Groups and fields in arithmetic

Kosters, M.F.

Groups and fields in arithmetic

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 4 juni 2014
klokke 10:00 uur

door

Michiel Kosters

geboren te Leidschendam
in 1987

Samenstelling van de promotiecommissie:

Promotor:	Prof. dr. H. W. Lenstra
Overige leden:	Prof. dr. T. Chinburg (University of Pennsylvania) Prof. dr. R. Cramer (Centrum Wiskunde & Informatica) Prof. dr. B. Edixhoven Prof. dr. B. Moonen (Radboud Universiteit Nijmegen) Prof. dr. P. Stevenhagen Prof. dr. D. Wan (University of California Irvine)

Groups and fields in arithmetic

Michiel Kosters

Typeset using LaTeX

Printed by Ridderprint, Ridderkerk

The 63 'squares' on the cover correspond to the units of a finite field of 64 elements. The placement of the squares is based on the module structure over the subfield of 8 elements. There are 6 types of squares corresponding to the 6 different multiplicative orders of the elements. Self-similarities have been added for aesthetic reasons.

Contents

Introduction

The title of this thesis is 'Groups and fields in arithmetic'. This title has been chosen in such a way that every chapter has to do with at least two of the nouns in the title. This thesis consists of 8 chapters in which we discuss various topics and every chapter has its own introduction. In this introduction we will discuss each chapter very briefly and give only the highlights of this thesis.

Chapter 1 and 2 are preliminary chapters. In Chapter 1 we discuss algebraic extensions of valued fields. This chapter has been written to fill a gap in the literature. It does contain some new results. In Chapter 2 we discuss normal projective curves, especially over finite fields. This chapter does not contain any significant new results.

Chapter 3 and 4 concern polynomial maps between fields. In Chapter 3 we study the following. A field k is called *large* if every irreducible k-curve C with a k-rational smooth point has infinitely many smooth k-points. We prove the following theorem (Corollary 1.3 from Chapter 3).

Theorem 0.1. *Let k be a perfect large field. Let $f \in k[x]$. Consider the induced evaluation map $f_k \colon k \to k$. Assume that $k \setminus f(k)$ is not empty. Then $k \setminus f(k)$ has the same cardinality as k.*

In the case that k is an infinite algebraic extension of a finite field, we prove density statements about the image (Theorem 1.4 from Chapter 3).

In Chapter 4 we prove the following theorem (Theorem 1.2 from Chapter 4).

Theorem 0.2. *Let k be a finite field and put $q = \#k$. Let n be in $\mathbf{Z}_{\geq 1}$. Let $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$ not all constant and consider the evaluation map $f = (f_1, \ldots, f_n) \colon k^n \to k^n$. Set $\deg(f) = \max_i \deg(f_i)$. Assume that $k^n \setminus f(k^n)$ is not empty. Then we have*

$$|k^n \setminus f(k^n)| \geq \frac{n(q-1)}{\deg(f)}.$$

In Chapter 5 we give an algebraic proof of the following identity (Theorem 1.1 from Chapter 5).

Theorem 0.3. *Let G be an abelian group of size n and let $g \in G$, $i \in \mathbf{Z}$ with $0 \leq i \leq n$. Then the number of subsets of G of cardinality i which sum up to g is equal to*

$$N(G, i, g) = \frac{1}{n} \sum_{s \mid \gcd(\exp(G), i)} (-1)^{i+i/s} \binom{n/s}{i/s} \sum_{d \mid \gcd(e(g), s)} \mu\Big(\frac{s}{d}\Big) \#G[d],$$

where $\exp(G)$ is the exponent of G, $e(g) = \max\{d : d \mid \exp(G),\ g \in dG\}$, μ is the Möbius function, and $G[d] = \{g \in G : dg = 0\}$.

Chapter 6 is a preliminary chapter for Chapter 7. In Chapter 6 we introduce the concept of the shape parameter of a non-empty subset of a finite abelian group. We use this in Chapter 7 to prove the following (Theorem 1.1 from chapter 7).

Theorem 0.4. *For any $\epsilon > 0$ there is a deterministic algorithm which on input a hyperelliptic curve C of genus g over a finite field k of cardinality q outputs a set of generators of $\mathrm{Pic}^0(C)$ in time $O(g^{2+\epsilon}q^{1/2+\epsilon})$.*

In Chapter 8 we study automorphism groups of extensions which are not algebraic. One of our results is the following (Theorem 5.8 from Chapter 8).

Theorem 0.5. *Let Ω be an algebraically closed field and let k be a subfield such that the transcendence degree of Ω over k is finite but not zero. Endow Ω with the discrete topology, Ω^Ω with the product topology and $\mathrm{Aut}_k(\Omega) \subseteq \Omega^\Omega$ with the induced topology. Then there is a surjective continuous group morphism from $\mathrm{Aut}_k(\Omega)$, the field automorphisms of Ω fixing k, to a non finitely generated free abelian group with the discrete topology.*

Chapter 1

The algebraic theory of valued fields

1. Introduction

General valuation theory plays an important role in many areas in mathematics. Also in this thesis, we will quite often need valuation theory, although for our applications the theory of discrete valuations suffices. There exist many books on valuation theory, such as [**End72**], [**EP05**], [**Kuh**] and [**Efr06**]. They do not treat the case of algebraic extensions of valuations theory completely. Furthermore, definitions of certain concepts are not uniform. This chapter is written to fill this gap in the literature and provide a useful reference, even when restricting to the case of discrete valuations. Our definitions are motivated by our Galois theoretic approach. No previous knowledge on the theory of valuations is needed and only a slight proficiency in commutative algebra suffices (see for example [**AM69**] and [**Lan02**]).

With this in mind, this chapter starts with definitions and the main statements. In the second part of this chapter we will provide complete proofs. In the last part of this chapter we give examples of extensions with a defect and we discuss the theory of Frobenius elements.

Our treatment of valuation theory starts with normal extensions of valued fields. Later, by looking at group actions on fundamental sets, we prove statements for algebraic extensions of valued fields. The beginning of our Galois-theoretic approach follows parts of [**End72**] and [**EP05**], although we prove that certain actions are transtive in a different way. The upcoming book [**Kuh**] uses at certain points a very similar approach.

Even though most of the statements in this chapter are known, there are a couple of new contributions.

- We define when algebraic extensions of valued fields are *immediate*, *unramified*, *tame*, *local*, *totally ramified* or *totally wild* (Definition 3.2). The definitions are motivated by practicality coming from Galois theory. We also study maximal respectively minimal extensions with these properties (Theorem 3.15).
- We compute several quantities, such as separable residue field degree extension, tame ramification index and more in finite algebraic extensions of valued fields in terms of automorphism groups (Proposition 3.7). We will give necessary and sufficient conditions for algebraic extensions of valued fields to be immediate, unramified, ... in terms of automorphism groups and fundamental sets (Theorem 3.10). Current literature only seems to handle the Galois case.

For a field K we denote by $\overline{K}$ an algebraic closure. For a domain R we denote by $Q(R)$ its field of fractions.

2. Definition of valuations

Let K be a field.

Definition 2.1. A *valuation ring* on K is a subring $\mathcal{O} \subseteq K$ such that for all $x \in K^*$ we have $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$.

Lemma 2.2. *There is a bijection between the set of valuation rings of K and the set of relations $\leq$ on K^* which satisfy for $x, y, z \in K^*$*

i. $x \leq y$ *or* $y \leq x$;
ii. $x \leq y$, $y \leq z \implies x \leq z$;
iii. $x \leq y \implies xz \leq yz$;
iv. *if* $x + y \neq 0$, *then* $x \leq x + y$ *or* $y \leq x + y$.

This bijection maps a valuation ring $\mathcal{O}$ to the relation which for $x, y \in K^*$ is defined by: $x \leq y$ iff $y/x \in \mathcal{O}$. The inverse maps $\leq$ to $\{x \in K^* : 1 \leq x\} \sqcup \{0\}$.

Proof. Let $\mathcal{O}$ be a valuation ring and consider the obtained relation $\leq$. Then i holds by definition. Property ii, iii hold as $\mathcal{O}$ is a ring. For iv, suppose that $x \leq y$, that is, $y/x \in \mathcal{O}$. Then we have $1 + y/x = (x + y)/x \in \mathcal{O}$. Hence $x \leq x + y$ as required.

Given $\leq$, we claim that $\mathcal{O} = \{x \in K^* : 1 \leq x\} \sqcup \{0\}$ is a valuation ring. Let $x \in K^*$. We have $1 \leq 1$ (i) and hence $1 \in \mathcal{O}$. Furthermore, $-1 \in \mathcal{O}$. Indeed, by i we have $1 \leq -1$ or $-1 \leq 1$. In the first case we are done, in the second case we can multiply by -1 to obtain $1 \leq -1$ (iii). Take $x, y \in \mathcal{O} \setminus \{0\}$. Then if we multiply $x \geq 1$ by y we obtain $xy \geq y \geq 1$ (iii), and hence we have $xy \in \mathcal{O}$ (ii). If $x + y \neq 0$, we find $x + y \geq x \geq 1$ or $x + y \geq y \geq 1$. From ii we conclude that $x + y \geq 1$. Take $z \in K^*$. Then we have Finally, we have $1 \leq z$ or $z \leq 1$ (i). In the first case, we have $z \in \mathcal{O}$. In the second case, we multiply by z^{-1} and iv gives $1 \leq z^{-1}$. Hence $z^{-1} \in \mathcal{O}$. This shows that $\mathcal{O}$ is a valuation ring. □

Let $\mathcal{O}$ be a valuation on K. Consider the relation $\leq$ on K^* induced from $\mathcal{O}$ as in the lemma above. One easily sees that $\mathcal{O}^* = \{x \in K^* : 1 \leq x \text{ and } x \leq 1\}$. Furthermore, if $x, y \in \mathcal{O} \setminus \mathcal{O}^*$, we deduce from property iv and ii that $x + y$ is not a unit. Hence $\mathcal{O}$ is a local ring. The induced relation $\leq$ on K^* makes $K^*/\mathcal{O}^*$ into an *ordered abelian group*. An ordered abelian group is an abelian group P, written additively, together with a relation $\leq$ such that for $a, b, c \in P$ we have:

i. $a \leq b$, $b \leq a \implies a = b$;
ii. $a \leq b$, $b \leq c \implies a \leq c$;
iii. $a \leq b$ or $b \leq a$;
iv. $a \leq b \implies a + c \leq b + c$.

The group morphism $v\colon K^* \to K^*/\mathcal{O}^*$ is called the *valuation map* and it satisfies for $x, y \in K^*$ with $x + y \neq 0$: $v(x + y) \geq \min(v(x), v(y))$. The ordered abelian group $K^*/\mathcal{O}^*$ is called the *value group*.

To shorten notation we just write v for a valuation. We denote by $\mathcal{O}_v$ the valuation ring with maximal ideal $\mathfrak{m}_v$. The residue field is denoted by $\mathrm{k}_v = \mathcal{O}_v/\mathfrak{m}_v$. The value

group is denoted by $\Delta_v = K^*/\mathcal{O}^*$, for which we use additive notation. We use the notation $v\colon K^* \to \Delta_v$. We set

$$\mathrm{p}_v = \begin{cases} \mathrm{char}(\mathrm{k}_v) & \text{if } \mathrm{char}(\mathrm{k}_v) \neq 0 \\ 1 & \text{if } \mathrm{char}(\mathrm{k}_v) = 0. \end{cases}$$

A pair (K, v) as above is called a *valued field*. Note that a valuation v gives rise to the valued field $(Q(\mathcal{O}_v), v)$ where $Q(\mathcal{O}_v)$ is the fraction field of $\mathcal{O}_v$. If K' is a subfield, then we denote by $v|_{K'}$ the valuation on K' corresponding to the valuation ring $\mathcal{O}_v \cap K$.

3. Main results

In this section we will provide statements of the main results. Proofs of the statements follow in Sections 4, 5, 6 and 7 and will occupy most of this chapter.

3.1. Properties of extensions of valuations. Let $M \supseteq N$ be an extension of field. When we say that M/N is separable we mean that it is algebraic and separable. Similarly, normal means normal and algebraic (but not necessarily separable). Assume that M/N is finite. We set $[M : N]_{\mathrm{s}}$ for the separability degree of the extension and $[M : N]_{\mathrm{i}}$ for the inseparability degree. Note that $[M : N] = [M : N]_{\mathrm{s}} \cdot [M : N]_{\mathrm{s}}$.

Let (K, v) be a valued field and let L be an extension of K. An *extension* of v to L is a valuation w on L satisfying $\mathcal{O}_w \cap K = \mathcal{O}_v$, equivalently, $\mathfrak{m}_w \cap K = \mathfrak{m}_v$. Such extensions do exist (Proposition 5.6). We denote such an extension by $(L, w) \supseteq (K, v)$ or w/v. Sometimes we write $w|v$ if w extends v. The number of extensions of v to L is denoted by $\mathrm{g}_{L,v}$, which is finite if L/K is finite (Proposition 5.6). Such an extension $(L, w) \supseteq (K, v)$ is called *finite* if L/K is finite. In a similar way we define such an extension to be normal, separable, ... An extension induces inclusions $\Delta_v \to \Delta_w$ and $\mathrm{k}_v \to \mathrm{k}_w$. The following proposition defines a lot of quantities relating to a finite extension of valued fields and gives some properties of these quantities (see Proposition 7.1).

Proposition 3.1. *Let $(L, w) \supseteq (K, v)$ be a finite extension of valued fields. Then one has:*

- $\mathrm{e}(w/v) := (\Delta_w : \Delta_v) \in \mathbf{Z}_{\geq 1}$ *(*ramification index*);*
- $\mathrm{e_t}(w/v) := \mathrm{lcm}\{m \in \mathbf{Z}_{\geq 1} : m | \mathrm{e}(w/v),\ \gcd(m, \mathrm{p}_v) = 1\} \in \mathbf{Z}_{\geq 1}$ *(*tame ramification index*);*
- $\mathrm{e_w}(w/v) := \frac{\mathrm{e}(w/v)}{\mathrm{e_t}(w/v)} \in \mathrm{p}_v^{\mathbf{Z}_{\geq 0}}$ *(*wild ramification index*);*
- $\mathrm{f}(w/v) := [\mathrm{k}_w : \mathrm{k}_v] \in \mathbf{Z}_{\geq 1}$ *(*residue field degree*);*
- $\mathrm{f_s}(w/v) := [\mathrm{k}_w : \mathrm{k}_v]_{\mathrm{s}} \in \mathbf{Z}_{\geq 1}$ *(*separable residue field degree*);*
- $\mathrm{f_i}(w/v) := [\mathrm{k}_w : \mathrm{k}_v]_{\mathrm{i}} \in \mathrm{p}_v^{\mathbf{Z}_{\geq 0}}$ *(*inseparable residue field degree*);*
- *Let M/K be a finite normal extension containing L. We define the* local degree *by $\mathrm{n}(w/v) := \frac{\mathrm{g}_{M,w}}{\mathrm{g}_{M,v}} \cdot [L : K] \in \mathbf{Z}_{\geq 1}$ and this does not depend on the choice of M;*
- $\mathrm{d}(w/v) := \frac{\mathrm{n}(w/v)}{\mathrm{e}(w/v)\,\mathrm{f}(w/v)} \in \mathrm{p}_v^{\mathbf{Z}_{\geq 0}}$ *(*defect*);*
- $\mathrm{d_w}(w/v) := \mathrm{d}(w/v)\,\mathrm{e_w}(w/v)\,\mathrm{f_i}(w/v) \in \mathrm{p}_v^{\mathbf{Z}_{\geq 0}}$ *(*wildness index*);*

The quantities e, $\mathrm{e_t}$, $\mathrm{e_w}$, f, $\mathrm{f_s}$, $\mathrm{f_i}$, n, d *and* $\mathrm{d_w}$ *are multiplicative in towers.*

Definition 3.2. Let $(L,w) \supseteq (K,v)$ be a finite extension of valued fields. Then we have the following properties which $(L,w) \supseteq (K,v)$ can satisfy:

- *immediate*: $\mathrm{d_w}(w/v) = \mathrm{e_t}(w/v) = \mathrm{f_s}(w/v) = 1$, equivalently, $\mathrm{n}(w/v) = 1$;
- *unramified*: $\mathrm{d_w}(w/v) = \mathrm{e_t}(w/v) = 1$;
- *tame*: $\mathrm{d_w}(w/v) = 1$;
- *local*: $\mathrm{g}_{L,v} = 1$;
- *totally ramified*: $\mathrm{f_s}(w/v) = \mathrm{g}_{L,v} = 1$;
- *totally wild*: $\mathrm{e_t}(w/v) = \mathrm{f_s}(w/v) = \mathrm{g}_{L,v} = 1$.

We say that v is *totally split* in L if $g_{L,v} = [L:K]$.

As the various degrees are multiplicative, we can extend this definition in the following way. Let $(L,w) \supseteq (K,v)$ be an algebraic extension of valued fields. Then w/v is *immediate* (respectively *unramified*, *tame*, *local*, *totally ramified*, *totally wild*) if all intermediate extensions (L',w') of $(L,w) \supseteq (K,v)$ where L'/K is finite are immediate (respectively unramified, tame, local, totally ramified, totally wild). We say that v is *totally split* in L if all intermediate extensions (L',w') of $(L,w) \supseteq (K,v)$ with L'/K finite are totally split.

3.2. Normal extensions.

Definition 3.3. Let $(M,x) \supseteq (K,v)$ be a normal algebraic extension of valued fields and let $G = \mathrm{Aut}_K(M)$. Note that G acts on the set of valuations on M extending v by $\mathcal{O}_{g(x')} = g(\mathcal{O}_{x'})$. Let $\mathrm{D}_{x,K} = \{g \in G : gx = x\}$ be the *decomposition group* of x over K. We define the *inertia group* $\mathrm{I}_{x,K} \subseteq \mathrm{D}_{x,K}$ of x over K to be the kernel of the natural group morphism $\mathrm{D}_{x,K} \to \mathrm{Aut}_{\mathrm{k}_v}(\mathrm{k}_x)$. Furthermore, there is a natural group morphism

$$\begin{aligned} \mathrm{I}_{x,K} &\to \mathrm{Hom}(\Delta_x/\Delta_v, \mathrm{k}_x^*) \\ \overline{c} &\mapsto \frac{\overline{g(c)}}{c} \end{aligned}$$

(see Lemma 6.3). We define the *ramification group* of x over K to be its kernel. We denote it by $\mathrm{V}_{x,K}$.

Let $\Gamma_{x,v} = \mathrm{im}\left(\mathrm{Aut}_{\mathrm{k}_v}(\mathrm{k}_x) \to \mathrm{Aut}_{\mathrm{k}_v^*}(\mathrm{k}_x^*)\right)$. Let $\mathrm{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x))$ be the subgroup of $\mathrm{Aut}(M^*/(1+\mathfrak{m}_x))$ consisting of those automorphisms such that the restriction to k_x^* lies in $\Gamma_{x,v}$ and which are the identity on $K^*/(1+\mathfrak{m}_v)$. We have a natural map $\mathrm{D}_{x,K} \to \mathrm{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x))$ (see the discussion after Lemma 6.3).

We endow G with the profinite topology. This means that we view G as a subset of M^M. We endow M with the discrete topology, M^M with the product topology and G with the induced topology. Similarly we define profinite topologies on $\mathrm{Aut}_{\mathrm{k}_v}(\mathrm{k}_x) \subseteq \mathrm{k}_x^{\mathrm{k}_x}$ and $\mathrm{Hom}(\Delta_x/\Delta_v, \mathrm{k}_x^*) \subseteq (\mathrm{k}_x^*)^{\Delta_x/\Delta_v}$ where k_x and k_x^* have the discrete topology. Furthermore, let S be the set of valuations extending v to M. For $x' \in S$ and a finite extension L of K in M we set $U_{x',L} = \{x'' \in S : x''|_L = x'|_L\}$. This is a basis for a topology on S. We give $\mathrm{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x))$ the following topology. We give $C = M^*/(1+\mathfrak{m}_x)$ the discrete topology, C^C the product topology and $\mathrm{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x))$ the induced topology.

Definition 3.4. Let L/K be a field extension. We set $L_{K,\mathrm{sep}}$ for the field extension of K consisting of the elements in L which are separable and algebraic over K.

Definition 3.5. Let $(M,x) \supseteq (K,v)$ be a normal algebraic extension of valued fields. We define $K_{\mathrm{h},x} = M_{K,\mathrm{sep}}^{\mathrm{D}_{x,K}}$ (*decomposition field*, h stands for Henselization), $K_{\mathrm{i},x} = M_{K,\mathrm{sep}}^{\mathrm{I}_{x,K}}$ (*inertia field*) and $K_{\mathrm{v},x} = M_{K,\mathrm{sep}}^{\mathrm{V}_{x,K}}$ (*ramification field*). Note that all these extensions are separable over K and that we have $K \subseteq K_{\mathrm{h},x} \subseteq K_{\mathrm{i},x} \subseteq K_{\mathrm{v},x} \subseteq M$.

Recall that for a prime p and a profinite group H a pro-p-Sylow subgroup H' is a maximal subgroup of H such that H' is a projective limit of finite groups of p-power order.

We define the *Steinitz monoid* as the following set. Let $\mathcal{P} \subset \mathbf{Z}$ be the set of primes. *Steinitz numbers* are of the form $\prod_{p\in\mathcal{P}} p^{n_p}$ with $n_p \in \mathbf{Z}_{\geq 0} \sqcup \{\infty\}$. This set has an obvious monoid structure and there is an obvious way for defining gcd and lcm for arbitrary sets of Steinitz numbers. Furthermore, there is an obvious notion of divibility.

Let H be a profinite group. Then we define its *order* to be

$$\mathrm{ord}(H) = \mathrm{lcm}\{[H:N] : N \text{ open normal subgroup of } H\},$$

and we define its *exponent* to be

$$\exp(H) = \mathrm{lcm}\{\exp(H/N) : N \text{ open normal subgroup of } H\}.$$

Both are Steinitz numbers. Furthermore, if $H = \varprojlim_{i\in I} H_i$ where the H_i are finite, then one has $\mathrm{ord}(H) = \mathrm{lcm}(\mathrm{ord}(H_i) : i \in I)$ and $\exp(H) = \mathrm{lcm}(\exp(H_i) : i \in I)$.

The proof of the following theorem can be found on Page 21.

Theorem 3.6. *Let $(M,x) \supseteq (K,v)$ be a normal algebraic extension of valued fields and let $G = \mathrm{Aut}_K(M)$. Then G acts continuously on the set S consisting of the valuations of M extending v and induces an isomorphism of topological G-sets*

$$\begin{aligned} G/\,\mathrm{D}_{x,K} &\to S \\ \overline{g} &\mapsto gx. \end{aligned}$$

For $g \in G$ one has $\mathrm{D}_{g(x),K} = g\,\mathrm{D}_{x,K}\,g^{-1}$, $\mathrm{I}_{g(x),K} = g\,\mathrm{I}_{x,K}\,g^{-1}$ and $\mathrm{V}_{g(x),K} = g\,\mathrm{V}_{x,K}\,g^{-1}$. One also has $K_{\mathrm{h},g(x)} = gK_{\mathrm{h},x}$, $K_{\mathrm{i},g(x)} = gK_{\mathrm{i},x}$ and $K_{\mathrm{v},g(x)} = gK_{\mathrm{v},x}$.

Furthermore, we have exact sequences of profinite groups

$$0 \to \mathrm{I}_{x,K} \to \mathrm{D}_{x,K} \to \mathrm{Aut}_{\mathrm{k}_v}(\mathrm{k}_x) \to 0,$$

$$0 \to \mathrm{V}_{x,K} \to \mathrm{I}_{x,K} \to \mathrm{Hom}(\Delta_x/\Delta_v, \mathrm{k}_x^*) \to 0$$

and

$$0 \to \mathrm{V}_{x,K} \to \mathrm{D}_{x,K} \to \mathrm{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x)) \to 0.$$

The extension $\mathrm{k}_x/\mathrm{k}_v$ is normal and $\mathrm{V}_{x,K}$ is the unique pro-p_v-Sylow subgroup of $\mathrm{I}_{x,K}$. Then for any integer $r \in \mathbf{Z}_{\geq 1}$ dividing $\exp(\mathrm{I}_{x,K}\,/\,\mathrm{V}_{x,K})$ the field k_x contains a primitive r-th root of unity.

Let (L,w) be an intermediate extension of $(M,x) \supseteq (K,v)$ and let $H = \mathrm{Aut}_L(M)$. Then one has:

i. $\mathrm{D}_{x,L} = \mathrm{D}_{x,K} \cap H$, $\mathrm{I}_{x,L} = \mathrm{I}_{x,K} \cap H$ *and* $\mathrm{V}_{x,L} = \mathrm{V}_{x,K} \cap H$;

ii. $L_{\mathrm{h},x} = K_{\mathrm{h},x}L$, $L_{\mathrm{i},x} = K_{\mathrm{i},x}L$ *and* $L_{\mathrm{v},x} = K_{\mathrm{v},x}L$.

If in addition we assume that L/K *is normal, then we have exact sequences*

$$0 \to \mathrm{D}_{x,L} \to \mathrm{D}_{x,K} \to \mathrm{D}_{w,K} \to 0,$$

$$0 \to \mathrm{I}_{x,L} \to \mathrm{I}_{x,K} \to \mathrm{I}_{w,K} \to 0,$$

and

$$0 \to \mathrm{V}_{x,L} \to \mathrm{V}_{x,K} \to \mathrm{V}_{w,K} \to 0.$$

Under the normality assumption we have $K_{\mathrm{h},x|_L} = K_{\mathrm{h},x} \cap L$, $K_{\mathrm{i},x|_L} = K_{\mathrm{i},x} \cap L$ *and* $K_{\mathrm{v},x|_L} = K_{\mathrm{v},x} \cap L$.

If the extension M/K is finite, the previous theorem implies the following (proof on Page 25).

Proposition 3.7. *Let* $(M,x) \supseteq (K,v)$ *be a finite normal extension of valued fields. Then one has*

$$\begin{aligned}
[K_{\mathrm{h},x} : K] &= \mathrm{g}_{M,v} \\
[K_{\mathrm{i},x} : K_{\mathrm{h},x}] &= \mathrm{f_s}(x/v) = \mathrm{f_s}(x|_{K_{\mathrm{i},x}}/x|_{K_{\mathrm{h},x}}) \\
[K_{\mathrm{v},x} : K_{\mathrm{i},x}] &= \mathrm{e_t}(x/v) = \mathrm{e_t}(x|_{K_{\mathrm{v},x}}/x|_{K_{\mathrm{i},x}}) \\
[M : K_{\mathrm{v},x}] &= \mathrm{d_w}(x/v) = \mathrm{d_w}(x/x|_{K_{\mathrm{v},x}}).
\end{aligned}$$

Let (L,w) *be an intermediate extension of* $(M,x) \supseteq (K,v)$. *Then one has*

$$\begin{aligned}
[L_{\mathrm{h},x} : K_{\mathrm{h},x}] &= \mathrm{d_w}(w/v)\,\mathrm{e_t}(w/v)\,\mathrm{f_s}(w/v) \\
[L_{\mathrm{i},x} : K_{\mathrm{i},x}] &= \mathrm{d_w}(w/v)\,\mathrm{e_t}(w/v) \\
[L_{\mathrm{v},x} : K_{\mathrm{v},x}] &= \mathrm{d_w}(w/v).
\end{aligned}$$

The proof of the following theorem can be found on Page 23.

Theorem 3.8. *Let* $(M,x) \supseteq (K,v)$ *be a normal extension of valued fields. Then the following hold.*

i. *Assume that* k_x *has no cyclic extensions of prime order dividing the order of* $\mathrm{I}_{x,K} / \mathrm{V}_{x,K}$. *Then the exact sequence*

$$0 \to \mathrm{I}_{x,K} / \mathrm{V}_{x,K} \to \mathrm{D}_{x,K} / \mathrm{V}_{x,K} \to \mathrm{D}_{x,K} / \mathrm{I}_{x,K} \to 0$$

is right split.

ii. *Assume that* k_x *has no cyclic extensions of prime order dividing* p_v *or that* $\mathrm{p}_v \nmid \mathrm{ord}(\mathrm{I}_{x,K})$. *Then the exact sequence*

$$0 \to \mathrm{V}_{x,K} \to \mathrm{D}_{x,K} \to \mathrm{D}_{x,K} / \mathrm{V}_{x,K} \to 0$$

is right split.

iii. *Assume that* k_x *has no cyclic extensions of prime order dividing* $\mathrm{ord}(\mathrm{I}_{x,K})$. *Then the exact sequence*

$$0 \to \mathrm{I}_{x,K} \to \mathrm{D}_{x,K} \to \mathrm{D}_{x,K} / \mathrm{I}_{x,K} \to 0$$

is right split.

3.3. Algebraic extensions. A well-known result in the following (proof on Page 25).

Theorem 3.9 (Fundamental equality)**.** *Let (K, v) be a valued field and let L/K be a finite field extension. Then we have*

$$\begin{aligned}[L : K] &= \sum_{w|v \text{ on } L} \mathrm{n}(w/v) = \sum_{w|v \text{ on } L} \mathrm{d}(w/v)\,\mathrm{e}(w/v)\,\mathrm{f}(w/v) \\ &\geq \sum_{w|v \text{ on } L} \mathrm{e}(w/v)\,\mathrm{f}(w/v).\end{aligned}$$

Two algebraic field extensions L, L' of a field K are called *linearly disjoint* over K if $L \otimes_K L'$ is a field.

If L, L' are subfields of a field Ω, then we set the *compositum* $LL' = \mathrm{im}(L \otimes_{\mathbf{Z}} L' \to \Omega)$. This is the smallest ring containing both L and L' in Ω. This is a field if the elements of L are algebraic over L' or if the elements of L' are algebraic over L.

The following proposition studies extensions of valuations using fundamental sets (Proof on 25). If $L \supseteq K$ and $M \supseteq K$ are extensions of fields, we denote by $\mathrm{Hom}_K(L, M)$ the set of field homomorphisms from L to M which are the identity on K.

