(A) = n$, where n is the order of G.*

Proof. See [AT68, Chapter 3]. □

When proving the first inequality for global fields, we will use the following definitions.

Definition 4.52. Let F be a function field and let K/F be an abelian extension of degree n. Let

$$U = \prod_{\mathfrak{q} \in \mathbb{P}_K} U_{K_\mathfrak{q}}, \qquad J_0 = \{(x_\mathfrak{q})_\mathfrak{q} \in J_K \mid \prod v_\mathfrak{q}(x_\mathfrak{q}) = 1\},$$

which we respectively call the *unit idèles of* K and the *idèles of absolute value 1 of* K. Note that $U \subseteq J_0$ and $K^* \subseteq J_0$ and therefore $UK^* \subseteq J_0$.

Theorem 4.53 (First Inequality for global fields)**.** *Let F be a global field and let K/F be a cyclic extension of degree n with Galois group G. Then*

$$h_{2/1}(C_K) = n.$$

Proof sketch. It turns out that the proof of the first inequality is a lot easier in function fields than in general global fields, so we will prove it for function fields only. We follow Chapter V of [AT68]. Using the definitions above, we see that $\sigma \in G$ sends any element of U to another element of U and any element of J_0 to another element of J_0. From this we see that both $J_0/K^* \subseteq J/K^*$ and $UK^*/K^* \subseteq J_0/K^*$ are subgroups invariant under G. By multiplicativity of $h_{2/1}$ we thus have

$$h_{2/1}(C_K) = h_{2/1}(J_K/K^*) = h_{2/1}(J_K/J_0) \cdot h_{2/1}(J_0/UK^*) \cdot h_{2/1}(UK^*/K^*).$$

We see that J_0 is the kernel of the degree map: $J_K \to \mathbb{Z}$, $(a_\mathfrak{q})_\mathfrak{q} \mapsto \sum v_\mathfrak{q}(a_\mathfrak{q})$, from which it follows that J_K/J_0 is isomorphic to $\mathbb{Z}$. Therefore we have that $h_{2/1}(J_K/J_0) = n$ by Proposition 4.51.3 .

On the other hand, we can construct a map from the idèle class group to the divisor class group, by sending an idèle $(a_\mathfrak{q})_\mathfrak{q} \mapsto \sum v_\mathfrak{q}(a_\mathfrak{q})\mathfrak{q}$. Since the elements of the local fields $K_\mathfrak{q}$ can be written as $u \cdot \mathfrak{q}^n$ we see that the kernel of this map is exactly UK^*. From this it follows that J_0/UK^* is isomorphic to the degree 0 divisor class group. We know that there are only finitely many degree 0 divisor classes of a function field by Proposition 1.22, so from this it follows that J_0/UK^* is finite. From this we see that that $h_{2/1}(J_0/UK^*) = 1$. Lastly, showing $h_{2/1}(UK^*/K^*) = 1$ follows from $UK^*/K^* \cong U/(U \cap K^*)$, noting that $U \cap K^*$ is finite since it is the multiplicative group of the finite constant field of K, and using Shapiro's lemma (Lemma 3.33) to show that $h_{2/1}(U) = 1$. Putting this together gives us that $h_{2/1}(C_K) = n$ and thus that

$$h_2(C_K) = [K : F] \cdot h_1(C_K)$$

for all abelian extensions K/F. □

Theorem 4.54 (Second Inequality for global fields)**.** *Let F be a global field and let K/F be a normal extension. Then the norm index $(C_F : N_{K/F}C_K)$ divides the degree $[K : F]$.*

Proof sketch. Since the proof of the second inequality for global fields is rather long and technical, we will only give an overview of the steps taken. First, two reductions are made. The first reduction states that if the second inequality holds for all cyclic extensions of prime degree, then it holds in all normal extensions (see Lemma 4.6). The second reduction is that whenever the prime degree l of the extension is not equal to the characteristic of the ground field, then it suffices to prove the second inequality for all cyclic fields of prime degree l such that this extension contains a primitive l-th root of unity. In the proof of both cases Kummer theory is used to characterize the extensions of this form. For more information, we refer the reader to Chapter VI of [AT68], which is dedicated entirely to this proof. □

We will now work towards proving that the global formation satisfies Axiom II. We will prove most statements, sometimes skipping proofs of auxiliary statements that will not help us gain important insights. In the course of proving that the global formation satisfies Axiom II, we will define an invariant map for the global formation which, as we have seen in Theorem 4.26 is crucial for understanding the global norm-residue map. We start by defining the invariant map on the set of idèles.

Let F be a global field and let K/F be a normal extension of degree n with Galois group G. Let $\mathfrak{p}$ be a place of F and let $\mathfrak{q}$ be a place of K above $\mathfrak{p}$. Proposition 4.49 tells us that

$$\hat{H}^2(G, \prod_{\mathfrak{q}|\mathfrak{p}} K_{\mathfrak{q}}) \cong \hat{H}^2(G_{\mathfrak{p}}, K_{\mathfrak{p}}).$$

We can thus see $\hat{H}^2(G, J_K)$ as the direct sum of the local cohomology groups $\hat{H}^2(G_{\mathfrak{p}}, K_{\mathfrak{p}})$ by assigning to each cocycle class $c \in \hat{H}^2(G, J_K)$ the local components $c_{\mathfrak{p}} \in \hat{H}^2(G_{\mathfrak{p}}, K_{\mathfrak{p}})$. We see that these local components determine c completely.

Definition 4.55. We define the *idèle invariant* to be the map

$$\mathrm{inv}_{K/F} : \hat{H}^2(G, J_K) \to \mathbb{Q}/\mathbb{Z}, \qquad c \mapsto \sum_{\mathfrak{p}} \mathrm{inv}_{K_{\mathfrak{p}}/F_{\mathfrak{p}}}\ c_{\mathfrak{p}}.$$

We have seen that the local invariants $\mathrm{inv}_{K_{\mathfrak{p}}/F_{\mathfrak{p}}}\ c_{\mathfrak{p}}$ determine $c_{\mathfrak{p}}$ completely. This is not the case for the idèle invariant map. In particular, we see that $\mathrm{inv}_{K/F}\ c = 0$ does not imply at all that c is the class of 1 in $\hat{H}^2(G, J_K)$. The largest part of the remainder of this chapter will be dedicated to showing that $\mathrm{inv}\ c = 0$ if and only if $c \in \hat{H}^2(G, K^*)$. Note that we can see $\hat{H}^2(G, K^*)$ as a subgroup of $\hat{H}^2(G, J_K)$ as follows. From the exact sequence

$$0 \to K^* \to J_K \to C_K \to 0$$

we get an exact sequence

$$\hat{H}^1(G, C_K) \to \hat{H}^2(G, K^*) \to \hat{H}^2(G, J_K) \to \hat{H}^2(G, C_K). \tag{10}$$

Combining the first and second inequality tells us that $\hat{H}^1(G, C_K) = 0$ from which it follows that the map $\hat{H}^2(G, K^*) \to \hat{H}^2(G, J_K)$ is injective. Whenever we speak of $\hat{H}^2(G, K^*)$ as a subgroup of $\hat{H}^2(G, J_K)$, we implicitly use this injection. From now on, we will work with cohomology groups of both J_K and C_K. For clarity we will use the following convention.

We will now work towards defining the norm-residue map for global fields. Let $c \in \hat{H}^2(G, J_K)$, then we know that $c = \overline{a} \cup \delta\chi$ for some $a \in J_F$ by Theorem 3.49. We can then write $c_{\mathfrak{p}}$ as $\overline{a}_{\mathfrak{p}} \cup \delta\chi_{\mathfrak{p}}$. Here $\chi_{\mathfrak{p}} = \mathrm{Res}_{G_{\mathfrak{p}}}\chi$, which is well-defined since χ is an element of $\hat{H}^1(G, \mathbb{Q}/\mathbb{Z})$. Denote by $(a_{\mathfrak{p}}, K_{\mathfrak{p}}/F_{\mathfrak{p}})$ the local norm-residue symbol. Then

$$\begin{aligned} \mathrm{inv}_{\mathfrak{p}}\ \overline{a} \cup \delta\chi &= \mathrm{inv}_{\mathfrak{p}}\ \overline{a}_{\mathfrak{p}} \cup \delta\chi_{\mathfrak{p}} \\ &= \chi_{\mathfrak{p}}((a_{\mathfrak{p}}, K_{\mathfrak{p}}/F_{\mathfrak{p}})) \\ &= \chi((a_{\mathfrak{p}}, K_{\mathfrak{p}}/F_{\mathfrak{p}})), \end{aligned}$$

where we see $(\overline{a}_{\mathfrak{p}}, K_{\mathfrak{p}}/F_{\mathfrak{p}})$ as an element of G. Note that Theorem 4.48 tells us that $(a_{\mathfrak{p}}, K_{\mathfrak{p}}/F_{\mathfrak{p}}) = 1$ whenever $a_{\mathfrak{p}}$ is a unit and $\mathfrak{p}$ unramified. From this we see that the following map is well-defined.

Definition 4.56. Let K/F be a normal extension, and let $a \in J_F$. Then we define the idèle norm-residue map to be

$$J_F \to \mathrm{Gal}(K/F), \qquad a \mapsto (a, K/F) := \prod_{\mathfrak{p}} (a_{\mathfrak{p}}, K_{\mathfrak{p}}/F_{\mathfrak{p}}).$$

This is well-defined since $(a_{\mathfrak{p}}, K_{\mathfrak{p}}/F_{\mathfrak{p}}) = 1$ at almost all places and G is abelian.

We will see in Theorem 4.74 that this map induces the norm-residue map for class groups.

We will now state some lemmas that will help us prove that $\hat{H}^2(G, K^*)$ is exactly the kernel of the idèle invariant map. All proofs can be found in [AT68, Chapter VII.3].

Lemma 4.57. *Let $L/K/F$ be extensions with both L/K and K/F normal and let $c \in \hat{H}^2(G_{K/F}, J_K)$. Let $\mathfrak{p}$ be a place of F, and recall that we could write $\mathrm{inv}_{\mathfrak{p}} = \mathrm{inv}_{K_{\mathfrak{p}}}$ for $\mathrm{inv}_{E_{\mathfrak{q}}/K_{\mathfrak{p}}}$ for any extension $E_{\mathfrak{q}}/K_{\mathfrak{p}}$. Then the local invariant does not change under inflation, i.e.*

$$\mathrm{inv}_{\mathfrak{p}} \ \mathrm{Inf}_L \ c = \mathrm{inv}_{\mathfrak{p}} \ c.$$

From this it follows that for the idèle invariant we have

$$\mathrm{inv}_{L/F} \ \mathrm{Inf}_L \ c = \mathrm{inv}_{K/F} \ c.$$

Corollary 4.58. *Let K_1/F and K_2/F be two normal extensions and denote by $L = K_1K_2$ their compositum. Let $c_1 \in \hat{H}^2(G_{K_1/F}, J_{K_1})$ and $c_2 \in \hat{H}^2(G_{K_2/F}, J_{K_2})$. If $\mathrm{Inf}_L \ c_1 = \mathrm{Inf}_L \ c_2$, then $\mathrm{inv}_{K_1/F}(c_1) = \mathrm{inv}_{K_2/F}(c_2)$.*

This lemma tells us that the idèle invariant map $\mathrm{inv}_{K/F}$ is only a function of F, and we may thus write inv_F for this map.

Lemma 4.59. *Let H be a subgroup of G and denote by E the fixed field of F under H. Let $c \in \hat{H}^2(G, J_K)$. Then*

$$\mathrm{inv}_E \ \mathrm{Res}_E \ c = [E : F] \cdot \mathrm{inv}_F \ c.$$

This lemma will be very useful for two reasons. First of all, it tells us that the idèle invariant map satisfies the second item of Axiom II. Secondly, we will use it in the proof of Theorem 4.62, in which we show that $\hat{H}^2(G_{K/F}, K^*)$ lies in the kernel of the idèle invariant map.

We can now show that $\hat{H}^2(G_{K/F}, K^*) \subseteq \ker(\mathrm{inv}_{K/F})$.

Proposition 4.60. *Let F be a function field and K/F be a cyclic cyclotomic extension. Let $c \in \hat{H}^2(G_{K/F}, K^*)$. Then $\mathrm{inv}_{K/F}(c) = 0$.*

Proof. We note that K/F is a cyclic unramified extension. Hence we can write $(a_{\mathfrak{p}}, K_{\mathfrak{p}}/F_{\mathfrak{p}}) = \varphi_{\mathfrak{p}}^{v_{\mathfrak{p}}(a_{\mathfrak{p}})}$ where $\varphi_{\mathfrak{p}}$ is the generator of $\mathrm{Gal}(K_{\mathfrak{p}}/F_{\mathfrak{p}})$. Let k_0 be the constant field of F; recall that $\deg(\mathfrak{p}) = [\widetilde{F}_{\mathfrak{p}} : k_0]$. If k_0 has q elements, then the residue class field $\widetilde{F}_{\mathfrak{p}}$ thus has $q^{\deg(\mathfrak{p})}$ elements. From this it follows that in the residue class field,

$$\varphi_{\mathfrak{p}}^{v_{\mathfrak{p}}(a)} : x \mapsto (x^{q^{\deg(\mathfrak{p})}})^{v_{\mathfrak{p}}(a)} \text{ for } x \in F_{\mathfrak{p}}.$$

Now, let $c \in \hat{H}^2(G_{K/F}, K^*)$. Then we can write $c = \overline{a} \cup \delta\chi$ for some $a \in F$. Embed a as an idèle, so as $(..., a, a, a, ...)$. We know that the degree of any principal divisor (a) is zero

(see Proposition 1.20), so this means that $\sum_{\mathfrak{p}\in\mathbb{P}_F} \deg(\mathfrak{p})\cdot v_{\mathfrak{p}}(a) = 0$. By definition, we have $(a, K/F) = \prod_{\mathfrak{p}\in\mathbb{P}_F} (a_{\mathfrak{p}}, K_{\mathfrak{p}}/F_{\mathfrak{p}})$. Therefore, the element in $G_{K/F}$ that represents $(a, K/F)$ is

$$x \mapsto x^{q^{\sum \deg(\mathfrak{p}) v_{\mathfrak{p}}(a)}} = x^{q^0} = x,$$

which means that $(a, K/F)$ is the identity. We have thus proven that $\chi((a, K/F)) = 0$ for all characters χ and thus that $\mathrm{inv}(\overline{a} \cup \delta\chi) = 0$. □

Proposition 4.61. *Let K/F be a normal extension of function fields, and $c \in \hat{H}^2(G_{K/F}, K^*)$. Then there exists a cyclic cyclotomic extension F'/F such that*

$$\mathrm{Res}_{F'}\ \mathrm{Inf}_{KF'}\ c = 1.$$

Proof. See [AT68, Chapter VII, page 46]. □

Theorem 4.62. *Let K/F be a normal extension of function fields of degree n. Let $c \in \hat{H}^2(G_{K/F}, K^*)$. Then* $\mathrm{inv}_{K/F}\ c = 0$.

Proof. Proposition 4.61 tells us that there exists a cyclic cyclotomic extension F'/F such that $\mathrm{Res}_{F'}\ \mathrm{Inf}_{KF'}\ c = 1$. This means that F' is a splitting field for $\mathrm{Inf}_L\ c$, which means that there exists a cocycle class $c' \in \hat{H}^2(G_{F'/F})$ such that $\mathrm{Inf}_L\ c = \mathrm{Inf}_L\ c'$. From Corollary 4.58 it then follows that $\mathrm{inv}_F\ c = \mathrm{inv}_F\ c'$ and since the latter is zero by Proposition 4.60 we see that $\mathrm{inv}_F\ c = 0$.

□

Now that we know that $\hat{H}^2(G_{K/F}, K^*)$ is part of the kernel of the idèle invariant map, we can create an invariant map from $\hat{H}^2(G_{K/F}, C_K)$ to $\mathbb{Q}/\mathbb{Z}$. We have seen in the exact sequence (10) that there exists a map $\hat{H}^2(G_{K/F}, J_K) \to \hat{H}^2(G_{K/F}, C_K)$, which we will denote by j. The most intuitive option to create a map from $\hat{H}^2(G_{K/F}, C_K)$ to $\mathbb{Q}/\mathbb{Z}$ is to assign each element of the form $jc \in \hat{H}^2(G_{K/F}, C_K)$ the same invariant map as the element $c \in \hat{H}^2(G_{K/F}, J_K)$. However, since the map j is not always surjective, this will not give us a map that satisfies all requirements of Axiom II. We will therefore define the invariant map on $\hat{H}^2(G_{K/F}, C_K)$ in a different way. First, we will write down three auxiliary statements that are essentially corollaries of Theorem 4.62.

Corollary 4.63. *Let K/F be a normal extension with group G, and let $\overline{c} \in \hat{H}^2(G, C_K)$. Suppose $\overline{c} = jc = jd$ for some $c, d \in \hat{H}^2(G, J_K)$. Then* $\mathrm{inv}_F\ c = \mathrm{inv}_F\ d$.

Corollary 4.64. *Let $\overline{c} \in j\hat{H}^2(G, J_K)$, say $\overline{c} = jc$. Let $L/K/F$ be extensions with both L/K and K/F normal. Then inflation commutes with j, so we have*

$$\mathrm{Inf}_L\ \overline{c} = \mathrm{Inf}_L\ (jc) = j\ \mathrm{Inf}_L\ c.$$

From this it follows that if $\overline{c}$ is the image of j in any layer, then its inflation to any bigger layer is also in the image of j.

Corollary 4.65. *Let $\overline{c} \in \hat{H}^2(G, C_K)$. Let L_1/K and L_2/K be two normal extensions with Galois groups G_1 and G_2. Suppose that $\mathrm{Inf}_{L_1}\ \overline{c} = jc_1$ and $\mathrm{Inf}_{L_2}\ \overline{c} = jc_2$ for some $c_1 \in \hat{H}^2(G_1, J_{L_1})$, $c_2 \in \hat{H}^2(G_2, J_{L_2})$. Denote by L the compositum of L_1 and L_2. Then we have*

$$\mathrm{Inf}_L\ \overline{c} = j\ \mathrm{Inf}_L\ c_1 = j\ \mathrm{Inf}_L\ c_2.$$

From this it follows that $\mathrm{inv}_F\ \mathrm{Inf}_L\ c_1 = \mathrm{inv}_F\ \mathrm{Inf}_L\ c_2$, *and thus* $\mathrm{inv}_F\ c_1 = \mathrm{inv}_F\ c_2$.

We cannot yet define a so-called global invariant map, that sends all of $\hat{H}^2(G_{K/F}, C_K) \to \mathbb{Q}/\mathbb{Z}$. However, using the statements above we can define an invariant map on a subset of $\hat{H}^2(G_{K/F}, C_K)$.

Definition 4.66. Let K/F be a normal extension. Then we call a cocycle class $\overline{c} \in \hat{H}^2(G_{K/F}, C_K)$ *regular* (or a *regular element*) if there exists a normal extension L/K such that $\operatorname{Inf}_L \overline{c} = jc$ for some cocycle class $c \in \hat{H}^2(G_{L/F}, J_L)$. We denote the set of regular elements by $\overline{H}^2(G_{K/F}, C_K)$.

We can use the corollaries above to see that $\overline{H}^2(G_{K/F}, C_K)$ is closed under multiplication, and therefore conclude that $\overline{H}^2(G_{K/F}, C_K)$ is a group. We now define the invariant map for regular elements, which we will also call the *regular invariant map*.

Definition 4.67. Let $\overline{c} \in \overline{H}^2(G_{K/F}, C_K)$ be a regular element, and let L/K be a normal field extension such that $\operatorname{Inf}_L \overline{c} = jc$ for some $c \in \hat{H}^2(G_{L/F}, J_L)$. Then we define

$$\overline{\operatorname{inv}_F} : \overline{H}^2(G_{K/F}, C_K) \to \mathbb{Q}/\mathbb{Z}, \quad \overline{c} \mapsto \operatorname{inv}_F c.$$

We see that our definition is independent of the choice of representative by Corollary 4.63. From Corollary 4.65 we see that it is also independent of the choice of L. We can see that the regular invariant map on $\overline{H}^2(G_{K/F}, C_K)$ is a homomorphism by noting that for two regular elements $\overline{c}, \overline{d}$ we can always find a field L such that $\operatorname{Inf}_L \overline{c} = jc$, $\operatorname{Inf}_L \overline{d} = jd$. Then $\operatorname{Inf}_L \overline{c}\overline{d} = j(cd)$ and $\overline{\operatorname{inv}_F}\ (\overline{c}\overline{d}) = \overline{\operatorname{inv}_F}\ \overline{c} + \overline{\operatorname{inv}_F}\ \overline{d}$.

We will now prove that the invariant map on regular cocycles satisfies the second condition of Axiom II.

Proposition 4.68. *Let K/F be a normal extension, and let $G_{K/F}$ be the Galois group. Let H be a subgroup of $G_{K/F}$ and denote by E the fixed field of H. Let $\overline{c} \in \overline{H}^2(G_{K/F}, C_K)$ be a regular cocycle. Then $\operatorname{Res}_E \overline{c}$ is also a regular cocycle and*

$$\overline{\operatorname{inv}_E} \operatorname{Res}_E \overline{c} = [E : F]\ \overline{\operatorname{inv}_F}\ \overline{c}.$$

Proof. Let L/K be an extension such that $\operatorname{Inf}_L \overline{c} = jc$ for some $c \in \hat{H}^2(G_{L/F}, J_L)$. By commutativity of the maps $\operatorname{Inf}, \operatorname{Res}$ and j we see that

$$\operatorname{Inf}_L \operatorname{Res}_E \overline{c} = \operatorname{Res}_E \operatorname{Inf}_L \overline{c} = \operatorname{Res}_E jc = j \operatorname{Res}_E c.$$

From this it follows that $\operatorname{Res}_E \overline{c}$ is also a regular cocycle and that we can assign to the cocycle $\operatorname{Res}_E \overline{c}$ a regular invariant map according to Definition 4.67. Now by Lemma 4.59 we see that

$$\operatorname{inv}_E \operatorname{Res}_E c = [E : F] \operatorname{inv}_F c$$

which proves the proposition since we know that assigning invariants is independent of chosen field extensions and representatives. □

Lemma 4.69. *Let K/F be a cyclic extension of degree n. Then there exists a regular cocycle class $\overline{c} \in \overline{H}^2(G_{K/F}, C_K)$ having invariant $1/n$.*

Proof. See [AT68, Chapter VII, Lemma 5]. □

Proposition 4.70. *Let K/F be a cyclic extension of degree n. The map*

$$j : \hat{H}^2(G_{K/F}, J_K) \to \hat{H}^2(G_{K/F}, C_K)$$

is surjective. This means that every cocycle class of C_K is regular. Moreover, for $\overline{c} \in \overline{H}^2(G_{K/F}, C_K)$ we have that $\overline{\mathrm{inv}_F}\ \overline{c} = 0$ if and only if $\overline{c} = 1$. Hence $\hat{H}^2(G_{K/F}, C_K)$ is cyclic of degree n.

Proof. Lemma 4.69 tells us that there exists a regular cocycle class $\overline{c} \in \overline{H}^2(G_{K/F}, C_K)$ which has $\overline{\mathrm{inv}_F}\ \overline{c} = 1/n$. From this we see that the powers of $\overline{c}$ form a cyclic group of order $\geq n$. Denote this group of powers of $\overline{c}$ by $B \subseteq \overline{H}^2(G_{K/F}, C_K)$. By Theorem 3.29, we know that for cyclic groups $G_{K/F}$, we have $\overline{H}^2(G_{K/F}, C_K) \cong C_F/N_{K/F}C_K$. However, the second inequality tells us that $(C_F : N_{K/F}C_K) \leq n$. Combining these arguments tells us that B contains all of $\overline{H}^2(G_{K/F}, C_K)$. Moreover, we see that for any integer m, if $\overline{\mathrm{inv}_F}\overline{c}^m = 0$ then $\overline{c}^m = 1$, which finishes our proof. □

Proposition 4.71. *Let K/F be a normal extension of degree n. Then all elements of $\hat{H}^2(G_{K/F}, C_K)$ are regular and $\hat{H}^2(G_{K/F}, C_K)$ is cyclic.*

Proof. Let F' be any cyclic extension of degree n over F (take for example a cyclic cyclotomic extension) and denote by L the compositum KF'. Let $\overline{c} \in \hat{H}^2(G_{F'/F}, C_{F'})$ such that $\overline{\mathrm{inv}_F}\ \overline{c} = 1/n$ (such a class exists by Lemma 4.69). By Lemma 4.57 we see that $\mathrm{Inf}_L\ \overline{c}'$ then also has invariant $1/n$, and by Proposition 4.68 we see that $\mathrm{Res}_K\ \mathrm{Inf}_L\ \overline{c}'$ then has invariant 0. Since L/K is cyclic, Lemma 4.69 tells us that $\mathrm{Res}_K\ \mathrm{Inf}_L\ \overline{c}' = 1$, which means that there exists $\overline{c} \in \hat{H}^2(G_{K/F}, C_K)$ such that $\mathrm{Inf}_L\ \overline{c}' = \mathrm{Inf}_L\ \overline{c}$.

Since $\mathrm{Inf}_L\ \overline{c}$ is a cocycle class of invariant $1/n$ that means that $\overline{c}$ is regular and has invariant $1/n$. The group generated by $\overline{c}$ is then cyclic of order $\geq n$. Again, the second inequality shows that the order of the group generated by $\overline{c}$ is exactly n. From this it follows that $\overline{H}^2(G_{K/F}, C_K) = \hat{H}^2(G_{K/F}, C_K)$ is cyclic of order n. □

Definition 4.72. Since all elements of $\hat{H}^2(G_{K/F}, C_K)$ are regular, we see that the domain of the regular invariant map was actually already all of $\hat{H}^2(G_{K/F}, C_K)$. We can therefore use the name *global invariant map* for the regular invariant map.

Now that we have a well-defined global invariant map, we are ready to prove that the global formation is indeed a class formation.

Theorem 4.73. *Let F be a global field, and Ω its separable closure. Denote by $\mathfrak{G}$ the Galois group of Ω/F. Then $(\mathfrak{G}, \{\mathfrak{G}_K\}; C_K)$ satisfies Axiom II and therefore is a class formation.*

Proof. Proposition 4.71 tells us that we can assign for each cocycle class $\overline{c} \in \hat{H}^2(G_{K/F}, C_K)$ an invariant $\overline{\mathrm{inv}_F}\ \overline{c} \in \mathbb{Q}/\mathbb{Z}$. This homomorphism is injective since we have that $\overline{\mathrm{inv}_F}\ \overline{c} = 0$ if and only if $\overline{c} = 1$. Since the assigned invariant of $\overline{c}$ is independent of the field L to which $\overline{c}$ can be inflated, we are allowed to assign invariants to all elements of $\hat{H}^2(\mathfrak{G}, C_\Omega)$. This map is surjective since there exist extensions of all degrees, and therefore we see that the map

$$\hat{H}^2(\mathfrak{G}, C_\Omega) \to \mathbb{Q}/\mathbb{Z}$$

is an isomorphism satisfying the requirements of Axiom II. □

Now that we have shown that the global formation is indeed a class formation, we can apply the Main Theorem of class field theory to get a global norm-residue map.

Theorem 4.74. *Let K/F be a finite extension of global fields and let $a \in C_F$ an idèle class, with $(a_\mathfrak{p})_\mathfrak{p} \in J_F$ any idèle that represents a. Then the norm-residue map is the surjective homomorphism*

$$\theta_{K/F} : C_F \to \mathrm{Gal}(K/F), \qquad a \mapsto (a, K/F) := \prod_{\mathfrak{p} \in \mathbb{P}_F} (a_\mathfrak{p}, K_\mathfrak{p}/F_\mathfrak{p}).$$

As a consequence, the global reciprocity isomorphism is the map

$$\omega_{K/F} : C_F/N_{K/F}C_K \to \mathrm{Gal}(K/F), \qquad a + N_{K/F}C_K \mapsto (a, K/F).$$

Proof. We start by noting that this product is well-defined, since almost all places $\mathfrak{p}$ are unramified, and $a_\mathfrak{p}$ is a unit for almost all places $\mathfrak{p}$. We need to show that for every character χ of $G_{K/F}$,

$$\chi((a, K/F)) = \chi(\prod (a_\mathfrak{p}, K_\mathfrak{p}/F_\mathfrak{p})).$$

We know that

$$\begin{aligned}(a, K/F) &= \mathrm{inv}(\overline{a} \cup \delta\chi) \\ &= \sum_\mathfrak{p} \mathrm{inv}_\mathfrak{p}(a_\mathfrak{p} \cup \delta\chi_\mathfrak{p})\end{aligned}$$

where $\chi_\mathfrak{p}$ is again $\mathrm{Res}_{G_\mathfrak{p}}\chi$ and we denote by $\overline{a}$ the class of a in $C_F/N_{K/F}C_K$. By Definition 4.47, we see that $\mathrm{inv}_\mathfrak{p}(a_\mathfrak{p} \cup \delta\chi_\mathfrak{p}) = \chi(a_\mathfrak{p}, K_\mathfrak{p}/F_\mathfrak{p})$. We thus have that

$$\mathrm{inv}(\overline{a} \cup \delta\chi) = \sum_{\mathfrak{p} \in \mathbb{P}_F} \chi(a_\mathfrak{p}, K_\mathfrak{p}/F_\mathfrak{p}) = \chi(\prod_\mathfrak{p} (a_\mathfrak{p}, K_\mathfrak{p}/F_\mathfrak{p}))$$

which finishes the proof. □

From Theorem 4.74 we see that the global norm-residue map is indeed induced by the map of Definition 4.56. We have already seen in Chapter 2 that our algorithm relies on knowledge of intermediate extensions $F \subseteq M \subseteq K$. We will now analyze the properties of these subextensions. First of all, we have the following important theorem, which is also called the existence theorem. We prove this only for geometric extensions, as this simplifies the proof quite a bit. For a full proof, see [AT68, Section VIII.3].