Theorem 3.10. *Let (K, v) be a valued field and let L/K be an algebraic extension. Let $(M, x) \supseteq (K, v)$ be a normal extension with group $G = \mathrm{Aut}_K(M)$ such that the G-set $X = \mathrm{Hom}_K(L, M)$ is not empty. Then the natural map*

$$\begin{aligned}\pi\colon X &\to \{w \text{ on } L \text{ extending } v\} \\ \sigma &\mapsto w \text{ s.t. } \mathcal{O}_w = \sigma^{-1}(\mathcal{O}_x \cap \sigma(L))\end{aligned}$$

is surjective. Let $\sigma \in X$ and set $w = \pi(\sigma)$ and let G_σ be the stabilizer in G of σ. Then we have:

i. *w/v is immediate $\iff$ $\sigma(L) \subseteq K_{\mathrm{h},x}$ $\iff$ $\mathrm{D}_{x,K} \subseteq G_\sigma$;*
ii. *w/v is unramified $\iff$ $\sigma(L) \subseteq K_{\mathrm{i},x}$ $\iff$ $\mathrm{I}_{x,K} \subseteq G_\sigma$;*
iii. *w/v is tame $\iff$ $\sigma(L) \subseteq K_{\mathrm{v},x}$ $\iff$ $\mathrm{V}_{x,K} \subseteq G_\sigma$;*
iv. *w/v is local $\iff$ $\sigma(L)$ and $K_{\mathrm{h},x}$ are linearly disjoint over K $\iff$ $\mathrm{D}_{x,K}\,\sigma = X$;*
v. *w/v is totally ramified $\iff$ $\sigma(L)$ and $K_{\mathrm{i},x}$ are linearly disjoint over K $\iff$ $\mathrm{I}_{x,K}\,\sigma = X$;*
vi. *w/v is totally wild $\iff$ $\sigma(L)$ and $K_{\mathrm{v},x}$ are linearly disjoint over K $\iff$ $\mathrm{V}_{x,K}\,\sigma = X$.*

Furthermore we have:

vii. *x/w is immediate $\iff$ $M = \sigma(L)K_{\mathrm{h},x}$ $\iff$ $M/\sigma(L)$ is separable and $G_\sigma \cap \mathrm{D}_{x,K} = 0$;*
viii. *x/w is unramified $\iff$ $M = \sigma(L)K_{\mathrm{i},x}$ $\iff$ $M/\sigma(L)$ is separable and $G_\sigma \cap \mathrm{I}_{x,K} = 0$;*
ix. *x/w is tame $\iff$ $M = \sigma(L)K_{\mathrm{v},x}$ $\iff$ $M/\sigma(L)$ is separable and $G_\sigma \cap \mathrm{V}_{x,K} = 0$;*
x. *x/w is local $\iff$ $\sigma(L) \supseteq K_{\mathrm{h},x}$ $\iff$ $G_\sigma \subseteq \mathrm{D}_{x,K}$;*
xi. *x/w is totally ramified $\iff$ $\sigma(L) \supseteq K_{\mathrm{i},x}$ $\iff$ $G_\sigma \subseteq \mathrm{I}_{x,K}$;*

xii. *x/w is totally wild* $\iff$ $\sigma(L) \supseteq K_{\mathrm{v},x} \iff G_\sigma \subseteq \mathrm{V}_{x,K}$.

Finally we have:

xiii. *v is totally split in L* $\iff$ *for all $\sigma \in X$ we have $\sigma(L) \subseteq K_{\mathrm{h},x} \iff \mathrm{D}_{x,K}$ acts trivially on X;*

xiv. *w is totally split in M* $\iff$ *$M/\sigma(L)$ is separable and only the trivial element of G_σ is conjugate to an element of $\mathrm{D}_{x,K}$.*

The above proposition has a lot of corollaries. The proof of the first corollary can be found on Page 26.

Corollary 3.11. *Let (K, v) be a valued field and let L and L' be two algebraic extensions of K in some algebraic closure of K. Let x be a valuation on LL' extending v and let $w = x|_L$ and $w' = x|_{L'}$. Then the following statements hold:*

i. *if w/v is immediate, then x/w' is immediate;*
ii. *if w/v is unramified, then x/w' is unramified;*
iii. *if w/v is tame, then x/w' is tame;*
iv. *if v is totally split in L, then w' is totally split in LL'.*

The proof of the following corollary can be found on Page 26.

Corollary 3.12. *Let $(L, w) \supseteq (K, v)$ be an algebraic extension of valued fields and let (K', w') be an intermediate extension. Then w/v is immediate (respectively unramified, tame, local, totally ramified, totally wild) iff w/w' and w'/v are immediate (respectively unramified, tame, local, totally ramified, totally wild).*

The proof of the following proposition can be found on Page 11.

Proposition 3.13. *Let Ω be a field and let $L, L' \subseteq \Omega$ be subfields. Then there is a subfield M of L such that for all subfields F of L the natural map $L \otimes_F (L'F) \to LL'$ is an isomorphism iff $M \subseteq F$. Furthermore, M can be described in the following two ways, where $\mathbf{F}$ is the prime of field of Ω.*

i. *Let $\mathfrak{B} \subseteq L'$ be a basis of LL' over L. For $b \in \mathfrak{B}$ and $x \in L'$ write $x = \sum_{b\in\mathfrak{B}} c_{x,b} b$ with $c_{x,b} \in L$ almost all zero. Then one has $M = \mathbf{F}(c_{x,b} : x \in L',\ b \in \mathfrak{B})$.*

ii. *Set*

$$S = \Big\{ c \in L : \exists I \subseteq L' \text{ finite, ind. over } L \text{ and } (c_i)_{i\in I} \in L^I \text{ s.t. } \exists i \in I \text{ s.t. } c_i = c \text{ and } \sum_{i\in I} c_i i \in L' \Big\}.$$

Then one has $M = \mathbf{F}(S)$.

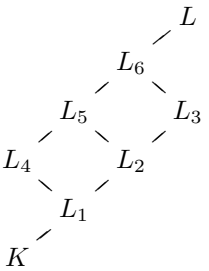
Definition 3.14. The field M in the above theorem is called the *field of definition* of L' over L and is denoted by $L \setminus\!\!\setminus L'$.

The proof of the following theorem can be found on Page 27.

Theorem 3.15. *Let $(L, w) \supseteq (K, v)$ be an algebraic extension of valued fields. Then then following statements hold:*

i. *There is a unique maximal subextension L_1 of L/K such that $w|_{L_1}/v$ is immediate (respectively L_2 for unramified and L_3 for tame).*
ii. *There is a unique minimal subextension L_4 of L/K such that $w/w|_{L_4}$ is local (respectively L_5 for totally ramified and L_6 for totally wild).*

We have the following diagram of inclusions:



For any $(M,x) \supseteq (L,w) \supseteq (K,v)$ extension of valued fields where M/K is normal, we have $L_1 = K_{\mathrm{h},x} \cap L$, $L_2 = K_{\mathrm{i},x} \cap L$ and $L_3 = K_{\mathrm{v},x} \cap L$, $L_4 = L_{K,\mathrm{sep}} \setminus K_{\mathrm{h},x}$, $L_5 = L_{K,\mathrm{sep}} \setminus K_{\mathrm{i},x}$ and $L_6 = L_{K,\mathrm{sep}} \setminus K_{\mathrm{v},x}$.

If there is a normal extension M/K containing L such that $\mathrm{g}_{M,w} = 1$, then $L_1 = L_4$, $L_2 = L_5$ and $L_3 = L_6$.

The proof of the following corollary can be found on Page 27.

Corollary 3.16. *Let (K,v) be a valued field and let L and L' be two algebraic extensions contained in an algebraic extension L'' of K. Let x be a valuation on L'' extending v and let $w = x|_L$ and $w' = x|_{L'}$. Assume that $K = L \cap L'$ and there exists a normal extension M/K containing LL' such that $\mathrm{g}_{M,w} = 1$. Then the following statements hold:*

i. *if x/w' is local, then w/v is local;*
ii. *if x/w' is totally ramified, then w/v is totally ramified;*
iii. *if x/w' is totally wild, then w/v is totally wild.*

The proof of the following proposition can be found on Page 29.

Proposition 3.17. *Let (K,v) be a valued field and let L be a finite separable algebraic extension of K. Let $(M,x) \supseteq (K,v)$ be a finite normal extension of valued fields with group $G = \mathrm{Aut}_K(M)$ such that the G-set $X = \mathrm{Hom}_K(L,M)$ is not empty. Then the map*

$$\begin{aligned} \varphi\colon \mathrm{D}_{x,K} \setminus X &\to \{w \text{ of } L \text{ extending } v\} \\ \mathrm{D}_{x,K}\, s &\mapsto w \text{ s.t. } \mathcal{O}_w = \sigma^{-1}(\mathcal{O}_x \cap \sigma(L)) \end{aligned}$$

is a bijection of sets. If $\varphi(\mathrm{D}_{x,K}\, s) = w$ we have:

i. *$\#\,\mathrm{D}_{x,K}\, s = \mathrm{d_w}(w/v)\,\mathrm{e_t}(w/v)\,\mathrm{f_s}(w/v) = \mathrm{n}(w/v)$;*
ii. *the number of orbits under $\mathrm{I}_{x,K}$ of $\mathrm{D}_{x,K}\, s$ is equal to $\mathrm{f_s}(w/v)$ and each orbit has length $\mathrm{d_w}(w/v)\,\mathrm{e_t}(w/v)$;*
iii. *the number of orbits under $\mathrm{V}_{x,K}$ of $\mathrm{D}_{x,K}\, s$ is equal to $\mathrm{e_t}(w/v)\,\mathrm{f_s}(w/v)$ and each orbit has length $\mathrm{d_w}(w/v)$.*

The proof of the following corollary can be found on Page 29.

Corollary 3.18. *Let (K, v) be a valued field and let L be a finite algebraic extension of K. Let $(M, x) \supseteq (K, v)$ be a finite normal extension of valued fields with group $G = \mathrm{Aut}_K(M)$ such that the G-set $X = \mathrm{Hom}_K(L, M)$ is not empty. Then the cardinality of the set of valuations w on L extending v such that $\mathrm{f_s}(w/v) = 1$ is equal to $\#\left(\mathrm{I}_{x,K} \backslash X\right)^{\mathrm{D}_{x,K} \,/\, \mathrm{I}_{x,K}}$.*

4. Preliminaries

4.1. Field theory.

4.1.1. *Linearly disjoint extensions.* Let Ω be a field and let $L, L' \subseteq \Omega$. We set $LL' = \mathrm{im}\,(L \otimes_{\mathbf{Z}} L' \to \Omega)$, that is, the smallest ring containing both L and L'. This is a field if the elements of L are algebraic over L' or if the elements of L' are algebraic over L.

Two algebraic field extensions L, L' of a field K are called *linearly disjoint* over K if $L \otimes_K L'$ is a field. This holds if and only if all pairs of finite subextensions of L/K respectively L'/K are linearly disjoint over K.

Let M/K is a normal field extension with group $G = \mathrm{Aut}_K(M)$. Then the latter group is a topological group with the topology coming from viewing $G \subset M^M$ where M has the discrete topology and M^M the product topology.

Lemma 4.1. *Let M/K be a normal extension of fields with group $G = \mathrm{Aut}_K(M)$ and let L, L' be two intermediate extensions. Put $H = \mathrm{Aut}_L(M)$ and $H' = \mathrm{Aut}_{L'}(M)$. Then one has: $\overline{\langle H, H' \rangle} = G$ iff $L \cap L'$ over K is purely inseparable.*

Proof. Set $p = \mathrm{char}(K)$ if $\mathrm{char}(K)$ is positive and 1 otherwise. It is very easy to see that $M_{L,\mathrm{ins}} \cap M_{L',\mathrm{ins}} = M_{L \cap L',\mathrm{ins}}$. Note that $H = \mathrm{Aut}_{M_{L,\mathrm{ins}}}(M)$, $H' = \mathrm{Aut}_{M_{L',\mathrm{ins}}}(M)$ and $G = \mathrm{Aut}_{M_{K,\mathrm{ins}}}(M)$ and that M is Galois over $M_{K,\mathrm{ins}}$, $M_{L,\mathrm{ins}}$ and $M_{L',\mathrm{ins}}$ (Proposition 4.9). From Galois theory it follows that $\overline{\langle H, H' \rangle}$ corresponds to $M_{L,\mathrm{ins}} \cap M_{L',\mathrm{ins}} = M_{L \cap L',\mathrm{ins}}$ and that G corresponds to $M_{K,\mathrm{ins}}$. Hence one has: $\overline{\langle H, H' \rangle} = G$ iff $M_{L \cap L',\mathrm{ins}} = M_{K,\mathrm{ins}}$ iff $L \cap L'/K$ is purely inseparable. □

For a field K we denote by K_{sep} its separable closure.

Proposition 4.2. *Let M/K be a normal extension of fields with group $G = \mathrm{Aut}_K(M)$ and let L, L' be two intermediate extensions. Put $H = \mathrm{Aut}_L(M)$ and $H' = \mathrm{Aut}_{L'}(M)$. Assume that L/K is separable. Then the following statements are equivalent:*

i. *L and L' are linearly disjoint over K;*
ii. *$L \otimes_K L'$ is a domain;*
iii. *the natural map $L \otimes_K L' \to LL'$ is an isomorphism;*
iv. *$G = H \cdot H'$;*
v. *H' acts transitively on G/H;*
vi. *the natural map $\mathrm{Hom}_{L'}(LL', K_{\mathrm{sep}}) \to \mathrm{Hom}_K(L, K_{\mathrm{sep}})$ is a bijection.*

If L/K or L'/K is normal, then the above statements are equivalent to $L \cap L' = K$.

Proof. i $\iff$ ii: One implication is obvious. Suppose that $L \otimes_K L'$ is a domain. To show that every element has an inverse, we may reduce to the case where both

L/K and L'/K are finite. The result follows since a domain which is finite over a field is a field.

i $\iff$ iii: Obvious.

iv $\iff$ v: Obvious.

v $\iff$ vi: The map in vi is the natural injective map $H'/(H \cap H') \to G/H$. It is surjective iff H' acts transitively on G/H.

i $\implies$ vi: The natural map $\mathrm{Hom}_{L'}(LL', K_{\mathrm{sep}}) \to \mathrm{Hom}_K(L, K_{\mathrm{sep}})$ is injective. Let $\varphi \in \mathrm{Hom}_K(L, K_s)$ be given. Let L'' be a finite extension of K contained in L. Since L and L' are disjoint over K, we find $[LL' : L'] = [L : K]$. This shows, since L/K is separable, that the natural injective map $\mathrm{Hom}_{L'}(L''L', K_{\mathrm{sep}}) \to \mathrm{Hom}_K(L'', K_{\mathrm{sep}})$ is a bijection. Hence there is a unique morphism in $\mathrm{Hom}_{L'}(L''L', K_s)$ mapping to $\varphi|_{L''}$. By uniqueness we can glue these morphisms to a unique morphism mapping to φ.

iv $\implies$ i: If $G = H \cdot H'$, then for any finite subextension of L/K the same holds. Hence all finite extensions of L/K are linearly disjoint from L'. But then it easily follows that L and L' are linearly disjoint over K.

We will now prove the last part. If $L \otimes_K L'$ is a field, then obviously we have $L \cap L' = K$. For the other implication, assume first that L/K is normal. This means that $H = \ker(\mathrm{Aut}_K(M) \to \mathrm{Aut}_K(L))$ is a normal subgroup of G. But then one easily sees that $H \cdot H' = \langle H, H' \rangle$. A similar statement holds if L'/K is normal. Furthermore, as H and H' are compact groups, one sees that $H \cdot H'$ is closed. Hence $\overline{\langle H, H' \rangle} = H \cdot H'$. From 4.1, as L/K is separable, it follows that $H \cdot H' = \overline{\langle H, H' \rangle} = G$. The result follows. □

Proof of Proposition 3.13. Let $\mathfrak{L}$ be the set of subfields F of L such that the natural map $L \otimes_F L'F \to LL'$ is an isomorphism. Consider the notation from i. Directly from the definitions it follows that for a subfield F of L we have $F \in \mathfrak{L}$ iff $\mathfrak{B}$ spans $L'F$ as F-vector space. But $L'F$ is generated as an F-vector space by L' and each $x \in L'$ can be written in a unique way as $x = \sum_{b \in \mathfrak{B}} c_{x,b} b$ where $c_{x,b} \in L$ and almost all $c_{x,b}$ are 0. Let $\mathbf{F}$ be the primefield of L. Hence we conclude that $F \in \mathfrak{L}$ iff for all $x \in L$ and $b \in \mathfrak{B}$ we have $c_{x,b} \in F$ iff F contains $M = \mathbf{F}(c_{x,b} : x \in L, b \in \mathfrak{B})$. Description ii follows directly from description one since we can extend an independent set to a basis. □

Definition 4.3. The field M in the above theorem is called the *field of definition* of L' over L and is denoted by $L \setminus\!\!\setminus L'$.

We deduce some properties of $L \setminus\!\!\setminus L'$.

Lemma 4.4. *Let Ω be a field and let $L, L' \subseteq \Omega$ be subfields. Then the following hold:*

i. $L \cap L' \subseteq L \setminus\!\!\setminus L'$;

ii. $L \cap L' = L \setminus\!\!\setminus L'$ *iff* $L \cap L' = L' \setminus\!\!\setminus L$ *iff* $L \setminus\!\!\setminus L' = L' \setminus\!\!\setminus L$.

Proof. i: Suppose $x \in L \cap L' \setminus L \setminus\!\!\setminus L'$. Then the nonzero element $x \otimes 1 - 1 \otimes x$ maps to zero under $L \otimes_{L \setminus\!\!\setminus L'} (L \setminus\!\!\setminus L')L' \to LL'$, contradiction.

ii: By symmetry, it suffices to show that the first and last statement are equivalent. Suppose that $L \cap L' = L \setminus\!\!\setminus L'$. Then one has an isomorphism $L \otimes_{L \cap L'} (L \cap L')L' \to LL'$ and from i one deduces that $L' \setminus\!\!\setminus L = L' \cap L = L \setminus\!\!\setminus L'$. Suppose $L \setminus\!\!\setminus L' = L' \setminus\!\!\setminus L$. Then one has $L \setminus\!\!\setminus L' \subseteq L \cap L'$ and the result follows from i. □

Lemma 4.5. *Let G be a group and let $H, H' \subseteq G$ be subgroups. Let J' be a subgroup of HH' containing H. Then H acts transitively on $J'/J' \cap H'$ if and only if J' is contained in the group $\{g \in G : gHH' = HH'\}$.*

PROOF. First notice $J'/J'\cap H' \cong J'(H'/H') \subseteq G/H'$ (as J'-sets). Put $x = H'/H'$. Hence we need to find the largest J' such that H acts transitively on $J'x$, that is $Hx = J'x$. Notice that $J = \{g \in G : gHH' = HH'\} = \{g \in G : gHx = Hx\}$. If H acts transitively on $J'x$, we have for $j' \in J'$:

$$j'Hx = j'J'x = J'x = Hx,$$

hence $j' \in J$. Conversely, J is a subgroup containing H with the property that $Jx = JHx = Hx$. □

Proposition 4.6. *Let L, L' be subfields of a field Ω. Assume that $L/L\cap L'$ is separable. Let M be a normal extension of $L \cap L'$ containing LL' with groups $G = \mathrm{Aut}_{L\cap L'}(M)$, $H = \mathrm{Aut}_L(M)$ and $H' = \mathrm{Aut}_{L'}(M)$. Let $J = \{g \in G : gHH' = HH'\}$. Then one has:*

$$L \setminus L' = (LL')^J \cap L.$$

PROOF. Proposition 4.2 shows that we need to find a maximal subgroup $J' \subseteq HH'$ containing H such that H acts transitively on $J'/J'\cap H'$. The unique maximal subgroup with this property is J (Lemma 4.5). It remains to show that J is a closed subgroup. Notice that H and H' are compact, and hence that HH' is compact (because it is the image of $H \times H'$ under the map $G \times G \to G$) and since we are in a Hausdorff space, it is closed. Similarly, $H'H$ is compact and hence closed. Note that the translation maps are continous. One then has

$$J = \bigcap_{\tau \in HH'} \left(\tau H'H \cap HH'\tau^{-1}\right).$$

Hence J is an intersection of closed subgroups, and hence closed. □

4.1.2. *Separably disjoint extensions.* Let L/K be an algebraic extension of fields and let p be the characteristic of K if this is nonzero, and 1 otherwise. Then we put

$$L_{K,\mathrm{ins}} = \left\{x \in L : \exists j \in \mathbf{Z}_{\geq 0} : x^{p^j} \in K\right\},$$

the maximal purely inseparable field extension of K in L. Notice that $L_{K,\mathrm{ins}} \cap L_{K,\mathrm{sep}} = K$.

Definition 4.7. An algebraic field extension L/K is called *separably disjoint* if $L = L_{K,\mathrm{sep}}L_{K,\mathrm{ins}}$.

Lemma 4.8. *Let L/K be an algebraic extension of valued fields. Then L/K is separably disjoint if and only if $L/L_{K,\mathrm{ins}}$ is separable.*

PROOF. $\Longrightarrow$: Follows directly from the definitions.

$\Longleftarrow$: Note that $L/L_{K,\mathrm{sep}}$ is purely inseparable and hence $L/L_{K,\mathrm{sep}}L_{K,\mathrm{ins}}$ is purely inseparable and separable. It follows that $L = L_{K,\mathrm{sep}}L_{K,\mathrm{ins}}$. □

Proposition 4.9. *Let L/K be a normal extension of fields. Then L/K is separably disjoint.*

PROOF. See [**Lan02**, Chapter V, Proposition 6.11].

Here is a similar proof. Take $x \in L \setminus L_{K,\mathrm{ins}}$. As x is not purely inseparable over $L_{K,\mathrm{ins}}$ and as L/K is normal, there is an element of $\mathrm{Aut}_K(L)$ which does not fix x (use Zorn to find such a morphism). Hence $L^{\mathrm{Aut}_K(L)} = L_{K,\mathrm{ins}}$ and from Galois theory it follows that $L/L_{K,\mathrm{ins}}$ is separable. Apply Lemma 4.8. □

Notice that any algebraic field extension L/K has a unique maximal separably disjoint subextension, namely $L_{K,\mathrm{sep}}L_{K,\mathrm{ins}}$.

Proposition 4.10. *Let L/K be an algebraic extension of fields. Then*

$$\begin{aligned}\varphi\colon \{E : K \subseteq E \subseteq L\} &\to \{(D,F) : K \subseteq D \subseteq L_{K,\mathrm{sep}} \subseteq F \subseteq L,\ F/D \text{ sep. disj.}\}\\ E &\mapsto (E_{K,\mathrm{sep}}, EL_{K,\mathrm{sep}})\end{aligned}$$

is a bijection with inverse

$$(D,F) \mapsto F_{D,\mathrm{ins}}.$$

PROOF. First we show that φ is well-defined. Notice that $E/E_{K,\mathrm{sep}}$ is purely inseparable and that $L_{K,\mathrm{sep}}/E_{K,\mathrm{sep}}$ is separable. Hence we find that $EL_{K,\mathrm{sep}}/E_{K,\mathrm{sep}}$ is separably disjoint.

Let ψ be the proposed inverse as above. We have $\psi(\varphi(E)) = (EL_{K,\mathrm{sep}})_{E_{K,\mathrm{sep}},\mathrm{ins}}$, and this is equal to E since it obviously contains E and $EL_{K,\mathrm{sep}}/E$ is separable. Conversely we have $\varphi(\psi((D,F))) = ((F_{D,\mathrm{ins}})_{K,\mathrm{sep}}, F_{D,\mathrm{ins}}L_{K,\mathrm{sep}})$. One directly finds $(F_{D,\mathrm{ins}})_{K,\mathrm{sep}} = D$. As F/D is separably disjoint, we find $F_{D,\mathrm{ins}}L_{K,\mathrm{sep}}) = F$. This shows that both maps are inverse to each other. □

4.2. Tate's lemma. Let G be a compact topological group which acts continuously on a commutative ring A which is endowed with the discrete topology. This means that the map $G \times A \to A$ is continuous. For $a \in A$ the map $G \times \{a\} \to A$ is continuous and the image is compact and hence finite. This shows that all orbits are finite.

Proposition 4.11 (Tate)**.** *Let (G,A) be as above. Let R be a domain and let $\sigma, \tau\colon A \to R$ be ring morphisms. Suppose that $\sigma|_{A^G} = \tau|_{A^G}$. Then there exists $g \in G$ such that $\tau = \sigma \circ g$.*

PROOF. Let $E \subseteq A$ be a finite set. Let $f_E \in A[Y]$ be a polynomial such that all elements of E occur as coefficients of f_E. Extend the action of G to $A[Y][X]$ by letting G act on the coefficients. We extend $\sigma, \tau\colon A[Y][X] \to R[Y][X]$ by $X \mapsto X$, $Y \mapsto Y$. Then consider the polynomial $h_E = \prod_{h' \in Gf_E}(X - h') \in A^G[Y][X]$. We have

$$\prod_{h' \in Gf_E}(X - \sigma(h')) = \sigma(h_E) = \tau(h_E) = \prod_{h' \in Gf_E}(X - \tau(h')).$$

As $R[Y]$ is a domain, we can compare the roots and conclude that there is $g \in G$ such that $\tau(h_E) = \sigma(g(h_E)) \in R[Y][X]$. Hence for this g we have $\tau|_E = \sigma \circ g|_E$.

For any $E \subseteq A$ put $G_E = \{g \in G : \tau|_E = \sigma \circ g|_E\}$. Notice that $G_{\bigcup_i E_i} = \bigcap_i G_{E_i}$ for any collection of subsets $E_i \subseteq A$. For finite E we have shown $G_E \neq \emptyset$. We claim that for finite E the set G_E is closed in G. One easily shows that for $e \in E$ the map

$\psi_e\colon G \to R$ given by $\psi_e(g) = \sigma(e) - \tau(g(e))$ is continuous. Hence $\psi_e^{-1}(0) = G_{\{e\}}$ is closed. As $G_E = \bigcap_{e\in E} G_{\{e\}}$, the set G_E is closed.

By compactness of G we have $G_A = \bigcap_{E\subseteq A,\ E \text{ finite}} G_E \neq \emptyset$. This means that there is $g \in G$ such that $\tau = \sigma \circ g$. □

Corollary 4.12. *Suppose that (G, A) is as above. Let $\mathfrak{p} \subset A^G$ be prime. Then G acts transitively on the set of primes of A lying above $\mathfrak{p}$.*

Proof. Let $\mathfrak{q}, \mathfrak{q}' \subset A$ be primes lying above $\mathfrak{p}$. We will now construct two maps from A to $\overline{Q(A^G/\mathfrak{p})}$, the algebraic closure of $Q(A^G/\mathfrak{p})$. Since the orbits of the actions are finite, the extension $Q(A/\mathfrak{q}) \supseteq Q(A^G/\mathfrak{p})$ is algebraic. Hence there is a morphism $\sigma\colon A \to A/\mathfrak{q} \to Q(A/\mathfrak{q}) \to \overline{Q(A^G/\mathfrak{p})}$ which is the identity on $A^G/\mathfrak{p}$. Similarly one defines another map $\tau\colon A \to A/\mathfrak{q}' \to Q(A/\mathfrak{q}') \to \overline{Q(A^G/\mathfrak{p})}$. Both maps agree on A^G. Proposition 4.11 says that there is $g \in G$ such that $\tau = \sigma g$. Taking kernels gives $\mathfrak{q}' = \ker\tau = \ker(\sigma g) = g^{-1}(\ker\sigma) = g^{-1}\mathfrak{q}$. We get $g\mathfrak{q}' = \mathfrak{q}$ and this finishes the proof. □

Corollary 4.13. *Let (G, A) be as above. Let $\mathfrak{q} \subset A$ be a prime lying above a prime $\mathfrak{p} \subset A^G$. Let $G_{\mathfrak{q}/\mathfrak{p}} = \{g \in G : g(\mathfrak{q}) = \mathfrak{q}\}$. Let $l = Q(A/\mathfrak{q})$ and let $k = Q(A^G/\mathfrak{p})$. Then the natural map $G_{\mathfrak{q}/\mathfrak{p}} \to \mathrm{Aut}_k(l)$ is surjective and l/k is normal algebraic.*

Proof. It is easy to see that l/k is algebraic. Let $\overline{k}$ be an algebraic closure of k containing l. We have a natural map $G_{\mathfrak{q}/\mathfrak{p}} \to \mathrm{Aut}_k(l) \subseteq \mathrm{Hom}_k(l, \overline{k})$. Let $\varphi \in \mathrm{Hom}_k(l, \overline{k})$. Consider the natural map $\sigma\colon A \to Q(A/\mathfrak{q}) = l \subseteq \overline{k}$, which restricts to the natural map $A^G \to Q(A^G/\mathfrak{p}) = k$. Let $\tau = \varphi\sigma$. Apply Proposition 4.11 to see that there is $g \in G$ with $\varphi\sigma = \sigma g$. But then for $a \in A$ we have

$$g \circ (\sigma(a)) = \sigma(g(a)) = \varphi\sigma(a).$$

This means that g maps to σ. It follows that $\mathrm{Aut}_k(l) = \mathrm{Hom}_k(l, \overline{k})$ and hence l/k is normal. □

4.3. Ordered abelian groups.

Lemma 4.14. *Let $(P, \leq)$ be an ordered abelian group. Let $n \in \mathbf{Z}_{\geq 1}$ and $x, y \in P$. If $nx = ny$, then one has $x = y$. The group P has no non-trivial torsion and $P \otimes_{\mathbf{Z}} \mathbf{Q}$ is an ordered abelian group where we put $x \leq y$ if for all $n \in \mathbf{Z}_{\geq 1}$ such that $nx, ny \in P$ we have $nx \leq ny$.*

Proof. Suppose that $x < y$. Then $x + x < x + y < y + y$, and in a similar fashion, $nx < ny$, which is a contradiction.

If x is torsion, apply the first part to x and 0 to obtain the second result.

The last part is an easy calculation which is left to the reader. □

Let $(P, \leq)$ and $(Q, \leq)$ be ordered abelian groups. A morphism $\varphi\colon P \to Q$ is a group homomorphism respecting the ordering. One easily sees that respecting the order is equivalent to $p \geq 0 \implies \varphi(p) \geq 0$. Indeed, let $p, p' \in P$ with $p \geq p'$. Then we have $p - p' \geq 0$, which gives $\varphi(p) - \varphi(p') = \varphi(p - p') \geq 0$. This gives $\varphi(p) \geq \varphi(p')$.