Theorem 4.75. *Let K be a global function field. Then the open subgroups of finite index of C_K are exactly the norm subgroups.*

Proof. We have to prove that any open subgroup of finite index is of the form $N_{L/K}C_L$ according to Definition 4.27. Let B be an open subgroup of finite index in C_K. Denote by $\theta_{L/K} : C_K \to \mathfrak{G}$ the norm-residue map and set $\mathfrak{h} = \theta_{L/K}(B)$. Since $\theta_{L/K}$ is a surjective homomorphism, we see that $(C_K : B) = (\mathfrak{G} : \mathfrak{h})$. Let L be the fixed field of $\mathfrak{h}$. Then we have $(C_K : B) = [L : K]$. By definition, we have that L is fixed under $\theta_{L/K}(N_{L/K}C_L)$, so we see that $\theta_{L/K}(N_{L/K}C_L) \subseteq \mathfrak{h}$ or equivalently, $N_{L/K}C_L \subseteq B$. Now the main theorem of class field theory tells us that $(C_K : N_{L/K}C_L) = [L : K]$ so from this we see that $(C_K : B) = [L : K] = (C_K : N_{L/K}C_L)$. Combining this with $N_{L/K}C_L \subseteq B$ gives the desired result. □

Combining this result with Theorem 4.30 gives us the following theorem.

Theorem 4.76. *For every open subgroup M of C_K of finite index, there exists an abelian extension E/K such that $M = N_{E/K}C_E$ and the reciprocity isomorphism induces an isomorphism between C_K/M and the Galois group of E/K.*

The goal of this chapter was to understand the isomorphism between idèle class groups and Galois groups. We have seen in Chapter 2 that having enough knowledge of this algorithm enables us to find field extensions with many rational places. We will now illustrate how the ramification behaviour of each place is related to the subgroups of J_K. In the next chapter, we will utilize this knowledge to construct an algorithm that finds many new records.

Theorem 4.77. *Let L/K be a finite abelian extension. Let $\mathfrak{p}$ be a place of K and $\mathfrak{q}$ a place of L lying above $\mathfrak{p}$. Let m be the smallest non-negative integer such that the m-th ramification group V_m of $L_\mathfrak{q}/K_\mathfrak{p}$ is trivial. Then the ramification degree of $\mathfrak{p}$ in L/K is $\psi_l'(m) = \psi_r'(m-1)$.*

Proof. We know by Theorem 1.53 that the order of the inertia group $G_T(\mathfrak{q}|\mathfrak{p})$ is exactly $e(\mathfrak{q}|\mathfrak{p})$. Moreover, we have seen that the inertia group of $\mathfrak{q}$ over $\mathfrak{p}$ is equal to the 0-th ramification group of the extension $L_\mathfrak{q}/K_\mathfrak{p}$ (see Definition 4.35). From this it follows that

$$e(\mathfrak{q}|\mathfrak{p}) = |V_0| = (V_0 : 1) = (V_0 : V_m).$$

Now by Proposition 4.40 we see that the slope of φ between $m-1$ and m is exactly $\frac{1}{(V_0:V_m)} = \frac{1}{e}$. We thus see that the left derivative of ψ at m is exactly $e(\mathfrak{q}|\mathfrak{p})$. We thus see that $e(\mathfrak{q}|\mathfrak{p}) = \psi_l'(m) = \psi_r'(m-1)$. □

Theorem 4.78. *Let M be an open subgroup of C_K of finite index. Let L/K be a finite abelian extension such that $N_{L/K}(C_L) = M$. Let be H the subgroup of J_K containing K^* such that $M = H/K^*$. Then for every place $\mathfrak{p}$ of K we have the following:*

1. *$\mathfrak{p}$ is unramified in $L/K \iff U_{K_\mathfrak{p}} \subseteq H$;*
2. *$\mathfrak{p}$ splits completely in $L/K \iff K_\mathfrak{p}^* \subseteq H$;*
3. *$\mathfrak{p}$ has ramification degree $\psi_l'((\psi(n)) \iff n$ is the smallest non-negative integer such that $U_{K_\mathfrak{p}}^{(n)} \subseteq H$.*

Proof. 1. By definition of the local norm-residue map (Theorem 4.48) we have that $\theta_{L_\mathfrak{q}/K_\mathfrak{p}}$ maps $U_{K_\mathfrak{p}} = U_{K_\mathfrak{p}}^{(0)}$ onto $V_{\psi(0)}(L_\mathfrak{q}/K_\mathfrak{p}) = V_0(L_\mathfrak{q}/K_\mathfrak{p}) = G_T(\mathfrak{q}|\mathfrak{p})$. We also know that $U_{K_\mathfrak{p}} \subseteq H$ if and only if the local norm residue map sends $U_{K_\mathfrak{p}}$ to $\{\mathrm{id}\}$ as H is the kernel of the global norm-residue map. We thus have that:

$$U_{K_\mathfrak{p}} \subseteq H \iff G_T(Q|P) = \{\mathrm{id}\} \iff \mathfrak{p} \text{ is unramified in } L/K$$

where the last implication follows from Theorem 1.55.

2. We know that the local norm residue map sends $K_\mathfrak{p}^*$ to $\mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p}) = G_Z(\mathfrak{q}|\mathfrak{p})$ since it is surjective. We thus have that

$$K_\mathfrak{p}^* \subseteq H \iff G_Z(\mathfrak{q}|\mathfrak{p}) = \{\mathrm{id}\} \iff \mathfrak{p} \text{ splits completely in } L/K$$

where again the last implication follows from Theorem 1.55

3. Let $\mathfrak{q}$ be a place of L lying above $\mathfrak{p}$. Theorem 4.43 tells us that $U_{K_\mathfrak{p}}^{(i)} \subseteq N_{L_\mathfrak{q}/K_\mathfrak{p}} L_\mathfrak{q}$ if and only if $V_{\psi(i)} = 1$. Let n be the smallest non-negative integer such that $U_{K_\mathfrak{p}}^{(n)} \subseteq N_{L_\mathfrak{q}/K_\mathfrak{p}} L_\mathfrak{q}$. Then we see that $V_{\psi(n)}$ is the first trivial ramification group. From Theorem 4.77 it then follows that the ramification degree of $\mathfrak{p}$ in L/K is $\psi_l'(\psi(n))$ if and only if $U_{K_\mathfrak{p}}^{(n)} \subseteq H$.

□

5 Ramified Extensions

In this chapter, we will show how global class field theory defined in the previous chapter can be used to create curves over finite fields with many rational points. We will start by proving Theorem 2.17 is indeed an isomorphism. After that, we will define a similar looking but slightly more complicated isomorphism that also takes into account ramified extensions. Once we have done that, we will construct an algorithm that finds ramified extensions with many rational places. Applying this algorithm to genus 2 hyperelliptic function fields gives the results stated in Table 5.4. We will finish this chapter by talking about the limitations of this algorithm and suggesting some directions for future research.

5.1 Unramified isomorphism

We start by investigating the relation between the idèle class group of a function field K and the divisor class group of K.

Theorem 5.1. *Let K be a function field. Then there exists a surjective homomorphism from the idèle class group C_K to the divisor class group* Cl_K.

Proof. We claim that the map sending

$$\prod (x_\mathfrak{p})_\mathfrak{p} \in J_K \mapsto \sum v_\mathfrak{p}(x_\mathfrak{p})\mathfrak{p} \in \mathrm{Cl}_K$$

is well-defined. By definition of idèles, only finitely many entries $x_\mathfrak{p}$ are allowed to have non-zero valuation. We see that it is surjective since every completion $K_\mathfrak{p}$ has a uniformizer, which we denote by $t_\mathfrak{p}$, and

$$(1, ...1, t_{\mathfrak{p}_1}^{n_{\mathfrak{p}_1}}, 1, ..., 1, t_{\mathfrak{p}_2}^{n_{\mathfrak{p}_2}}, 1, ..., 1, t_{\mathfrak{p}_j}^{n_{\mathfrak{p}_j}}, 1, ...) \mapsto \sum_{i=1}^{j} n_{\mathfrak{p}_i}\mathfrak{p}_i.$$

Now we also see that the idèles that correspond to elements of K^* are sent to the principal divisors. Taking the quotient by K^* thus gives a surjective homomorphism from the idèle class group to the divisor class group. □

In order to prove Theorem 2.17 we will have to look at the behaviour of subsets of C_K under this homomorphism. Once we have established which subgroups of the divisor class group correspond to which subgroups of the idèle class group, we can combine this with Theorem 4.74. This will then give us the desired isomorphism. We start with some definitions.

Definition 5.2. Let S be a non-empty finite set of places of a function field K. Then we define the following sets.

$$\begin{aligned} \mathrm{Div}_S &= \{\sum_{\mathfrak{p}\notin S} n_\mathfrak{p}\mathfrak{p} \mid n_\mathfrak{p} = 0 \text{ for almost all } \mathfrak{p}\}; \\ \mathrm{Princ}_S &= \{\sum_{\mathfrak{p}\notin S} v_\mathfrak{p}(z)\mathfrak{p} \mid z \in K^*\}; \\ \mathrm{Cl}_S &= \mathrm{Div}_S/\mathrm{Princ}_S. \end{aligned}$$

where we call Cl_S the *S-divisor class group.*

Proposition 5.3. *If $S = \{\mathfrak{p}\}$ for some place $\mathfrak{p}$ of degree d, then there exists an exact sequence*

$$0 \to \mathrm{Cl}_K^0 \to \mathrm{Cl}_S \to \mathbb{Z}/d\mathbb{Z} \to 0.$$

Proof. We start by defining a map

$$\theta : \mathrm{Div}^0(K) \to \mathrm{Cl}_S, \qquad \sum_{\mathfrak{q}} m_{\mathfrak{q}}\mathfrak{q} \mapsto \sum_{\mathfrak{q}\neq\mathfrak{p}} m_q\mathfrak{q} + \mathrm{Princ}_S.$$

Assume that two divisor classes $[\sum n_{\mathfrak{q}}\mathfrak{q}]$ and $[\sum m_{\mathfrak{q}}\mathfrak{q}]$ are sent to the same element in Cl_S. Then we see that $n_{\mathfrak{q}} = m_{\mathfrak{q}}$ for all $\mathfrak{q} \neq \mathfrak{p}$ and since we have $\sum_{\mathfrak{q}} n_q = \sum_{\mathfrak{q}} m_{\mathfrak{q}} = 0$ we see that $n_{\mathfrak{p}} = m_{\mathfrak{p}}$. From this it follows that θ is an injective homomorphism. Moreover, we see that the principal divisors in $\mathrm{Div}^0(K)$ are all sent to the identity in Cl_S. θ can therefore be seen as an injective map from $\mathrm{Cl}_K^0 \to \mathrm{Cl}_S$. We define the map

$$\phi : \mathrm{Cl}_S \to \mathbb{Z}/d\mathbb{Z}, \qquad \sum_{\mathfrak{q}\neq\mathfrak{p}} m_q\mathfrak{q} + \mathrm{Princ}_S \mapsto \sum_{\mathfrak{q}\neq\mathfrak{p}} m_{\mathfrak{q}} \deg(\mathfrak{q}) + d\mathbb{Z}.$$

We see that this map is surjective since the degree map is surjective by Proposition 1.18. Moreover, since the degree of a principal divisor is zero, and the degree of $\mathfrak{p}$ is d, we see that any principal S-divisor will be sent to the kernel by ϕ. We thus see that ϕ induces a surjective homomorphism

$$\phi : \mathrm{Cl}_S \to \mathbb{Z}/d\mathbb{Z}.$$

We see that $\ker(\phi) = \mathrm{Im}(\theta)$, which finishes the proof. □

Corollary 5.4. *If $S = \{\mathfrak{p}\}$ for some rational place $\mathfrak{p}$ then $\mathrm{Cl}_K^0 \cong \mathrm{Cl}_S$.*

A more general version of Proposition 5.3 is the following, whose proof can be found in [Ros73].

Definition 5.5. Let S be a finite set of places of a function field K. We use the following notation

$$\mathcal{D}(S) = \{\sum_{\mathfrak{p}\in S} n_{\mathfrak{p}}\mathfrak{p} \mid n_{\mathfrak{p}} = 0 \text{ for almost all } \mathfrak{p}\}, \qquad \mathcal{P}(S) = \mathrm{Princ}_K \cap \mathcal{D}(S);$$
$$\mathcal{D}_S = \{\sum_{\mathfrak{p}\notin S} n_{\mathfrak{p}}\mathfrak{p} \mid n_{\mathfrak{p}} = 0 \text{ for almost all } \mathfrak{p}\}, \qquad \mathcal{P}_S = \{\sum_{\mathfrak{p}\notin S} v_{\mathfrak{p}}(a)\mathfrak{p} \mid a \in K^*\}.$$

Theorem 5.6. *Let d be the smallest positive degree of a divisor in $\mathcal{D}(S)$ and i the smallest degree of a positive divisor in $\mathrm{Div}(K)$. Let C be a cyclic group of order d/i. Then the following sequence is exact.*

$$0 \to \mathcal{D}(S)^0/\mathcal{P}(S) \to \mathrm{Div}^0(K)/\mathrm{Princ}_K \to \mathcal{D}_S/\mathcal{P}_S \to C \to 0.$$

Corollary 5.7. *Let K be a function field and S a finite set of places. The S-divisor class group is a finite abelian group.*

We will now define some subsets of the idèle class group that turn out to correspond to the S-divisor class group.

Definition 5.8. Let S be a finite non-empty subset of $\mathbb{P}_K$. We define the ring

$$A_S = \{(a_\mathfrak{p})_\mathfrak{p} \in \prod_{\mathfrak{p}\in\mathbb{P}_K} K_\mathfrak{p} \mid v_\mathfrak{p}(a_\mathfrak{p}) \geq 0 \ \forall\ \mathfrak{p} \notin S\} = \prod_{\mathfrak{p}\in S} K_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} \mathcal{O}_{K_\mathfrak{p}}.$$

We see that A_S is a subset of A_K: in A_S it is determined beforehand which places are allowed to have negative valuations, whereas in A_K we only know that this is allowed for a finite number of places, but there is still a freedom to choose those places. A_S is called the *S-integral ring* of A_K. Similarly we define the *S-idèle group* and the *S-idèle class group*:

$$J_S = \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}\notin S} U_{K_\mathfrak{p}} \qquad \text{and} \qquad C_S = (K^* \cdot J_S)/K^*.$$

The S-idèle class group is a subgroup of the idèle class group, as can be seen from Definition 5.8. We also see that when the set S becomes larger, the idèle group J_S also becomes larger. When applying class field theory to this, we will see that this leads to smaller extensions.

Theorem 5.9. *Let K be a function field and S be a finite set of places of K. Then the map*

$$\varphi : C_K \to \mathrm{Cl}_S, \qquad [(\alpha_\mathfrak{p})_\mathfrak{p}] \mapsto [\sum_{\mathfrak{p}\notin S} v_\mathfrak{p}(\alpha_\mathfrak{p})\ \mathfrak{p}]$$

induces an isomorphism $C_K/C_S \cong \mathrm{Cl}_S$.