Lemma 4.15. *Let $(P, \leq)$ be an ordered abelian group and let $\varphi \in \mathrm{Aut}(P)$ such that all orbits are finite. Then φ is the identity.*

PROOF. Let $p \in P$ and assume that $\varphi^n(p) = p$. Then one has $p = \varphi^n(p) \geq \ldots \geq \varphi(p) \geq p$. Hence we obtain $\varphi(p) = p$. □

5. Extending valuations

Lemma 5.1. *Let (K, v) be a valued field. Then $\mathcal{O}_v$ is integrally closed.*

PROOF. Suppose $x \in \mathcal{O}_v$ nonzero is integral over $\mathcal{O}_v$. Then there is a relation $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ with $a_i \in \mathcal{O}_v$ and this shows that $x \in \mathcal{O}_v[x] \cap \mathcal{O}_v[x^{-1}]$. By the definition of a valuation ring we have $\mathcal{O}_v[x] \cap \mathcal{O}_v[x^{-1}] = \mathcal{O}_v$ and the result follows. □

Proposition 5.2. *Let K be a field. Let $R \subseteq K$ be a subring and let $\mathfrak{p} \in \mathrm{Spec}(R)$. Let $S = \{(A, I) : R \subseteq A \subseteq K,\ A \text{ ring},\ I \subseteq A \text{ ideal},\ I \cap R = \mathfrak{p}\}$, ordered by $(A, I) \leq (B, J)$ if $A \subseteq B$ and $I \subseteq J$. Then a pair $(\mathcal{O}, \mathfrak{m})$ is maximal if and only if $\mathcal{O}$ is a valuation ring of K and $\mathfrak{m}$ is its maximal ideal.*

PROOF. Let $(\mathcal{O}, \mathfrak{m})$ be a maximal element of S. Notice that $\mathfrak{m}_\mathfrak{p} \subset \mathcal{O}_\mathfrak{p}$ satisfies $\mathfrak{m}_\mathfrak{p} \cap R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$ and $\mathfrak{m}_\mathfrak{p} \cap R = \mathfrak{p}$. Hence by maximality we have $\mathcal{O} = \mathcal{O}_\mathfrak{p}$ and $\mathfrak{m} = \mathfrak{m}_\mathfrak{p}$. A maximal ideal of $\mathcal{O}$ containing $\mathfrak{m}$ still lies above the maximal ideal of $R_\mathfrak{p}$. We conclude that $\mathfrak{m}$ is maximal.

We claim that $\mathcal{O}$ is a valuation ring. Suppose that there is $x \in K^*$ with $x, x^{-1} \notin \mathcal{O}$. From the maximality and the fact that $\mathfrak{m}$ lies above $\mathfrak{p}R_\mathfrak{p}$ one obtains $\mathfrak{m}\mathcal{O}[x] = \mathcal{O}[x]$ and $\mathfrak{m}\mathcal{O}[x^{-1}] = \mathcal{O}[x^{-1}]$. Take n, m minimal such that $1 = \sum_{i=0}^{n} a_i x^i$, $1 = \sum_{i=0}^{m} b_i x^{-i}$ with $a_i, b_i \in \mathfrak{m}$. Without loss of generality, assume $m \leq n$. Multiply the second equation by x^n, and notice that $1 - b_0 \in \mathcal{O}^*$, to obtain $x^n = \frac{1}{1-b_0} \sum_{i=1}^{m} b_i x^{n-i}$. Use this relation together with the first relation to see that n is not minimal, contradiction.

Conversely, suppose that $\mathcal{O}$ is a valuation ring of K with maximal ideal $\mathfrak{m}$, containing R and satisfying $\mathfrak{m} \cap R = \mathfrak{p}$. Suppose that $(\mathcal{O}, \mathfrak{m}) \leq (A, \mathfrak{n})$. Let $x \in A$ nonzero. Then $xx^{-1} = 1 \notin \mathfrak{n}$ and hence $x^{-1} \notin \mathfrak{m}$. As $\mathcal{O}$ is a valuation ring, we obtain $x \in \mathcal{O}$. Hence $(\mathcal{O}, \mathfrak{m})$ is maximal. □

Since we assume the Axiom of Choice, maximal elements as in Proposition 5.2 exist.

Corollary 5.3. *Let $R \subseteq L$ be a subring where L is a field. Then the intersection of all valuation rings of L containing R in L is the integral closure of R in L.*

PROOF. As a valuation ring is integrally closed (Lemma 5.1), the right hand side is contained in the left hand side. Suppose $x \in L$ is not integral over R. Consider the ring $R[x^{-1}]$, which does not contain x as x is not integral. Hence x^{-1} is contained in a maximal ideal $\mathfrak{m} \subset R[x^{-1}]$. Proposition 5.2 gives us a valuation v with $x^{-1} \in \mathfrak{m}_v \cap R[x^{-1}] = \mathfrak{m}$. This is equivalent to $x \notin \mathcal{O}_v$. □

Proposition 5.4. *Let (K, v) be a valued field and let L/K be an algebraic extension of fields. Let R be the integral closure of $\mathcal{O}_v$ in L. Then there is a bijection between the set of maximal ideals of R and the set of valuations extending v to L, given by $\mathfrak{m} \mapsto R_\mathfrak{m}$. The inverse maps a valuation $\mathcal{O}$ with maximal ideal $\mathfrak{m}$ to $\mathfrak{m} \cap R$.*

PROOF. Let $\mathfrak{p} \in \mathrm{MaxSpec}(R)$. Then by Proposition 5.2 there exists a valuation ring $\mathcal{O}_w$ of L with $\mathcal{O}_w \supseteq R_{\mathfrak{p}}$ and $\mathfrak{m}_w \cap R = \mathfrak{p}$. We will show $R_{\mathfrak{p}} = \mathcal{O}_w$.

Let $a \in \mathcal{O}_w$ nonzero. As L/K is algebraic, there exists is a polynomial $f = \sum_{i=0}^{n} a_i x^i \in \mathcal{O}_v[x]$ with $f(a) = 0$ and a coefficient which is not in the maximal ideal. Let k minimal such that $a_{k+1}, \ldots, a_n \in \mathfrak{m}_v$. Put $f_0 = a_0 + \ldots + a_{k-1}x^{k-1}$ and $-f_1 = a_k + \ldots + a_n x^{n-k}$. Note that $f_1(a) \in \mathcal{O}_w^*$. Then from $0 = f(a) = f_0(a) - a^k f_1(a)$ we obtain for $b = f_0(a)a^{-k+1} \in \mathcal{O}_v[a^{-1}]$, $c = f_1(a) \in \mathcal{O}_v[a] \setminus \{0\}$ that $a = \frac{b}{c}$. We claim: $b, c \in R$. It is enough to show that b and c are contained in any valuation ring extending R (Corollary 5.3). Let $\mathcal{O}$ be such a valuation ring. If $a \in \mathcal{O}$, then one has $c \in \mathcal{O}$ and hence $b = ac \in \mathcal{O}$. If $a \notin \mathcal{O}$, then one has $a^{-1} \in \mathcal{O}$. Hence $b \in \mathcal{O}$ and $c = ba^{-1} \in \mathcal{O}$. This finishes the proof of the claim. Furthermore, by construction we have $c \notin \mathfrak{m}_w$. Hence $c \notin \mathfrak{m}_w \cap R = \mathfrak{p}$. We see that $a = \frac{b}{c} \in R_{\mathfrak{p}}$. This gives $R_{\mathfrak{p}} = \mathcal{O}_w$ and this shows that the proposed map is well-defined.

Suppose w extends v to L. We want to show that $\mathfrak{m}_w \cap R$ is a maximal ideal of R. But $\mathfrak{m}_w \cap \mathcal{O}_v$ is maximal, and $\mathcal{O}_v \to R$ is integral. Hence by [**AM69**, Corollary 5.8] $\mathfrak{m}_w \cap R$ is a maximal ideal of R. This shows that the proposed inverse is well-defined.

Note that for $\mathfrak{p} \in \mathrm{MaxSpec}(R)$ we have $\mathfrak{p} = \mathfrak{p}R_{\mathfrak{p}} \cap R$. Furthermore, we have already seen $R_{\mathfrak{m}_w \cap R} = \mathcal{O}_w$. This shows that both maps are inverse to each other. □

We will now prove a weak approximation theorem.

Corollary 5.5. *Let (K, v) be a field and let L/K be an algebraic field extension. Let $w_1, \ldots, w_n$ be different extensions of v to L. Let $(a_i)_{i=1}^n \in \prod_{i=1}^n \mathcal{O}_{w_i}$ and $r_1, \ldots, r_n \in \mathbf{Z}_{\geq 1}$ be given. Then there exists $a \in L$ with $a - a_i \in \mathfrak{m}_{w_i}^{r_i}$ for $i = 1, \ldots, n$.*

PROOF. Let R be the integral closure of $\mathcal{O}_v$ in L. Proposition 5.4 gives us maximal ideals $\mathfrak{m}_i \in \mathrm{MaxSpec}(R)$ with $R_{\mathfrak{m}_i} = \mathcal{O}_{w_i}$. Using the Chinese remainder theorem, one obtains a surjective map $R \to \prod_{i=1}^n R/\mathfrak{m}_i^{r_i} = \prod_{i=1}^n \mathcal{O}_{w_i}/\mathfrak{m}_{w_i}^{r_i}$ and the result follows. □

Proposition 5.6. *Let (K, v) be a valued field and let L/K be a field extension. Then one has $1 \leq \mathrm{g}_{L,v}$ and $\mathrm{g}_{L,v} = 1$ if L/K is purely inseparable. If (L, x) a finite extension of (K, v), then one has $\mathrm{e}(x/v)\,\mathrm{f}(x/v) \leq [L : K]$ and $\mathrm{g}_{L,v}$ is finite. If the extension is normal with group $G = \mathrm{Aut}_K(L)$, then G acts transitively on the set of valuations extending v to L, and $\mathrm{e}(x/v)$ and $\mathrm{f}(x/v)$ do not depend on the choice of x.*

PROOF. The fact that $\mathrm{g}_{L,v} \geq 1$ follows from Proposition 5.2.

Assume that L/K is purely inseparable. Let x be an extension of v to L. Then one directly sees $\mathfrak{m}_x = \{r \in L : \exists i : r^{\mathrm{p}_v^i} \in \mathfrak{m}_v\}$. A valuation is determined by its maximal ideal.

Assume that L/K is finite. Take a preimage $S \subseteq L$ of a basis of $\mathrm{k}_x/\mathrm{k}_v$ and take $T \subseteq L^*$ elements which map bijectively to Δ_x/Δ_v. The one easily sees that ST of cardinality $\mathrm{e}(x/v)\,\mathrm{f}(x/v)$ is linearly independent over K and $\mathrm{e}(x/v)\,\mathrm{f}(x/v) \leq [L : K]$ follows.

Assume that L/K is normal. The transitivity follows from Corollary 4.12 and Proposition 5.4, and the statements about $\mathrm{e}(x/v)$ and $\mathrm{f}(x/v)$ are obvious. In particular, if L/K is finite normal, the quantity $\mathrm{g}_{L,v}$ is finite. It follows from Proposition 5.2 that $\mathrm{g}_{L,v}$ is finite when L/K is finite. □

Lemma 5.7. *Let (K,v) be a valued field and let L be a finite normal extension of K of degree n. Assume that x is the unique extension of v to L. Then for all $a \in L$ one has $x(a) = \frac{1}{n} v(N_{L/K}(a))$. Furthermore, we have $n\Delta_x \subseteq \Delta_v$.*

Proof. Let $G = \mathrm{Aut}(L/K)$. Then it is well-known that for $a \in L$ one has $N_{L/K}(a) = \left(\prod_{g\in G} g(a)\right)^{[L:K]_{\mathrm{i}}}$. We have, keeping in mind Lemma 4.14,

$$x(a) = \frac{[L:K]_{\mathrm{i}}}{n} \sum_{g\in G} x(g(a)) = \frac{1}{n} x(N_{L/K}(a)) = \frac{1}{n} v(N_{L/K}(a)).$$

The last result follows directly. □

Lemma 5.8. *Let $(L,w) \supseteq (K,v)$ be a finite purely inseparable extension of valued fields. Then $\mathrm{k}_w/\mathrm{k}_v$ is purely inseparable and we have $\mathrm{e}(w/v) = \mathrm{e}_{\mathrm{w}}(w/v)$.*

Proof. It is obvious that $\mathrm{k}_w/\mathrm{k}_v$ is purely inseparable. Proposition 5.6 together with Lemma 5.7 imply $\mathrm{e}(w/v) = \mathrm{e}_{\mathrm{w}}(w/v)$. □

6. Normal extensions

We will first consider finite extensions of valued fields, and then take a limit.

6.1. Finite normal extensions. In this subsection we let $(M,x) \supseteq (K,v)$ be a finite normal extension of valued fields with $G = \mathrm{Aut}_K(M)$. For simplicity, we put $x_{\mathrm{i}} = x|_{K_{\mathrm{i},x}}$, $x_{\mathrm{h}} = x|_{K_{\mathrm{h},x}}$, $x_{\mathrm{v}} = x|_{K_{\mathrm{v},x}}$ and $x_{\mathrm{s}} = x|_{M_{K,\mathrm{sep}}}$.

Proposition 6.1. *One has $[K_{\mathrm{h},x} : K] = \mathrm{g}_{M,v}$. Furthermore x is the unique extension of x_{h} to M and one has $\mathrm{e}(x_{\mathrm{h}}/v) = \mathrm{f}(x_{\mathrm{h}}/v) = 1$.*

Proof. Since the action of G on the set of valuations of M extending v is transitive (Proposition 5.6), we have $[K_{\mathrm{h},x} : K] = \mathrm{g}_{M,v}$. The second statement also follows from the transitivity of the action.

We will show $\mathrm{f}(x_{\mathrm{h}}/v) = 1$. Let $a \in \mathcal{O}_{x_{\mathrm{h}}}$, and pick $\alpha_a \in K_{\mathrm{h},x}$ satisfying $\alpha_a - a \in \mathfrak{m}_{x_{\mathrm{h}}}$ and α_a in the maximal ideal of any other valuation extending v to $K_{\mathrm{h},x}$ (Corollary 5.5). This means that for $\overline{g} \in G/\,\mathrm{D}_{x,K}$ with $g \neq \mathrm{D}_{x,K}$ we have $g(\alpha) \in \mathfrak{m}_{x_{\mathrm{h}}}$. Then, by looking in M, one obtains

$$\mathrm{tr}_{K_{\mathrm{h},x}/K}(\alpha_a) = \sum_{\overline{g}\in G/\,\mathrm{D}_{x,K}} g(\alpha) \in a + \mathfrak{m}_{x_{\mathrm{h}}}.$$

Notice that $\mathrm{tr}_{K_{\mathrm{h},x}/K}(\alpha_a) \in K \cap \mathcal{O}_{x_{\mathrm{h}}} = \mathcal{O}_v$. Hence the natural map $\mathrm{k}_v \to \mathrm{k}_{x_{\mathrm{h}}}$ is surjective. This gives $\mathrm{f}(x_{\mathrm{h}}/v) = 1$.

Next we will prove $\mathrm{e}(x_{\mathrm{h}}/v) = 1$. Let $b \in K^*_{\mathrm{h},x}$. Take $m \in \mathbf{Z}$ such that for all $g \in G \setminus \mathrm{D}_{x,K}$, we have $x_{\mathrm{h}}(\alpha_1^m b) \neq x_{\mathrm{h}}(g(\alpha_1^m b))$. To do this, one needs to make sure that for all $g \in G \setminus \mathrm{D}_{x,K}$ one has $m(x(\alpha_1) - x(g(\alpha_1))) \neq x(g(b)) - x(b)$, which can easily be achieved since $x(\alpha_1) \neq x(g(\alpha_1))$, the group Δ_x is torsion-free and G is finite. Put $\beta = \alpha_1^m b$ and $f = \prod_{\overline{g}\in G/\,\mathrm{D}_{x,K}} (X - \overline{g}(\beta)) = \sum_{i=0}^n a_i X^i \in K[X]$ with $a_n = 1$. Let $S = \{\overline{g}(\beta) : \overline{g} \in G/\,\mathrm{D}_{x,K} \text{ s.t. } x_{\mathrm{h}}(\overline{g}(\beta)) < x_{\mathrm{h}}(\beta)\}$ and set $r = \#S$. Then one sees $x_{\mathrm{h}}(a_{n-r}) = x_{\mathrm{h}}(\prod_{c\in S} c)$ and $x_{\mathrm{h}}(a_{n-r-1}) = x_{\mathrm{h}}(\beta \prod_{c\in S} c)$. This gives $x_{\mathrm{h}}(b) = x_{\mathrm{h}}(\beta) = x_{\mathrm{h}}(a_{n-r-1}/a_{n-r}) \in \Delta_v$ and we are done. □

Proposition 6.2. *We have a short exact sequence*

$$0 \to \mathrm{I}_{x,K} \to \mathrm{D}_{x,K} \to \mathrm{Aut}_{\mathrm{k}_v}(\mathrm{k}_x) \to 0$$

and k_x *is normal over* k_v*. Furthermore we have* $[K_{\mathrm{i},x} : K_{\mathrm{h},x}] = \mathrm{f}(x_\mathrm{i}/x_\mathrm{h}) = \mathrm{f}_\mathrm{s}(x_\mathrm{i}/x_\mathrm{h}) = \mathrm{f}_\mathrm{s}(x/v)$ *and* $\mathrm{e}(x_\mathrm{i}/x_\mathrm{h}) = 1$*.*

Proof. The exactness of the sequence and the normality of k_x over k_v follow from Corollary 4.13 and Proposition 5.4. We will now prove the last two statements. Look at the normal extension $M/K_{\mathrm{i},x}$ with group $\mathrm{I}_{x,K}$. From the exact sequence for the extension $M/K_{\mathrm{i},x}$ just obtained we see that the zero map $\mathrm{I}_{x,K} \to \mathrm{Aut}_{\mathrm{k}_{x_\mathrm{i}}}(\mathrm{k}_x)$ is surjective. We find $\mathrm{Aut}_{\mathrm{k}_{x_\mathrm{i}}}(\mathrm{k}_x) = 0$. As $\mathrm{k}_x/\mathrm{k}_{x_\mathrm{i}}$ is normal, this gives that $\mathrm{k}_x/\mathrm{k}_{x_\mathrm{i}}$ is purely inseparable. Consider the Galois extension $K_{\mathrm{i},x}/K_{\mathrm{h},x}$ with group $\mathrm{D}_{x,K}\,/\,\mathrm{I}_{x,K}$. We obtain an exact sequence $\mathrm{D}_{x,K}\,/\,\mathrm{I}_{x,K} \to \mathrm{Aut}_{\mathrm{k}_{x_\mathrm{h}}}(\mathrm{k}_{x_\mathrm{i}}) = \mathrm{Aut}_{\mathrm{k}_v}(\mathrm{k}_x) \to 0$ (note that $\mathrm{k}_v = \mathrm{k}_{x_\mathrm{h}}$ by Proposition 6.1). The first map is injective and hence we have an isomorphism. Using Proposition 5.6 we obtain:

$$\begin{aligned}\mathrm{e}(x_\mathrm{i}/x_\mathrm{h}) \cdot \mathrm{f}(x_\mathrm{i}/x_\mathrm{h}) &\le [K_{\mathrm{i},x} : K_{\mathrm{h},x}] = \#\,\mathrm{Aut}_{\mathrm{k}_{x_\mathrm{h}}}(\mathrm{k}_{x_\mathrm{i}}) \\ &= \#\,\mathrm{Aut}_{\mathrm{k}_v}(\mathrm{k}_x) \le [\mathrm{k}_{x_\mathrm{i}} : \mathrm{k}_{x_\mathrm{h}}] = \mathrm{f}(x_\mathrm{i}/x_\mathrm{h}).\end{aligned}$$

Hence we find $[K_{\mathrm{i},x} : K_{\mathrm{h},x}] = \mathrm{f}(x_\mathrm{i}/x_\mathrm{h}) = \mathrm{f}_\mathrm{s}(x_\mathrm{i}/x_\mathrm{h}) = \mathrm{f}_\mathrm{s}(x/v)$ and $\mathrm{e}(x_\mathrm{i}/x_\mathrm{h}) = 1$. □

Lemma 6.3. *Let* $0 \to A \to B \xrightarrow{f} C \to 0$ *be an exact sequence of abelian groups. Let* H *be the group of automorphisms of this sequence consisting of automorphisms which are the identity on* C*. Let* $H' \subseteq H \subseteq \mathrm{Aut}(B)$ *the set of automorphisms which are the identity on* A*. Then the map*

$$\begin{aligned}\varphi\colon H &\to \mathrm{Hom}(C, A) \rtimes \mathrm{Aut}(A) \\ h &\mapsto (f(b) \mapsto h(b) - b, h|_A)\end{aligned}$$

is an injective morphism of groups. One has:

i. $\varphi|_{H'}\colon H' \to \mathrm{Hom}(C, A)$ *is an isomorphism;*
ii. *if* $0 \to A \to B \to C \to 0$ *is split, then* φ *is an isomorphism.*

Proof. One easily shows that φ is well-defined and that it is a morphism of groups.

i: Consider the following map:

$$\begin{aligned}\psi\colon \mathrm{Hom}(C, A) &\to H' \\ \sigma &\mapsto (b \in B \mapsto b + \sigma(f(b)))\end{aligned}$$

One then easily checks that this is the inverse of $\varphi|_{H'}$. This also shows that φ is injective.

ii: Consider the exact sequence $0 \to A \to A \oplus C \to C \to 0$. Consider the map

$$\begin{aligned}\chi\colon \mathrm{Hom}(C, A) \rtimes \mathrm{Aut}(A) &\to H \\ (\sigma, \tau) &\mapsto ((a, c) \mapsto (\sigma(c) + \tau(a), c))\,.\end{aligned}$$

One easily checks that both maps are inverse to each other. □

We have an exact sequence $1 \to \mathcal{O}_x^*/(1+\mathfrak{m}_x) \cong \mathrm{k}_x^* \to M^*/(1+\mathfrak{m}_x) \to \Delta_x \to 1$. Note that $\mathrm{D}_{x,K}$ acts on such sequences and it acts on this sequence trivially on Δ_x (Lemma 4.15), it fixes $K^*/(1+\mathfrak{m}_v)$ and the action on k_x^* comes from a field automorphism. Set $\Gamma_{x,v} = \operatorname{im}\left(\operatorname{Aut}_{\mathrm{k}_v}(\mathrm{k}_x) \to \operatorname{Aut}_{\mathrm{k}_v^*}(\mathrm{k}_x^*)\right)$. Let $\operatorname{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x))$ be the group of automorphisms of the sequence, seen as subgroup of $\operatorname{Aut}(M^*/(1+\mathfrak{m}_x))$, which are the identity on $K^*/(1+\mathfrak{m}_x)$ and which induce an element of $\Gamma_{x,v}$ on k_x^* (note that the two conditions already imply that they act as the identity on Δ_x). We get a morphism $\mathrm{D}_{x,K} \to \operatorname{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x))$.

Note that the group $\mathrm{I}_{x,K}$ acts trivially on k_x^* and $K^*/(1+\mathfrak{m}_v)$ and Δ_x. The automorphisms of the exact sequence with these properties correspond to $\operatorname{Hom}(\Delta_x/\Delta_v, \mathrm{k}_x^*)$ by Lemma 6.3 and this gives a morphism

$$\begin{aligned} \mathrm{I}_{x,K} &\to \operatorname{Hom}(\Delta_x/\Delta_v, \mathrm{k}_x^*) \\ g &\mapsto \left(\overline{c} \mapsto \overline{g(c)/c}\right). \end{aligned}$$

By definition $\mathrm{V}_{x,K}$ is the kernel of the last morphism.

Lemma 6.4. *Let $(L',u') \supseteq (L,u)$ be a finite normal extension of valued fields with group H. Assume that for all $a \in L'^*$ and $h \in H$ we have*

$$\frac{h(a)}{a} \in 1+\mathfrak{m}_{u'}.$$

Then H is a p_u-group.

Proof. We can directly reduce to the case where L'/L is Galois and $[L':L] > 1$. Let $a \in L'^*$ satisfy $\operatorname{tr}_{L'/L}(a) = 0$, which exists by looking at dimensions. Then we have

$$0 = \frac{\operatorname{tr}_{L'/L}(a)}{a} \in [L':L] + \mathfrak{m}_{u'}.$$

This shows $\#H = [L':L] = 0 \in \mathrm{k}_u$ and hence H is a p_u-group. □

Proposition 6.5. *The subgroup $\mathrm{V}_{x,K}$ is the unique p_v-Sylow subgroup of $\mathrm{I}_{x,K}$. The sequences*

$$0 \to \mathrm{V}_{x,K} \to \mathrm{I}_{x,K} \to \operatorname{Hom}(\Delta_x/\Delta_v, \mathrm{k}_x^*) \to 0$$

and

$$0 \to \mathrm{V}_{x,K} \to \mathrm{D}_{x,K} \to \operatorname{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x)) \to 0$$

are exact. One has $[K_{\mathrm{v},x} : K_{\mathrm{i},x}] = \mathrm{e}(x_\mathrm{v}/x_\mathrm{i}) = \mathrm{e}_\mathrm{t}(x_\mathrm{v}/x_\mathrm{i})$ and $\mathrm{f}(x_\mathrm{v}/x_\mathrm{i}) = 1$. We also have $[M : K_{\mathrm{v},x}] \in \mathrm{p}_v^{\mathbf{Z}_{\geq 0}}$ and $\mathrm{e}(x/x_\mathrm{v}) = \mathrm{e}_\mathrm{w}(x/x_\mathrm{v})$. Set $s = \operatorname{ord}(\mathrm{I}_{x,K} / \mathrm{V}_{x,K})$. Then k_x has an s-th primitive root of unity.

Proof. Let $\varphi\colon \mathrm{I}_{x,K} \to \operatorname{Hom}(\Delta_x/\Delta_v, \mathrm{k}_x^*)$ be the morphism with kernel $\mathrm{V}_{x,K}$. Since k_x^* has no non-trivial elements of p_v-power order, all elements of order a power of p_v of $\mathrm{I}_{x,K}$ are in $\mathrm{V}_{x,K}$. Consider the normal extension $M/K_{\mathrm{v},x}$ with automorphism group $\mathrm{V}_{x,K}$. One obtains that $\mathrm{V}_{x,K}$ is a p_v-group by Lemma 6.4. Hence $\mathrm{V}_{x,K}$ is the unique p_v-Sylow subgroup of $\mathrm{I}_{x,K}$.

Consider the Galois extension $K_{\mathrm{v},x}/K_{\mathrm{i},x}$ with group $\mathrm{I}_{x,K}\,/\,\mathrm{V}_{x,K}$. As the order of $\mathrm{I}_{x,K}\,/\,\mathrm{V}_{x,K}$ is coprime with p_v, we have an exact sequence $0 \to \mathrm{I}_{x,K}\,/\,\mathrm{V}_{x,K} \to \mathrm{Hom}(\Delta_{x_\mathrm{v}}/\Delta_{x_\mathrm{i}}, \mathrm{k}^*_{x_\mathrm{v}})$. Using Proposition 5.6 we obtain

$$\mathrm{f}(x_\mathrm{v}/x_\mathrm{i}) \cdot \mathrm{e}(x_\mathrm{v}/x_\mathrm{i}) \leq [K_{\mathrm{v},x} : K_{\mathrm{i},x}] \leq \#\,\mathrm{Hom}(\Delta_{x_\mathrm{v}}/\Delta_{x_\mathrm{i}}, \mathrm{k}^*_{x_\mathrm{v}}) \leq \mathrm{e}_\mathrm{t}(x_\mathrm{v}/x_\mathrm{i}) \leq \mathrm{e}(x_\mathrm{v}/x_\mathrm{i}).$$

We obtain $\mathrm{f}(x_\mathrm{v}/x_\mathrm{i}) = 1$ and $[K_{\mathrm{v},x} : K_{\mathrm{i},x}] = \mathrm{e}(x_\mathrm{v}/x_\mathrm{i}) = \mathrm{e}_\mathrm{t}(x_\mathrm{v}/x_\mathrm{i})$. We also obtain $\#\,\mathrm{Hom}(\Delta_{x_\mathrm{v}}/\Delta_{x_\mathrm{i}}, \mathrm{k}^*_{x_\mathrm{v}}) = \#\,(\mathrm{I}_{x,K}\,/\,\mathrm{V}_{x,K})$. Finally we obtain that $\mathrm{k}_{x_\mathrm{v}}$ has an s-th primitive root of unity.

One easily obtains $[M : K_{\mathrm{v},x}] \in \mathrm{p}_v^{\mathbf{Z}_{\geq 0}}$. Furthermore, $\mathrm{e}(x/x_\mathrm{v}) = \mathrm{e}_\mathrm{w}(x/x_\mathrm{v})$ follows from Lemma 5.7.

The extension $\mathrm{k}_x/\mathrm{k}_{x_\mathrm{v}}$ is purely inseparable (Proposition 6.2). This shows that the torsion of k^*_x is equal to the torsion of $\mathrm{k}^*_{x_\mathrm{v}}$. Note that $\Delta_v = \Delta_{x_\mathrm{i}}$ by Proposition 6.1 and Proposition 6.2. Hence we have a natural map $\mathrm{Hom}(\Delta_x/\Delta_v, \mathrm{k}^*_x) \to \mathrm{Hom}(\Delta_{x_\mathrm{v}}/\Delta_{x_\mathrm{i}}, \mathrm{k}^*_{x_\mathrm{v}})$. Because $\Delta_x/\Delta_{x_\mathrm{v}}$ is a p_v-group, this map is injective. We find

$$\#\,(\mathrm{I}_{x,K}\,/\,\mathrm{V}_{x,K}) \leq \#\,\mathrm{Hom}(\Delta_x/\Delta_v, \mathrm{k}^*_x) \leq \#\,\mathrm{Hom}(\Delta_{x_\mathrm{v}}/\Delta_{x_\mathrm{i}}, \mathrm{k}^*_{x_\mathrm{v}}) = \#\,(\mathrm{I}_{x,K}\,/\,\mathrm{V}_{x,K})\,.$$

This shows that the sequence $0 \to \mathrm{V}_{x,K} \to \mathrm{I}_{x,K} \to \mathrm{Hom}(\Delta_x/\Delta_v, \mathrm{k}^*_x) \to 0$ is exact.

We will show that the second sequence is exact. Recall that this sequence comes from the action of $\mathrm{D}_{x,K}$ on $0 \to \mathrm{k}^*_x \to M^*/(1+\mathfrak{m}_x) \to \Delta_x \to 0$. If $\sigma \in \mathrm{D}_{x,K}$ acts trivially on the exact sequence, then it acts trivially on k_x and hence lies in $\mathrm{I}_{x,K}$ and hence in $\mathrm{V}_{x,K}$. We will count $\mathrm{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x))$. Note that the restriction map to $\mathrm{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x)) \to \Gamma_{x,v}$, a group of cardinality $\#\,\mathrm{D}_{x,K}\,/\#\,\mathrm{I}_{x,K}$, is surjective (Proposition 6.2). Let $h \in \Gamma_{x,v}$. The set of automorphisms inducing h is in bijection with $\mathrm{Hom}(\Delta_x/\Delta_v, \mathrm{k}^*_x)$ (Lemma 6.3), and this set is of cardinality $\#\,\mathrm{I}_{x,K}\,/\#\,\mathrm{V}_{x,K}$. We find:

$$\#\,\mathrm{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x)) = \#\,\mathrm{D}_{x,K}\,/\#\,\mathrm{I}_{x,K} \cdot \#\,\mathrm{I}_{x,K}\,/\#\,\mathrm{V}_{x,K} = \#\,\mathrm{D}_{x,K}\,/\#\,\mathrm{V}_{x,K}\,.$$

Hence the last sequence is exact. □

We later use the following lemma, which summarizes part of the situation. In Proposition 3.7 we will give a more readable form.

Lemma 6.6. *Let $(M,x) \supseteq (K,v)$ be a finite normal extension of valued fields. Then the following statements hold:*

i. $[K_{\mathrm{h},x} : K] = \mathrm{g}_{M,v}$, $\mathrm{e}(x_\mathrm{h}/v) = \mathrm{f}(x_\mathrm{h}/v) = 1$;
ii. $[K_{\mathrm{i},x} : K_{\mathrm{h},x}] = \mathrm{f}_\mathrm{s}(x_\mathrm{i}/x_\mathrm{h}) = \mathrm{f}(x_\mathrm{i}/x_\mathrm{h}) = \mathrm{f}_\mathrm{s}(x/v)$, $\mathrm{e}(x_\mathrm{i}/x_\mathrm{h}) = 1$;
iii. $[K_{\mathrm{v},x} : K_{\mathrm{i},x}] = \mathrm{e}_\mathrm{t}(x_\mathrm{v}/x_\mathrm{i}) = \mathrm{e}(x_\mathrm{v}/x_\mathrm{i}) = \mathrm{e}_\mathrm{t}(x/v)$, $\mathrm{f}(x_\mathrm{v}/x_\mathrm{i}) = 1$;
iv. $[M : K_{\mathrm{v},x}] \in \mathrm{p}_v^{\mathbf{Z}_{\geq 0}}$, $\mathrm{e}(x/x_\mathrm{v}) = \mathrm{e}_\mathrm{w}(x/x_\mathrm{v}) = \mathrm{e}_\mathrm{w}(x/v)$, $\mathrm{f}(x/x_\mathrm{v}) = \mathrm{f}_\mathrm{i}(x/x_\mathrm{v}) = \mathrm{f}_\mathrm{i}(x/v)$.

Proof. This follows from combining Proposition 6.1, Proposition 6.2, Proposition 6.5 and Proposition 5.6. □

6.2. Normal extensions.

Remark 6.7. Let $(M,x) \supseteq (K,v)$ be a normal extension of valued fields and let $G = \mathrm{Aut}_K(M)$. Let $\mathfrak{T}$ be the set of finite normal extensions of K in M. By definition

one has

$$\begin{aligned} \mathrm{D}_{x,K} &= \varprojlim_{M' \in \mathfrak{T}} \mathrm{D}_{x|_{M'},K}; \\ \mathrm{I}_{x,K} &= \varprojlim_{M' \in \mathfrak{T}} \mathrm{I}_{x|_{M'},K}; \\ \mathrm{V}_{x,K} &= \varprojlim_{M' \in \mathfrak{T}} \mathrm{V}_{x|_{M'},K}\,. \end{aligned}$$

All maps in the projective limits come from the natural restriction maps.

Lemma 6.8. *Let $K \subseteq L \subseteq M$ be algebraic extensions of fields. Then we have $M_{L,\mathrm{sep}} = M_{K,\mathrm{sep}}L$.*

Proof. Assume $p = \mathrm{char}(K) \neq 0$. One obviously has $M_{L,\mathrm{sep}} \supseteq M_{K,\mathrm{sep}}L$. For $x \in M \setminus M_{K,\mathrm{sep}}L$ there is $i \in \mathbf{Z}_{\geq 0}$ such that $x^{p^i} \in M_{K,\mathrm{sep}}$, and hence $M/M_{K,\mathrm{sep}}L$ is purely inseparable and we are done. □

We need the following technical lemma.

Lemma 6.9. *Let $M \supseteq L \supseteq K$ be algebraic extensions of fields where M/K is normal. Let $G = \mathrm{Aut}_K(M)$ and $H = \mathrm{Aut}_L(M) \subseteq G$. Let $G' \subseteq G$ be a subgroup. Then one has $(M_{L,\mathrm{sep}})^{G' \cap H} = (M_{K,\mathrm{sep}})^{G'} L$.*

Proof. By Proposition 4.10 it is enough to show that both fields have the same compositum and intersection with $M_{K,\mathrm{sep}}$. We start with the intersection, where we use Galois theory (for the first equality, note that $(M_{K,\mathrm{sep}})^{G'} L / (M_{K,\mathrm{sep}})^{G'} (L \cap M_{K,\mathrm{sep}})$ is purely inseparable):

$$\begin{aligned} \left((M_{K,\mathrm{sep}})^{G'} L\right) \cap M_{K,\mathrm{sep}} &= (M_{K,\mathrm{sep}})^{G'} (L \cap M_{K,\mathrm{sep}}) \\ &= (M_{K,\mathrm{sep}})^{G'} (M_{K,\mathrm{sep}})^{H} = (M_{K,\mathrm{sep}})^{G' \cap H} \\ &= (M_{L,\mathrm{sep}})^{G' \cap H} \cap M_{K,\mathrm{sep}}. \end{aligned}$$

For the compositum, we have:

$$\left((M_{K,\mathrm{sep}})^{G'} L\right) M_{K,\mathrm{sep}} = M_{K,\mathrm{sep}}L$$

and by Lemma 6.8 we have

$$LM_{K,\mathrm{sep}} \subseteq (M_{L,\mathrm{sep}})^{H \cap G'} M_{K,\mathrm{sep}} \subseteq M_{L,\mathrm{sep}}M_{K,\mathrm{sep}} = LM_{K,\mathrm{sep}}.$$

The result follows. □

Proof of Theorem 3.6. We will first prove that the map $G \times S \to S$ is continuous. Take $x' \in S$, L a finite extension of K and suppose that $g \cdot x'' \in U_{x',L}$. Let N/K be a finite normal extension containing L in M. Then one has $\{g' \in G : g|_N = g'|_N\} \cdot U_{x'',N} \subseteq U_{x',L}$. This shows that the action is continuous. By definition the stabilizer of x is $\mathrm{D}_{x,K}$ and this gives us the isomorphism $G/\mathrm{D}_{x,K} \to S$.

One easily obtains for $g \in G$ the equalities $\mathrm{D}_{g(x),K} = g\,\mathrm{D}_{x,K}\,g^{-1}$ and $K_{\mathrm{h},g(x)} = gK_{\mathrm{h},x}$. The other cases are similar.

We want to show that the sequences are exact. The idea is that the result is a limit of the statements for finite normal extensions. This is the reason why the maps are morphisms of profinite groups. Let $0 \to A_i \to B_i \to C_i \to 0$ (i is some indexed set) be exact sequences of groups such that we can take a projective limit. Then the remaining sequence is left-exact. It is exact if all the maps $A_i \to A_j$ in the system are surjective (in this case, the so-called Mittag-Leffler condition is satisfied). See for example [**AM69**, Proposition 10.2] for a statement which is sufficient. Hence we take the limit of the sequences from Proposition 6.2 and Proposition 6.5.

Let M', M'' be finite normal over K with $K \subseteq M' \subseteq M'' \subseteq M$. We claim that the natural maps $\mathrm{I}_{x|_{M''},K} \to \mathrm{I}_{x|_{M'},K}$ and $\mathrm{V}_{x|_{M''},K} \to \mathrm{V}_{x|_{M'},K}$ are surjective. Take $g \in \mathrm{I}_{x|_{M'},K}$ with lift $g' \in \mathrm{Aut}_K(M'')$. We have an exact sequence $0 \to \mathrm{I}_{x|_{M''},M'} \to \mathrm{D}_{x|_{M''},M'} \to \mathrm{Aut}_{\mathrm{k}_{x|_{M'}}}(\mathrm{k}_{x|_{M''}}) \to 0$ from Proposition 6.2. This shows that there is a $g'' \in \mathrm{D}_{x|_{M''},M'} \subseteq \mathrm{Aut}_{M'}(M'')$ such that $g'g'' \in \mathrm{I}_{x|_{M''},K}$ and $\overline{g'g''} = g \in \mathrm{Aut}_K(M')$. A similar proof, using Proposition 6.5 and the result just obtained, shows the surjectivity of $\mathrm{V}_{x|_{M''},K} \to \mathrm{V}_{x|_{M'},K}$.

This shows that all sequences in the limit remain exact (for the first one, we could have also used Corollary 4.13). Since $\mathrm{k}_{x|_{M'}}$ has enough roots of unity (Proposition 6.5) we find

$$\mathrm{Hom}(\Delta_x/\Delta_v, \mathrm{k}_x^*) = \mathrm{Hom}\left(\varinjlim_{M'} \Delta_{x|_{M'}}/\Delta_v, \mathrm{k}_x^*\right) = \varprojlim_{M'} \mathrm{Hom}(\Delta|_{x|_{M'}}/\Delta_v, \mathrm{k}_{x|_{M'}}^*).$$

For the limit of the third sequence, we need to prove

$$\mathrm{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x)) = \varprojlim_{M'} \mathrm{Aut}_{K^*,\Gamma_{x|_{M'},v}}(M'^*/(1+\mathfrak{m}_{x|_{M'}}))$$

It is easy to see that the right group is contained in the left group. The other implication follows since such an automorphism of

$$1 \to \mathrm{k}_x^* \to M^*/(1+\mathfrak{m}_x) \to \Delta_x \to 1$$

induces an automorphism of

$$1 \to \mathrm{k}_{x|_{M'}}^* \to M'^*/(1+\mathfrak{m}_{x|_{M'}}) \to \Delta_{x|_{M'}} \to 1$$

because $\mathrm{k}_{x|_{M'}}/\mathrm{k}_v$ is normal (Proposition 6.2).

The statement about the pro-p_v-Sylow statement follow from Proposition 6.5. The normality of $\mathrm{k}_x/\mathrm{k}_v$ follows from Proposition 6.2. Proposition 6.5 also gives the statement about the roots of unity.

Statement i directly follows from the definition. Statement ii follows from statement i and Lemma 6.9.

We will prove the exactness of the last three sequences. The only non-trivial part is the surjectivity of the last maps. The exactness for the last two sequences is as before, and the exactness of the first sequence follows from the transitivity of the action of G on S. The last statements then follow directly. □

Lemma 6.10. *Suppose we have the following commutative diagram of groups with exact rows:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \xrightarrow{h} & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \xrightarrow{h'} & C' & \longrightarrow & 0. \end{array}$$

Assume that $s\colon C \to B$ is a splitting of the first exact sequence and assume that $\mathrm{Hom}(\ker(g), A') = 0$. Then the map

$$s'\colon C' \to B'$$
$$c' = g(c) \mapsto f \circ s(c)$$

is well-defined and it is a splitting of the second exact sequence.

Proof. Consider the morphism $f \circ s|_{\ker(g)}\colon \ker(\varphi) \to B'$. Note that the image actually lands in A' and hence this is the 0 map. Hence s' is a well-defined map. Take $c_1', c_2' \in C'$, say with preimage c_1 respectively c_2 in C. Then $c_1 + c_2$ is a preimage of $c_1' + c_2'$ and hence have

$$s'(c_1' + c_2') = f \circ s(c_1 + c_2) = f \circ s(c_1) + f \circ s(c_2) = s'(c_1') + s'(c_2').$$

This shows that s' is a morphism. For $c' \in C'$ with preimage $c \in C$ we find

$$h'(s'(c')) = h' \circ f \circ s(c) = g \circ h \circ s(c) = g(c) = c'.$$

□

Proof of Theorem 3.8. We may assume that $K = K_{\mathrm{h},x}$. Set $\Gamma = \mathrm{Aut}_{\mathrm{k}_v}(\overline{\mathrm{k}_x})$.

i: Let $\overline{M}$ be an algebraic closure of M with valuation x' extending x. Let S be the set of intermediate fields L of $\mathrm{K}_{\mathrm{v},x'}/K$ with the property that $(L, x'|_L) \supseteq (K, v)$ is totally ramified and tame. Order this set by inclusion. This set is not empty. Note that a chain has an upper bound, namely the union. By Zorn there is a maximal element, say L'. Notice that $\Delta_{x'}/\Delta_{x'|_{L'}}$ is a p_v-group. Indeed, if not, we could find a totally and tamely ramified extension of L' in $\overline{M}$ by taking a root of an element of L'. Using the exact sequences (Theorem 3.6) it is not hard to see that $\mathrm{Gal}(K_{\mathrm{v},x'}/L') \cong \Gamma$ (the extension $K_{\mathrm{v},x'}/L'$ has trivial V and hence trivial I). This shows that the sequence $0 \to \mathrm{I}_{x',K}/\mathrm{V}_{x',K} \to \mathrm{D}_{x',K}/\mathrm{V}_{x',K} \to \Gamma \to 0$ is split. We have the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{I}_{x',K}/\mathrm{V}_{x',K} & \longrightarrow & \mathrm{D}_{x',K}/\mathrm{V}_{x',K} & \longrightarrow & \Gamma & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{I}_{x,K}/\mathrm{V}_{x,K} & \longrightarrow & \mathrm{D}_{x,K}/\mathrm{V}_{x,K} & \longrightarrow & \mathrm{Aut}_{\mathrm{k}_v}(\mathrm{k}_x) & \longrightarrow & 0. \end{array}$$

Lemma 6.10 gives us a splitting of the second sequence provided that we can show $\mathrm{Hom}(\mathrm{Aut}_{\mathrm{k}_x}(\overline{\mathrm{k}_x}), \mathrm{I}_{x,K}/\mathrm{V}_{x,K}) = 0$. Note that $\mathrm{I}_{x,K}/\mathrm{V}_{x,K} \cong \mathrm{Hom}(\Delta_x/\Delta_v, \mathrm{k}_x^*)$ (Theorem 3.6). Suppose we have such a non-trivial morphism. Then as Δ_x/Δ_v is torsion, we can find an element of prime order l coprime to p_v in Δ_x/Δ_v not mapping to zero (note that the order of l divids $\mathrm{ord}(\mathrm{I}_{x,K}/\mathrm{V}_{x,K})$). This gives us a surjective morphism $\mathrm{Aut}_{\mathrm{k}_x}(\overline{\mathrm{k}_x}) \to \mathbf{Z}/l\mathbf{Z}$. By assumption such a morphism does not exist.

ii: Note that $\mathrm{V}_{x,K}$ is the unique pro-p_v-Sylow subgroup of $\mathrm{I}_{x,K}$ (Theorem 3.6) and hence the statement trivially follows when $\mathrm{p}_v = 1$ or when $\mathrm{p}_v \nmid \mathrm{ord}(\mathrm{I}_{x,K})$. Assume $\mathrm{p}_v \neq 1$ and $\mathrm{p}_v \mid \mathrm{ord}(\mathrm{I}_{x,K})$. It is enough to show that the cohomological p_v-dimension of $\mathrm{D}_{x,K} / \mathrm{V}_{x,K}$, $\mathrm{cd}_{\mathrm{p}_v}(\mathrm{D}_{x,K} / \mathrm{V}_{x,K})$, is at most 1 [**Ser02**, Chapter I, Proposition 16]. We have an exact sequence $0 \to \mathrm{I}_{x,K} / \mathrm{V}_{x,K} \to \mathrm{D}_{x,K} / \mathrm{V}_{x,K} \to \mathrm{D}_{x,K} / \mathrm{I}_{x,K} \to 0$. From Theorem 3.6 it follows that $\mathrm{D}_{x,K} / \mathrm{I}_{x,K}$ is isomorphic to $\mathrm{Aut}_{\mathrm{k}_v}(\mathrm{k}_x)$. This group has cohomological dimension at most 1 (see the proof of [**Ser02**, Chapter II, Proposition 3] or [**Efr06**, Theorem 22.2.1], in combination with Artin-Schreier theory). We have an isomorphism $\mathrm{I}_{x,K} / \mathrm{V}_{x,K} \cong \mathrm{Hom}(\Delta_x/\Delta_v, \mathrm{k}_x^*)$ and its order is coprime to p_v. Hence we have $\mathrm{cd}_{\mathrm{p}_v}(\mathrm{I}_{x,K} / \mathrm{V}_{x,K}) = 0$ ([**Ser02**, Chapter I, Corollary 2 on Page 19]). Using [**Ser02**, Chapter I, Proposition 15] we see that $\mathrm{cd}_{\mathrm{p}_v}(\mathrm{D}_{x,K} / \mathrm{V}_{x,K}) \leq 1$ and the result follows.

iii: This follows after combining i and ii and the fact that $\mathrm{V}_{x,K}$ is a p_v-group (Theorem 3.6). □

7. Algebraic extensions

7.1. Proofs.

Proposition 7.1. *Let $(L, w) \supseteq (K, v)$ be a finite extension of valued fields. Let (M, x) be a finite normal extension of (K, v) containing (L, w). Then the following hold:*

i. *the quantity $\mathrm{n}(w/v)$ is well-defined and one has $n(w/v) = \frac{\mathrm{g}_{M,w}}{\mathrm{g}_{M,v}} \cdot [L : K] = [L_{\mathrm{h},x} : K_{\mathrm{h},x}]$;*
ii. *$\mathrm{d}(w/v)$ is well-defined and has values in $\mathrm{p}_v^{\mathbf{Z}_{\geq 0}}$.*

Furthermore, the quantities d, d_{w}, e, e_{t} e_{w}, f, f_{s}, f_{i} and n are multiplicative in towers.

Proof. i. We will show that $\mathrm{n}(w/v)$ is well-defined, i.e. does not depend on the choice of M. Let M' be another normal extension of K containing L with $G = \mathrm{Aut}_K(M')$. Without loss of generality, we may assume $M' \supseteq M$. Put $H = \mathrm{Aut}_M(M')$. Let X (respectively X') be the set of primes of M (respectively M') extending v. Note that G acts transitively on X', and G/H acts transitively on X (Proposition 5.6). Then one easily shows that the map $X' \to X$ has equally sized fibers. Hence $\mathrm{g}_{M',v} = \#X' = \#X \cdot \#(\text{fiber above } x) = \mathrm{g}_{M,v} \cdot \mathrm{g}_{M',x}$ as required. Similarly, if one replaces K by L, one obtains $\mathrm{g}_{M',w} = \mathrm{g}_{M,w} \cdot \mathrm{g}_{M',x}$. Hence the required ratio does not depend on the choice of M.

From Lemma 6.6 and Theorem 3.6ii one obtains $[K_{\mathrm{h},x} : K] = \mathrm{g}_{M,v}$ and $[LK_{\mathrm{h},x} : L] = [L_{\mathrm{h},x} : L] = \mathrm{g}_{M,w}$. Hence we have

$$[L_{\mathrm{h},x} : K_{\mathrm{h},x}] = [LK_{\mathrm{h},x} : K_{\mathrm{h},x}] = \frac{[LK_{\mathrm{h},x} : L]}{[K_{\mathrm{h},x} : K]} \cdot [L : K] = \frac{\mathrm{g}_{M,w}}{\mathrm{g}_{M,v}} \cdot [L : K] = \mathrm{n}(w/v).$$

We will now prove the last statement. It is obvious that e, e_{t} e_{w}, f, f_{s}, f_{i} are multiplicative. If we show that n is multiplicative, it directly follows that d and d_{w} are multiplicative. Hence it is enough to show that n is multiplicative. Let (L', w') be a finite extension of (L, w). Let M be a finite normal extension of K containing L'.

Then one has

$$\begin{aligned}\mathrm{n}(w'/w)\,\mathrm{n}(w/v) &= \frac{\mathrm{g}_{M,w'}}{\mathrm{g}_{M,w}} \cdot [L' : L] \cdot \frac{\mathrm{g}_{M,w}}{\mathrm{g}_{M,v}} \cdot [L : K] \\ &= \frac{\mathrm{g}_{M,w'}}{\mathrm{g}_{M,v}} [L' : K] = \mathrm{n}(w'/v).\end{aligned}$$

ii. It is now obvious that $\mathrm{d}(w/v)$ is well-defined. One has $\mathrm{d}(w/v) = \frac{[L_{\mathrm{h},x} : K_{\mathrm{h},x}]}{\mathrm{e}(w/v)\,\mathrm{f}(w/v)} \in \mathbf{Z}_{\geq 1}$ by Proposition 5.6, Proposition 6.1 and the multiplicativity of e and f.

If L/K is normal, one has

$$\mathrm{d}(w/v) = \frac{[L : K_{\mathrm{h},w}]}{\mathrm{e}(w/v)\,\mathrm{f}(w/v)} = \frac{[L : K_{\mathrm{v},w}]}{\mathrm{e}_{\mathrm{w}}(w/v)\,\mathrm{f}_{\mathrm{s}}(w/v)} \in \mathrm{p}_v^{\mathbf{Z}}$$

(Lemma 6.6). Together with the multiplicativity of d, this shows $\mathrm{d}(w/v) \in \mathrm{p}_v^{\mathbf{Z}_{\geq 0}}$ in general. □

Proof of Proposition 3.7. This follows directly from Lemma 6.6 and the definitions. □

Proof of Theorem 3.9. The first equality is easily from the definition, the second follows by definition and the third follows from Proposition 7.1ii. □

Remark 7.2. Let $(L, w) \supseteq (K, v)$ be an algebraic extension of valued fields. Note that immediate implies unramified, unramified implies tame, totally wild implies totally ramified and totally ramified implies local.

Suppose that one of the following hold:

i. w/v is immediate and local;
ii. w/v is unramified and totally ramified;
iii. w/v is tame and totally wild.

Then from Theorem 3.9 it follows that $L = K$.

Remark 7.3. Let $(L, w) \supseteq (K, v)$ be an algebraic extension of valued fields which is purely inseparable. Then one easily sees that it is totally wild (Lemma 5.8).

Proof of Theorem 3.10. The surjectivity of π follows directly from the transitivity as in Proposition 5.6 and the extension property as in Proposition 5.2.

Let $\sigma \in X$. This gives us embeddings $(K, v) \subseteq (L, w) \subseteq (M, x)$. Write $H = \mathrm{Gal}(M/L)$. Then X corresponds to G/H. Let $\mathfrak{T}$ be the set of finite normal subextensions of M/K. We first consider w/v:

i, ii, iii: w/v is immediate $\iff$ for all $M' \in \mathfrak{T}$ the extension $w|_{M' \cap L}/v$ is immediate $\iff$ for all $M' \in \mathfrak{T}$ we have $\#\,\mathrm{D}_{x|_{M'},K} = \#\,\mathrm{D}_{x|_{M'},L\cap M'}$ (Proposition 3.7, look at degrees such as $[K : K_{\mathrm{h},x|_{M'}}] = \#\,\mathrm{D}_{x|_{M'},K}$) $\iff$ for all $M' \in \mathfrak{T}$ we have $\mathrm{D}_{x|_{M'},K} = \mathrm{D}_{x|_{M'},L\cap M'} = \mathrm{D}_{x|_{M'},K} \cap \mathrm{Aut}_{L\cap M'}(M')$ (Theorem 3.6) $\iff$ for all $M' \in \mathfrak{T}$ we have $\mathrm{D}_{x|_{M'},K} \subseteq \mathrm{Aut}_{L\cap M'}(M')$ $\iff$ $\mathrm{D}_{x,K} \subseteq H$ (Theorem 3.6) $\iff$ $L \subseteq K_{\mathrm{h},x}$. The other cases are similar.

iv, v, vi: w/v is local $\iff$ for all $M' \in \mathfrak{T}$ the extension $w|_{M' \cap L}/v$ is local $\iff$ for all $M' \in \mathfrak{T}$ we have $[L \cap M' : K][K_{\mathrm{h},x|_{M'}} : K] = [(L \cap M')_{\mathrm{h},x|_{M'}} : K_{\mathrm{h},x|_{M'}}][K_{\mathrm{h},x|_{M'}} : K] = [(L \cap M')K_{\mathrm{h},x|_{M'}} : K]$ (Proposition 3.7 and Theorem 3.6) $\iff$ for all $M' \in \mathfrak{T}$ we have $\mathrm{Aut}_K(M') = \mathrm{D}_{x|_{M'},K}\,\mathrm{Aut}_{L\cap M'}(M')$ (as $K_{\mathrm{h},x}$ is separable,

one can apply Proposition 4.2) $\iff$ for all $M' \in \mathfrak{T}$ the group $\mathrm{D}_{x|_{M'},K}$ acts transitively on $\mathrm{Aut}_K(M')/\mathrm{Aut}_{L\cap M'}(M')$.

We prove that the last statement is equivalent with $\mathrm{D}_{x,K}$ acting transitively on G/H. If $\mathrm{D}_{x,K}$ acts transitively on G/H, then one easily sees from the surjectivity $G/H \to \mathrm{Aut}_K(M')/\mathrm{Aut}_{L\cap M'}(M')$ for $M' \in \mathfrak{T}$ and Theorem 3.6, that $\mathrm{D}_{x|_{M'},K}$ acts transitively on $\mathrm{Aut}_K(M')/\mathrm{Aut}_{L\cap M'}(M')$. Conversely, given $u, v \in G/H$, consider the projective system of non-empty finite sets which at level M' consists of those elements mapping $u|_{M'}$ to $v|_{M'}$. One can easily show that this set is non-empty and deduce the result. The other cases are similar.

Now consider x/w:

vii, viii, ix: x/w is immediate $\iff$ $M \subseteq L_{\mathrm{h},x} = LK_{\mathrm{h},x}$ (using i and Theorem 3.6) $\iff$ $M = LK_{\mathrm{h},x}$. The latter is equivalent to $[\sigma(L) : K]_{\mathrm{i}} = [M : K]_{\mathrm{i}}$ and $G_\sigma \cap \mathrm{D}_{x,K} = 0$ by Galois theory. The proofs of viii and ix are similar.

x, xi, xii: x/w is local $\iff$ M and $L_{\mathrm{h},x} = LK_{\mathrm{h},x}$ are linearly disjoint over L (using ii and Theorem 3.6) $\iff$ $K_{\mathrm{h},x} \subseteq L$ iff $G_\sigma \subseteq \mathrm{D}_{x,K}$. The proofs of xi and xii are similar.

Consider the last statements.

xiii: This follows from i and the surjectivity of π.

xiv: w is totally split in M $\iff$ $M/\sigma(L)$ is separable and for all $g \in G$ we have $G_\sigma \cap \mathrm{D}_{g(x),K} = 0$ (vii and Theorem 3.6) iff M/L is separable and only the trivial element of G_σ is conjugate to $\mathrm{D}_{x,K}$ (Theorem 3.6). □

Proof of Corollary 3.11. Let (E, x') be a normal extension of (K, v) extending (LL', x).

i, ii, iii, iv: Assume that w/v is immediate. Theorem 3.10 gives us that $L \subseteq K_{h,x'}$. But then we have $LL' \subseteq L'K_{h,x'} = L'_{h,x'}$ (Theorem 3.6). Hence Theorem 3.10 shows that x/w' is immediate. The proofs for the other cases are similar. □

Remark 7.4. Statements as in Corollary 3.11 are false for local, totally ramified or totally wild extensions. Here is an example from algebraic number theory. Let $K = \mathbf{Q}$, $L = \mathbf{Q}(\sqrt{7})$ and $L' = \mathbf{Q}(\sqrt{-1})$ and look at the primes above 2. In this case L/K and L'/K is totally wild (and hence local and totally ramified). In the extension $L'' = \mathbf{Q}(\sqrt{-7})$ of $\mathbf{Q}$ the prime 2 splits. Hence in the extension $LL'/K = \mathbf{Q}(\sqrt{7}, \sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ the prime above 2 splits. The extension LL'/K is not local.

Proof of Corollary 3.12. Let (M, x) be a normal extension of (K, v) containing (L, w).

For the immediate case, we have the following: $L \subseteq K_{\mathrm{h},x}$ $\iff$ $K' \subseteq K_{\mathrm{h},x}$ and $L \subseteq K'_{\mathrm{h},x} = K'K_{\mathrm{h},x}$ (Theorem 3.6). The result follows from Theorem 3.10. The unramified and tame cases are similar.

Now consider the local case. One has: $L \otimes_K K_{\mathrm{h},x}$ is a domain $\iff$ $L \otimes_{K'} K'_{\mathrm{h},x}$ and $K' \otimes_K K_{\mathrm{h},x}$ are domains. Assume first that $K' \otimes_K K_{\mathrm{h},x}$ is a domain. Observe that

$$\begin{aligned} L \otimes_{K'} K'_{\mathrm{h},x} &= L \otimes_{K'} (K'K_{\mathrm{h},x}) \\ &= L \otimes_{K'} K' \otimes_K K_{\mathrm{h},x} \\ &= L \otimes_K K_{\mathrm{h},x} \end{aligned}$$

(Theorem 3.6). This directly proves $\Longleftarrow$. The implication $\Longrightarrow$ follows from $K' \otimes_K K_{\mathrm{h},x} \subseteq L \otimes_K K_{\mathrm{h},x}$ and the above observation observation.

The result follows from Theorem 3.10. The totally ramified and totally wild cases are similar.

□

Proof of Corollary 3.15. Pick an extension $(M,x) \supseteq (L,w) \supseteq (K,v)$ such that M/K is normal. Using Theorem 3.10 we see $L_1 = K_{\mathrm{h},x} \cap L$, $L_2 = K_{\mathrm{i},x} \cap L$ and $L_3 = K_{\mathrm{v},x} \cap L$.

We will now construct a minimal local subextension. Assume that L' is a field such that $w/w|_{L'}$ is local. Then $w/w|_{L'_{K,\mathrm{sep}}}$ is also local (Lemma 5.8). Hence we can replace L by $L_{K,\mathrm{sep}}$. Using Theorem 3.10 and Theorem 3.6, we see that we need to find the smallest intermediate field L' of $L_{K,\mathrm{sep}}/K$ such that $L_{K,\mathrm{sep}}$ and $L'_{\mathrm{h},x} = L'K_{\mathrm{h},x}$ are linearly disjoint over L'. Such a field exists by Theorem 3.13 and it is denoted by $L_{K,\mathrm{sep}} \setminus\!\!\setminus K_{\mathrm{h},x}$. The proofs of the other cases are similar when D is replaced by I respectively V.

We will now prove that $L_1 \subseteq L_4$. As $w|_{L_1}/v$ is immediate, it follows that the extension $w|_{L_1L_4}/w|_{L_4}$ is immediate (Corollary 3.11). Hence L_1L_4/L_4 is immediate and local. From Remark 7.2 it follows that $L_1L_4 = L_4$, that is, $L_1 \subseteq L_4$. The inclusions $L_2 \subseteq L_5$ and $L_3 \subseteq L_6$ follow in a similar manner.