Proof. We start by proving that this map is well-defined. Let $[(\alpha_\mathfrak{p})_\mathfrak{p}] \in K^* \subseteq J_K$. We want to show that $\varphi[(\alpha_\mathfrak{p})_\mathfrak{p}]$ is the identity in Cl_S, meaning that it gets sent to the class of Princ_S. Since $\mathrm{Princ}_S = \{\sum_{\mathfrak{p}\notin S} v_\mathfrak{p}(z)\mathfrak{p} \mid z \in K^*\}$, we see that this condition is satisfied by definition. To see that the map is surjective, we note that for any element $\sum_{\mathfrak{p}_j\notin S} n_{\mathfrak{p}_j}\mathfrak{p}_j \in \mathrm{Div}_S$ we have that

$$\varphi((1,...,1,t_{\mathfrak{p}_1}^{n_{\mathfrak{p}_1}},1,...,1,t_{\mathfrak{p}_2}^{n_{\mathfrak{p}_2}},1,...,t_{\mathfrak{p}_m}^{n_{\mathfrak{p}_m}},1,....)) = \sum_{\mathfrak{p}_j\notin S} n_{\mathfrak{p}_j}\mathfrak{p}_j.$$

We thus see that φ is a well-defined and surjective map. All that is left is to show that the kernel of this map consists of C_S. We have that $C_S = (K^*\cdot J_S/K^*)$ so $C_K/C_S \cong J_K/K^*\cdot J_S$. We thus have to prove that the kernel of the map $J_K \to \mathrm{Cl}_S$ is exactly $K^*\cdot J_S$. We see that

$$K^*\cdot J_S = \{(\alpha_\mathfrak{p})_\mathfrak{p} \mid \alpha_\mathfrak{p} = \beta_\mathfrak{p}\cdot\gamma,\ v_\mathfrak{p}(\beta_\mathfrak{p}) = 0 \text{ for all } \mathfrak{p}\notin S,\ \gamma\in K^*\}.$$

From this it follows almost immediately that $K^*\cdot J_S$ is sent to the identity in the S-divisor class group, since the map sends

$$(\alpha_\mathfrak{p})_\mathfrak{p} \mapsto \sum_{\mathfrak{p}\notin S} v_\mathfrak{p}(\alpha_\mathfrak{p})\ \mathfrak{p} = \sum_{\mathfrak{p}\notin S} v_\mathfrak{p}(\beta_\mathfrak{p})\ \mathfrak{p} + \sum_{\mathfrak{p}\notin S} v_\mathfrak{p}(\gamma)\ \mathfrak{p} = 0 + \sum_{\mathfrak{p}\notin S} v_\mathfrak{p}(\gamma)\ \mathfrak{p} \in \mathrm{Princ}_S.$$

Moreover, we have that any idèle that is sent to the identity in the S-class group must be of this form, from which we see that the map induces an isomorphism $C_K/C_S \cong \mathrm{Cl}_S$. □

We can now prove Theorem 2.17, which we will state again for convenience.

Theorem 2.17. *Let K be a global function field. Then the map $\varphi_{\mathfrak{o}}$ sending*

$$\mathrm{Cl}_K^0 \to \mathrm{Gal}(K^{\mathfrak{o}}/K), \quad [\mathfrak{p} - \deg(\mathfrak{p})\mathfrak{o}] \mapsto \left(\frac{K^{\mathfrak{o}}|K}{\mathfrak{p}}\right)$$

is an isomorphism.

Proof. We first prove that if $S = \{\mathfrak{o}\}$, then C_S is indeed the subgroup of C_K that corresponds to an extension $K^{\mathfrak{o}}/K$ according to Theorem 4.76. Theorem 4.78 tells us that a place $\mathfrak{p}$ of K splits completely in the extension corresponding to a subgroup $H \subseteq J_K$ if and only if $K_{\mathfrak{p}}^* \subseteq H$. In our case, we have that $H = K^* \cdot J_S$. Since

$$J_S = J_{\{\mathfrak{o}\}} = K_{\mathfrak{o}}^* \times \prod_{\mathfrak{p} \neq \mathfrak{o}} U_{K_{\mathfrak{p}}},$$

we see that the only place that splits completely in the extension is $\mathfrak{o}$. Moreover, Theorem 4.78 tells us that a place $\mathfrak{p}$ of K if and only if $U_{K_{\mathfrak{p}}} \subseteq K$. From this it follows that all places of K are unramified in the extension, and thus that the extension of K that corresponds to C_S is exactly $K^{\mathfrak{o}}/K$.

We see that we can write any divisor class of degree zero as $[\sum n_{\mathfrak{p}}\mathfrak{p} - (\sum n_{\mathfrak{p}} \cdot \deg(\mathfrak{p}))\mathfrak{o}]$. Let us look at such a degree zero divisor class. Then the isomorphism of Proposition 5.3 sends this divisor class to the class $[\sum n_{\mathfrak{p}}\mathfrak{p}]$ in Cl_S, which will in turn be sent to the idèle class $[(\alpha_{\mathfrak{p}})_{\mathfrak{p}}]$ where $\alpha_{\mathfrak{p}} = t_{\mathfrak{p}}^{n_{\mathfrak{p}}}$ for all $\mathfrak{p} \neq \mathfrak{o}$, with $n_{\mathfrak{p}} = 0$ for almost all $\mathfrak{p}$. Now Theorem 4.74 tells us that the main isomorphism for global fields sends

$$(\alpha_{\mathfrak{p}})_{\mathfrak{p}} \in C_K \mapsto \prod_{\mathfrak{p} \in \mathbb{P}_F} (\alpha_{\mathfrak{p}}, (K^{\mathfrak{o}})_{\mathfrak{p}}/K_{\mathfrak{p}}).$$

We know that for unramified extensions,

$$(\alpha_{\mathfrak{p}}, (K^{\mathfrak{o}})_{\mathfrak{p}}/K_{\mathfrak{p}}) = \left(\frac{K^{\mathfrak{o}}|K}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})},$$

so the local norm residue map sends an element x of the local field $K_{\mathfrak{p}}$ to the $v_{\mathfrak{p}}(x)$-th power of the Artin symbol of $\mathfrak{p}$. From this it follows that the composition of the isomorphisms of Corollary 5.4, Theorem 5.9 and Theorem 4.74 gives an isomorphism

$$\mathrm{Cl}_K^0 \to \mathrm{Gal}(K^{\mathfrak{o}}/K), \qquad [\mathfrak{p} - \deg(\mathfrak{p})\mathfrak{o}] \mapsto \left(\frac{K^{\mathfrak{o}}|K}{\mathfrak{p}}\right).$$

□

For completeness, we recall the following fact.

Proposition 5.10. *Let K be a function field and $\mathfrak{o}$ a rational place of K. Let $\varphi_{\mathfrak{o}}$ be the map sending $\mathrm{Cl}_K^0 \to \mathrm{Gal}(K^{\mathfrak{o}}/K)$. Let G be a subgroup of Cl_K^0 and $\mathcal{G}$ the corresponding subgroup in $\mathrm{Gal}(K^{\mathfrak{o}}/K)$. Then a place $\mathfrak{p}_i$ splits completely in $(K^{\mathfrak{o}})^{\mathcal{G}}$ if and only if $[\mathfrak{p}_i - \deg(\mathfrak{p}_i)\mathfrak{o}] \in G$.*

Proof. This now follows immediately from Theorem 2.17 and Theorem 4.78. □

We will state one more fact about unramified extensions before looking at ramified extensions. We call the field that corresponds by Theorem 4.76 to the group C_K/C_S, the S - *Hilbert class field*, which we denote by H_S. This is the maximal unramified abelian extension in which the places in S split completely. For more information about the Hilbert class field in function fields, see [Ros87]. We will point out one property of Hilbert class fields. This property tells us that whenever the set S contains a rational place, or two places of coprime degree, then the S-Hilbert class field is a purely geometric extension. This explains why the extension $K^{\mathfrak{o}}$ from Chapter 2 was a purely geometric extension.

Proposition 5.11. *Let K be a function field with constant field $\mathbb{F}_q$ and let S be a finite set of places. Then the full constant field of the Hilbert class field is $\mathbb{F}_{q^d}$, where d is the greatest common divisor of the degrees of places in S.*

Proof. Denote by $\mathfrak{p}_1, ..\mathfrak{p}_k$ the places in S and denote by H_S the S-Hilbert class field. Recall that Theorem 1.54 tells us that if we denote by $T_{\mathfrak{p}}$ and $Z_{\mathfrak{p}}$ the fixed fields under the inertia group and decomposition group of a place $\mathfrak{p}$ of K, then the Hilbert class field can be written as

$$(\bigcap_{\mathfrak{p}_i \in S} Z_{\mathfrak{p}_i}) \cap (\bigcap_{\mathfrak{q} \notin S} T_{\mathfrak{q}}).$$

This means that for all places $\mathfrak{q} \notin S$, we have $e(\mathfrak{q}) = 1$ but not that $f(\mathfrak{q}) = 1$. However, for the places $\mathfrak{p}_i \in S$ we have that $e(\mathfrak{p}_i) = f(\mathfrak{p}_i) = 1$. This means that for all those places

$$1 = f(\mathfrak{p}_i) = \frac{\deg(\mathfrak{p}_i')}{\deg(\mathfrak{p}_i)} \cdot [k' : k],$$

where k' is the constant field of the S-Hilbert class field and $\mathfrak{p}_i'$ is a places in H_S lying above $\mathfrak{p}_i$. Since the Hilbert class field is the maximal abelian unramified extension in which the places in S split completely, $[k' : k]$ will attain the highest possible value. We see that $\deg(\mathfrak{p}_i) = \deg(\mathfrak{p}_i') \cdot [k' : k]$ for all places $\mathfrak{p}_i \in S$. From this it follows that $[k' : k]$ is the greatest common divisor of the degrees of the places of S. □

5.2 Ramified isomorphism

In this subsection, we will state an isomorphism similar to Theorem 2.17, that also takes into account ramified extensions. Ideally, we would talk about ramified extensions of a function field K where no place is forced to split completely. However, Proposition 5.11 tells us that the full constant field of the maximal unramified field extension in which some places are forced to split completely is d, the greatest common divisor of the degrees of those places. Continuing that thought, we see that if we require none of the places of K to split completely, the field that we will work with has an infinitely large constant field. This is undesirable for two reasons. First of all, the theory that we established in Chapter 4 is written in terms of Tate cohomology groups, which means that it is only valid for finite groups. In order to create finite Galois groups, we have to work with subgroups H of C_K of finite index. Therefore, we do not gain any practical advances when extending our theory to infinite extensions. On the other hand, we have seen in Chapter 2 that the rational places that split completely in the extension are exactly those that provide rational places in the extension field. This means that for our purposes it is actually favourable to look at extensions in which we demand that at least one place splits completely, if we choose that place to be rational. An additional benefit of this construction is that we work with only

geometric extensions, which simplifies our proofs a bit and makes sure that we stay in the constant field $\mathbb{F}_q$.

Let us start with a couple of definitions. We will start by defining an analogue to the divisor class group, which is called the ray divisor class group.

Definition 5.12. Let $D = \sum n_\mathfrak{p}\mathfrak{p}$ be an effective divisor of a function field K. We say that an element $x \in K^*$ is *equivalent to 1 mod D*, denoted by $x \equiv 1 \mod D$, if

$$\text{for all } \mathfrak{p} \in \operatorname{supp}(D),\ v_\mathfrak{p}(x) = 0 \text{ and } v_\mathfrak{p}(x-1) \geq n_\mathfrak{p}.$$

We see that when $v_\mathfrak{p}(x-1) \geq n_p$, x is an element of the function field that resembles the identity locally very closely. If that is true for all places in the support of the divisor D, that means that x lies very close to 1 modulo D, which motivates the notation $x \equiv 1 \mod D$

Definition 5.13. Let D be an effective divisor of a function field K. We define the following sets.

$$\begin{aligned}
\mathcal{I}(D) &= \{ \sum_{\mathfrak{p} \in \mathbb{P}_K} n_\mathfrak{p}\mathfrak{p} \mid n_\mathfrak{p} = 0 \text{ if } \mathfrak{p} \in \operatorname{supp}(D)\};\\
\mathcal{P}(D) &= \{ \sum_{\mathfrak{p} \in \mathbb{P}_K} v_\mathfrak{p}(z)\mathfrak{p} \mid z \equiv 1 \mod D\};\\
\mathrm{Cl}_D &= \mathcal{I}(D)/\mathcal{P}(D).
\end{aligned}$$

where we call Cl_D the *ray divisor class group modulo D*.

Just like with the divisor class group, we can define the degree zero part of the ray divisor class group, which we will denote by Cl_D^0.

Proposition 5.14. *Let D be an effective divisor of a function field K. Then Cl_D^0 is a finite abelian group.*

Proof. See [Ros02, p. 139]. □

The ray divisor class group, just like the divisor class group, is something that MAGMA can compute. We are therefore looking for an isomorphism between subsets of the ray divisor class group and the Galois group of certain abelian extensions. We will proceed analogously to the previous section to create such an isomorphism. We will start by defining the S-ray class group modulo D. We will always assume that the support of a divisor D lies outside of the set S. The reason for that is the following. We want the places of S to split completely in an extension and we will see that the places in D are exactly the places that are allowed to ramify. As Theorem 1.54 tells us that demanding that a place splits completely is a stronger requirement than allowing it to ramify, we see that putting places of S in the support of the divisor D makes no sense.

Definition 5.15. Let S be a finite non-empty subset of $\mathbb{P}_K$ and D be a divisor such that $\operatorname{supp}(D) \cap S = \emptyset$. Denote by $T = S \cup \operatorname{supp}(D)$. Then we define

$$\mathrm{Div}_{D,S} = \{\sum_{\mathfrak{p} \notin T} n_\mathfrak{p}\mathfrak{p} \mid n_\mathfrak{p} = 0 \text{ for almost all } \mathfrak{p}\};$$

$$\mathrm{Princ}_{D,S} = \{\sum_{\mathfrak{p} \notin S} v_\mathfrak{p}(z)\mathfrak{p} |\ z \in K^*,\ z \equiv 1 \mod D\};$$

$$\mathrm{Cl}_{D,S} = \mathrm{Div}_{D,S}/\mathrm{Princ}_{D,S}.$$

We call $\mathrm{Cl}_{D,S}$ the *S-ray class group modulo D*.

We see that when $D = 0$, we get exactly the definition of the S-class group, i.e. $\mathrm{Cl}_{0,S} = \mathrm{Cl}_S$. The proof of the following proposition is completely analogous to that of Proposition 5.3.

Proposition 5.16. *Let K be a function field, S a subset of places of K and D an effective divisor with support outside of S. If S consists of only one place $\mathfrak{p}$ of degree d, then we have a short exact sequence*

$$0 \to \mathrm{Cl}_D^0 \to \mathrm{Cl}_{D,S} \to \mathbb{Z}/d\mathbb{Z} \to 0.$$

Corollary 5.17. *Let D be an effective divisor and $S = \{\mathfrak{p}\}$ for some rational place $\mathfrak{p}$ of a function field K. Then the map*

$$\theta : \mathrm{Cl}_D^0 \to \mathrm{Cl}_{D,S},\ [\sum_{q} n_{\mathfrak{q}}\mathfrak{q}] \mapsto [\sum_{\mathfrak{q}\neq\mathfrak{p}} n_{\mathfrak{q}}\mathfrak{q}]$$

is an isomorphism.

Now let D be an effective divisor of K and let S be a finite subset of $\mathbb{P}_K$ such that $\mathrm{supp}(D) \cap S = \emptyset$. We can then define the following subgroups of the idèle (class) group.