Assume that $\mathrm{g}_{M,w} = 1$ for some normal extension M/K containing L. Note that $\mathrm{g}_{M,w} = 1$ is equivalent to $H = \mathrm{Aut}_L(M) \subseteq \mathrm{D}_{x,K}$ (Theorem 3.10x). From Theorem 3.10 it follows that we need to show that $\mathrm{D}_{x,K} \to \langle H, \mathrm{D}_{x,K}\rangle/H$, $\mathrm{I}_{x,K} \to \langle H, \mathrm{I}_{x,K}\rangle/H$ and $\mathrm{V}_{x,K} \to \langle H, \mathrm{V}_{x,K}\rangle/H$ are surjective. The surjectivity of the first map is obvious, and the surjectivity of the second and third map is implied by the normality of $\mathrm{I}_{x,K}$ respectively $\mathrm{V}_{x,K}$ in $\mathrm{D}_{x,K}$ (Theorem 3.6). □

Proof of Corollary 3.16. We will prove ii. The other proofs are similar.

Assume that $\mathrm{g}_{M,w} = 1$. Assume that w/v is not totally ramified. Then one has $L_2 = L_5$ in Corollary 3.15. And hence there is a non-trivial unramified extension in L/K. But then L_5L'/L' is unramified and non-trivial (Corollary 3.11 respectively $L \cap L' = K$). Contradiction. □

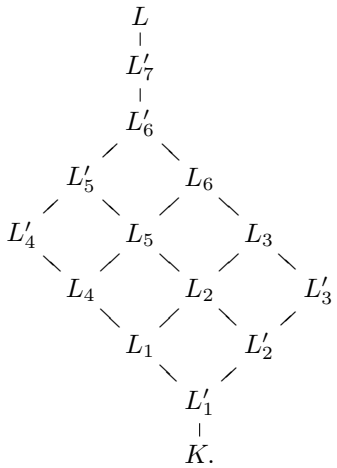
Example 7.5. In Corollary 3.16 it is not enough to require that $L \cap L' = K$. Here is an example where all three statements are false. Consider the extension $L = \mathbf{Q}(\alpha)$ of $\mathbf{Q}$ where α is a root of $x(x-1)^2 + 2$. Well-known techniques show that there are two primes above (2), namely $\mathfrak{p} = (2, \alpha)$ and $\mathfrak{q} = (2, \alpha - 1)$. One has $(2) = \mathfrak{p}\mathfrak{q}^2$. It follows that $\mathbf{Q}(\alpha)/\mathbf{Q}$ is not Galois. Hence the Galois closure M of this extension has group S_3. Let $\overline{\alpha}$ be another root in this Galois closure and let $L' = \mathbf{Q}(\overline{\alpha})$. Then the prime (2) has the same splitting behavior in $L'/\mathbf{Q}$ as in $L/\mathbf{Q}$, say $(2) = \mathfrak{p}'\mathfrak{q}'^2$. Note that $LL' = M$, $L \cap L' = \mathbf{Q}$. Furthermore, we know the splitting behavior of (2) in M: $(2) = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2$ where there is just one prime above $\mathfrak{p}$ respectively $\mathfrak{p}'$, which is totally wild, and there are two primes above $\mathfrak{q}$ respectively $\mathfrak{q}'$. Say that $\mathfrak{p}_1$ lies above $\mathfrak{p}'$. Then $\mathfrak{p}_1/\mathfrak{p}'$ is totally wild, but $\mathfrak{p}_1|_L/2\mathbf{Z}$ is not even local. Hence statements i, ii and iii of Corollary 3.16 do not hold in this case.

The same example shows that in Corollary 3.15 it is not necessarily true that $L_1 = L_4$, $L_2 = L_5$ or $L_3 = L_6$. Indeed, for the extension $(\mathbf{Q}(\alpha), \mathfrak{q})/(\mathbf{Q}, 2\mathbf{Z})$ we have $L_1 = L_2 = L_3 = \mathbf{Q}$ and $L_4 = L_5 = L_6 = \mathbf{Q}(\alpha)$.

Example 7.6. Let K be a field with field extensions L, L' inside a field M. Assume that $L \cap L' = K$ and that M/L' is purely inseparable. Then L/K is purely inseparable. Indeed, if $\mathrm{char}(k) = p > 0$, then for $x \in L$ there is $n \in \mathbf{Z}_{\geq 1}$ with $x^{p^n} \in L \cap L' = K$.

This statement also follows from our general theory. Consider the trivial valuation on K, that is, K is the valuation ring. This valuation has a unique valuation to any algebraic field extension of K. Furthermore, M/L' is totally wild. Hence from Corollary 3.16 it follows that L/K is totally wild and the result follows.

Actually, one can make the diagram a bit bigger. For $i = 1, 2, 3$ we define L'_i to be the intersection of the L_i while varying over the extensions of v to L. Similarly, for $i = 4, 5, 6$ we define L'_i to be the compositum of the L_i while varying over the extensions of v to L. For example, L'_1 is the maximal extension such that v is totally split. If we put $L'_7 = L_{K,\mathrm{sep}}$, we get the following diagram,



Proposition 7.7. *Let (K, v) be a valued field and let L be an algebraic extension of K. Let $(M, x) \supseteq (K, v)$ be a normal extension of valued fields with group $G = \mathrm{Aut}_K(L)$ such that the G-set $X_L = \mathrm{Hom}_K(L, M)$ is not empty. Then for any intermediate extension L' of L/K we have the following commutative diagram, where the maps are the natural maps:*

$$\begin{array}{ccc} G \times X_L & \longrightarrow & X_L \\ \downarrow & & \downarrow \\ G \times X_{L'} & \longrightarrow & X_{L'}. \end{array}$$

The map

$$\begin{aligned} \varphi\colon \mathrm{D}_{x,K} \backslash X_L &\to \{w \text{ of } L \text{ extending } v\} \\ \mathrm{D}_{x,K}\, \sigma &\mapsto w \text{ s.t. } \mathcal{O}_w = \sigma^{-1}(\mathcal{O}_x \cap \sigma(L)) \end{aligned}$$

is a bijection of sets. Furthermore, for $\sigma \in X_L$ we have the following bijections:

$$\begin{aligned} \mathrm{D}_{x,K}\,\sigma &\to \mathrm{Hom}_{K_{\mathrm{h},x}}(\sigma(L)_{\mathrm{h},x}, M) \\ t\sigma &\mapsto t|_{\sigma(L)_{\mathrm{h},x}}, \end{aligned}$$

$$\begin{aligned} \mathrm{I}_{x,K}\,\sigma &\to \mathrm{Hom}_{K_{\mathrm{i},x}}(\sigma(L)_{\mathrm{i},x}, M) \\ t\sigma &\mapsto t|_{\sigma(L)_{\mathrm{i},x}}, \end{aligned}$$

and

$$\begin{aligned} \mathrm{V}_{x,K}\,\sigma &\to \mathrm{Hom}_{K_{\mathrm{v},x}}(\sigma(L)_{\mathrm{v},x}, M) \\ t\sigma &\mapsto t|_{\sigma(L)_{\mathrm{v},x}}. \end{aligned}$$

Proof. The commutativity of the diagram is obvious.

Define $\varphi' \colon X_L \to \{w \text{ of } L \text{ extending } v\}$ by putting $\sigma \mapsto w$ s.t. $\mathcal{O}_w = \sigma^{-1}(\mathcal{O}_x \cap \sigma(L))$. One should think of φ' as mapping an embedding $L \subseteq M$ to the restriction of x to L. The surjectivity is part of Theorem 3.10. Suppose $\varphi'(s) = \varphi'(t)$. There exists $h \in G$ such that $ht = s$. But then by Proposition 5.6 there exists $g \in \mathrm{Aut}_{s(L)}(M)$ with $gh(x) = x$, that is, $gh \in \mathrm{D}_{x,s(L)} \subseteq \mathrm{D}_{x,K}$. We have $ght = ht = s$. It is obvious that $\varphi'(\mathrm{D}_{x,K}\, s) = \varphi'(s)$. This shows that the map is a bijection.

We will show that the map $\mathrm{D}_{x,K}\, s \to \mathrm{Hom}_{K_{\mathrm{h},x}}(s(L)_{\mathrm{h},x}, M)$ is a bijection. The other cases are similar. Suppose we have $\tau \in \mathrm{Hom}_{K_{\mathrm{h},x}}(s(L)_{\mathrm{h},x}, M)$. Then we can extend it to a morphism $\tau' \in \mathrm{Aut}_{K_{\mathrm{h},x}}(M) = \mathrm{D}_{x,K}$ and $\tau' \mapsto \tau$. □

Proof of Proposition 3.17. The first statement directly follows from Proposition 7.7. The last statements follows from Proposition 7.7 and Proposition 3.7 and the separability of L/K. □

Proof of Corollary 3.18. From Proposition 3.17 one sees that the set of valuations with the given properties is in bijection with the set of orbits of X under $\mathrm{D}_{x,K}$ such that the length of such an orbit is equal to the length of the orbit under $\mathrm{I}_{x,K}$. And this easily translates to the required statement. □

7.2. Finding extensions explicitly.

Proposition 7.8. *Let (K, v) be a valued field and let L/K be a finite extension. Pick $a \in L$ which is integral over $\mathcal{O}_v$ with minimal polynomial $f \in \mathcal{O}_v[x]$. Suppose that $\overline{f} = \prod_{i=1}^{m} f_i^{n_i} \in \mathrm{k}_v[x]$ where the f_i are monic irreducible and pairwise distinct. Then the following hold:*

i. *for $i = 1, \ldots, m$ there are pairwise distinct valuations w_i on L with $\mathrm{f}(w_i/v) \geq \deg(f_i)$;*
ii. *if $\overline{f}$ is separable, then the w_i are all valuations extending v to L and one has $\mathrm{f}(w_i/v) = \deg(f_i)$, $\mathrm{e}(w_i/v) = \mathrm{d}(w_i/v) = 1$.*

Proof. Notice that $fK[x] \cap R[x] = fR[x]$ as f is monic. Statement i follows directly from Proposition 5.2 and Proposition 5.4. Statement ii follows from i and Theorem 3.9. □

If the valuation in the above statement is discrete, one can say a bit more. See for example [**Sti09**, Theorem 3.3.7].

8. Defects in the discrete case

In this section we will give examples of defects and show that under certain circumstances, defects do not occur. This section is quite different from the other sections in this article, but we felt it was needed to show the reader that defects are not necessarily a defect of our theory.

We start with an example where there is a defect.

Example 8.1. Let $(L, w) \supseteq (K, v)$ be a finite purely inseparable extension of valued fields where v is discrete, that is, $\Delta_v \cong \mathbf{Z}$. Then one can have $\mathrm{d}(w/v) > 1$. Let p be a prime number. Consider $\mathbf{F}_p(t) \subseteq \mathbf{F}_p((t))$ with the valuation w_0 on $\mathbf{F}_p((t))$ with $w_0(t) = 1$. Let v_0 be its restriction to $\mathbf{F}_p(t)$. Then we have $\Delta_{v_0} = \Delta_{w_0}$ and $\mathrm{k}_{v_0} = \mathrm{k}_{w_0}$. Let $s \in \mathbf{F}_p((t))$ be transcendental over $\mathbf{F}_p(t)$ (such s exist, because $\overline{\mathbf{F}_p(t)}$ is countable, and $\mathbf{F}_p((t))$ is uncountable) and consider $K = \mathbf{F}_p(t, s^p) \subseteq \mathbf{F}_p(t, s) = L$, with restricted valuations v respectively w. This is a purely inseparable extension of degree p with the property that $\mathrm{g}_{L,v} = \mathrm{e}(w/v) = \mathrm{f}(w/v) = 1$. From Proposition 5.6 and Theorem 3.9 we conclude $\mathrm{d}(w/v) = p$.

We will show that in certain cases, there is no defect. We use the following lemma.

Lemma 8.2. *Let k be a field and let A be a localization at a multiplicative set of a finitely generated k-algebra which is a domain. Put $K = Q(A)$ and let L/K be a finite extension of fields. Then the integral closure $\overline{A}$ of A in L is finite as A-module.*

Proof. Assume first that A is finitely generated as k-algebra.

Notice that it is enough to prove the statement for a finite extension of L. Indeed, a finitely generated module over a noetherian ring is a noetherian module ([**AM69**, Proposition 6.5]), and hence all submodules are finitely generated.

Noether normalization, [**Liu02**, Proposition 2.1.9], tells us that A is finite over a polynomial ring $A' = k[x_1, \ldots, x_n]$ with quotient field K'. We show that the integral closure of A' in L, which is $\overline{A}$, is a finite A'-module and hence a finite A-module. This reduces to the case where $A = k[x_1, \ldots, x_n]$.

We will start enlarging L. First enlarge it such that L/K is normal. We can split L/K into a tower $L \supseteq L' \supseteq K$ where L'/K is purely inseparable and L/L' is separable. Hence we are reduced to proving the following two cases:

i. L/K separable;
ii. L/K purely inseparable and $A = k[x_1, \ldots, x_n]$.

Assume that L/K is separable. Let $y_1, \ldots, y_m$ be a basis of L/K with $y_i \in \overline{A}$. Let $y_1', \ldots, y_m'$ be a dual basis of L/K with respect to the trace. Then it follows that $Ay_1 \oplus \ldots \oplus Ay_n \subseteq \overline{A} \subseteq Ay_1' \oplus \ldots \oplus Ay_n'$. Note that $Ay_1' \oplus \ldots \oplus Ay_n'$ is a finitely generated module over a noetherian ring, and hence a finite A-module. It follows that $\overline{A}$ is a finite A-module.

Assume that L/K is purely inseparable and $A = k[x_1, \ldots, x_n]$. Since L/K is finite, we see that L is contained in $L' = l(x_1^{-p^d}, \ldots, x_n^{-p^d})$ for some $d \in \mathbf{Z}_{\geq 0}$ large enough and l a finite (purely inseparable) extension of k. Replace L by L'. Notice that $A' = l[x_1^{-p^d}, \ldots, x_n^{-p^d}]$ is integral over A and it is integrally closed. Hence the integral closure of A in L is A', and it is finite over A.

We will now treat the general case. Write $A = S^{-1}B$ where B is a finitely generated k-algebra and S a multiplicative set. From [**AM69**, Proposition 5.12] we obtain $\overline{A} = S^{-1}\overline{B}$. We have shown that B is a finite A-module and hence $\overline{A}$ is a finite A-module. □

Proposition 8.3. *Let $(L, w) \supseteq (K, v)$ be a finite extension of valued fields. Suppose one of the following hold:*

i. *L/K is separable and $\Delta_v \cong \mathbf{Z}$;*
ii. *$\mathcal{O}_v$ contains a field k, $\mathcal{O}_v \neq K$, K finitely generated over k, and* $\operatorname{trdeg}_k(K) = 1$.

Then we have $\Delta_v \cong \mathbf{Z}$ and $\mathrm{d}(w/v) = 1$.

Proof. First we prove that in the second case we also have $\Delta_v \cong \mathbf{Z}$. Let $x \in \mathcal{O}_v$ transcendental over k. Then $\mathfrak{p} = k[x] \cap \mathfrak{m}_v$ is a prime ideal. If it is zero, then $\mathcal{O}_v \supseteq k(x)$ and since K is finite over $k(x)$, it follows that $\mathcal{O}_v = K$, contradiction. Hence $\mathcal{O}_v \cap k(x) = k[x]_{\mathfrak{p}}$ (this follows since we know all valuations on $k(x)$ which are trivial on k). Notice that $k[x]_{\mathfrak{p}}$ is a discrete valuation ring, and hence the same follows for $\mathcal{O}_v$ (as e is finite). Replace $\mathcal{O}_v$ by $k[x]_{\mathfrak{p}}$ and K by $k(x)$ in this case. We will show the statement about $\mathrm{d}(w/v)$ for the bigger extension, and the result about $\mathrm{d}(w/v)$ follows from multiplicativity.

Now we will consider both cases at once. Let $\mathcal{O}$ be the integral closure of $\mathcal{O}_v$ in L. Assume first that $\mathcal{O}$ is a finitely generated $\mathcal{O}_v$-module. Then one easily sees that $\mathcal{O}$ is a free $\mathcal{O}_v$-module of rank $[L : K]$, since $\mathcal{O}_v$ is a discrete valuation ring. Consider $\mathcal{O}/\mathfrak{m}_v\mathcal{O}$, which is isomorphic to $\prod_{w|v} \mathcal{O}_w/\mathfrak{m}_v\mathcal{O}_w$ (Proposition 5.4, in combination with theorems on artinian rings from [**AM69**]). Notice that $\mathcal{O}_w/\mathfrak{m}_v\mathcal{O}_w$ is a vector space over k_v of dimension $\mathrm{e}(w/v)\,\mathrm{f}(w/v)$ and the result follows.

Hence we are finished if we can show that $\mathcal{O}$ is finite over $\mathcal{O}_v$. In the first case, this follows directly from the trace pairing. In the second case, use Lemma 8.2. □

We will finish this section by giving an example of a separable extension of valued fields which has a defect. We start with the following lemma, which goes back to [**Sch77**]. We follow a proof from [**Ste88**].

Lemma 8.4. *Let K be a field and $n \in \mathbf{Z}_{\geq 1}$ be an integer coprime with* $\operatorname{char} K$. *Let w be the number of n-th roots of unity in K. Let L be the splitting field of $x^n - a \in K[x]$. Then one has: L/K is abelian iff $a^w \in K^n$.*

Proof. We may assume $a \neq 0$.

$\Longrightarrow$: Fix $\alpha \in L$ with $\alpha^n = a$ and let ζ_n be an n-th root of unity. Let $\sigma \in G = \mathrm{Gal}(L/K)$. Write $\sigma(\zeta_n) = \zeta_n^{k(\sigma)}$. For $\tau \in G$ one has

$$\frac{\tau\sigma(\alpha)}{\sigma(\alpha)} = \frac{\sigma\tau(\alpha)}{\sigma(\alpha)} = \sigma\left(\frac{\tau(\alpha)}{\alpha}\right) = \left(\frac{\tau(\alpha)}{\alpha}\right)^{k(\sigma)} = \frac{\tau(\alpha^{k(\sigma)})}{\alpha^{k(\sigma)}}.$$

Hence $\alpha^{k(\sigma)}/\sigma(\alpha)$ is fixed by τ and hence lies in K. Its n-th power is $a^{k(\sigma)-1} \in K^n$. Let r be the greatest common divisor of n and $k(\sigma) - 1$ for $\sigma \in G$. Then we have $a^r \in K^n$. As $\langle \zeta_n^{n/r} \rangle$ is the set of G-invariant n-th roots of unity, one has $r = w$.

$\Longleftarrow$: Suppose $a^w = b^n$ for some $b \in K$. One has $K \subseteq L \subseteq L' = K(b^{1/w}, \zeta_{nw})$. Notice that L'/K is abelian and hence L/K is abelian. □

Remark 8.5. Next we will give an example of a separable extension which has a defect. Let p be a prime and consider the field $\mathbf{Q}_p$ with its standard p-adic valuation. It is well-known that this valuation has a unique extension to each algebraic extension ($\mathbf{Q}_p$ is *henselian*). Let L be the maximal tamely ramified extension of $\mathbf{Q}_p$. Put $L' = L(\zeta_{p^i} : i \in \mathbf{Z}_{\geq 1})$. We claim that for any finite extension L''/L' we have $\mathrm{d}(L''/L') = [L'' : L']$ (we do not specify the valuations, since they are unique). Indeed, from the construction one easily sees that $\mathrm{e} = \mathrm{f} = 1$ (the residue field of L is already algebraically closed, and the value group of L' is $\mathbf{Q}$) and as the extension is unique, the degree is equal to the defect. We will now find a non-trivial extension L''/L'. We claim that $\sqrt[p^2]{p} \notin L'$. Suppose $\sqrt[p^2]{p} \in L'$, then $L(\sqrt[p^2]{p})/L$ is an abelian Galois extension. Note that $\#\{x \in L : x^{p^2} = 1\} = p$, as $\mathbf{Q}_p(\zeta_{p^2})/\mathbf{Q}_p$ is wild. Lemma 8.4 gives us $p^p \in L^{p^2}$. But this means that $L/\mathbf{Q}_p$ is not tame, contradiction. Hence we can take $L'' = L'(\sqrt[p^2]{p})$.

9. Frobenius formalism

Let G be a profinite group. Then we define

$$\hat{\mathbf{Z}} \times G \to G$$
$$(u, g) \mapsto g^u$$

as follows. Write $G = \varprojlim_i G_i$ with G_i finite and for $g = (g_i)_i$ set

$$g^u = \left(g_i^{u \pmod{\mathrm{ord}(g_i)}}\right)_i.$$

If G is abelian, this makes G a topological $\hat{\mathbf{Z}}$-module.

9.1. Definitions. Let k be a perfect field such that $\mathrm{Gal}(k_{\mathrm{sep}}/k) = \overline{\langle F \rangle}$ is procyclic with generator F. Such a field k together with a procyclic generator of its absolute Galois group, is called a *quasi-cyclic field*. Remark that a quasi-cyclic field with absolute Galois group isomorphic to $\hat{\mathbf{Z}}$ is called a quasi-finite field ([**Ser79**, Section 2 of Chapter XXIII]).

Lemma 9.1. *Let H be a subgroup of $\hat{\mathbf{Z}}$. Then the following are equivalent:*

i. *H is closed;*
ii. *H is a principal ideal of $\hat{\mathbf{Z}}$.*

Proof. i $\implies$ ii: Let N be an open subgroup of $\hat{\mathbf{Z}}$. Then $[\hat{\mathbf{Z}} : N]$ is finite, say $[\hat{\mathbf{Z}} : N] = n$ and hence $n\hat{\mathbf{Z}} \subseteq N$. Note that $[\hat{\mathbf{Z}} : n\hat{\mathbf{Z}}] = n$, and hence we obtain $N = n\hat{\mathbf{Z}}$.

A closed subgroup of a profinite group is an intersection of open subgroups ([**RV99**, Theorem 1.18]). Hence there are integers n_i such that

$$H = \bigcap_{i \in I} n_i \hat{\mathbf{Z}}.$$

Consider the Steinitz number $r = \mathrm{lcm}(n_i : i \in I) = \prod_p p^{m_p}$. Let $s = (p^{m_p})_p \in \hat{\mathbf{Z}}$. One then easily finds $H = (s)$.

ii $\implies$ i: This follows easily. □

From the lemma above one deduces that a closed subgroup of $\mathrm{Gal}(k_{\mathrm{sep}}/k)$ is of the form $F^{s\hat{\mathbf{Z}}}$ with $s \in \hat{\mathbf{Z}}$. The corresponding field extension of k is denoted by $k_s = k_{\mathrm{sep}}^{F^{s\hat{\mathbf{Z}}}}$. In this case $\mathrm{Gal}(k_{\mathrm{sep}}/k_s) = F^{s\hat{\mathbf{Z}}}$ and hence is topologically generated by the element F^s. One obtains all separable extensions of k in this way by Lemma 9.1 and Galois theory. Note that for such a field k_s, there is at most one extension of a given finite degree n, corresponding to $F^{ns\hat{\mathbf{Z}}}$. Such an extension is automatically Galois and it exists iff $n | \mathrm{ord}(\mathrm{Gal}(k_{\mathrm{sep}}/k_s)) = \prod_{p:\ \mathrm{ord}_p(s)\neq\infty} p^\infty$.

Let (K, v) be a valued field. Assume that we are given an embedding $k_s \subseteq \mathrm{k}_v$ such k_v/k_s is finite. Let $(M, x) \supseteq (K, v)$ be a normal extension of valued fields with group $G = \mathrm{Aut}_K(M)$. Then one has an exact sequence (Theorem 3.6)

$$0 \to \mathrm{I}_{x,K} \to \mathrm{D}_{x,K} \xrightarrow{\varphi} \mathrm{Gal}(\mathrm{k}_x/\mathrm{k}_v) \to 0.$$

We will construct a canonical topological generator of $\mathrm{Gal}(\mathrm{k}_x/\mathrm{k}_v)$. Note that the group $\mathrm{Gal}(k_{\mathrm{sep}}/\mathrm{k}_v)$ has a canonical generator $F^{[\mathrm{k}_v:k_s]s}$. Let $t \in \mathrm{Hom}_{\mathrm{k}_v}(\mathrm{k}_x, k_{\mathrm{sep}})$. Note that t is injective and let $t^{-1}\colon \mathrm{im}(t) \to \mathrm{k}_x$ be its inverse. This gives us a map $\tau\colon \mathrm{Gal}(k_{\mathrm{sep}}/\mathrm{k}_v) \to \mathrm{Gal}(k_x/k_v)$. We claim that this map does not depend on t. Suppose $t' \in \mathrm{Hom}_{\mathrm{k}_v}(\mathrm{k}_x, k_{\mathrm{sep}})$. Then $t' = t''t$ for some $t'' \in \mathrm{Gal}(k_{\mathrm{sep}}/\mathrm{k}_v)$. Consider the corresponding map τ'. Using that $\mathrm{Gal}(k_{\mathrm{sep}}/\mathrm{k}_v)$ is abelian, one finds for $\sigma \in \mathrm{Gal}(k_{\mathrm{sep}}/\mathrm{k}_v)$

$$\tau'(\sigma) = t'^{-1} \circ \sigma \circ t' = t^{-1} \circ t''^{-1} \circ \sigma \circ t'' \circ t = t^{-1} \circ \sigma \circ t = \tau(\sigma).$$

This allows us to define the *Frobenius class* as

$$(x, M/K, s) = \varphi^{-1}\left(\tau\left(F^{[\mathrm{k}_v:k_s]s}\right)\right).$$

Note that it is a coset modulo $\mathrm{I}_{x,K}$. The notation $(x, M/K, s)$ implicitly implies that we have a given map $k_s \subseteq \mathrm{k}_{x|_K}$ and that $\mathrm{k}_{x|K}/k_s$ is finite. If $s = 1$ we usually write $(x, M/K, s) = (x, M/K)$.

As G acts transitively on the set of primes above v, one can show that for $g \in G$ we have $(gx, M/K, s) = g(x, M/K, s)g^{-1}$. Hence we define $(v, M/K, s)$ to be the orbit of $(x, M/K, s)$ under conjugation in G. This is an element of G if G is abelian and x/v is unramified.

Let k be a finite field. Then $\mathrm{Gal}(k_{\mathrm{sep}}/k) \cong \hat{\mathbf{Z}}$. We have a natural generator $F : x \mapsto x^{\#k}$.

9.2. Properties.

Proposition 9.2. *Let $s, t \in \hat{\mathbf{Z}}$ with $t|s$. Let L, M be algebraic extensions of a field K in a fixed algebraic closure of K and assume that M/K is normal. Let x be a valuation on LM. Assume that $x|_M/x|_K$ is unramified and that we have a commutative diagram as follows:*

$$\begin{array}{ccc} k_s & \longrightarrow & \mathrm{k}_{x|_L} \\ \uparrow & & \uparrow \\ k_t & \longrightarrow & \mathrm{k}_{x|_K}. \end{array}$$

Then one has:

$$(x, LM/L, s)|_M = (x|_M, M/K, t)^{\frac{[\mathrm{k}_{x|_L}:k_s]s}{[\mathrm{k}_{x|_K}:k_t]t}}.$$

PROOF. Take $t \in \mathrm{Hom}_{\mathrm{k}_{x|_L}}(\mathrm{k}_x, k_{\mathrm{sep}})$. This induces the following commutative diagram (the isomorphisms are obtained from Theorem 3.6):

$$\begin{array}{ccccc}
\mathrm{D}_{x,L} & \xrightarrow{\sim} & \mathrm{Gal}(\mathrm{k}_x/\mathrm{k}_{x|_L}) & \longleftarrow & \mathrm{Gal}(k_{\mathrm{sep}}/\mathrm{k}_{x|_L}) \ni F^{[\mathrm{k}_{x|_L}:k_s]s} \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{D}_{x|_M,K} & \xrightarrow{\sim} & \mathrm{Gal}(\mathrm{k}_{x|_M}/\mathrm{k}_{x|_K}) & \longleftarrow & \mathrm{Gal}(k_{\mathrm{sep}}/\mathrm{k}_{x|_K}) \ni F^{[\mathrm{k}_{x|_K}:k_t]t}.
\end{array}$$

From this diagram we deduce the result directly. □

If $s = t$ in the above Lemma, then the exponent in the above expression becomes $[k_{x|_L} : k_{x|_K}] = \mathrm{f}(x|_L/x|_K)$.

We introduce some notation to simplify part of the statement of the above lemma. Let K be a field. Let M/K be a finite normal extension such that $G = \mathrm{Aut}_K(M)$ is abelian. Let V be a set of discrete valuations of K which are unramified in M and assume that we have natural maps $k_s \subseteq \mathrm{k}_v$ for every $v \in V$ such that k_v/k_s is finite (for some fixed s). Let $D = \sum_{v\in V} D_v v \in \bigoplus_{v\in V} \mathbf{Z}v = \mathrm{div}(V)$. We set $(D, M/K, s) = \prod_{v\in V}(v, M/K, s)^{D_v} \in G$ (this requires that G is abelian). Let L/K be a finite extension of K in some algebraic closure of K containing M and let V' be the set of valuations of L extending a valuation of V. We have a natural map of groups

$$\begin{aligned}
\mathrm{Norm}_{L/K}\colon\ & \mathrm{div}(V') \to \mathrm{div}(V) \\
& v' \in V' \mapsto \mathrm{f}(v'/v'|_K)v'|_K.
\end{aligned}$$

Corollary 9.3. *Under the assumptions above one has for $D' \in \mathrm{div}(V')$:*

$$(D', LM/L)|_M = (\mathrm{Norm}_{L/K}(D'), M/K).$$

PROOF. Note that D' only consists of unramified primes (Corollary 3.11). The statement follows directly from Proposition 9.2. □

Lemma 9.4. *Let L, M be algebraic extensions of a field K in a fixed algebraic closure and assume that L/K and M/K are normal and let x be a valuation on LM such that $x|_L/x|_K$ is unramified. Then in*

$$\mathrm{Aut}_K(LM) = \mathrm{Aut}_K(L) \times_{\mathrm{Aut}_K(L\cap M)} \mathrm{Aut}_K(M)$$

one has

$$(x, LM/K) = (x|_L, L/K) \times (x|_M, M/K).$$

Furthermore, one has a natural injective map $\mathrm{D}_{x,L} \,/\, \mathrm{I}_{x,L} \to \mathrm{D}_{x|_M,K} \,/\, \mathrm{I}_{x|_M,K}$.