Definition 5.18. Let S be a finite subset of $\mathbb{P}_K$ and let $D = \sum n_{\mathfrak{p}}\mathfrak{p}$ be a positive divisor with $\mathrm{supp}(D) \cap S = \emptyset$. We define the *S-congruence subgroup modulo D* by

$$J_S^D = \prod_{\mathfrak{p}\in S} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\notin S} U_{K_{\mathfrak{p}}}^{(n_{\mathfrak{p}})}.$$

We define the corresponding class group by $C_S^D = (K^* \cdot J_S^D)/K^*$.

We see that for all places that are not in the support of D, this definition is locally equivalent to the definition of J_S. However, for the places that are in the support of the divisor, we see that only a subset of the unit group is part of the S-idèle group modulo D. The following theorem gives the relation between the S-ray class group modulo D and the S-congruence class group.

Theorem 5.19. *Let S be a finite set and $D = \sum m_{\mathfrak{p}}\ \mathfrak{p}$ be an effective divisor with $\mathrm{supp}(D) \cap\ S = \emptyset$. Let $T = \mathrm{supp}(D) \cup\ S$. The following map is an isomorphism:*

$$\varphi : C_K/C_S^D \to \mathrm{Cl}_{D,S}, \qquad [(x_{\mathfrak{p}})] \mapsto [\sum_{\mathfrak{p}\notin T} v_{\mathfrak{p}}(y_{\mathfrak{p}})\ \mathfrak{p}].$$

Proof. We first define the following set:

$$J^D = \{(x_{\mathfrak{p}}) \in J_K \mid x_{\mathfrak{p}} \in U_{K_{\mathfrak{p}}}^{(m_{\mathfrak{p}})} \text{ for all } \mathfrak{p} \in \mathrm{supp}(D)\}.$$

We claim that $J_K = K^* \cdot J^D$. Clearly $K^* \cdot J^D \subseteq J_K$. To prove the other inclusion, let $(x_{\mathfrak{p}}) \in J_K$ be any idèle. One can use the strong approximation theorem (Theorem 1.12) to find an element $z \in K^*$ such that $v_{\mathfrak{p}}(x_{\mathfrak{p}}z - 1) \geq m_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{supp}(D)$. We then see that $(z)(x_{\mathfrak{p}}) \in J^D$ and moreover that $(x_{\mathfrak{p}}) = (z^{-1})(z)(x_{\mathfrak{p}}) \in K^*J^D$. We may thus conclude $J_K = K^* \cdot J^D$ and we can write any idèle $(x_{\mathfrak{p}}) \in J_K$ as $(z)(y_{\mathfrak{p}}) \in K^* \cdot J^D$.

The map that will give us the desired isomorphism is the following:

$$\varphi : C_K \to \mathrm{Cl}_{D,S} \qquad [(x_\mathfrak{p})] \mapsto [\sum_{\mathfrak{p}\notin T} v_\mathfrak{p}(y_\mathfrak{p})\ \mathfrak{p}].$$

We will prove that this map is a surjective homomorphism with kernel C_S^D. First, we show that this map is a well-defined group homomorphism. Every idèle of the form (x) for some $x \in K^*$ will have $(y_\mathfrak{p}) = \mathrm{id}$ and therefore $v_\mathfrak{p}(y_\mathfrak{p}) = 0$ for all $\mathfrak{p} \in T$. This means that K^* is sent to the identity by φ, thus φ is well-defined. Next, we note that the map is surjective. Let $D' = \sum n_\mathfrak{p}\mathfrak{p} \in \mathrm{Div}_{D,S}$. Then we know $n_\mathfrak{p} = 0$ for all $\mathfrak{p} \in \mathrm{supp}(D)$. Therefore any idèle class $[(x_\mathfrak{p})]$ with $v_\mathfrak{p}(x_\mathfrak{p}) = n_p$ for all $\mathfrak{p} \notin S$ will be mapped onto $[D']$.

To finish this proof, we need to show that the kernel of φ is exactly C_S^D. We start by showing that $\ker(\varphi) \subseteq C_S^D$. By definition,

$$J_S^D = \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}\notin S} U_{K_\mathfrak{p}}^{(m_\mathfrak{p})}.$$

This means that $x_\mathfrak{p} \in U_{K_\mathfrak{p}}$ for $\mathfrak{p} \notin T$. From this we see that $v_\mathfrak{p}(x_\mathfrak{p}) = 0$ for any $(x_\mathfrak{p}) \in J_S^D$. We thus see that any class in C_S^D will be sent to the zero class in $\mathrm{Cl}_{D,S}$ and thus $C_S^D \subseteq \ker(\varphi)$.

On the other hand, let $[(x_\mathfrak{p})]$ be a divisor class that is sent to the principal S-divisor class modulo D. We will show that $(x_\mathfrak{p}) \in J_S^D$. We have seen that we can write $(x_\mathfrak{p}) = (z)(y_\mathfrak{p})$ for some $z \in K^*, (y_\mathfrak{p}) \in J^D$. Now saying that $[(x_\mathfrak{p})]$ is sent to $\mathrm{Princ}_{D,S}$ is equivalent to saying that there exists some $u \in K^* \cap J^D$ such that

$$v_\mathfrak{p}(u) = v_\mathfrak{p}(y_\mathfrak{p}) \text{ for all } \mathfrak{p} \notin T.$$

Let us look at the idèle $(w_\mathfrak{p}) = (u^{-1})(y_\mathfrak{p})$. We see that for places $\mathfrak{p} \notin T$ we have that $v_\mathfrak{p}(u) = v_\mathfrak{p}(y_\mathfrak{p})$. Therefore $v_\mathfrak{p}(w_\mathfrak{p}) = 0$, and $w_\mathfrak{p} \in U_{K_\mathfrak{p}}$. For places in the support of D, we see that $y_\mathfrak{p} \in U_{K_\mathfrak{p}}^{(m_\mathfrak{p})}$ by definition, since $(y_\mathfrak{p}) \in J^D$. On the other hand, we have that

$$v_\mathfrak{p}(u^{-1} - 1) = v_\mathfrak{p}(u^{-1}) + v_\mathfrak{p}(1 - u) = -v_\mathfrak{p}(u) + v_\mathfrak{p}(u - 1) \geq m_p,$$

where $v_\mathfrak{p}(u) = 0$ by Definition 5.12. From this it follows that for all $\mathfrak{p} \in \mathrm{supp}(D)$ we have that $u \cdot y_\mathfrak{p} \in U_{K_\mathfrak{p}}^{(m_\mathfrak{p})}$, and we see that $(w_p) = (u)(y_\mathfrak{p}) \in J_S^D$. Now we see that $[(x_\mathfrak{p})]K^* = [(w_p)]K^*$ and therefore we conclude that $(x_\mathfrak{p}) \in C_S^D$. We have thus seen that

$$[(x_\mathfrak{p})] \in \ker(\varphi) \iff (x_\mathfrak{p}) \in C_S^D,$$

which concludes our proof. □

Proposition 5.20. *Let S be a finite set of places of K and D a divisor with $\mathrm{supp}(D) \cap S = \emptyset$. Then C_S^D is a subgroup of finite index in C_K.*

Proof. We have seen in Proposition 5.16 that whenever S consists of one finite place, $\mathrm{Cl}_{D,S}$ is finite. Requiring another place to split completely will only make the divisor group smaller. Theorem 5.19 tells us that C_K/C_S^D is isomorphic to $\mathrm{Cl}_{D,S}$, and as $\mathrm{Cl}_{D,S}$ is a finite group, C_S^D has finite index in C_K. □

We can now characterize the field extensions that correspond to this subgroup of the idèle class group under the reciprocity law isomorphism.

Definition 5.21. Let S be a finite set of places of K and D a divisor with $\mathrm{supp}(D) \cap S = \emptyset$. Then Proposition 5.20 tells us that C_S^D is a subgroup of finite index in C_K and therefore by Theorem 4.76 there exists an extension E such that $C_K/C_S^D \cong \mathrm{Gal}(E/K)$. We call this extension the *S-ray class field modulo D*, and denote it by K_S^D. We say that D is the *conductor* of the field E.

Theorem 5.22. *The S-ray class field modulo D is the maximal abelian extension such that*

1. *The places in S split completely;*
2. *The places in the support of D ramify with ramification degree $\psi_l'(\psi(n_\mathfrak{p}))$;*
3. *All other places are unramified.*

Proof. This follows immediately from Theorem 4.78. □

Let us now look at the situation where S consists of only one rational place $\mathfrak{o}$. We have seen that in that case we have an isomorphism

$$\theta : \mathrm{Cl}_D^0 \to \mathrm{Cl}_{D,S}, \qquad [\sum_\mathfrak{p} n_\mathfrak{p}\mathfrak{p} - \sum_\mathfrak{p} n_\mathfrak{p} \deg(\mathfrak{p})\mathfrak{o}] \mapsto [\sum_{\mathfrak{p}\neq\mathfrak{o}} n_\mathfrak{p}\mathfrak{p}].$$

Since we also have an isomorphism

$$\varphi : C_K/C_S^D \to \mathrm{Cl}_{D,S}, \qquad [(x_\mathfrak{p})] \mapsto [\sum_{\mathfrak{p}\in T} v_\mathfrak{p}(y_\mathfrak{p})\ \mathfrak{p}],$$

we can look at $\varphi^{-1} \circ \theta$, which gives us an isomorphism

$$\mathrm{Cl}_D^0 \to C_K/C_S^D,$$
$$[\sum_{i=i}^m n_{\mathfrak{p}_i}\mathfrak{p}_i - \sum_{i=1}^m n_{\mathfrak{p}_i} \deg(\mathfrak{p}_i)\mathfrak{o}] \mapsto [(1, ..., 1, t_{\mathfrak{p}_1}^{n_{\mathfrak{p}_1}}, 1, ..., 1, t_{\mathfrak{p}_2}^{n_{\mathfrak{p}_2}}, 1, ..., 1, t_{\mathfrak{p}_m}^{n_{\mathfrak{p}_m}}, 1, ...).$$

Theorem 5.23. *Let K be a function field, $\mathfrak{o}$ a rational place of K and $S = \{\mathfrak{o}\}$. Let D be a divisor such that $\mathfrak{o}$ is not in the support of D. Combining the map $\varphi^{-1} \circ \theta : \mathrm{Cl}_D^0 \to C_K/C_S^D$ with the reciprocity law isomorphism gives a map*

$$\psi : \mathrm{Cl}_D^0 \to \mathrm{Gal}(K_S^D/K).$$

Let G be a subgroup of Cl_D^0. Denote by $\mathcal{G}$ the corresponding subgroup in $\mathrm{Gal}(K_S^D/K)$ and let $E = (K_S^D)^\mathcal{G}$ be the corresponding intermediate extension. Let $H \subseteq \mathcal{I}(D)$ such that $G = H/\mathcal{P}(D)$. Then

1. *a place $\mathfrak{p}$ splits completely in E/K if and only if $[\mathfrak{p} - \deg(\mathfrak{p})\mathfrak{o}] \in G$;*
2. *E has conductor $D' \leq D$ if and only if*

$$\{\sum_{\mathfrak{p}\neq\mathfrak{o}} v_\mathfrak{p}(z)\mathfrak{p} \mid z \equiv 1 \mod D'\} \subseteq H.$$

Proof. 1. We know from Theorem 4.78 that in the isomorphism $C_K/M \to \mathrm{Gal}(L/K)$ a place $\mathfrak{p}$ splits completely if and only if $K_\mathfrak{p} \subseteq H$, where $M = H/K^*$. We see that under the isomorphism $\varphi^{-1} \circ \theta$, the generator of $K_\mathfrak{p}$, which is the idèle $(1, ..., 1, t_\mathfrak{p}, 1, ...)$ gets sent to $[\mathfrak{p} - \deg(\mathfrak{p})\mathfrak{o}]$. From this it follows that $K_\mathfrak{p} \subseteq H \iff [\mathfrak{p} - \deg(\mathfrak{p})\mathfrak{o}] \in G$. Therefore we see that $\mathfrak{p}_i$ splits completely in E/K if and only if $[\mathfrak{p} - \deg(\mathfrak{p})\mathfrak{o}] \in G$.

2. For the second statement, we see that

$$\mathrm{Cl}_D^0 = \mathcal{I}^0(D)/\mathcal{P}(D) = \frac{\{\sum_{\mathfrak{p}\in\mathbb{P}_K} n_{\mathfrak{p}}\mathfrak{p} \mid n_{\mathfrak{p}} = 0 \text{ if } \mathfrak{p} \in \mathrm{supp}(D),\ \sum n_{\mathfrak{p}} \deg(\mathfrak{p}) = 0\}}{\{\sum_{\mathfrak{p}\in\mathbb{P}_K} v_{\mathfrak{p}}(z)\mathfrak{p} \mid z \equiv 1 \mod D\}}.$$

Now if we take the quotient of Cl_D^0 with the set

$$\frac{\{\sum_{\mathfrak{p}\neq\mathfrak{o}} v_{\mathfrak{p}}(z)\mathfrak{p} \mid z \equiv 1 \mod D'\}}{\{\sum_{\mathfrak{p}\neq\mathfrak{o}} v_{\mathfrak{p}}(z)\mathfrak{p} \mid z \equiv 1 \mod D\}}$$

we see that we get exactly $\mathrm{Cl}_{D'}^0$. Theorem 5.19 then tells us that D' is the conductor of the intermediate field E.

□

5.3 Construction of the algorithm

In this section, we will show how we use the information above to construct an algorithm that finds ramified extensions fields with many rational places. The constant fields of these function fields are $\mathbb{F}_q$ with q prime between 5 and 13.

Let k be a finite field of cardinality q. We want to create an input set of suitable genus 2 function fields. As genus 2 function fields are always hyperelliptic, we can create a list of polynomials $f \in k(x)$ such that the function field $k(x,y)/(y^2 - f)$ is well-defined. In practice this means that we make a list containing separable degree 5 (and 6) polynomials with coefficients in k. If the hyperelliptic function field has enough rational places, we add the defining polynomial to the set `polmanyplaces`. We run the algorithm for each of these hyperelliptic function fields.

Just like in the unramified algorithm, we first need to create the auxiliary sets `Results` and `set`. This goes analogously to the construction in Chapter 2, apart from adding a divisor `1*pl1[3]` to the tuples in `set`. This is needed to ensure that the tuples in `set` are of the right type to save all needed information.

For each function field, we create a suitable set of divisors. Since every function field has infinitely many places, and therefore infinitely many divisors, one needs to specify a set of conditions. For example, for a function field K we can consider the set

$$\texttt{D2plus3} := \{1 \cdot \mathfrak{p}_2 + 1 \cdot \mathfrak{p}_3 \mid \mathfrak{p}_2, \mathfrak{p}_3 \in \mathbb{P}_K, \deg(\mathfrak{p}_2) = 2,\ \deg(\mathfrak{p}_3) = 3\}$$

consisting of all divisors that are the sum of a degree two and a degree three place.

For each of the divisors in this set we compute the ray divisor class group modulo D and its degree zero part Cl_D^0. We then compute the subgroups of Cl_D^0 of index less than 50. Once that is done, we run almost the same algorithm as in the unramified case, but with a few modifications. First of all, in unramified extensions we can use Hurwitz' genus formula together with Dedekind's different formula to immediately see $g' = d(g-1)+1$, where d is the index of the subgroup and g the genus of the ground field. Since we are working with ramified extensions now, Dedekind's different theorem does not provide such a

simple formula and we need to compute the genus explicitly. Secondly, in ramified extensions, it is no longer true that all rational places in the extension field come from rational places in the ground field that split completely. They can also come from rational places in the ground field that ramify completely (See Theorem 1.35). We avoided this situation by not putting any rational places in the divisor, but this is an important point nevertheless.

We will now dive into some more technical details of the algorithm. Most importantly, this algorithm is a lot more time-consuming to run than the unramified algorithm. This is mainly due to the fact that it runs over a large set of divisors for each hyperelliptic function field. This is why we let this algorithm run only over genus 2 function fields; the algorithm already took over a week to run over all irreducible polynomials over $\mathbb{F}_{13}$ that had coefficient 1 in front of its degree 9 and degree 8 terms. Another reason is that it has to compute the genus of each abelian extension explicitly, which is quite time-consuming already for small genera.

We tried to reduce this issue by running on a 20 CPU computer. In order to do so, we created a function that had as input a hyperelliptic polynomial, and as output a list containing for $1 \leq g \leq 50$ the highest number of rational places found in a function field of genus g, together with the data to reconstruct that function field (see Appendix). This was feasible, since the input set for the ramified algorithm consisted of a few thousand polynomials. Defining a function like this enabled us to run the algorithm in parallel, which speeds up the computation by a factor 20. The reason why we did not create a separate function to run in parallel for the unramified algorithm, where we worked with degree 9 polynomials, was that the input set there could easily consist of more than 10 million polynomials. Using a function means that you get an output for each polynomial in the input set. As this output consists of up to 50 tuples of a genus, a number of places, a divisor, a subgroup and a rational place, this will use too much storage when running over more than 10 million polynomials.

Let us look at what the output of the ramified algorithm tells us. The following was a small part of the output when running over genus 2 ground fields over $\mathbb{F}_7$.

```
36,  100,
<
y^2 + 6*x^5 + 2*x^4 + 5*x^3 + x^2 + 6,

(x + 5),

Abelian Group isomorphic to Z/42
Defined on 1 generator in supergroup:
$.1 = 20*$.1
Relations:
42*$.1 = 0,

(1/x, 1/x^3*y)
>
```

This output tells us the following. Most importantly, there exists a function field of genus 36 that has 100 rational places, a new record! How can we reconstruct this function field? We see that it is created as a field extension of the function field with defining

polynomial $y^2 + 6x^5 + 2x^4 + 5x^3 + x^2 + 6$. This function field has ray divisor class group modulo the degree 2 divisor $1 \cdot (x+5)$ isomorphic to $\mathbb{Z}/840\mathbb{Z}+\mathbb{Z}$. First, we take the degree zero part which corresponds to demanding that one fixed rational place S splits completely. This leaves us with a S-ray class group modulo D isomorphic to $\mathbb{Z}/840\mathbb{Z}$. Taking the subgroup isomorphic to $\mathbb{Z}/42\mathbb{Z}$ and looking at the fixed field of the $(1/x, 1/x^3y)$-ray class field modulo $(x + 5)$ gives a degree 20 field extension. We can check that this field extension indeed has genus 36 and 100 rational places in the following way.

First, we want to discover which places split completely in the extension that gives us 100 rational points. The reason for this is that for each index d, there exist different subgroups of the ray class group of that index. Although these subgroups are isomorphic, they give non-isomorphic field extensions. We can illustrate this difference as follows. If we ask MAGMA to check the number of rational places of the extension that we get using the output, we get the following.

```
A:=AbelianExtension(set[36][2], set[36][3]+Z);
Genus(A);
NumberOfPlacesOfDegreeOne(A);

36
20
```

We see that this extension has genus 36, but only 20 rational places, although our algorithm told us that it should have 100 rational places. This happens because MAGMA does not know which of the isomorphic subgroups of index 20 it needs to choose. We can force MAGMA to choose the subgroup that we want as follows. First, we make a list of those divisors that split completely in the extension that we are given.

```
for i in [1..#pl1] do
    D:= g(pl1[i]-pl1[1]);
    if D in S then
        print i;
    end if;
end for;

1
4
5
8
9
```

Using this, we can ask MAGMA for the subgroup that is completely generated by the image of those places in the ray class group. The map g sends the group of divisors to the ray class group. Using this subgroup (which is isomorphic to the subgroup taken above, but not equal), we can then form the corresponding abelian extension. Once we have done that, we can ask MAGMA to compute its genus and its number of rational points.

```
CC:=sub<C | g(pl1[1]), g(pl1[4]), g(pl1[5]), g(pl1[8]), g(pl1[9])>;
A:=AbelianExtension(set[36][2], CC);
Genus(A);
```

```
NumberOfPlacesOfDegreeOne(A);

36
100
```

This time, we do get a function field with 100 rational places and genus 36. At the moment of writing, there is no lower bound known at `manypoints.org`. The criterion for a lower bound to be accepted is that it is at least $\frac{U_g(q)-q-1}{\sqrt{2}}+q+1$ where $U_g(q)$ is the current best known upper bound. In the case of $g = 36, q = 7$ we have $U_g(q) = 117$. We thus see that the minimal lower bound is 86, and since our function field has 100 rational places this is clearly an improvement of the current situation.

5.4 Results and discussion

We will first state a table with all new records. We only added the results that are still records when we take into account the results from Chapter 2.

finite field	**genus**	**number of rational places**	**previous bound**
$\mathbb{F}_7$	8	36	35 - 38
$\mathbb{F}_7$	15	56	52 - 60
$\mathbb{F}_7$	16	56	55* - 63
$\mathbb{F}_7$	29	80	... - 98
$\mathbb{F}_7$	36	100	... - 117
$\mathbb{F}_7$	50	112	... - 152
$\mathbb{F}_{11}$	7	48	44 - 50
$\mathbb{F}_{11}$	13	64	60 - 77
$\mathbb{F}_{11}$	21	84	80 - 110
$\mathbb{F}_{11}$	22	96	91* - 114
$\mathbb{F}_{11}$	23	96	88 - 119
$\mathbb{F}_{11}$	24	96	92 - 123
$\mathbb{F}_{11}$	26	105	... - 131
$\mathbb{F}_{11}$	29	112	... - 142
$\mathbb{F}_{11}$	31	120	110* - 149
$\mathbb{F}_{11}$	34	132	121* - 160
$\mathbb{F}_{11}$	41	144	... - 185
$\mathbb{F}_{11}$	43	144	... - 192
$\mathbb{F}_{11}$	47	168	... - 206
$\mathbb{F}_{13}$	14	77	65 - 91
$\mathbb{F}_{13}$	19	96	90 - 115
$\mathbb{F}_{13}$	27	126	... - 152
$\mathbb{F}_{13}$	28	126	117* - 156
$\mathbb{F}_{13}$	40	168	156* - 207
$\mathbb{F}_{13}$	46	180	... - 231

Table 2: Records found using the ramified algorithm
* these are bounds that we found using the unramified algorithm in Chapter 2.

We have found these records by letting the algorithm run over the following sets.

1. Genus 2 over $\mathbb{F}_7$ with all irreducible degree 5 polynomials with at least 8 rational places and divisors consisting of 1 degree 2 or degree 3 place;

2. Genus 2 over $\mathbb{F}_7$ with all separable degree 5 polynomials with at least 8 rational places and divisors consisting of 1 degree 2 place;

3. Genus 2 over $\mathbb{F}_{11}$ with irreducible degree 5 polynomials with at least 12 rational places and divisors consisting of 1 degree 2 or degree 3 place. Ran over 1112 of the 3652 polynomials of this form.

4. Genus 2 over $\mathbb{F}_{11}$ with 430 separable degree 5 polynomials with at least 12 rational places and divisors consisting of 1 degree 2 place. All polynomials were of the form $x^5 + a_4x^4 + a_3x^3 + a_2x^2 + x$.

5. Genus 2 over $\mathbb{F}_{13}$ with all separable degree 5 polynomials of the form $x^5 + x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ where a_0 is either 0 or 1. These polynomials corresponded to function fields with at least 14 rational places. The divisors consisted of 1 degree 2 place

We see that the ramified algorithm gives a lot of records that cannot be found using the unramified algorithm. The ramified algorithm has several advantages over the unramified algorithm.

The first advantage is that the ramified algorithm creates extensions of all genera. The genus of the unramified algorithm is always of the form $d \cdot (g-1) + 1$, when g is the genus of the ground field. As we can see from the results on the previous page, the ramified algorithm gives records for many genera. Moreover, when looking at the output sets, we see that almost all genera were reached by the ramified algorithm.

As the unramified experiment has already been carried out for ground fields of genus 2 and 3 in [Rök12] and [Sol15] respectively, it is very likely that not many more records will be found this way. For hyperelliptic genus 4 function fields over finite field of cardinality less than 7, almost all results that can be found this way are found in this thesis. Running the unramified algorithm over larger input sets with separable polynomials of degree 9 or 10 over finite field with cardinality 11 of 13 might give some more records. One can also run the unramified algorithm over genus 5 polynomials, but this will only give possible records for genera that are 1 mod 4.

Moreover, we expect that the ramified algorithm can be used to find many more records, if more computer power becomes available. This is mainly due to the fact that this algorithm has only been run over a very small part of the (infinitely large) possible input set. First of all, for most cases it was not possible to run over all degree 5 polynomials that had enough rational places. Moreover, we did not even consider the degree 6 polynomials that correspond to genus 2 function fields. Even more importantly, we only considered genus 2 function fields. Considering the amount of records we found using this set, it is quite likely that running this algorithm over genus 3 function fields will give a lot of new records. But the most significant cut that we made is to only consider divisors consisting of one degree 2 place. When looking at the records found in [Rök13], we see that the divisors that generate the records are of different forms. All divisors that generated records there had degree larger than two, most of the time consisting of multiple places. If we compare those results

to ours, this leads to promising prospects. Considering the fact that only running over divisors consisting of one degree 2 place already lead to many new records, it is quite reasonable to expect that running the ramified algorithm over a larger set of divisors will give many more records. We can then also use Theorem 5.23 to control the ramification degree of the intermediate extensions. Unfortunately computers are not yet powerful enough to work with such large sets (input sets easily consist of 10 billion polynomials). However, once these computers do exist and become available to mathematicians, this would be a good place to start further research.

To conclude this discussion, we share one final observation. Whenever a record was found, it was found multiple times, quite often hundreds of times. This implies that there exists some kind of symmetry in the set of extensions. After analyzing the data, no direct relation has been found between the sets that generated the same record. It is not true in general that ground fields that produce a record for one genus have the same result for the other genera, nor are there any obvious relations between their defining polynomials. As we have not found an explanation for this phenomenon in the literature, this might be another interesting direction for future research.

6 Appendix

6.1 Unramified algorithm

We will start by writing down the unramified algorithm. Below is the code used for the algorithm that considered genus 4 function fields over $\mathbb{F}_5$. As this input set was still relatively small, the algorithm ran over all separable polynomials of both degree 9 and 10 whose corresponding function fields had many places.

```
k:=GF(5);
R<x> := PolynomialRing(k);
P<y> := PolynomialRing(R);
lijst9:=[ [a,b,c,d,e,f,g,h,i]:  a in k, b in k, c in k, d in k, e in k, f in k,
    g in k, h in k, i in k ];

poli459 :=[];
for i in [1..#lijst9] do
    f:= (x^9+lijst9[i][1]*x^8+lijst9[i][2]*x^7+lijst9[i][3]*x^6+lijst9[i][4]*x^5+
        lijst9[i][5]*x^4+lijst9[i][6]*x^3+lijst9[i][7]*x^2+ lijst9[i][8]*x+
        lijst9[i][9]);
    if IsSeparable(f) then
        Append(~poli459, f);
    end if;
end for;

k:=GF(5);
R<x> := PolynomialRing(k);
P<y> := PolynomialRing(R);
lijst10:=[ [a,b,c,d,e,f,g,h,i,j]: a in k, b in k, c in k, d in k, e in k,
    f in k, g in k, h in k, i in k, j in k ];

poli4510 :=[];
for i in [1..#lijst10] do
    f:= (x^10+ lijst10[i][10]*x^9+lijst10[i][1]*x^8+lijst10[i][2]*x^7+
        lijst10[i][3]*x^6+lijst10[i][4]*x^5+lijst10[i][5]*x^4+lijst10[i][6]*x^3+
        lijst10[i][7]*x^2+lijst10[i][8]*x+lijst10[i][9]);
    if IsSeparable(f) then
        Append(~poli4510, f);
    end if;
end for;

poli45:= poli459 cat poli4510;

polmanyplaces45:=[];
for i in [1..#poli45] do
    k:=GF(5);
    R<x> := PolynomialRing(k);
    P<y> := PolynomialRing(R);
    L<y> := FunctionField(y^2-poli45[i]);
```

```
    if #Places(L,1) gt 8 then
        Append(~polmanyplaces45, poli45[i]);
    end if;
end for;

% We now have a set of polynomials that correspond to function fields with
  at least 9 rational places

k:=GF(5);
R<x> := PolynomialRing(k);
P<y> := PolynomialRing(R);
h:= polmanyplaces45[1];
L<y> := FunctionField(y^2-h);
pl:=Places(L,1);
C, f, g:=ClassGroup(L);
l:=Ngens(C);
G:=Generators(C);
GG:=Exclude(G, C.l);
C0:= sub< C | GG>;
CC:=Subgroups(C0);
S:= CC[2]`subgroup;
m:=<h, S, pl[3]>;

% The tuple m that we create here is a place holder that is created so
  that when we create "set", the elements are of the right type.
% The chosen subgroup and rational place are completely random.
% "set" will store the defining polynomial, subgroup of the divisor class group
  and place that splits completely that give the record.

for i in [1..100] do
    Results[i]:= 0;
end for;
set:=[* *];
for i in [1..100] do
    Append(~set, m);
end for;

for b in [1..#polmanyplaces45] do
    k:=GF(5);
    R<x> := PolynomialRing(k);
    P<y> := PolynomialRing(R);
    L<y> := FunctionField(y^2-polmanyplaces45[b]);
    pl:=Places(L,1);
    C, f, g:=ClassGroup(L);
    l:=Ngens(C);
    G:=Generators(C);
    GG:=Exclude(G, C.l);
    C0:= sub< C | GG>;
```

```
    CC:=Subgroups(C0);
    for i in [2..#CC-1] do
        S:= CC[i]`subgroup;
        T:= Index(C0, S);
        if T lt 17 then
            for j in [1..#pl] do;
                kk:=0;
                for a in [1..#pl] do;
                    D:= g(pl[a]-pl[j]);
                    if (D in S) then
                        kk:=kk+1;
                    end if;
                 end for;
                 l:= kk*T;
                 x:= 3*T+1;
                 if Results[x] lt l then
                     Results[x]:= l;
                     set[x]:= <polmanyplaces45[b], S, pl[j]>;
                 end if;
            end for;
        end if;
    end for;
    if b eq 1 mod 1000 then
        for i in [1..50] do
            if Results[i] gt 0 then
                PrintFileMagma( "res45.m", <i, Results[i], set[i]>);
            end if
        end for;
    end if;
end for;

% The command above is to save the results in a file. If the algorithm
  stops halfway, this way we still have most of the valuable information.
% To immediately see all results after the algorithm has finished,
  we print them here as well.

for i in [1..50] do
    if Results[i] gt 0 then
        print <i, Results[i], set[i]>;
    end if;
end for;
```

We will now give a list of the information necessary to verify the results in Table 2.4. Note that in all cases the place that splits completely is the infinite place. This might seem a bit suspicious, but it is in fact very well explainable. When the algorithm runs over all possible candidates for the rational place $\mathfrak{o}$, it uses the order that MAGMA produces them in. When listing rational places in MAGMA, the first rational place is always the infinite place. In the example in Chapter 2.4 for $q = 5,\ g = 34,\ N = 77$ we see that places

1,2,3,6,7,10 and 11 split completely. Any of these places can fulfill the role of $\mathfrak{o}$ in this case. However, our algorithm is built in such a way that only the first place that gives a high number of rational places is saved. This set is only overwritten when a higher number of places is found, which is why it makes sense that the places that we encounter as $\mathfrak{o}$ are often the infinite ones. When looking at the results of the ramified algorithm, we will encounter some records that do not have the infinite place as the place that splits completely.