PROOF. We have a natural injective map $\mathrm{D}_{x,L} \to \mathrm{D}_{x|_M,K}$. Note that $x/x|_M$ is unramified. Hence we have $\mathrm{I}_{x,M} = 0$ and $\mathrm{I}_{x|_L,K} = 0$. Theorem 3.6 gives $\mathrm{I}_{x,L} = \mathrm{I}_{x,K} = \mathrm{I}_{x|_M,K}$. This shows that the above map is injective. Furthermore, one deduces the first statement from this directly. □

Remark 9.5. For ramified extensions such a statement does not hold. Here is an example which shows that things can go wrong. Consider the extension $L = k(\sqrt{x})$ over $K = k(x)$ where k is a finite field and $\mathrm{char}(k) \neq 2$. Consider the prime ∞ of $k(x)$. Let k' be the unique quadratic extension of k and let $M' = k'(x)$. The extension LM'/K has Galois group V_4. Let M be the third quadratic extension of K inside LM'. Notice that M/K is ramified, because there is a unique maximal unramified extension. Let ∞_L be the unique prime of L above ∞ and similarly ∞_M for M. The extension LM/L is not ramified and there is a unique prime ∞_{LM} above ∞_L in LM: the residue field gets enlarged. Consider the natural map $\mathrm{D}_{\infty_{LM},L} \,/\, \mathrm{I}_{\infty_{LM},L} = \mathrm{D}_{\infty_{LM},L} \to \mathrm{D}_{\infty_M,K} \,/\, \mathrm{I}_{\infty_M,K}$. The first group is a C_2, the second one is trivial. Hence the map is not injective. This phenomenon plays a crucial role in Chapter 7.

Suppose a group G acts on a set X. For $g \in G$ we set $X^g = \{x \in X : gx = x\}$. We have the following generalization of the Burnside's lemma.

Lemma 9.6. *Let G be a finite group acting on a finite set X. Let N be a normal subgroup and let $\alpha \in G$. Then we have*

$$\#(N\backslash X)^{\alpha N} = \frac{1}{\#N} \sum_{n \in N} \#X^{\alpha n}.$$

Proof. Consider the $\mathbf{Q}[G]$-modules $\mathbf{Q}^X \supseteq \left(\mathbf{Q}^X\right)^N \cong \mathbf{Q}^{N\backslash X}$. Let

$$\epsilon = \frac{1}{\#N} \sum_{n \in N} n.$$

Then we have $\epsilon^2 = \epsilon$. Hence $\mathbf{Q}^X = \epsilon\mathbf{Q}^X \oplus (1-\epsilon)\mathbf{Q}^X$. Notice that $\epsilon\mathbf{Q}^X = \left(\mathbf{C}^X\right)^N$. Using this decomposition, we will calculate the trace of α. We have:

$$\begin{aligned}
\sum_{n \in N} \#X^{\alpha n} &= \sum_{n \in N} \mathrm{tr}_{\mathbf{Q}^X/\mathbf{Q}}(\alpha n) = \#N \cdot \mathrm{tr}_{\mathbf{Q}^X/\mathbf{Q}}(\alpha\epsilon) \\
&= \#N \cdot \mathrm{tr}_{\epsilon\mathbf{Q}^X/\mathbf{Q}}(\alpha\epsilon) + \#N \cdot \mathrm{tr}_{(1-\epsilon)\mathbf{Q}^X/\mathbf{Q}}(\alpha\epsilon) \\
&= \#N \cdot \mathrm{tr}_{\mathbf{Q}^{N\backslash X}/\mathbf{Q}}(\alpha) + 0 \\
&= \#N \cdot \#(N\backslash X)^{\alpha N}.
\end{aligned}$$

□

Proposition 9.7. *Let (K, v) be a valued field and let L be an algebraic extension of K. Let $(M, x) \supseteq (K, v)$ be a normal extension of valued fields with group $G = \mathrm{Aut}_K(M)$ such that the G-set $X = \mathrm{Hom}_K(L, M)$ is not empty. Assume that we have a finite embedding $k_s \subseteq \mathrm{k}_v$. Then the cardinality of the set of valuations w on L extending v such that $\mathrm{f}(w/v) = 1$ is equal to*

$$\frac{1}{\#\,\mathrm{I}_{x,K}} \sum_{h \in (x, M/K, s)} \#X^h.$$

Proof. Combine Corollary 3.18 with Lemma 9.6. □

Information about the Galois group can be obtained from looking at Frobenius elements.

Proposition 9.8. *Let (K, v) be a valued field and let L/K be a finite separable extension. Assume that we have an embedding $k_s \subseteq \mathrm{k}_v$ with $[\mathrm{k}_v : k_s] < \infty$. Let M/K be a normal closure of L. Let $X_L = \mathrm{Hom}_K(L, M)$ and consider $G = \mathrm{Aut}_K(L) \subseteq \mathrm{Sym}(X_L)$. Let $w_1, \ldots, w_m$ be the different primes of L extending v. Then the following hold:*

i. *assume that the w_i/v are unramified, then G contains a disjoint product of cycles of length $\mathrm{f_s}(w_1/v), \ldots, \mathrm{f_s}(w_m/v)$.*
ii. *if $\prod_{i=1}^{m} \mathrm{n}(w_i/v) = l$ prime, then G contains an l-cycle.*

Proof. Let x be a prime of M extending v.

i. The extension x/v is unramified (Corollary 3.15). It follows that $\mathrm{D}_{x,K}$ is a cyclic group generated by $(x, M/K, s)$. Proposition 3.17 says that the action of $\mathrm{D}_{x,K}$ on X_L has orbits of size $\mathrm{f_s}(w_1/v), \ldots, \mathrm{f_s}(w_m/v)$. The Frobenius element has this cycle type.

ii. Proposition 3.17 implies that the orbits of the action of $\mathrm{D}_{x,K}$ on X_L have length $l, 1, 1, \ldots, 1$. Notice that a subgroup of S_l acting transitively on $\{1, \ldots, l\}$ contains an l-cycle as l is prime. Hence $\mathrm{D}_{x,K}$ contains an l-cycle. □

Chapter 2

Normal projective curves

1. Introduction

This chapter is meant to introduce the well-known theory of normal projective curves over finite fields. We discuss for example the genus and the Picard group of such a curve. We also discuss class field theory and show how one can use this to estimate character sums. There are three results which we would like to mention, some of which are well-known.

The first result is Corollary 3.15 and it will play an important role in Chapter 7.

Corollary 1.1. *Let k be a finite field and let k' be a finite extension of k. Let K be a function field over k. Then the map* $\mathrm{Norm}_{Kk'/K}\colon \mathrm{Pic}^0_{k'}(Kk') \to \mathrm{Pic}^0_k(K)$ *is surjective.*

Secondly, we give models for hyperelliptic curves over perfect fields (Theorem 4.4). The difference with most literature is that we give necessary and sufficient conditions for equations to give a hyperelliptic curve of a certain genus. For example, the curve in characteristic 2 given by $y^2 + y + x^{2949120} = 0$ has genus 42.

Finally, we calculate the 2-torsion of the Picard group of a hyperelliptic curve in Theorem 4.9.

Theorem 1.2. *Let k be a perfect field. Let K be a function field over k with* $\mathrm{Pic}^0_k(K) = 0$. *Let L be a Galois extension of degree 2 with* $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. *Suppose that ∞ is a rational prime of K with the property that there is a unique prime ∞' above it in L with* $\mathrm{e}(\infty'/\infty) = 2$. *Let* $S = \{w \in \mathcal{P}_{L/k} :\ \mathrm{e}(w/w|_K) = 2\} \setminus \{\infty'\}$. *Then for any $w \in S$ one has* $[w - \deg_k(w)\infty'] \in \mathrm{Pic}^0_k(L)[2]$. *We have a surjective map*

$$\begin{aligned} \psi\colon \mathbf{F}_2^S &\to \mathrm{Pic}^0_k(L)[2] \\ e_w &\mapsto [w - \deg_k(w)\infty'] \end{aligned}$$

with

$$\ker(\psi) = \begin{cases} \mathbf{F}_2 \cdot \left(\sum_{w\in S} e_w\right) & \text{if } \mathrm{char}(k) \neq 2 \\ 0 & \text{if } \mathrm{char}(k) = 2. \end{cases}$$

In this chapter, let k be a field and let $\overline{k}$ be an algebraic closure of k.

2. Normal projective curves

2.1. Properties of schemes. We follow [**Liu02**].

Definition 2.1. Let $(X, \mathcal{O}_X)$ be a scheme. Then X is called *reduced* (respectively *integral*) if for all $x \in X$ the stalk $\mathcal{O}_{X,x}$ is reduced (respectively integral). The scheme

is called *normal* if X is irreducible and if for all $x \in X$ the stalk $\mathcal{O}_{X,x}$ is integral an normal. The scheme X is reduced (respectively integral, respectively normal) if for all $U \subseteq X$ open non-empty the ring $\mathcal{O}_X(U)$ is reduced (respectively integral, respectively normal) ([**Liu02**, Proposition 2.4.2, Proposition 2.4.17, Proposition 4.1.5]).

If X is integral, with generic point ξ, we define the *function field* of X as $K(X) = \mathcal{O}_{X,\xi}$. If X is a scheme over k, we will write $k(X)$ instead of $K(X)$.

A scheme X/k is called *projective* over k if X is isomorphic to a closed subscheme of $\mathbf{P}^n_k$ for some $n \in \mathbf{Z}_{\geq 0}$.

2.2. Algebraic varieties.

Definition 2.2. Let k be a field. An *affine algebraic variety* over k is a scheme isomorphic to $\mathrm{Spec}(A)$ where A is a finitely generated k-algebra. An *algebraic variety* is a scheme which has an open cover by finitely many affine algebraic varieties. The algebraic varieties form a category $\mathfrak{Var}_k$ for which morphisms are morphisms of k-schemes. We let $\mathfrak{RVar}_k$ be the full subcategory of the category of algebraic varieties which are reduced.

Lemma 2.3. *Let k be a field and let R, S be k-algebras. Assume that S is finitely generated as k-algebra and reduced. Let $\alpha, \beta \colon R \to S$ be morphisms over k which induce the same map $\overline{\alpha} = \overline{\beta} \colon \mathrm{Hom}_k(S, \overline{k}) \to \mathrm{Hom}_k(R, \overline{k})$. Then $\alpha = \beta$.*

Proof. The nilradical of S is equal to the Jacobson radical of S ([**Liu02**, Lemma 2.1.18]). Let $\mathfrak{m} \in \mathrm{MaxSpec}(S)$. Then $S/\mathfrak{m}$ is a finite field extension of k ([**Liu02**, Corollary 2.1.12]). Pick a morphism $s \in \mathrm{Hom}_k(S, \overline{k})$ with kernel $\mathfrak{m}$. Then the two induced maps give the same map $R \to S \to S/\mathfrak{m}$. Hence $\mathfrak{D} = \{\alpha(r) - \beta(r) : r \in R\} \subseteq \mathfrak{m}$. Hence, $\mathfrak{D}$ is contained in the nilradical of S, which is 0 since S is reduced. Hence $\alpha = \beta$. □

Let $\mathfrak{Sets}$ be the category of sets.

Proposition 2.4. *The functor*

$$\mathfrak{RVar}_k \to \mathfrak{Sets}$$
$$X \mapsto X(\overline{k}) = \mathrm{Hom}_{\mathrm{Spec}(k)}(\mathrm{Spec}(\overline{k}), X)$$

is faithful.

Proof. One can reduce to the affine case and then apply Lemma 2.3. □

Remark 2.5. The above statement is no longer true if one removes the word reduced. For example, let $X = \mathrm{Spec}(k[\epsilon]/(\epsilon^2))$. Consider the identity $\mathrm{id} \colon X \to X$ and the k-morphism $\varphi \colon X \to X$ coming from $\epsilon \mapsto 0$. One has $X(\overline{k}) = \mathrm{Hom}_k(k[\epsilon]/(\epsilon^2), \overline{k}) = \{\big(k[\epsilon]/(\epsilon^2) \to \overline{k}, \epsilon \mapsto 0\big)\}$. Hence both morphisms will induce the same map on $X(\overline{k})$.

2.3. Normal projective curves.

Definition 2.6. An algebraic variety over k whose irreducible components are of dimension 1 is called an *algebraic curve* over k. We will often just say that it is a curve.

We are interested in normal projective varieties because they can be studied by looking at their function fields. A morphism between irreducible schemes is called *dominant* if it maps the generic point to the other generic point.

Definition 2.7. A *function field* K over k is a finitely generated field extension of k of transcendence degree 1.

Theorem 2.8. *Let k be a field. Then there is an anti-equivalence of categories between the category of normal projective curves over k with finite morphisms and the category of function fields over k with finite k-morphisms of fields. This equivalence maps a curve C to its function field $k(C)$ and a finite morphism $C \to D$ to the inclusion $k(D) \subseteq k(C)$ induced by $C \to D$.*

PROOF. See [**Liu02**, Proposition 7.3.13]. □

The book of Stichtenoth, [**Sti09**], focuses on this function field approach to normal projective curves. We will mostly follows this approach. A finite morphism between normal projective curves is called *separable* if the corresponding inclusion of function fields is separable.

For a normal projective curve there is a relation between the set of $\overline{k}$-points and the set of valuations which are trivial on k.

Definition 2.9. Let K be a function field over k. Let $\mathcal{P}_{K/k}$ be the set of valuation rings of K which contain k but are not equal to K. We use the notation $\mathcal{P}^1_{K/k}$ for the valuations which residue field is k. Assume that $k' \subset K$ is integral over k. Then one has $\mathcal{P}_{K/k} = \mathcal{P}_{K/k'}$.

Remark 2.10. Assume that $K = k(x)$, where x is transcendental over k. Then there is a bijection between $\{f \in k[x] : f \text{ monic irreducible}\} \cup \{\infty\}$ and $\mathcal{P}_{K/k}$. An irreducible monic $f \in k[x]$ corresponds to the valuation ring $k[x]_{(f)}$ and ∞ corresponds to $k[x^{-1}]_{(x^{-1})}$.

Proposition 2.11. *Let k be a field and let C be a normal projective curve over k with function field $k(C)$. Then we have a natural action $\mathrm{Aut}(\overline{k}/k)$ on $C(\overline{k})$ and a bijection*

$$\begin{aligned} \varphi\colon \mathrm{Aut}(\overline{k}/k) \setminus C(\overline{k}) &\to \mathcal{P}_{k(C)/k} \\ \mathrm{Aut}(\overline{k}/k)\tau &\mapsto \mathcal{O}_{C,\tau(\mathrm{Spec}(\overline{k}))}. \end{aligned}$$

The length of an orbit of an element of $C(\overline{k})$ is equal to the separability degree of the residue field extension over k of the corresponding valuation.

PROOF. One easily obtains the action. An element of $C(\overline{k})$ is nothing more than the choice of a point $P \in C$ and a k-morphism $\mathcal{O}_{C,P} \to \overline{k}$. Let η be the generic point of C. Notice that $\mathcal{O}_{C,\eta}$ has transcendence degree 1 over k and cannot be embedded in $\overline{k}$.

We claim that we have a bijection

$$\begin{aligned} C \setminus \{\eta\} &\to \mathcal{P}_{k(C)/k} \\ P &\mapsto \mathcal{O}_{C,P}. \end{aligned}$$

Let $x \in k(C)$ be transcendental over k. Then we have an inclusion $k[x] \to k(C)$. Valuations where x has a non-negative valuations correspond to (non-zero) primes of the integral closure of $k[x]$ in $k(C)$ (Theorem 5.4 from Chapter 1). This corresponds to the (non-generic) points of an affine chart of C ([**Liu02**, Proposition 3.13]).

This shows that φ is a bijection. The statement about the length of an orbit follows easily. □

Let K be a function field over k. We sometimes refer to elements of $\mathcal{P}_{K/k}$ as *places* or *points*. Notice that all elements of $\mathcal{P}_{K/k}$ are discrete valuations (see Proposition 8.3 from Chapter 1). For all $v \in \mathcal{P}_{K/k}$ we assume from now on that $\Delta_v = \mathbf{Z}$. This is not really a restriction, since there is a unique order preserving isomorphism $\Delta_v \cong \mathbf{Z}$.

We define the *divisor group* of K/k as $\mathrm{div}_k(K) = \bigoplus_{v \in \mathcal{P}_{K/k}} \Delta_v = \mathbf{Z}^{(\mathcal{P}_{K/k})}$, the free abelian group on the elements of $\mathcal{P}_{K/k}$. Elements of $\mathrm{div}_k(K)$ are called *divisors* and are denoted by $D = \sum_{v \in \mathcal{P}_{K/k}} c_v v$ where $c_v \in \mathbf{Z}$ almost always zero (often we will use P instead of v in such a sum). For $v \in \mathcal{P}_{K/k}$ we set $D_v = c_v$. The *support* of D is $\mathrm{supp}(D) = \{v \in \mathcal{P}_{K/k} : D_v \neq 0\}$.

For $D, D' \in \mathrm{div}_k(K)$, we define the *gcd* and *lcm*

$$\gcd(D, D') = \sum_{v \in \mathcal{P}_{K/k}} \min(D_v, D'_v) v$$

$$\mathrm{lcm}(D, D') = \sum_{v \in \mathcal{P}_{K/k}} \max(D_v, D'_v) v,$$

and similarly for any finite set of divisors. For $D \in \mathrm{div}_k(K)$ we put

$$D_0 = \sum_{v \in \mathcal{P}_{K/k} : D_v \geq 0} D_v v$$

and

$$D_\infty = \sum_{v \in \mathcal{P}_{K/k} : D_v \leq 0} -D_v v.$$

One has $D = D_0 - D_\infty$. For $D \in \mathrm{div}_k(K)$ one defines its *degree*

$$\deg_k(D) = \sum_{v \in \mathcal{P}_{K/k}} D_v [k_v : k] \in \mathbf{Z}$$

(note that this definition depends on k). This gives a group morphism

$$\deg_k : \mathrm{div}_k(K) \to \mathbf{Z}.$$

Its kernel is denoted by $\mathrm{div}_k^0(K)$. We have a natural map $K^* \to \mathrm{div}_k^0(K)$, which satisfies $a \mapsto (a) = \sum_{v \in \mathcal{P}_{K/k}} v(a) v$. This can be seen from the following lemma.

Lemma 2.12. *Let K be a function field over k and let $x \in K$ be transcendental over k. Then one has*

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

Proof. The proof will be given in the proof of Lemma 2.16. □

Sometimes we put $(a)_K$ to clarify which function field we use. We define $\mathrm{Pic}_k(K)$ by means of the exact sequence

$$K^* \to \mathrm{div}_k(K) \to \mathrm{Pic}_k(K) \to 0$$

and we define the *Picard group* $\mathrm{Pic}^0_k(K)$ of K over k by the exactness of

$$K^* \to \mathrm{div}^0_k(K) \to \mathrm{Pic}^0_k(K) \to 0.$$

The *full constant field* of K/k is defined to be the field extension of k which consists of the set of elements in K which are algebraic over k. If k is the full constant field in K, we say that K is *geometrically irreducible* (see [**Liu02**, Corollary 3.2.14]). A finite field extension L/K is called *geometric* if the full constant fields are the same. It is called *geometric over* k if k is the full constant field of L. Let k' be the full constant field of K. We say that L/K is *unramified* if the extension L/K is unramified at all $v \in \mathcal{P}_{K/k}$.

The kernel of the map $K^* \to \mathrm{div}_k(K)$ and $K^* \to \mathrm{div}^0_k(K)$ is equal to k'^*. The image of a divisor $D = \sum_v D_v v$ under the map to $\mathrm{Pic}_k(K)$ or $\mathrm{Pic}^0_k(K)$ is written as $[D] = \sum_v D_v[v]$. Note that $\mathrm{Pic}_k(K) \cong \mathrm{Pic}^0_k(K) \times \mathbf{Z}$, but not in a canonical way. If k is finite, the group $\mathrm{Pic}^0_k(K)$ is finite ([**Sti09**, Proposition 5.1.3]) and its order is denoted by h_K.

For $D, D' \in \mathrm{div}_k(K)$ we say $D \geq D'$ if for all $v \in \mathcal{P}_{K/k}$ one has $D_v \geq D'_v$. For $D \in \mathrm{div}_k(K)$ we define its *Riemann-Roch space*, a k-vector space, by

$$\mathfrak{L}_k(D) = \{a \in K^* : (a) + D \geq 0\} \cup \{0\}$$

and

$$l_k(D) = \dim_k(\mathfrak{L}(D)).$$

One has the following important theorem.

Theorem 2.13 (Riemann-Roch)**.** *Assume that k is the full constant field of K. Then there exists $g = g(K) \in \mathbf{Z}_{\geq 0}$ such that for all $D \in \mathrm{div}_k(K)$ of degree $> 2g - 2$ one has*

$$l_k(D) = \deg_k(D) + 1 - g.$$

If $W \in \mathrm{div}_k(K)$ satisfies $\deg(W) = 2g - 2$, $l(W) \geq g$, one has for all $D \in \mathrm{div}_k(K)$:

$$l_k(D) = \deg_k(D) + 1 - g + l_k(W - D).$$

Furthermore, such W exists.

Proof. This follows from [**Sti09**, Theorem 1.4.17, Theorem 1.5.15, Proposition 1.6.2] □

The quantity $g(K)$ in the above theorem is called the *genus* of K. If k is not the full constant field, we set $g(K)$ to be the genus of K with respect to its full constant field. If we want to stress that k is the full constant field, we sometimes write $g_k(K)$.

Proposition 2.14. *Assume that k is a perfect field. Set $p = \mathrm{char}(k)$ is $\mathrm{char}(k) \neq 0$ and $p = 1$ otherwise. Then the following hold:*

i. *for an algebraic extension k'/k we have $g(K) = g(Kk')$;*

ii. *if L/K is a finite purely inseparable extension, then there is $n \in \mathbf{Z}_{\geq 0}$ such that $L^{p^n} = K$ and $g(L) = g(K)$.*

PROOF. See [**Sti09**, Theorem 3.6.3 and Proposition 3.10.2]. □

Let k be a finite field. Then $\mathrm{Gal}(\overline{k}/k)$ is a procyclic group generated by $\mathrm{Frob}_k : x \mapsto x^{\#k}$. Let L/K be a finite Galois extension of function fields over k with group G. We can use the Frobenius formalism from Section 9 to define Frobenius elements for primes P of K which are unramified in L. This is a conjugacy class of G and we denote it by $(P, L/K) \subseteq G$. If G is abelian, we view $(P, L/K)$ as an element of G. If G is abelian and if $D = \sum_P D_v v$ is a divisor with support in unramified primes, then we define $(D, L/K) = \prod_{v \in \mathrm{supp}(D)} (v, L/K)^{D_v} \in G$.

Proposition 2.15. *Let K be a geometrically irreducible function field over a finite field k. Let $n \in \mathbf{Z}_{\geq 1}$ and let k_n be the unique field extension of k of degree n in an algebraic closure of K. Let F be the canonical generator $(x \mapsto x^{\#k})$ of $\mathrm{Gal}(k_n/k) \cong \mathrm{Gal}(Kk_n/K)$. Then first of all Kk_n/K is unramfied. For $D \in \mathrm{div}_k(K)$ one has $(D, Kk_n/K) = F^{\deg_k(D)} \in \mathrm{Gal}(Kk_n/K)$.*

PROOF. This follows from [**Sti09**, Theorem 3.6.3]. □

Let K be a function field over k and let L be a finite extension of K. If $v' \in \mathcal{P}_{L/k}$ we set $v' \cap K$ or $v'|_K$ for the valuation of K corresponding to the valuation ring $\mathcal{O}_{v'} \cap K$. We have two maps on divisor groups, the *norm* and the *conorm*:

$$\begin{aligned} \mathrm{Norm}_{L/K} \colon \mathrm{div}_k(L) &\to \mathrm{div}_k(K) \\ D = \sum_{v'} D_{v'} v' &\mapsto \sum_{v'} D_{v'} \, \mathrm{f}(v'/v'|_K) v'|_K \end{aligned}$$

and

$$\begin{aligned} \mathrm{Conorm}_{L/K} \colon \mathrm{div}_k(K) &\to \mathrm{div}_k(L) \\ D = \sum_{v} D_v v &\mapsto \sum_{v'} D_{v'|_K} \, \mathrm{e}(v'/v'|_K) v'|_K. \end{aligned}$$

Lemma 2.16. *Set $n = [L : K]$. Then the following diagram commutes:*

$$\begin{array}{ccccc} \mathrm{div}_k(K) & \xrightarrow[\mathrm{Conorm}_{L/K}]{} & \mathrm{div}_k(L) & \xrightarrow[\mathrm{Norm}_{L/K}]{} & \mathrm{div}_k(K) \\ \big\downarrow{\scriptstyle \deg_k} & & \big\downarrow{\scriptstyle \deg_k} & & \big\downarrow{\scriptstyle \deg_k} \\ \mathbf{Z} & \xrightarrow[\cdot n]{} & \mathbf{Z} & \xrightarrow[\mathrm{id}]{} & \mathbf{Z} \end{array} \qquad \text{(with } \cdot n \text{ : } \mathrm{div}_k(K) \to \mathrm{div}_k(K)\text{)}$$

Furthermore, $\mathrm{Conorm}_{L/K}$ *induces the following commutative diagram of groups:*

$$\begin{array}{ccccccc} K^* & \longrightarrow & \mathrm{div}_k^0(K) & \longrightarrow & \mathrm{Pic}_k^0(K) & \longrightarrow & 0 \\ {\scriptstyle i}\big\downarrow & & \big\downarrow & & \big\downarrow & & \\ L^* & \longrightarrow & \mathrm{div}_k^0(L) & \longrightarrow & \mathrm{Pic}_k^0(L) & \longrightarrow & 0. \end{array}$$

Similarly, $\mathrm{Norm}_{L/K}$ *induces the following commutative diagram of groups:*

$$\begin{array}{ccccccc} L^* & \longrightarrow & \mathrm{div}_k^0(L) & \longrightarrow & \mathrm{Pic}_k^0(L) & \longrightarrow & 0 \\ \downarrow{\scriptstyle \mathrm{Norm}_{L/K}} & & \downarrow & & \downarrow & & \\ K^* & \longrightarrow & \mathrm{div}_k^0(K) & \longrightarrow & \mathrm{Pic}_k^0(K) & \longrightarrow & 0. \end{array}$$

Proof of Lemma 2.16 and Lemma 2.12. The commutativity of the first diagram follows easily from the Fundamental inequality (Corollary 3.9 from Chapter 1) and the fact that there is no defect (Proposition 8.3 from Chapter 1).

The commutativity of the second diagram follows directly, except for the fact that we land in the 0 degree parts. We will prove Lemma 2.12. For $x \in K$ transcendental over k one considers the extension $K/k(x)$ and one obtains:

$$\begin{aligned} \deg_k((x)_{K,0}) &= \deg_k \mathrm{Conorm}_{K/k(x)}((x)_{k(x),0}) \\ &= [K : k(x)] \cdot \deg_k((x)_{k(x),0}) \\ &= [K : k(x)]. \end{aligned}$$

The other equality is similar.

To prove that the third diagram is commutative, is a bit harder. We prove the statement in several steps. One easily sees that it is enough to prove the case where L/K is separable and the case where L/K is purely inseparable. Assume that L/K is purely inseparable and let $x \in L^*$. As $\mathrm{div}_k^0(K)$ is torsion-free, we may assume that $x \in K^*$. We then have

$$\begin{aligned} (\mathrm{Norm}_{L/K}(x))_K &= (x^n)_K = n(x)_K = n\sum_v v(x)v \\ &= \sum_v \sum_{v'|v} \mathrm{f}(v'/v)\,\mathrm{e}(v'/v)v(x)v'|_K = \sum_{v'} \mathrm{f}(v'/v|_K)v'(x)v'|_K \\ &= \mathrm{Norm}_{L/K}((x)_L). \end{aligned}$$

Now assume that L/K is Galois with group G. For $x \in L^*$ one has

$$\mathrm{Norm}_{L/K}((x)_L) = \sum_{v'} \mathrm{f}(v'/v'|_K)v'(x)v'|_K.$$

For $g \in G$ and $v' \in \mathcal{P}_{L/k}$ one has $v'(g(x)) = \left(g^{-1}v'\right)(x)$. For $v \in \mathcal{P}_{K/k}$ we set $\mathrm{e}(v) = \mathrm{e}(v'/v)$ where v' extends v to L. This does not depend on v' (Theorem 3.6 from Chapter 1). Using this transitive action and the fundamental equality (Corollary 3.9 from Chapter 1) one has

$$\begin{aligned} \left(\mathrm{Norm}_{L/K}(x)\right)_K &= \left(\prod_{g\in G} g(x)\right)_K = \sum_v v(\prod_{g\in G} g(x))v \\ &= \sum_v \frac{1}{\mathrm{g}_{v,L}\,\mathrm{e}(v)} \sum_{v'|v} v'(\prod_{g\in G} g(x))v = \sum_v \frac{[L:K]}{\mathrm{g}_{v,L}\,\mathrm{e}(v)} \sum_{v'|v} v'(x)v \\ &= \sum_{v'} \mathrm{f}(v'/v'|_K)v'(x)v'|_K = \mathrm{Norm}_{L/K}((x)_L) \end{aligned}$$

as required. Assume that L/K is separable. Let M/K be a Galois extension containing L. Then one has for $x \in L^*$, using the first diagram and the Galois case,

$$\begin{aligned}\mathrm{Norm}_{L/K}((x)_L) &= \frac{1}{[M:L]}\,\mathrm{Norm}_{M/K} \circ \mathrm{Conorm}_{M/L}((x)_L)\\ &= \frac{1}{[M:L]}\,\mathrm{Norm}_{M/K}((x)_M) = \frac{1}{[M:L]}(\mathrm{Norm}_{M/K}(x))_K\\ &= \frac{1}{[M:L]}(\mathrm{Norm}_{L/K}(x)^{[M:L]})_K = (\mathrm{Norm}_{L/K}(x))_K.\end{aligned}$$

□

Let L/K be a finite separable extension of a function field K/k. Let $v \in \mathcal{P}_{K/k}$ and let $v' \in \mathcal{P}_{L/k}$ extend v. Let $L_{v'}$ respectively K_v be the completion of L at v' respectively K at v with valuations v'_{c} respectively v_{c}. Set

$$\delta(v'/v) = -\min\{v'(x) : x \in L_{v'},\ \mathrm{tr}_{L_{v'}/K_v}(x\mathcal{O}_{v'_{\mathrm{c}}}) \subseteq \mathcal{O}_{v_{\mathrm{c}}}\} \in \mathbf{Z}_{\geq 0},$$

where the valuation is the valuation on the fractional ideals (recall that $\mathcal{O}_{v'}$ is a discrete valuation ring). We define the *different*

$$\mathrm{diff}(L/K) = \sum_{v' \in \mathcal{P}_{L/k}} \delta(v'/v)v' \in \mathrm{div}_k(L).$$

We define the *discriminant* of L/K to be

$$\mathrm{disc}(L/K) = \mathrm{Norm}_{L/K}(\mathrm{diff}(L/K)).$$

We define the *quasi-different* as

$$\mathrm{qdiff}(L/K) = \sum_{v' \in \mathcal{P}_{L/k}} (\mathrm{e}(v'/v'|_K) - 1)\, v' \in \mathrm{div}_k(L).$$

Remark 2.17. One can avoid the use of completions in the definition of the different. See [**Ser79**, Section 3 and 4 in Chapter III].