For some subgroups, we have written down the generators. We do this whenever multiple isomorphic subgroups exist. For example, in the case of the record for genus 46 over $\mathbb{F}_{11}$, there are 18 different subgroups of the degree zero class group that are isomorphic to $\mathbb{Z}/1935\mathbb{Z}$. By writing down these generators one can easily see which subgroup provides the new record.

$\mathbb{F}_7$	$g = 16,\ N = 55$
polynomial	$y^2 + 6*x^9 + 4*x^8 + 5*x^7 + 1*x^6 + 6*x^5 + 2*x^3 + 5*x^2 + 6*x + 6$
subgroup	$\mathbb{Z}/1661\mathbb{Z}$
$\mathfrak{o}$	$(1/x, 1/x^5 * y)$

$\mathbb{F}_7$	$g = 28,\ N = 81$
polynomial	$y^2 + 6*x^9 + 3*x^8 + 6*x^7 + 5*x^6 + 2*x^5 + 2*x^4 + 5*x^3 + 6*x^2 + 6$
subgroup	$\mathbb{Z}/795\mathbb{Z}$
$\mathfrak{o}$	$(1/x, 1/x^5 * y)$

$\mathbb{F}_7$	$g = 31,\ N = 90$
polynomial	$y^2 + 6*x^9 + 6*x^8 + 5*x^7 + 5*x^6 + 5*x^4 + 2*x^3 + 3*x^2 + 3*x$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/260\mathbb{Z},\quad X.1 = C0.1,\ X.2 = C0.2 + 5*C0.3$
$\mathfrak{o}$	$(1/x, 1/x^5 * y)$

$\mathbb{F}_7$	$g = 34,\ N = 99$
polynomial	$y^2 + 6*x^9 + 6*x^8 + 5*x^7 + 5*x^6 + 2*x^5 + 5*x^4 + 2*x^3 + 4*x^2 + 5*x$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/42\mathbb{Z}$
$\mathfrak{o}$	$(1/x, 1/x^5 * y)$

$\mathbb{F}_7$	$g = 37,\ N = 108$
polynomial	$y^2 + 6*x^9 + 6*x^8 + 4*x^7 + 5*x^6 + 4*x^5 + 4*x^4 + 1*x^2 + 3*x$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/42\mathbb{Z}$
	$X.1 = C0.2,\ X.2 = C0.1,\ X.3 = 3*C0.4,\ X.4 = 2*C0.5$
$\mathfrak{o}$	$(1/x, 1/x^5 * y)$

$\mathbb{F}_7$	$g = 43,\ N = 112$
polynomial	$y^2 + 6*x^9 + 6*x^8 + 5*x^7 + 3*x^6 + 2*x^5 + 6*x^4 + 4*x^3 + 6*x^2 + 5*x + 6$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/162\mathbb{Z},\quad X.1 = C0.1,\ X.2 = C0.2 + 7*C0.3$
$\mathfrak{o}$	$(1/x, 1/x^5 * y)$

$\mathbb{F}_7$	$g = 46,\ N = 120$
polynomial	$y^2 + 6*x^9 + 6*x^8 + 5*x^7 + 1*x^6 + 1*x^5 + 4*x^4 + 6*x^2 + 5*x$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/42\mathbb{Z}$
$\mathfrak{o}$	$(1/x, 1/x^5 * y)$

$\mathbb{F}_7$	$g = 49,\ N = 128$
polynomial	$y^2 + 6*x^9 + 6*x^8 + 5*x^7 + 2*x^6 + 3*x^5 + 6*x^4 + 4*x^3 + 6*x^2 + 2*x$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/34\mathbb{Z}$
	$X.1 = C0.1,\ X.2 = C0.2,\ X.3 = C0.3,\ X.4 = 16*C0.4$
o	$(1/x, 1/x^5*y)$

$\mathbb{F}_{11}$	$g = 16,\ N = 75$
polynomial	$y^2 + 10*x^9 + 10*x^8 + 9*x^7 + 2*x^6 + 3*x^5 + 5*x^4 + 5*x^3 + 8*x^2 + 9*x + 2$
subgroup	$\mathbb{Z}/7823\mathbb{Z}$
o	$(1/x, 1/x^5*y)$

$\mathbb{F}_{11}$	$g = 22,\ N = 91$
polynomial	$y^2 + 10*x^9 + 10*x^8 + 9*x^7 + 7*x^6 + x^5 + x^4 + 3*x^3 + 3*x^2 + 10$
subgroup	$\mathbb{Z}/6177\mathbb{Z}$
o	$(1/x, 1/x^5*y)$

$\mathbb{F}_{11}$	$g = 25,\ N = 104$
polynomial	$y^2 + 10*x^9 + 10*x^8 + 6*x^6 + 7*x^5 + 5*x^4 + 1*x^3 + 7*x^2 + 10*x + 10$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$,
	$X.1 = C0.12,\ X.2 = C0.1 + C0.3,\ X.3 = C0.3 + C0.4 + 2*C0.5$
o	$(1/x, 1/x^5*y)$

$\mathbb{F}_{11}$	$g = 31,\ N = 120$
polynomial	$y^2 + 10*x^9 + 10*x^8 + 10*x^6 + 10*x^5 + 6*x^4 + 6*x^3 + 4*x^2 + 7*x$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/1390\mathbb{Z},\quad X.1 = C0.1,\ X.2 = 9*C0.2 + 2*C0.3$
o	$(1/x, 1/x^5*y)$

$\mathbb{F}_{11}$	$g = 34,\ N = 121$
polynomial	$y^2 + 10*x^9 + 10*x^8 + 10*x^7 + 3*x^6 + 5*x^5 + 8*x^4 + 5*x^3 + 10*x + 10$
subgroup	$\mathbb{Z}/2015\mathbb{Z}$
o	$(1/x, 1/x^5*y)$

$\mathbb{F}_{11}$	$g = 37,\ N = 132$
polynomial	$y^2 + 10*x^9 + 10*x^8 + 6*x^6 + 7*x^5 + 5*x^4 + 6*x^3 + 3*x^2 + 10*x$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/254\mathbb{Z}$
	$X.1 = C0.1,\ X.2 = C0.3,\ X.3 = C0.4,\ X.4 = C0.2 + 6*C0.5$
o	$(1/x, 1/x^5*y)$

$\mathbb{F}_{11}$	$g = 40,\ N = 143$
polynomial	$y^2 + 10*x^9 + 10*x^8 + 9*x^6 + 4*x^5 + 1*x^4 + 6*x^3 + +6*x^2 + 7*x + 7$
subgroup	$\mathbb{Z}/7\mathbb{Z} + \mathbb{Z}/273\mathbb{Z}$
o	$(1/x, 1/x^5*y)$

$\mathbb{F}_{11}$	$g = 43,\ N = 168$
polynomial	$y^2 + 10*x^9 + 10*x^8 + 9*x^6 + 6*x^5 + 2*x^4 + 4*x^3 + 4*x^2 + 9*x$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/434\mathbb{Z}$,
	$X.1 = C0.1,\ X.2 = 7*C0.2,\ X.3 = 12*C0.2 + 2*C0.3$
o	$(1/x, 1/x^5*y)$

$\mathbb{F}_{11}$	$g = 46,\ N = 165$
polynomial	$y^2 + 10 * x^9 + 10 * x^8 + 2 * x^7 + 8 * x^5 + 2 * x^4 + 3 * x^3 + 6 * x^2 + 9 * x + 2$
subgroup	$\mathbb{Z}/1935\mathbb{Z},\quad X.1 = 9 * C0.1 + 1162 * C0.2$
o	$(1/x, 1/x^5 * y)$

$\mathbb{F}_{11}$	$g = 49,\ N = 176$
polynomial	$y^2 + 10 * x^9 + 10 * x^8 + 10 * x^6 + 6 * x^5 + 5 * x^4 + 8 * x^3 + 9 * x^2 + 10 * x$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/200\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$
	$X.1 = C0.2,\ X.2 = C0.1,\ X.3 = C0.3 + C0.4,\ X.4 = C0.3 + 8 * C0.5$
o	$(1/x, 1/x^5 * y)$

$\mathbb{F}_{13}$	$g = 22,\ N = 112$
polynomial	$y^2 + 12 * x^9 + 12 * x^8 + 12 * x^6 + 5 * x^5 + 4 * x^4 + 2 * x^3 + 2 * x + 2$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/1704\mathbb{Z}$
	$X.1 = C0.1,\ X.2 = C0.2 + 2 * C0.3,\ X.3 = C0.3 + 3406 * C0.4,$
o	$(1/x, 1/x^5 * y)$

$\mathbb{F}_{13}$	$g = 28,\ N = 117$
polynomial	$y^2 + 12 * x^9 + 12 * x^8 + 12 * x^7 + 9 * x^4 + 12 * x^3 + 9 * x^2 + 4 * x + 9$
subgroup	$\mathbb{Z}/4905\mathbb{Z}$
o	$(1/x, 1/x^5 * y)$

$\mathbb{F}_{13}$	$g = 31,\ N = 130$
polynomial	$y^2 + 12 * x^9 + 12 * x^8 + 12 * x^6 + 7 * x^5 + 5 * x^4 + 3 * x^3 + 11 * x + 2$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/1780\mathbb{Z}$
	$X.1 = C0.1,\ X.2 = 5 * C0.3$
o	$(1/x, 1/x^5 * y)$

$\mathbb{F}_{13}$	$g = 34,\ N = 143$
polynomial	$y^2 + 12 * x^9 + 12 * x^8 + 12 * x^6 + 2 * x^5 + 3 * x^4 + 5 * x^3 + 8 * x^2 + 10 * x + 4$
subgroup	$\mathbb{Z}/4\mathbb{Z} + \mathbb{Z}/1216\mathbb{Z}$
o	$(1/x, 1/x^5 * y)$

$\mathbb{F}_{13}$	$g = 37,\ N = 156$
polynomial	$y^2 + 12 * x^9 + 12 * x^8 + 12 * x^6 + 7 * x^5 + 8 * x^4 + 7 * x^2 + 9 * x + 2$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2034\mathbb{Z}$
	$X.1 = 3 * C0.3,\ X.2 = C0.2 + C0.4$
o	$(1/x, 1/x^5 * y)$

$\mathbb{F}_{13}$	$g = 40,\ N = 156$
polynomial	$y^2 + 12 * x^9 + 12 * x^8 + 12 * x^6 + 10 * x^5 + 8 * x^4 + 3 * x^3 + 1 * x^2 + 12 * x + 4$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/522\mathbb{Z}$
o	$(1/x, 1/x^5 * y)$

$\mathbb{F}_{13}$	$g = 49,\ N = 192$
polynomial	$y^2 + 12 * x^9 + 12 * x^8 + 12 * x^6 + 1 * x^5 + 7 * x^4 + 5 * x^3 + 6 * x^2 + 6 * x + 4$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/432\mathbb{Z}$
	$X.1 = C0.1,\ X.2 = C0.2,\ X.3 = 2 * C0.3,\ X.4 = 8 * C0.4$
o	$(1/x, 1/x^5 * y)$

6.2 Ramified algorithm

For the unramified algorithm, the big obstacle was that we had to run our relatively fast algorithm over an extremely large set of polynomials. For the ramified algorithm, the set of polynomials stays a lot smaller, since we consider only degree 5 or 6 polynomials as we are looking at genus 2 function fields (which are always hyperelliptic), but the algorithm itself takes a lot more time per polynomial. The reason behind this is the fact that for each polynomial, a set of divisors is formed and the algorithm has to be executed for each of those divisors. Therefore it is necessary to run this algorithm on multiple cores, since otherwise the running time becomes unreasonably large. As we only store at most 50 results per polynomial, and in practice only about 10 results per polynomial, this does not take up too much memory.

In the algorithm below we first create a set of polynomials to run the algorithm over. We then define a function that has as input a polynomial of degree 5 over $\mathbb{F}_{13}$, and as output a list that consists of tuples with the genus, the number of rational places and the necessary information to verify that outcome for each integer $2 \leq i \leq 50$ such that `Results[i]` is non-zero. Once that function is defined, we can run it on a number of cores. In this case, it could be run on a computer with 20 cores. The i-th core took as input the polynomials that were on an entry that was equivalent to i mod 20. The algorithms took several days to run, with over 1 day for $\mathbb{F}_7$ and about 10 days for $\mathbb{F}_{13}$.

```
    k:=GF(13);
R<x> := PolynomialRing(k);
P<y> := PolynomialRing(R);
lijst5:=[ [1,b,c,d,e,f]: b in k, c in k, d in k, e in k, f in k];
poli5 :=[];

for i in [1..#lijst5] do
    f:= (x^5+lijst5[i][2]*x^4+lijst5[i][3]*x^3+lijst5[i][4]*x^2+
        lijst5[i][5]*x+lijst5[i][6]);
    if IsSeparable(f) then
        Append(~poli5, f);
    end if;
end for;

polmanyplaces213 :=[* *];
for i in [1..#poli5] do
    k:=GF(13);
    R<x> := PolynomialRing(k);
    P<y> := PolynomialRing(R);
    L<y> := FunctionField(y^2-poli5[i]);
    if #Places(L,1) gt 17 then
        Append(~polmanyplaces213, poli5[i]);
    end if;
end for;

k:=GF(13);
R<x> := PolynomialRing(k);
```

```
P<y> := PolynomialRing(R);
L<y> := FunctionField(polmanyplaces213[1]);
pl:=Places(L,1);
C, f, g:=ClassGroup(L);
l:=Ngens(C);
G:=Generators(C);
GG:=Exclude(G, C.l);
C0:= sub< C | GG>;
CC:=Subgroups(C0);
S:= CC[2]`subgroup;
m:=<polmanyplaces213[1], 1* pl[3], S, pl[3]>;

% We again create the tuple m to construct "set" with, so that the elements
  of the tuple are of the right type.
% Below, we create the list "D23" that consists of all divisors of
  the form 1*pl, for some degree 2 or 3 place pl.

ramalgfct:=function(b);
    k:=GF(13);
    R<x> := PolynomialRing(k);
    P<y> := PolynomialRing(R);
    L := FunctionField(b);
    pl1:= Places(L,1);
    pl2:=Places(L,2);
    pl3:=Places(L,3);
    pl23:= pl2 cat pl3;
    D23:=[];
    for i in [1..#pl23] do
        D:= 1*pl23[i];
        Append(~D23, D);
    end for;
    Results:= [1..150];
    for i in [1..150] do
        Results[i]:= 0;
    end for;
    set:=[* *];
    for i in [1..150] do
        Append(~set, m);
    end for;
    for k in [1..#D23] do
        Div:=D23[k];
        C, f:=RayClassGroup(Div);
        g:= Inverse(f);
        l:= Ngens(C);
        G:= Generators(C);
        GG:= Exclude(G, C.l);
        C0:= sub< C | GG>;
        CC:=Subgroups(C0);
```

```
        Z:= sub<C | C.1>;
        for i in [1..#CC] do
            Ci:=CC[i]`subgroup;
            T:= Index(C0, Ci);
            if T lt 50 then
                for j in [1..#pl1] do
                    kk:=0;
                    for a in [1..#pl1] do
                        D0:=g(pl1[a]-pl1[j]);
                        if D0 in Ci then
                            kk:=kk+1;
                        end if;
                    end for;
                    l:= kk*T;
                    A:=AbelianExtension(Div, Ci +Z);
                    x:= Genus(A);
                    if Results[x] lt l then
                        Results[x]:= l;
                        set[x]:= <b, Div, Ci, pl1[j]>;
                    end if;
                end for;
            end if;
        end for;
    end for;
    final:=[];
    for i in [1..50] do
        if Results[i] gt 0 then
            Append(~final, <i, Results[i], set[i]>);
        end if;
    end for;
    return final;
end function;
```

We will state the necessary information to verify all results from Table 5.4. Note that in most cases, the place that splits completely is still the infinite place, but there are also some cases where a different place leads to a record. See the records over $\mathbb{F}_{11}$ for genus 7, 21 and 23.

$\mathbb{F}_7$	$g = 8,\ N = 36$
polynomial	$y^2 + 6 * x^5 + 3 * x^4 + 6 * x^3 + 6 * x^2 + 5 * x + 6$
divisor	$1 * (x + 6)$
subgroup	$\mathbb{Z}/216\mathbb{Z}\ \ X.1 = 2 * C0.1 + 109 * C0.2$
$\mathfrak{o}$	$(1/x, 1/x^3 * y)$

$\mathbb{F}_7$	$g = 15,\ N = 56$
polynomial	$y^2 + 6 * x^5 + 3 * x^4 + 3 * x^3 + 4 * x^2 + 5 * x + 6$
divisor	$1 * (x + 5)$
subgroup	$\mathbb{Z}/108\mathbb{Z}\ \ X.1 = C0.1 + 220 * C0.2$
$\mathfrak{o}$	$(1/x, 1/x^3 * y)$

$\mathbb{F}_7$	$g = 16,\ N = 56$
polynomial	$y^2 + 6 * x^5 + 3 * x^4 + 5 * x^3 + 5 * x^2 + 6$
divisor	$1 * (x + 4)$
subgroup	$\mathbb{Z}/108\mathbb{Z}\ \ X.1 = 7 * C0.1 + 85 * C0.2$
o	$(1/x, 1/x^3 * y)$

$\mathbb{F}_7$	$g = 29,\ N = 80$
polynomial	$y^2 + 6 * x^5 + 2 * x^4 + 3 * x^3 + 4 * x^2 + 6 * x$
divisor	$1 * (x + 2)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/10\mathbb{Z}\ \ X.1 = C0.1, X.2 = C0.2, X.3 = 16 * C0.3$
o	$(1/x, 1/x^3 * y)$

$\mathbb{F}_7$	$g = 36,\ N = 100$
polynomial	$y^2 + 6 * x^5 + 4 * x^4 + 6 * x^3 + 1 * x^2 + 3$
divisor	$1 * (x + 3)$
subgroup	$\mathbb{Z}/42\mathbb{Z}$
o	$(1/x, 1/x^3 * y)$

$\mathbb{F}_7$	$g = 50,\ N = 112$
polynomial	$y^2 + 6 * x^5 + 5 * x^4 + 2 * x^3 + 2 * x^2 + 4 * x$
divisor	$1 * (x + 4)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/10\mathbb{Z}\ \ X.1 = C0.1, X.2 = 18 * C0.2$
o	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{11}$	$g = 7,\ N = 48$
polynomial	$y^2 + 10 * x^5 + 9 * x^4 + 1 * x^3 + 9 * x^2 + 10 * x$
divisor	$1 * (x^2 + 10 * x + 1, y)$
subgroup	$\mathbb{Z}/4\mathbb{Z} + \mathbb{Z}/8\mathbb{Z} + \mathbb{Z}/24\mathbb{Z},\ X.1 = C0.2,\ X.2 = C0.1 + C.03,$ X.3=C.01+2*C.04
o	$(x + 7, y + 1)$

$\mathbb{F}_{11}$	$g = 13,\ N = 64$
polynomial	$y^2 + 10 * x^5 + 2 * x^4 + 8 * x^3 + 10 * x$
divisor	$1 * (x + 5)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/30\mathbb{Z}$
o	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{11}$	$g = 21,\ N = 84$
polynomial	$y^2 + 10 * x^5 + 6 * x^4 + 9 * x^3 + 10 * x$
divisor	$1 * (x^2 + x + 6, y + 5 * x + 9)$
subgroup	$\mathbb{Z}/216\mathbb{Z},\ X.1 = C0.1 + 292 * C0.2$
o	$(x + 7, y + 4)$

$\mathbb{F}_{11}$	$g = 22,\ N = 96$
polynomial	$y^2 + 10 * x^5 + 6 * x^4 + 7 * x^3 + 10 * x$
divisor	$1 * (x + 3)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/36\mathbb{Z},\ X.1 = C0.2,\ X.2 = C0.1 + 22 * C0.2,$ X.3=C0.3 + 105*C0.4
o	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{11}$	$g = 23,\ N = 96$
polynomial	$y^2 + 10 * x^5 + 1 * x^4 + 8 * x^3 + 4 * x^2 + 10 * x$
divisor	$1 * (x + 6)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/48\mathbb{Z},\ X.1 = C0.2 + 3 * C0.3,\ X.2 = C0.1,\ X.3 = 2 * C0.4$
o	$(x + 7, y + 3)$

$\mathbb{F}_{11}$	$g = 24,\ N = 96$
polynomial	$y^2 + 10 * x^5 + 5 * x^4 + 10 * x^3 + 10 * x$
divisor	$1 * (x + 9)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/38\mathbb{Z},\ X.1 = C0.2,\ X.2 = C0.1,\ X.3 = C0.3 + 6 * C0.4$
o	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{11}$	$g = 26,\ N = 105$
polynomial	$y^2 + 10 * x^5 + 9 * x^4 + 9 * x^3 + 10 * x$
divisor	$1 * (x + 7)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/32\mathbb{Z},\ X.1 = C0.2,\ X.2 = C0.1,\ X.3 = 15 * C0.3$
o	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{11}$	$g = 29,\ N = 112$
polynomial	$y^2 + 10 * x^5 + 6 * x^4 + 7 * x^3 + 10 * x$
divisor	$1 * (x + 1)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/54\mathbb{Z},\ X.1 = C0.1,\ X.2 = C0.3 + 4 * C0.4$
o	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{11}$	$g = 31,\ N = 120$
polynomial	$y^2 + 10 * x^5 + 1 * x^4 + 2 * x^3 + 7 * x^2 + 10 * x$
divisor	$1 * (x^2 + 7 * x + 9, y + 2 * x + 8)$
subgroup	$\mathbb{Z}/132\mathbb{Z},\ X.1 = 10 * C0.2$
o	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{11}$	$g = 34,\ N = 132$
polynomial	$y^2 + 10 * x^5 + 4 * x^4 + 3 * x^3 + 8 * x^2 + 10 * x$
divisor	$1 * (x + 9)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/6\mathbb{Z}$
o	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{11}$	$g = 41,\ N = 144$
polynomial	$y^2 + 10 * x^5 + 9 * x^4 + 5 * x^3 + 9 * x^2 + 10 * x$
divisor	$1 * (x + 6)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/48\mathbb{Z},\ X.1 = 3 * C0.2 + 96 * C0.3,\ X.2 = C0.1 + 5 * C0.2 + 12 * C0.3$
o	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{11}$	$g = 43,\ N = 144$
polynomial	$y^2 + 10 * x^5 + 6 * x^4 + 7 * x^3 + 10 * x$
divisor	$1 * (x + 3)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/18\mathbb{Z},\ X.1 = C0.2 + 96 * C0.3,\ X.2 = 2 * C0.3,$ X.3=C0.1 + 12*C0.4
o	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{11}$	$g = 47,\ N = 168$
polynomial	$y^2 + 10 * x^5 + 5 * x^4 + 8 * x^3 + 2 * x^2 + 10 * x$
divisor	$1 * (x + 2)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/36\mathbb{Z},\ X.1 = C0.1,\ X.2 = 9 * C0.2 + 2 * C0.3$
$\mathfrak{o}$	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{13}$	$g = 14,\ N = 77$
polynomial	$y^2 + 12 * x^5 + 6 * x^4 + 11 * x^3 + 9 * x^2 + 11 * x + 12$
divisor	$1 * (x + 1)$
subgroup	$\mathbb{Z}/602\mathbb{Z},\ X.1 = 5 * C0.1 + 431 * C0.2$
$\mathfrak{o}$	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{13}$	$g = 19,\ N = 96$
polynomial	$y^2 + 12 * x^5 + 12 * x^4 + 2 * x^3 + 2 * x^2 + 12 * x$
divisor	$1 * (x + 9)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/70\mathbb{Z},\ X.1 = C0.2,\ X.2 = C0.1,\ X.3 = C0.3 + 6 * C0.4$
$\mathfrak{o}$	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{13}$	$g = 27,\ N = 126$
polynomial	$y^2 + 12 * x^5 + 12 * x^4 + 7 * x^3 + 10 * x^2 + 12 * x$
divisor	$1 * (x + 5)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/4\mathbb{Z} + \mathbb{Z}/32\mathbb{Z},\ X.1 = C0.1,\ X.2 = C0.2,\ X.3 = 14 * C0.3$
$\mathfrak{o}$	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{13}$	$g = 28,\ N = 126$
polynomial	$y^2 + 12 * x^5 + 3 * x^4 + 9 * x^3 + 5 * x^2 + 12x$
divisor	$1 * (x + 4)$
subgroup	$\mathbb{Z}/253\mathbb{Z}$
$\mathfrak{o}$	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{13}$	$g = 27,\ N = 126$
polynomial	$y^2 + 12 * x^5 + 3 * x^4 + 9 * x^3 + 5 * x^2 + 0 * x + 12x$
divisor	$1 * (x + 4)$
subgroup	$\mathbb{Z}/253\mathbb{Z}$
$\mathfrak{o}$	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{13}$	$g = 40,\ N = 168$
polynomial	$y^2 + 12 * x^5 + 12 * x^4 + 12 * x^3 + 2 * x^2 + 5 * x$
divisor	$1 * (x + 7)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/70\mathbb{Z},\ X.1 = 7C0.1 + 105 * C0.2,\ X.2 = 12 * C0.1 + 183 * C0.2$
$\mathfrak{o}$	$(1/x, 1/x^3 * y)$

$\mathbb{F}_{13}$	$g = 46,\ N = 180$
polynomial	$y^2 + 12 * x^5 + 12 * x^4 + 4 * x^3 + 3 * x^2 + 11 * x$
divisor	$1 * (x^2 + 10 * x + 4, y + 4 * x + 1)$
subgroup	$\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/14\mathbb{Z},$ $X.1 = C0.2,\ X.2 = C0.1,\ X.3 = C0.3 + C0.4,\ X.4 = C0.3 + 15 * C0.5$
$\mathfrak{o}$	$(1/x, 1/x^3 * y)$

References

[AT68] Emil Artin and John Torrence Tate. *Class field theory*. Vol. 366. AMS Chelsea Publishing. American Mathematical Soc., 1968.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. "The Magma algebra system I: The user language". In: *Journal of Symbolic Computation* 24.3-4 (1997), pp. 235–265.

[Bro12] Kenneth S Brown. *Cohomology of groups*. Vol. 87. Graduate Texts in Mathematics. Springer Science & Business Media, 2012.

[CF10] John William Scott Cassels and Albrecht Fröhlich. *Algebraic number theory*. London Mathematical Society London, 2010.

[GS17] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*. Vol. 165. Cambridge studies in advanced mathematics. Cambridge University Press, 2017.

[Har13] Robin Hartshorne. *Algebraic geometry*. Vol. 52. Graduate Texts in Mathematics. Springer Science & Business Media, 2013.

[Has36] Helmut Hasse. "Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung." In: *Journal für die reine und angewandte Mathematik* 1936.175 (1936), pp. 193–208.

[Iha82] Yasutaka Ihara. "Some remarks on the number of rational points of algebratic curves over finite fields". In: *Journal of the Faculty of Science, the University of Tokyo. Sect. 1 A, Mathematics = . 1A,* 28.3 (Feb. 1982), pp. 721–724.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*. Vol. 6. Oxford Graduate Texts in Mathematics. Oxford University Press on Demand, 2002.

[Lor07] Falko Lorenz. *Algebra: Volume ii: Fields with structure, algebras and advanced topics*. Springer Science & Business Media, 2007.

[ÖTY13] Ferruh Özbudak, Burcu Gülmez Temür, and Oğuz Yayla. "An exhaustive computer search for finding new curves with many points among fibre products of two Kummer covers over F_5 and F_7". In: *Turkish Journal of Mathematics* 37.6 (2013), pp. 908–913.

[Rök12] Karl Rökaeus. "Computer search for curves with many points among abelian covers of genus 2 curves". In: *Arithmetic, geometry, cryptography and coding theory*. Vol. 574. Contemp. Math. Amer. Math. Soc., Providence, RI, 2012, pp. 145–150.

[Rök13] Karl Rökaeus. "New curves with many points over small finite fields". In: *Finite Fields and Their Applications* 21 (2013), pp. 58–66.

[Ros02] Michael Rosen. *Number theory in function fields*. Vol. 210. Graduate Texts in Mathematics. Springer Science & Business Media, 2002.

[Ros73] Michael Rosen. "S-units and S-class group in algebraic function fields". In: *Journal of Algebra* 26.1 (1973), pp. 98–108.

[Ros87] Michael Rosen. "The Hilbert class field in function fields". In: *Exposition. Math.* Vol. 5. 4. 1987, pp. 365–378.

[Ser13] Jean-Pierre Serre. *Local fields*. Vol. 67. Graduate Texts in Mathematics. Springer Science & Business Media, 2013.

[Ser20] Jean-Pierre Serre. *Rational points on curves over finite fields*. Société Mathematique de France, 2020.

[Ser83] Jean-Pierre Serre. "Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini". In: *CR Acad. Sci. Paris* 296.Série I (1983), pp. 397–402.

[Sol15] Pavel Solomatin. *Curves with many points over finite fields: the class field theory approach*. 2015. arXiv: `1508.00267 [math.NT]`.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*. Vol. 254. Graduate Texts in Mathematics. Springer Science & Business Media, 2009.

[Sza09] Tamás Szamuely. *Galois groups and fundamental groups*. Vol. 117. Cambridge studies in advanced mathematics. Cambridge University Press, 2009.

[Voi05] John Voight. "Curves over finite fields with many points: an introduction". In: *Computational aspects of algebraic curves*. World Scientific, 2005, pp. 124–144.