Let k be a perfect field. Let L/K be a finite extension of a function field K/k. Note that $\mathrm{Norm}_{L_{K,\mathrm{sep}}}$ is a bijection in this case (Proposition 5.6 from Chapter 1 and Lemma 5.8 from Chapter 1). We put

$$i_{L/K} = \mathrm{Norm}^{-1}_{L/L_{K,\mathrm{sep}}} \circ \mathrm{Conorm}_{L_{K,\mathrm{sep}}/K}\,.$$

We set

$$\mathrm{diff}(L/K) = i_{L/L_{K,\mathrm{sep}}}\,(\mathrm{diff}(L_{K,\mathrm{sep}}/K)) \in \mathrm{div}_k(L),$$

where $\mathrm{diff}(L_{K,\mathrm{sep}}/K)$ is the usual different. Similarly, we set

$$\mathrm{qdiff}(L/K) = i_{L/L_{K,\mathrm{sep}}}\,(\mathrm{qdiff}(L_{K,\mathrm{sep}}/K)) \in \mathrm{div}_k(L),$$

where $\mathrm{qdiff}(L_{K,\mathrm{sep}}/K)$ is the usual quasi-different.

Lemma 2.18. *Let $M \supseteq L \supseteq K$ be extensions of function fields over a perfect field k. Then one has $i_{M/K} = i_{M/L} \circ i_{L/K}$.*

Proof. One has $i_{M/K} = \frac{1}{[M:K]_i}\,\mathrm{Conorm}_{M/K}$ (Proposition 2.14), and from this expression, multiplicativity is obvious. □

Lemma 2.19. *Let M_0/K_0 be a finite extension of function fields over a perfect field k. Let L_0, L_1 be intermediate extensions of M_0/K_0 such that L_0/K_0 and M_0/L_1 are separable and M_0/L_0 and L_1/K_0 are purely inseparable. Then one has:*

i. $i_{M_0/L_0}(\mathrm{diff}(L_0/K_0)) = \mathrm{diff}(M_0/L_1)$;
ii. $i_{M_0/L_0}(\mathrm{qdiff}(L_0/K_0)) = \mathrm{qdiff}(M_0/L_1)$.

Proof. Let $q = [M_0 : K_0]_i$. From Proposition 2.14 it follows that $L_0 = M_0^q$, and $K_0 = L_1^q$. The statement then follows easily. □

Proposition 2.20. *Let $K \subseteq L \subseteq M$ be a tower of function fields over a field k. If M/K is separable, or k is perfect, one has*

i. $\mathrm{diff}(M/K) = \mathrm{diff}(M/L) + i_{M/L}\left(\mathrm{diff}(L/K)\right)$;
ii. $\mathrm{qdiff}(M/K) = \mathrm{qdiff}(M/L) + i_{M/L}\left(\mathrm{qdiff}(L/K)\right)$.

Proof. Assume first that M/K is separable. The case for the different follows from [**Ser79**, Proposition 8, Chapter III]. For the case of the quasi-different, let $w \in \mathcal{P}_{M/k}$. Then one has, as e is multiplicative:

$$\mathrm{e}(w/w|_K) - 1 = \mathrm{e}(w/w|_L) - 1 + \mathrm{e}(w/w|_L)\left(\mathrm{e}(w|_L/w|_K) - 1\right).$$

And this proves the result.

Let us assume that k is perfect. Then one has, using Lemma 2.18 and Lemma 2.19 and the separable case:

$$\begin{aligned}\mathrm{diff}(M/K) &= i_{M/M_{K,\mathrm{sep}}}\left(\mathrm{diff}(M_{K,\mathrm{sep}}/K)\right)\\ &= i_{M/M_{L,\mathrm{sep}}} \circ i_{M_{L,\mathrm{sep}}/M_{K,\mathrm{sep}}}\\ &\quad \circ \left(\mathrm{diff}(M_{K,\mathrm{sep}}/L_{K,\mathrm{sep}}) + i_{M_{K,\mathrm{sep}}/L_{K,\mathrm{sep}}}\left(\mathrm{diff}(L_{K,\mathrm{sep}}/K)\right)\right)\\ &= \mathrm{diff}(M/L) + i_{M/L}(\mathrm{diff}(L/K)).\end{aligned}$$

The proof for the quasi-different is very similar. □

Proposition 2.21. *Let L/K be a finite separable extension and assume that k is perfect. Then for $w \in \mathcal{P}_{L/k}$ one has $\left(\mathrm{diff}(L/K)\right)_w \geq \mathrm{e}(w/w|_K) - 1$ with equality iff $w/w|_K$ is tame.*

Proof. See [**Sti09**, Corollary 3.5.5]. □

Hence, if L/K is tame (this implies that L/K is separable), one has $\mathrm{diff}(L/K) = \mathrm{qdiff}(L/K)$.

One important tool to calculate the genus is the *Riemann-Hurwitz theorem*.

Theorem 2.22 (Riemann-Hurwitz)**.** *Let K be a function field with full constant field k and let L/K be a finite extension. Assume that k is perfect. Let k' be the full constant field of L. Then one has*

$$[k' : k](2g_{k'}(L) - 2) = [L : K]_{\mathrm{s}}(2g_k(K) - 2) + \deg_k \mathrm{diff}(L/K).$$

Proof. The case that L/K is separable, follows from [**Sti09**, Theorem 3.4.13].

From Proposition 2.14 it follows that we have a tower $K \subseteq L_{K,\mathrm{sep}} = L^{p^r} \subseteq L$ where $p = \mathrm{char}(k)$ if nonzero and $p = 1$ otherwise and $r \in \mathbf{Z}_{\geq 0}$. Notice that $g(L) = g(L^{p^r})$. Hence by the previous part, it is enough to show that $\deg_k \mathrm{diff}(L/K) = \deg_k \mathrm{diff}(L_{K,\mathrm{sep}}/K)$. It follows from Lemma 2.16 that this is the case. □

Notice that $\deg_k \operatorname{diff}(L/K) = \deg_k \operatorname{disc}(L/K)$.

2.3.1. *Topology on $\mathcal{P}_{K/k}$.* We will endow $\mathcal{P}_{K/k}$ with the cofinite topology. This makes $\mathcal{P}_{K/k}$ into a connected topological space. We consider the following sheaves on $\mathcal{P}_{K/k}$. First we consider the constant sheaf K^*, which associates to every non-empty open set the group K^*. Consider the following presheaf $\mathcal{F}$, which for an open $U \subseteq \mathcal{P}_{K/k}$ satisfies

$$\mathcal{F}(U) = \begin{cases} \bigcap_{v \in U} \mathcal{O}_v^* & \text{if } U \neq \emptyset \\ 0 & \text{if } U = \emptyset \end{cases} \subseteq K^*.$$

Lemma 2.23. *The presheaf $\mathcal{F}$ is a sheaf and for any $v \in \mathcal{P}_{K/k}$ one has $\mathcal{F}_v = \mathcal{O}_v^*$.*

Proof. It is obvious that $\mathcal{F}$ is a sheaf. For an open set U containing v, we have a natural map $\mathcal{F}(U) \to \mathcal{O}_v^*$. This induces a map $\mathcal{F}_v \to \mathcal{O}_v^*$, which is injective. Take $x \in \mathcal{O}_v^*$. Let S be the support of (x) and let $V = \mathcal{P}_{K/k} \setminus S$. Then one has $x \in \mathcal{F}(V)$ and the surjectivity follows. □

Lemma 2.24. *Let K be a function field over a field k. Let $D \in \operatorname{div}_k(K)$ with $D \geq 0$. Then there exists $x \in K$ with $(x)_\infty \geq D$ and $\operatorname{supp}((x)_\infty) = \operatorname{supp}(D)$.*

Proof. If $D = 0$, take $x = 1$. Assume $D > 0$.

Let $v \in \operatorname{supp}(D)$. For $n \in \mathbf{Z}_{\geq D_v}$ large enough there exists $x_v \in K$ with $x_v \in \mathfrak{L}_k(nv) \setminus \mathfrak{L}_k((n-1)v)$ (Riemann-Roch, Theorem 2.13). Put $x = \sum_{v \in \operatorname{supp}(D)} x_v$. □

Corollary 2.25. *Let K be a function field over a field k. Let $S \subseteq \mathcal{P}_{K/k}$ be finite and non-empty. Then the following hold:*

i. *$\bigcap_{v \in \mathcal{P}_{K/k} \setminus S} \mathcal{O}_v$ is a Dedekind domain.*

ii. *$\bigcap_{v \in S} \mathcal{O}_v$ is a Dedekind domain.*

Proof. Take a function $x \in K$ with $\operatorname{supp}(x)_\infty = S$ (Lemma 2.24).

i. The ring $\bigcap_{v \in \mathcal{P}_{K/k} \setminus S} \mathcal{O}_v$ is the integral closure of $k[x] \subset k(x)$ in K. As it is integral over $k[x]$, its dimension is 1. It is noetherian as well (Lemma 8.2 from Chapter 1, and for example Hilbert's Basis Theorem ([**AM69**, Theorem 7.5])). Hence this integral closure is a Dedekind domain.

ii. The ring $\bigcap_{v \in \setminus S} \mathcal{O}_v$ is the integral closure of $k[1/x]_{(1/x)}$ in K. The rest of the proof is the same as in i. □

Consider the exact sequence of sheaves

$$0 \to \mathcal{F} \to K^* \to K^*/\mathcal{F} \to 0.$$

Let $\mathfrak{di}_k(K) = \mathcal{F}/K^*$. Notice that for $v \in \mathcal{P}_{K/k}$ one has $\mathfrak{di}_k(K)_v = K^*/\mathcal{O}_v^* = \Delta_v$.

Lemma 2.26. *Let $U \subseteq \mathcal{P}_{K/k}$ be open. Then one has*

$$\mathfrak{di}_k(K)(U) = \begin{cases} \bigoplus_{v \in U} \Delta_v & \text{if } U \neq \emptyset \\ 0 & \text{if } U = \emptyset. \end{cases}$$

Proof. Let $\mathcal{G}$ be the sheaf defined as in the statement. We have a natural sequence $0 \to \mathcal{F} \to K^* \to \mathcal{G} \to 0$. On the stalks it is obviously an exact sequence, and hence the sequence is exact. □

Note that $\mathfrak{di}_k(K)(\mathcal{P}_{K/k}) = \operatorname{div}_k(K)$.

3. Curves over finite fields

In this section we will focus on curves over finite fields.

3.1. Surjectivity of the degree.

Proposition 3.1. *Let K be a geometrically irreducible function field over a finite field k. Then the degree map* $\deg_k \colon \operatorname{div}_k(K) \to \mathbf{Z}$ *is surjective.*

Proof. See [**Sti09**, Corollary 5.1.11]. □

3.2. Class field theory. Class field theory gives a connection between the abelian extensions of a global field and some intrinsic object corresponding to the field. The reason we include class field theory is that we will use it later to estimate character sums.

3.2.1. *Main statements.* We will provide a short idèlic treatment of *global class field theory* for function fields over a finite field. We will give an idèlic description of the theory. For our results, we use statements from [**CAS67**], [**AT09**], [**Ser79**] and [**Ros02**].

Let K be a function field over a finite field k. Let $v \in \mathcal{P}_{K/k}$ and let K_v be the *completion* of K at v with valuation which we conveniently call v as well. Let $U_v = U_v^{(0)}$ be the group of elements in K_v^* of valuation 0. For $i \in \mathbf{Z}_{\geq 1}$ we set $U_v^{(i)} = \{x \in K_v : v(x-1) \geq i\}$.

We define $\mathbb{I}_K$, the *idèle group* of K, as the subgroup of $\prod_{v \in \mathcal{P}_{K/k}} K_v^*$ of elements of which almost all coordinates lie in the corresponding U_v. We put a topology on $\mathbb{I}_K$ as follows: a base for the topology consists of the sets of the form $\prod_{v \in S} V_v \times \prod_{v \notin S} U_v$ where $S \subset \mathcal{P}_{K/k}$ is finite and V_v is open in K_v^* (with the topology coming from the valuation). We have a natural map $K^* \to \mathbb{I}_K$, $x \mapsto (x)_{v \in \mathcal{P}_{K/k}}$ and we have a map $K_w^* \to \mathbb{I}_K$, which maps x to the element which has x at coordinate w and 1 otherwise. We set the *idèle class group* as $C_K = \mathbb{I}_K / K^*$ with its induced topology.

If L/K is a finite extension, then we have a natural norm map $\operatorname{Norm}_{L/K} \colon C_L \to C_K$. This map comes from the natural norm map $\prod_{w|v} L_w \cong L \otimes K_v \to K_v$ for $v \in \mathcal{P}_{K/k}$. The main theorem of class field theory can be stated as follows.

Theorem 3.2 (Main theorem of class field theory)**.** *For any function field K over a finite field k there is a unique inclusion reversing bijection between the set of its finite abelian extensions contained in some fixed algebraic closure and the set of open subgroups of C_K of finite index such that for an extension L/K corresponding to $D \subseteq C_K$ we have:*

i. $D = \operatorname{Norm}_{L/K} C_L$*;*
ii. *there is a canonical isomorphism*

$$\psi_{L/K} \colon C_K / D \xrightarrow{\sim} \operatorname{Gal}(L/K)$$

such that for any $v \in \mathcal{P}_{K/k}$ with extension x to L we have
(a) $\psi_{L/K}(K_v^* \pmod D) = \mathrm{D}_{x,K}$*;*
(b) $\psi_{L/K}(U_v \pmod D) = \mathrm{I}_{x,K}$*;*
(c) $\psi_{L/K}(\{y \in K_v^* : v(y) = 1\}) = (x, L/K)$.

Furthermore, let L_1/K be a finite abelian extension, let E/K be a finite extension and let L_2/E be a finite abelian extension containing L_1. Then we have the following commutative diagram:

$$\begin{array}{ccc} C_E/\operatorname{Norm}_{L_2E/E}(C_{L_2E}) & \xrightarrow{\sim} & \operatorname{Gal}(L_2E/E) \\ \downarrow{\scriptstyle \operatorname{Norm}_{E/K}} & & \downarrow{\scriptstyle res} \\ C_K/\operatorname{Norm}_{L_1/K}(C_{L_1}) & \xrightarrow{\sim} & \operatorname{Gal}(L_1/K). \end{array}$$

The above statement consists of two parts. Statement i and the first part of ii provide a global reciprocity map. Statements iia, ib, iic are more of a local nature. They provide local class field theory.

Statements i and ii and the last statements follow from [**CAS67**, Chapter VII, Theorem 5.1], although for the function fields one also needs proofs from [**AT09**]. In [**CAS67**, Chapter VII, Section 6] by construction one sees that the restriction of K_v^* to $\psi_{L/K}$ gives local class field theory. Statements iia and iib follow from [**Ser79**, Chapter XV, Corollary 3 on page 228]. Statement iic for unramified extensions follows from [**Ser79**, Chapter XIII, Proposition 13]. The general case follows from this case by splitting up an extension in an unramified and totally ramified part and a functorial property ([**Ser79**, Chapter XIII, Proposition 12]).

Remark 3.3. Explicit class field theory for function fields over finite fields is provided by the theory of Drinfeld modules. See [**Ros02**, Chapter 13] for an introduction.

3.2.2. *Conductors.* In the previous subsubsection we have stated that abelian extensions of K correspond to open subgroups of C_K of finite index. For all $\mathfrak{f} \in \operatorname{div}_k(K)$ with $\mathfrak{f} \geq 0$ we define the open subgroup $D_\mathfrak{f} = \left(K^* \prod_v U_v^{(\mathfrak{f}_v)}\right)/K^* \subseteq C_K$. Let $D \subseteq C_K$ be an open subgroup. Then it contains a subgroup of the form $D_\mathfrak{f}$. One easily sees that there is a unique smallest $\mathfrak{f}$ with this property.

Definition 3.4. Let L/K be a finite abelian extension corresponding to $D \subseteq C_K$. Then we define the *conductor* $\mathfrak{f}(L/K) \in \operatorname{div}_k(K)$ to be the smallest divisor such that $D_\mathfrak{f} \subseteq D$.

Suppose L/K is a finite abelian extension such that L is the compositum of $L_1, \ldots, L_r$. Then one has $\mathfrak{f}(L/K) = \operatorname{lcm}(\{\mathfrak{f}(L_i/K) : i = 1, \ldots, r\})$. Indeed, for $x \in C_K$ we have $x \in \ker(\psi_{L/K})$ iff for $i = 1, \ldots, r$ we have $x \in \ker(\psi_{L_i/K})$. Notice that L is the compositum of its subextensions which are cyclic over K of prime power order.

Furthermore, this conductor is something local.

Proposition 3.5. *If w is an extension of v to L, then one has*

i. $K_v^* \cap \left(\operatorname{Norm}_{L/K} C_L\right) = \operatorname{Norm}_{L_w/K_v}(L_w^*)$;

ii. $\mathfrak{f}(L/K)_v = \min\left\{n \in \mathbf{Z}_{\geq 0} : U_v^{(n)} \subseteq \operatorname{Norm}_{L_w/K_v}(U_w)\right\}$.

Proof. i: Follows from the construction of global class field theory out of local class field theory as in [**CAS67**].

ii: This follows from i. □

Corollary 3.6. *Suppose L/K be a finite abelian extension and let $v \in \mathcal{P}_{K/k}$. Then the following hold:*

i. *v is unramified in L iff $\mathfrak{f}(L/K)_v = 0$;*
ii. *v is tamely ramified in L iff $\mathfrak{f}(L/K)_v \leq 1$.*

Proof. i. One has: v is unramified iff $\mathrm{I}_{x,K} = 0$ iff $\psi_{L/K}(U_v \pmod D) = 0$ (Theorem 3.2) iff $\mathfrak{f}(L/K)_v = 0$ (Proposition 3.5).

ii. Put $V = \mathrm{Norm}_{L_w/K_v}(U_w)$. We have an exact sequence

$$0 \to U_v^{(1)}/(V \cap U_v^{(1)}) \to U_v/V \to U_v/U_v^{(1)} \to 0.$$

Note that $\mathrm{p}_v \nmid \#U_v/U_v^{(1)}$ and that $U_v^{(1)}/(V \cap U_v^{(1)})$ is a p_v-group ([**Ser79**, Chapter IV, Proposition 6]). Hence we have: $\mathrm{p}_v \nmid \#\mathrm{I}_{x,K} = \#U_v/V$ (Theorem 3.2) iff $\mathrm{p}_v \nmid \#U_v^{(1)}/(V \cap U_v^{(1)})$ iff $V \cap U_v^{(1)} = U_v^{(1)}$ iff $U_v^{(1)} \subseteq V$. The result follows from Proposition 3.5. □

Let $\mathfrak{f} \in \mathrm{div}_k(K)$. Then one defines the *ray class field* $K_{(\mathfrak{f})}$ to be the compositum of all finite abelian extensions L of K with $\mathfrak{f}(L/K) \leq \mathfrak{f}$. Later in this thesis, we will construct some ray class fields.

There is another concept of conductors. We follow [**Ser79**, Chapter VI] and we assume some familiarity with character theory. Let L/K be a Galois extension of function fields over k with group G. Let $v \in \mathcal{P}_{K/k}$. One can associate to this extension a $\mathbf{C}$-character a_v on G called the *Artin representation*. This character is defined by looking at higher ramification groups. This character, after quite some work, turns out to be the character of a representation of G. Recall that there is a standard inner product between characters on G, for which the characters from irreducible representations form an orthonormal basis. Let χ be a character on G. We define the conductor of χ to be $\mathfrak{f}(\chi) = \sum_{v \in \mathcal{P}_{K/k}} (\chi, a_v)v \in \mathrm{div}_k(K)$. If v is unramified in L/K, then one has $a_v = 0$, and hence this sum is finite.

Theorem 3.7 (Führerdiskriminantenproduktformel)**.** *Let L/K be an extension of function fields over k with group G. Then one has*

$$\mathrm{disc}(L/K) = \sum_{\chi} \chi(1)\mathfrak{f}(\chi)$$

where the sum is over the irreducible characters of G.

Note that $\chi(1)$ is nothing more than the degree of the character χ. If G is abelian, all these degrees are 1 and one finds $\mathrm{disc}(L/K) = \sum_{\chi \in \mathrm{Hom}(G, \mathbf{C}^*)} \mathfrak{f}(\chi)$.

One has the following comparison theorem.

Proposition 3.8. *Let L/K be a finite Galois extension of function fields over k. Let $\chi \in \mathrm{Hom}(G, \mathbf{C}^*)$. Then one has*

$$\mathfrak{f}(L^{\ker(\chi)}/K) = \mathfrak{f}(\chi).$$

Proof. This follows from [**Ser79**, Page 103 and page 228] . □

3.2.3. *Maximal unramified abelian extension and surjectivity of the norm.*

Proposition 3.9. *Let L/K and L'/K be finite Galois extensions of functions fields over a finite field k. Suppose that the set of primes of K which totally split in L differs from the corresponding set of L' by only a finite number of primes. Then $L = L'$.*

PROOF. See [**Ros02**, Proposition 9.13]. □

Proposition 3.10. *Let K be a function field over a finite field k and let $D \in \mathrm{div}_k(K)$ be of degree 1. Then the maximal abelian unramified extension of K is the compositum of the following two linearly disjoint extensions: $\overline{k} \cdot K$ and a unique finite subextension $K_{[D]}$ with Galois group isomorphic to $\mathrm{Pic}^0_k(K)$ such that $(D, K_{[D]}/K) = 0$. For $D' \in \mathrm{div}_k(K)$ we have $(D', K_{[D]}/K) = [D'] - \deg_k(D')[D] \in \mathrm{Pic}^0_k(K)$.*

PROOF. We use global class field theory as in Theorem 3.2. Suppose L/K is finite abelian unramified. Then we have $\mathrm{Norm}_{L/K} C_L \supseteq (K^* \prod_v U_v^*)/K^* = U$. Note that $C_K/U \cong (\bigoplus_v K_v^*/U_v^*)/K^* = \mathrm{Pic}_k(K)$. The finite extensions we are looking for correspond to subgroups of finite index in $\mathrm{Pic}_k(K)$. We have an exact sequence $0 \to \mathrm{Pic}^0_k(K) \to \mathrm{Pic}_k(K) \to \mathbf{Z} \to 0$. This sequence splits by sending $1 \in \mathbf{Z}$ to D, and this gives an isomorphism $\mathrm{Pic}_k(K) \cong \mathrm{Pic}^0_k(K) \times \mathbf{Z}$, which maps $[D']$ to $([D'] - \deg_k(D)[D'], \deg(D'))$. A subgroup of finite index n of $\mathrm{Pic}^0_k(K) \times \mathbf{Z}$ contains $n\,\mathrm{Pic}^0_k(K) \times n\mathbf{Z}$. It follows that the maximal abelian unramified extension is the compositum of the extension corresponding to $\{0\} \times \mathbf{Z}$ and the various extensions corresponding to $\mathrm{Pic}^0_k(K) \times n\mathbf{Z}$. The first extension, $K_{[D]}$, has group $\mathrm{Pic}^0_k(K)$ and the Frobenius of a divisor $[D']$ is $[D'] - \deg_k(D')[D] \in \mathrm{Pic}^0_k(K)$. The extension K_n corresponding to $\mathrm{Pic}^0_k(K) \times n\mathbf{Z}$ has group $\mathbf{Z}/n\mathbf{Z}$ and has the property that the Frobenius of D is equal to $\deg_k(D) \pmod n \in \mathbf{Z}/n\mathbf{Z}$. If we let k_n be the unique extension of degree n of k, then the Frobenius elements are exactly the same (Proposition 2.15) and from Proposition 3.9 it follows that $K_n = k_n K$.

Notice that the compositum of two extensions where the Frobenius of D is trivial, has trivial Frobenius at D (Lemma 9.4 from Chapter 1). One easily sees from the descriptions above that $K_{[D]}$ is unique. The statement about the linear disjointness also follows directly. □

Remark 3.11. Let K be a function field over a finite field k. Suppose that $D, D' \in \mathrm{div}_k(K)$ are of degree 1. Then we have $K_{[D]} = K_{[D']}$ iff $[D - D'] = 0 \in \mathrm{Pic}^0_k(K)$. Indeed, one has $(D', K_{[D]}/K) = [D' - D] \in \mathrm{Pic}^0_k(K)$.

Remark 3.12. Divisors of degree 1 as in Proposition 3.10 always exist due to Proposition 3.1 if one considers K to be a curve over the full constant field of K.

Remark 3.13. Note that for an elliptic curve over a finite field k we have $E(k) \cong \mathrm{Pic}^0_k(k(E))$, $P \mapsto [P] - [\infty]$ (see [**Sil09**, Proposition 3.4]) and hence we have realized $E(k)$ as a Galois group with specific Frobenius elements.

Remark 3.14. One can explicitly find the extension in Proposition 3.10 in the case that $K = k(E)$ where E is an elliptic curve over a finite field k. It corresponds to the map on function fields coming from $\mathrm{Frob} - 1 \colon E \to E$. We will not need this more explicit description in the rest of this thesis.

Even though the norm map for constant field extensions as a map on div^0 is not surjective, it is surjective on the level of Pic^0.

Corollary 3.15. *Let k be a finite field and let k' be a finite extension of k. Let K be a function field over k. Then the map $\mathrm{Norm}_{Kk'/K}\colon \mathrm{Pic}^0_{k'}(Kk') \to \mathrm{Pic}^0_k(K)$ (Lemma 2.16) is surjective.*

Proof. Remark that $\mathrm{Pic}^0_k(K) = \mathrm{Pic}^0_{k_0}(K)$ where k_0 is the full constant field of K. Also, the norm does not depend on k in that sense. Hence we may assume that K is geometrically irreducible. Put $n = [k' : k]$. Let $D \in \mathrm{div}_k(K)$ be of degree 1 (Proposition 3.1). Let $D' = \mathrm{Conorm}_{Kk'/K}(D)$. Note that $\deg_{k'}(D') = 1$ (Lemma 2.16). Consider the fields $K_{[D]}$ and $(Kk')_{[D']}$ from Proposition 3.10. The calculation

$$(D', K_D k'/Kk')|_{K_{[D]}} = [\mathrm{Norm}_{Kk'/K}(D') - n\deg_{k'}(D')D] = [nD - nD] = 0.$$

shows that $K_{[D]}k' \subseteq (Kk')_{[D']}$. Theorem 3.2 give us the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Pic}^0_{k'}(Kk') \cong C_{Kk'}/\mathrm{Norm}_{(Kk')_{[D']}/Kk'}(C_{(Kk')_{[D']}}) & \xrightarrow{\sim} & \mathrm{Gal}((Kk')_{[D']}/Kk') \\ \downarrow{\scriptstyle \mathrm{Norm}_{Kk'/K}} & & \downarrow \\ \mathrm{Pic}^0_k(K) \cong C_K/\mathrm{Norm}_{K_{[D]}/K}(C_{K_{[D]}}) & \xrightarrow{\sim} & \mathrm{Gal}(K_{[D]}/K) \end{array}$$

From the definitions it easily follows that the induced surjective map $\mathrm{Pic}^0_{k'}(Kk') \to \mathrm{Pic}^0_k(K)$ agrees with the norm map. □

3.3. L-functions. Let L/K be a Galois extension of function fields over a finite field k. Let ρ be the character of a representation $G \to \mathrm{Aut}_{\mathbf{C}}(V)$ where V is a finite-dimensional vector space over $\mathbf{C}$ (we often do not distinguish between the character and the corresponding representation). For a divisor $D \in \mathrm{div}_k(K)$ we define its *absolute norm* as $\mathrm{N}(D) = (\#k)^{\deg_k(D)}$.

Let $v \in \mathcal{P}_{K/k}$ and assume $x \in \mathcal{P}_{L/k}$ satisfies $x|_K = v$. Then we have an induced representation $\rho_x\colon \mathrm{D}_{x,K}/\mathrm{I}_{x,K} \to \mathrm{Aut}_{\mathbf{C}}(V^{\mathrm{I}_{x,K}})$. One sets

$$L_v(s,\rho) = \det\left(1_{V^{\mathrm{I}_{x,K}}} - \rho_x((x, L/K))\,\mathrm{N}(v)^{-s}\right)^{-1},$$

which is a meromorphic function on $\mathbf{C}$. One easily shows that this definition does not depend on the choice of x (Theorem 3.6 from Chapter 1). We then define the *L-series* of ρ as follows:

$$L(s,\rho) = \prod_{v \in \mathcal{P}_{K/k}} L_v(s,\rho).$$

We define $\zeta_K(s) = L(s,1)$, where 1 is the trivial representation (this does not depend on L). More explicitly,

$$\zeta_K(s) = \prod_{v \in \mathcal{P}_{K/k}} \left(1 - \mathrm{N}(v)^{-s}\right)^{-1}.$$

From the definition one easily finds $L(s, \rho \times \rho') = L(s,\rho) \cdot L(s,\rho')$. Hence from now on we focus on irreducible characters.

One can easily show that the L-function defines a holomorphic function on some right half plane of $\mathbf{C}$ ([**Ros02**, Proposition 9.15]). It is much harder to show the following result.

Theorem 3.16. *Let L/K be a Galois extension of function fields over a finite field k of cardinality q such that k is the full constant field of L. Let $\rho\colon \mathrm{Gal}(L/K) \to \mathrm{Aut}_{\mathbf{C}}(V)$ be an irreducible representation. Then the following hold, where $u = q^{-s}$:*

i. *Assume that ρ is trivial. Then one has*

$$\zeta_K(s) = L(s,\rho) = \frac{L_K(u)}{(1-u)(1-qu)},$$

where $L_K(u) = \prod_{i=1}^{2g_k(K)}(1-\pi_i u) \in \mathbf{Z}[u]$ ($\pi_i \in \mathbf{C}$) satisfies
(a) *$|\pi_i| = \sqrt{q}$ ($i = 1, \ldots, 2g_k(K)$);*
(b) *$L_K(0) = 1$, $L_K(1) = h_K$, $L_K'(0) = \#\{v \in \mathcal{P}_{K/k} : N(v) = q\} - 1 - q$;*
(c) *for $\xi_K(s) = q^{(g-1)s}\zeta_K(s)$ one has $\xi_K(1-s) = \xi_K(s)$.*

ii. *Assume that ρ is not trivial. Then one has*

$$L(s,\rho) = \prod_{i=1}^{m}(1-\pi_i u)$$

($\pi_i \in \mathbf{C}$) which satisfies:
(a) *$|\pi_i| = \sqrt{q}$ ($i = 1, \ldots, m$);*
(b) *$m = \dim_{\mathbf{C}}(V)\cdot(2g_k(K)-2) + \deg_k(\mathfrak{f}(\rho))$.*

Proof. The first part follows directly from [**Ros02**, Theorem 5.9] and [**Sti09**, Theorem 5.1.15].

The second part follows from [**Ros02**, Theorem 9.16B] and its fifth remark. □

Corollary 3.17 (Hasse-Weil)**.** *Let C be a normal projective geometrically irreducible curve over a finite field k of cardinality q. Then one has $|\#C(k) - q - 1| \leq 2g \cdot \sqrt{q}$.*

Proof. Follows from Theorem 3.16 and Proposition 2.11. □

3.4. Character estimates and the calculation of the conductor. Let L/K be an extension of function fields over a field k and let $d \in \mathbf{Z}_{\geq 1}$. We put $\mathrm{unr}(L/K) \subseteq \mathcal{P}_{K/k}$ for the set of primes of K which are unramified in L. We put $\mathrm{unr}^d(L/K) \subseteq \mathcal{P}_{K/k}$ for the set of unramified primes of degree dividing d.

Theorem 3.18. *Let L/K be a Galois extension of function fields over a finite field k with group G such that the full constant field of L is k. Assume that we have $\chi \in \mathrm{Hom}(G, \mathbf{C}^*)$ injective. Let $d \in \mathbf{Z}_{\geq 1}$. Then we have*

$$\Big|\sum_{P \in \mathrm{unr}^d(L/K)} \deg_k(P)\chi((P,L/K))^{d/\deg_k(P)}\Big| \leq mq^{d/2},$$

where $m = 2g(K) - 2 + \deg_k(\mathfrak{f}(\chi))$. It is an equality if $m = 1$.

Proof. Let $q = \#k$, $u = q^{-s}$ and $m = 2g(K) - 2 + \deg_k(\mathfrak{f}(\chi))$. Since our character is one-dimensional and χ is injective, $L(s,\chi)$ depends only on the factors for

the unramified primes in L/K. By Theorem 3.16 we have

$$\prod_{P\in \mathrm{unr}(L/K)} \left(1-\chi((P,L/K))u^{\deg_k(P)}\right)^{-1} = L(s,\chi) = \prod_{i=1}^{m}(1-\pi_i(\chi)u),$$

where $|\pi_i(\chi)| = q^{1/2}$.

The statement then follows from the following manipulation of series. We apply $-u\frac{d\log}{du}$ to both expressions for $L(s,\chi)$ and we obtain:

$$\sum_{i=1}^{m}\sum_{j=1}^{\infty}(\pi_i(\chi)u)^j = \sum_{P\in \mathrm{unr}(L/K)} \deg_k(P)\sum_{j=1}^{\infty}\chi((P,L/K))^j u^{j\deg(P)}$$

Looking at the coefficient at u^d gives us

$$\sum_{i=1}^{m}\pi_i(\chi)^d = \sum_{P\in \mathrm{unr}^d(L/K)} \deg_k(P)\chi((P,L/K))^{d/\deg_k(P)}.$$

Using that $|\pi_i(\chi)| = q^{1/2}$, the result follows by taking absolute values. □

The above theorem is mostly interesting for $d = 1$.

We will now show how to calculate the conductor in specific cases.

Lemma 3.19. *Let K/k be a function field where k is a finite field. Let K_s be a separable closure of K. Let L, M be finite abelian Galois extensions of K inside K_s of prime degree p respectively prime degree l with $L\cap M = K$. Let $v\in\mathcal{P}_{K/k}$ and suppose that $r = \mathfrak{f}(L/K)_v \in \mathbf{Z}_{\geq 1}$ and $s = \mathfrak{f}(M/K)_v \in \mathbf{Z}_{\geq 1}$. Let w be the unique extension of v to L. Assume that LM/L is ramified at w if both $p = l$ and $r = s$. Then the following hold:*

i. *LM/K is totally ramified at v;*
ii. *if $p\neq l$ or $r\neq s$, we have $\mathfrak{f}(LM/L)_w = (p-1)\max(0,s-r)+s$;*
iii. *if $p = l$ and $r = s$, we have $r\geq \mathfrak{f}(LM/L)_w \geq t$ where $t = 2$ if p is the residue field characteristic of v and 1 otherwise.*

Proof. If $p\neq l$, the ramification indices are coprime, and hence LM/K is totally ramified. If $p = l$, $r\neq s$ then both extensions have different conductors. An easy calculation shows that LM/K is totally ramified at v (here we use that l and p are prime). Hence in all cases LM/K is totally ramified at v.

We use a well-known identity for towers of fields ([**Ser79**, Proposition 8 of Chapter III]):

$$\mathrm{disc}(LM/K) = \mathrm{Norm}_{L/K}(\mathrm{disc}(LM/L)) + l\cdot\mathrm{disc}(L/K).$$

Using the Führerdiskriminantenproduktformel (Theorem 3.7) we will calculate the discriminants $\mathrm{disc}(L/K)$ and $\mathrm{disc}(LM/K)$ at the prime v. This gives us $\mathrm{disc}(L/K)_v = (p-1)r$.

Assume first that $l\neq p$. Then then LM/K has one cyclic subextension of degree 1 with conductor 0 (at infinity), 1 of degree p with conductor r, 1 of degree l with conductor s and one of degree $p\cdot l$ of conductor $\max(r,s)$. Assume next that $r\neq s$ but $p = l$. Then LM/K has one cyclic subextension of degree 1 with conductor 0, 1 of

degree p with conductor s, one of degree p with conductor r, and $p-1$ of degree p with conductor $\max(r,s)$. We find if $l \neq p$ or $r \neq s$

$$\operatorname{disc}(LM/K)_v = (p-1)r + (l-1)s + (p-1)(l-1)\max(r,s).$$

If $l = p$ and $r = s$, then we cannot determine the conductor at v exactly. We have $p+1$ nontrivial cyclic extensions of degree p with conductor at most r. For a lower bound, notice that only one extension can have conductor strictly smaller than r, but that the conductor is still at least t where $t = 2$ if p is the residue field characteristic of v (wild ramification) and $t = 1$ otherwise (Corollary 3.6). We have

$$(p-1)(rp+r) \geq \operatorname{disc}(LM/K)_v \geq (p-1)(rp+t).$$

We then find, if $l \neq p$ or $r \neq s$:

$$\begin{aligned}\frac{\big(\operatorname{Norm}_{L/K}(\operatorname{disc}(LM/L))\big)_v}{l-1} &= \frac{\operatorname{disc}(LM/K)_v - l\operatorname{disc}(L/K)_v}{l-1} \\ &= (p-1)\max(0, s-r) + s.\end{aligned}$$

For $l = p$ and $r = s$ we find

$$r \geq \frac{\big(\operatorname{Norm}_{L/K}(\operatorname{disc}(LM/L)\big)_v}{l-1} \geq t.$$

Again using the Führerdiskriminantenproduktformel (Theorem 3.7) we deduce the result. □

One particular case of the above statement is when $p = l$, $2 = r = s$ and p is the characteristic of the residue field at v. We then obtain $\mathfrak{f}(LM/L)_w = 2$.

Lemma 3.20. *Let K/k be a function field where k is a finite field. Let L/K be a finite abelian Galois extension with group G. Let $\chi, \chi' \in G^\vee$. Then we have $\mathfrak{f}(\chi \cdot \chi') \leq \operatorname{lcm}(\mathfrak{f}(\chi), \mathfrak{f}(\chi'))$, with equality at $P \in \mathcal{P}_{K/k}$ if we have $\mathfrak{f}(\chi)_P \neq \mathfrak{f}(\chi')_P$ or if the orders of χ and χ' are coprime.*

Proof. Let $P \in \mathcal{P}_{K/k}$ and assume that $\mathfrak{f}(\chi')_P \leq \mathfrak{f}(\chi)_P$. For calculating the conductor, we may assume $L = L^{\ker(\chi)}L^{\ker(\chi')}$, that is $\ker(\chi) \cap \ker(\chi') = 0$ (Proposition 3.8). Hence we have

$$L^{\ker(\chi\cdot\chi')}L^{\ker(\chi')} = L^{\ker(\chi\cdot\chi')\cap\ker(\chi')} = L. \tag{1}$$

The first result follows.

If the orders of χ and χ' are coprime, then by looking at dimensions one obtains $L^{\ker(\chi\cdot\chi')} = L^{\ker(\chi)}L^{\ker(\chi')}$ and both extensions are actually linearly disjoint.

Assume that $\mathfrak{f}(\chi')_P < \mathfrak{f}(\chi)_P$. From Equation 1 we obtain $\mathfrak{f}(L^{\ker(\chi\cdot\chi')}/K)_P = \mathfrak{f}(L^{\ker(\chi)}/K)_P$ and the result follows from Proposition 3.8. □

4. Hyperelliptic curves

4.1. Definition and models. Let k be a perfect field.

Definition 4.1. A function field K/k is called *hyperelliptic* if it has full constant field k, the genus satisfies $g(K) \geq 1$, and there exists $x \in K$ with $[K : k(x)] = 2$.

Remark 4.2. In [**Liu02**, Definition 7.4.7] a hyperelliptic curve is defined as follows. Let C be a smooth projective geometrically connected curve over k, of genus $g \geq 1$. Then C is called hyperelliptic if there exists a finite morphism $X \to \mathbf{P}^1_k$ of degree 2.

Both definitions coincide. Indeed, normal is equivalent to smooth ([**Liu02**, Corollary 4.3.33 and Lemma 8.2.21]). We may assume that k is algebraically closed and we need to show that regular irreducible is equivalent to regular connected. Irreducible implies connected. Conversely, suppose that X has more than one irreducible component. There must exist components which meet, since otherwise our space is not connected. But the local ring of a point in the intersection of more than one irreducible component is not a domain ([**Liu02**, Proposition 2.4.7 and Proposition 2.4.12]). This contradicts the regularity.

Remark 4.3. More generally, a function field K/k is called hyperelliptic if it has full constant field k, if the genus satisfies $g(k) \geq 1$ and if there is a subfield K' of K with $[K : K'] = 2$ such that $g(K') = 0$. If k is finite, then from Hasse-Weil (Corollary 3.17) it follows that K' has a rational point and hence is isomorphic to $k(x)$. In the rest of this thesis we will not use this more general definition.

We want to have explicit models for hyperelliptic curves. By lack of a good reference, especially for the case of characteristic 2, we will prove such a theorem. For a polynomial $f = \sum_i c_i x^i \in k[x]$ we put $f_i = c_i$.

We use the following lemma for Artin-Schreier extensions.

Proposition 4.4. *Let k be a perfect field of characteristic p and let K be a function field over k. Let $(f, h) \in k(x)^2$ with $h \neq 0$ such that f/h^p is not in the image of $K \to K$, $s \mapsto s^p - s$. Then the extension $K_{f,h} = K[y]/(y^p - h^{p-1}y - f)$ is a field extension of degree p of K. Furthermore, the following hold for $P \in \mathcal{P}_{K/k}$ with uniformizer π at P. Put $r = \operatorname{disc}(K_{f,h}/K)_P$. Set $v_P(f/h^p) = -m$.*

i. *if $m \leq 0$: $r = 0$;*
ii. *if $m > 0$, $m \not\equiv 0 \pmod p$: $r = (p-1)(m+1)$;*
iii. *if $m > 0$, $m \equiv 0 \pmod p$, $v_p(f) \neq 0$: $r = \operatorname{disc}(K_{\pi^{-v_P(f)} f, \pi^{-v_P(f)/p} h})_P$;*
iv. *if $m > 0$, $m \equiv 0 \pmod p$, $v_p(f) = 0$: let $s \in \mathcal{O}_P$ with $s^p \equiv -f \in \mathrm{k}_P$ (k is perfect). Then one has: $r = \operatorname{disc}(K_{f+s^p-h^{p-1}s,h})_P$.*

Proof. We will prove the correctness of the four statements.

i, ii: Put $y' = y/h$. Then $y'^p - y' = f/h^p$. Apply [**Sti09**, Proposition 3.7.8].

iii: Set $y' = \pi^{-v_P(f)/p} y$. Then one has:

$$y'^p - (\pi^{-v_P(f)/p} h)^{p-1} y' - \pi^{-v_P(f)} f = \pi^{-v_P(f)} \cdot (y^p - hy - f) = 0,$$

and hence this step is correct.

iv: Notice that if we set $y' = y + s$ we obtain

$$y'^p - h^{p-1}y' = y^p - h^{p-1}y + s^p - h^{p-1}s = f + s^p - h^{p-1}s,$$

and hence the transformation is allowed.

□

Remark 4.5. The above proposition gives an algorithm to find the discriminant of $K_{f,h}/K$. Indeed, by step i, one has only to look at primes such that $v_P(f/h^p) < 0$. For these primes, one applies the appropriate steps sequentially until one finds r. One can easily show that the procedure terminates. In step iv, one has $v_P(f + s^p + sh) > v_p(f)$ and hence the value of decreases after such a step. One applies at most one step iii after a step iv, and hence the procedure terminates.

Theorem 4.6. *Let k be a perfect field. Let $g \in \mathbf{Z}_{\geq 1}$. Consider the following properties for $(f, h) \in k[x]^2$:*

i. $\deg(f) \in \{2g+1, 2g+2\}$
ii. *$y^2 + hy - f$ is separable and irreducible in $k(x)[y]$;*
iii. *if* $\mathrm{char}(k) \neq 2$ *the following hold:*
   (a) *$h = 0$;*
   (b) *f is separable in $k[x]$;*
iv. *if* $\mathrm{char}(k) = 2$*, then the following hold:*
   (a) $\deg(h) \leq g + 1$*;*
   (b) $(h, h'^2 f + f'^2) = k[x]$*;*
   (c) $(h_{g+1}, h_g^2 f_{2g+2} + f_{2g+1}^2) = k$.

Set $K_{f,h} = k(x)[y]/(y^2 + hy - f)$ with natural inclusion $k(x) \subseteq K_{f,h}$. If i, iiia and iva hold, then set $U' = \mathrm{Spec}(k[x,y]/(y^2 + h(x)y - f(x))$, $V' = \mathrm{Spec}(k[x', y']/(y'^2 + h_\infty(x')y' - f_\infty(x'))$ where $h_\infty(x') = h(1/x')x'^{g+1}$ and $f_\infty(x') = f(1/x')x'^{2g+2}$. Let $X = U' \cup V'$ glued together by $D(x) \cong D(x')$ with relations $x = 1/x'$ and $y = x^{g+1}y'$.

Then for a pair $(f, h) \in k[x]^2$ satisfying i, ii, iiia and iva the extension $K_{f,h}/k(x)$ is a hyperelliptic function field of genus g iff iii and iv hold. If i, ii, iii and iv are satisfied, one has

$$\mathrm{disc}(K_{f,h}/k(x)) = \begin{cases} \infty + (f) & \text{if } \mathrm{char}(k) \neq 2,\ \deg(f) = 2g+1 \\ (f) & \text{if } \mathrm{char}(k) \neq 2,\ \deg(f) = 2g+2 \\ (2g+2)\infty + 2(h) & \text{if } \mathrm{char}(k) = 2, \end{cases}$$

and a smooth model for the normal projective geometrically irreducible curve $C_{h,f}$ corresponding to $K_{h,f}$ is given by X.

Furthermore, any hyperelliptic function field of genus g is isomorphic to $K_{f,h}$ for certain $(f, h) \in k[x]^2$ satisfying i, ii, iii and iv.

Proof. Suppose that F is hyperelliptic of genus g. Then there exists an inclusion $k(x) \subseteq F$ of degree 2. Notice that this extension is separable (Proposition 2.14) and not a constant field extension. Let $D = \mathrm{Conorm}(\infty)$, of degree 2. Consider the Riemann-Roch space $\mathfrak{L}_k((g+1)D)$ of dimension $g+3$ (Theorem 2.13). It contains a linearly independent set $\{1, x, \ldots, x^{g+1}\}$ and another independent element $y \in F$, not in $k(x)$. The space $\mathfrak{L}_k(2(g+1)D)$ has dimension $3g+5$ and it contains $3g+6$ functions $1, x, \ldots, x^{g+1}, y, x^{g+2}, xy, \ldots, x^{2(g+1)}, x^{g+1}y, y^2$. As $y \notin k(x)$, it follows that $y^2 + hy - f = 0$ for some $h, f \in k[x]$ with $\deg(h) \leq g+1$ and $\deg(f) \leq 2g+2$ and that $F = k(x, y)$. If $y^2 + hy - f$ is inseparable, then F has genus 0 (Proposition 2.14), contradiction. If $\mathrm{char}(k) \neq 2$ we may complete the square and assume $h = 0$.

Assume $(h, f) \in k[x]^2$ satisfies $\deg(f) \geq 2g + 2$, ii, iiia, iva. We will show that $K = K_{f,h}$ is a hyperelliptic curve of genus g if and only if iii and iv are satisfied. To achieve this, we will calculate the genus $g(K)$ of K.

Assume first that $\mathrm{char}(k) \neq 2$. Changing y if necessary, we may assume that f is square-free. If f is constant, our extension is not geometric. Assume that f is not constant. We see that our extension is ramified exactly at the primes dividing f and possibly at ∞ (Proposition 7.8 from Chapter 1). After a transformation, one easily sees that $K/k(x)$ ramifies at ∞ iff $\deg(f)$ is odd. Using Riemann-Hurwitz (Theorem 2.22, in the squarefree case, we have $2g(K) - 2 = 2(-2) + \deg(f) + 1_{\deg(f) \text{ odd}}$). Hence we find $g(K) = -1 + \lceil \frac{\deg(f)}{2} \rceil$. Hence the genus is exactly g iff f is squarefree and of degree $2g + 1$ or $2g + 2$. Furthermore, we have

$$\mathrm{disc}(K/k(x)) = \begin{cases} \infty + (f) & \text{if } \mathrm{char}(k) \neq 2,\ \deg(f) = 2g + 1 \\ (f) & \text{if } \mathrm{char}(k) \neq 2,\ \deg(f) = 2g, \end{cases}$$

(Proposition 2.21).

Assume $\mathrm{char}(k) = 2$. We determine the genus by using Proposition 4.4 and Remark 4.5.

Let P be a prime of $k[x]$ and assume that $v_P(h) > 0$. Notice that $\mathrm{disc}(K/k(x))_P \leq 2v_P(h)$ with equality if and only if $v_P(f) \leq 1$ and if $v_P(f + s^2 - hs) = 1$ in step iv. In general we claim that $\mathrm{disc}(K/k(x))_P = 2v_P(h)$ iff $v_P((h, h'^2 f + f'^2)) = 0$. If $v_P(h) = 0$, this is obvious. Assume $v_P(h) > 0$. Then we have: $v_P((h, h'^2 f + f'^2)) > 0$ iff $v_P(h'^2 f + f'^2) > 0$ iff $v_P(f'^2 + h'^2 s^2) > 0$ iff $v_P(f' + h's) > 0$ iff $v_P(f' + h's + s'h) > 0$ iff $v_P(f + s^2 + hs) > 1$ (because the latter is ≥ 1). Furthermore, $v_P(f) \geq 2$ implies $v_P((h, h'^2 f + f'^2)) > 0$.

Let $P = \infty$. If $\deg(f) = 2g + 1$, then the discriminant is $\mathrm{disc}(K/k(x))_\infty = 2g + 2 - 2\deg(h)$. If $\deg(f) = 2g + 2$, then in step iii one replaces (f, h) by the pair $((1/x)^{2g+2} f, (1/x)^{g+1} h)$ and then one has $\mathrm{disc}(K/k(x))_\infty \leq 2(g + 1 - \deg(h) + 1) = 2g + 2 - 2\deg(h)$. We have equality precisely in the following cases:

i. $\deg(h) = g + 1$
ii. $\deg(h) < g + 1$ and $h_g^2 f_{2g+2} + f_{2g+1}^2 \neq 0$.

This is precisely assumption ivc.

We apply Riemann-Hurwitz (Theorem 2.22) and obtain:

$$\begin{aligned} 2g(K) - 2 &\leq -4 + (2g + 2 - 2\deg(h)) + \sum_{P|h} 2v_P(h)\deg_k(P) \\ &= (2g - 2 - 2\deg(h)) + 2\deg(h) = 2g - 2. \end{aligned}$$

Hence we have equality precisely if ivb and ivc hold.

The only remaining part is to show that X is in fact normal, which is equivalent to smooth since k is perfect ([**Liu02**, Corollary 4.3.33 and Lemma 8.2.21]).

Suppose first that $\mathrm{char}(k) \neq 2$. On U' the point (x_0, y_0) is smooth if not both $2y_0$ and $f'(x_0) = 0$ (Jacobi criterion as in [**Liu02**, Theorem 2.19], and [**Liu02**, Corollary 2.17]). This is equivalent to iiib. For smoothness on V', we only need to check $(0, y_0')$ and then $(2y_0', f_{2g+1})$ should not be zero. If $y_0' = 0$, then $f_{2g+2} = 0$ and hence f_{2g+1} is not zero by degree condition i.

Assume that $\mathrm{char}(k) = 2$. For this affine chart (over the algebraic closure), a point (x_0, y_0) is non-singular iff $h(x_0) \neq 0$ or $h'(x_0)^2 f(x_0) + f'(x_0)^2 \neq 0$, which is precisely ivb. For the other chart, we need to check that for $(0, y_0')$ we do not have $(h_{g+1}, h_g y_0' + f_{2g+1}) \neq 0$. But if $(0, y_0')$ is on the curve, one has $y_0'^2 + h_{g+1} y_0' + f_{2g+2})$. If $h_{g+1} \neq 0$ this gives us $y_0'^2 = f_{2g+2}$. Hence if we square the second equation, we see that in this case $h_g^2 f_{2g+2} + f_{2g+1}^2$ should not be zero, which is exactly ivc. □

Remark 4.7. The above theorem (Theorem 4.6) is very similar to [**CFA**$^+$**06**, Theorem 4.122]. Their statement contains an error: in characteristic 2 the point at infinity should not be singular. Let $d \in \mathbf{Z}_{\geq 1}$. Let k be a perfect field of characteristic 2 and consider the extension $L = k(x)[y]/(y^2 + y + x^d)$ of $k(x)$. Write $d = 2^i r$ with $\gcd(r, 2) = 1$ $(i, r \geq 0)$. Put $x' = x^{2^i}$ and consider the extension $K = k(x')[y]/(y^2 + y + x'^r)$ of $k(x')$ inside L. Theorem 4.6 tells us that $g(K) = \frac{r-1}{2}$ (do a separate calculation for $r = 1$). Note that L/K is purely inseparable and hence $g(L) = g(K) = \frac{r-1}{2}$ (see Proposition 2.14).

4.2. 2-torsion of the Picard group.

Lemma 4.8. *Let L/K be a finite Galois extension with group G of function fields over a field k. Let $D \in \mathrm{div}_k(L)$. Then one has*

$$\mathrm{Conorm}_{L/K} \circ \mathrm{Norm}_{L/K}(D) = \sum_{g \in G} gD.$$

Proof. One can check this statement for each prime of K. The result then follows from the transitivity in Theorem 3.6 from Chapter 1 and the fundamental equality (Theorem 3.9 from Chapter 1) □

Theorem 4.9. *Let k be a perfect field. Let K be a function field over k with $\mathrm{Pic}_k^0(K) = 0$. Let L be a Galois extension of degree 2 with $\mathrm{Gal}(L/K) = \langle \sigma \rangle$. Suppose that ∞ is a rational prime of K with the property that there is a unique prime ∞' above it in L with $\mathrm{e}(\infty'/\infty) = 2$. Let $S = \{w \in \mathcal{P}_{L/k} : \mathrm{e}(w/w|_K) = 2\} \setminus \{\infty'\}$. Then for any $w \in S$ one has $[w - \deg_k(w)\infty'] \in \mathrm{Pic}_k^0(L)[2]$. We have a surjective map*

$$\begin{aligned} \psi \colon \mathbf{F}_2^S &\to \mathrm{Pic}_k^0(L)[2] \\ e_w &\mapsto [w - \deg_k(w)\infty'] \end{aligned}$$

with

$$\ker(\psi) = \begin{cases} \mathbf{F}_2 \cdot \left(\sum_{w \in S} e_w\right) & \text{if } \mathrm{char}(k) \neq 2 \\ 0 & \text{if } \mathrm{char}(k) = 2. \end{cases}$$

Proof. We first claim that σ acts as -1 on $\mathrm{Pic}_k^0(L)$. Let $[D] \in \mathrm{Pic}_k^0(L)$. Then one has (Lemma 4.8):

$$D + \sigma(D) = \mathrm{Conorm}_{L/K} \circ \mathrm{Norm}_{L/K}(D).$$

As $\mathrm{Pic}_k^0(K) = 0$, there is $a \in k(x)$ with $(a) = \mathrm{Norm}_{L/K}(D)$. Hence $[D] + \sigma[D] = 0$ and the result follows. Hence a divisor $[D] \in \mathrm{Pic}_k^0(L)$ is killed by 2 iff $\sigma[D] = [D]$.

Let $w \in S$. We will prove that $[w - \deg_k(w)\infty'] \subseteq \mathrm{Pic}_k^0(L)[2]$. Indeed, $[w - \deg_k(w)\infty'] = \sigma[w - \deg_k(w)\infty'] = -[w - \deg_k(w)\infty']$.

We will now show that ψ is surjective with Hilbert 90.

Let $D \in \mathrm{div}_k^0(L)$ such that $D_{\infty'} = 0$. Assume $\sigma[D] = [D]$. We claim that there exists $D' \in \mathrm{div}_k^0(L)$ with $[D] = [D']$ and $\sigma D' = D'$. As $\sigma[D] = [D]$, there is $h \in L^*$ with $\sigma D - D = (h)$. This function is unique up to k^* (because we have ramification) and it has no zero or pole at ∞'. We make h unique by requiring $h(\infty') = 1$. If we apply σ to our relation, we obtain $(h^{-1}) = D - \sigma D = \sigma((h)) = (\sigma(h))$. It follows by uniqueness that $\sigma(h) = h^{-1}$. Hilbert 90 ([**Lan02**, Theorem 6.1, Chapter VI]) tells us that $h = \frac{h'}{\sigma(h')}$ for some $h' \in L^*$. Put $D' = D + (h')$. Then we have

$$\sigma(D') - D' = \sigma(D) + (\sigma(h')) - D - (h') = (h) + (h^{-1}) = 0,$$

and this proves the first claim.

Since ∞' is fixed under σ, any $D \in \mathrm{div}_k^0(L)$ with $\sigma[D] = [D]$ can be represented by $D' \in \mathrm{div}_k^0(L)$ with $[D'] = [D]$ and $\sigma D' = D'$. Let $P \in \mathcal{P}_{K/k}$. If P splits into P_1, P_2, then one easily sees that $[P_1 + P_2 - 2\deg_k(P)\infty'] = 0$. If P is inert, with prime P_1 above it, then $[P_1 - 2\deg_k(P)\infty'] = 0$. It then easily follows that ψ is surjective.

We will now show that ψ is injective. Suppose $f \in L^*$ satisfies $(f) = (\sigma(f))$. Then $\sigma(f)/f \in k^*$ and one obtains $\sigma(f) = \pm f$. If $\mathrm{char}(k) = 2$, one gets $f \in K^*$ and hence there is no kernel. If $\mathrm{char}(k) \neq 2$, then it follows $f^2 \in K^*$. There exists $f_0 \in K^*$ with $L \cong K[y]/(y^2 - f_0)$. Using Kummer-Theory, one sees that the only relation comes from $[(\sqrt{f_0})_L] = 0$. Since $\mathrm{Pic}_k^0(K) = 0$, we may assume that $(f_0)_K = v_1 + \ldots + v_m - r\infty$ where $v_1, \ldots, v_m, \infty$ are different primes. Hence one sees that L is ramified at $v_1, \ldots, v_m$ and at ∞. Furthermore, these are all the ramified primes by Proposition 7.8 from Chapter 1. Finally, Riemann-Hurwitz (Theorem 2.22) and Proposition 2.21 and the fact that the divisor of a function has degree 0 show that r is odd. Hence we get the required relation. □

Remark 4.10. The above theorem, in case $\mathrm{char}(k) \neq 2$ is finite and $K = k(x)$, has been obtained in [**Cor01**]. In this article, one finds the torsion over $\overline{k}$ and looks at Galois invariant orbits. In [**Bir09**] a similar statement is obtained for genus 2 curves.

Remark 4.11. The above statement applies when L is a hyperelliptic function field and where $K = k(x)$ such that $[L : k(x)] = 2$.

There are also other function fields with trivial Picard group. For example, the function field of an elliptic curve with precisely one rational point has trivial Picard group.

Chapter 3

Images of maps between curves

1. Introduction

1.1. Part 1. A natural question is the following.

Problem 1. Let k be an infinite field and let $f \in k[x]$. Then f induces an evaluation map $f_k \colon k \to k$. Can it be the case that $k \setminus f_k(k)$ is finite and non-empty?

This question was asked by Philipp Lampe on mathoverflow as Question 6820 in 2009 (see also Question 120175), and it still remains open.

In the first part we solve the problem for certain fields k.

Definition 1.1. A field k is called *large* if every irreducible k-curve C with a k-rational smooth point has infinitely many k-points.

Note that large fields are infinite. For more information on large fields see the survey [**Pop13**]. Some examples of large fields are $\mathbf{R}$, $\mathbf{Q}_p$ (p prime), $l((t))$ (where l is a field), infinite algebraic extensions of finite fields and any finite extension of such fields.

Theorem 1.2. *Let k be a perfect large field. Let C, D be normal projective curves over k. Let $f \colon C \to D$ be a finite morphism. Suppose that the induced map $f_k \colon C(k) \to D(k)$ is not surjective. Then one has $|D(k) \setminus f_k(C(k))| = |k|$.*

Corollary 1.3. *Let k be a perfect large field. Then the following hold.*

i. *Let $f \in k(x)$ such that the induced map $f_k \colon \mathbf{P}^1_k(k) \to \mathbf{P}^1_k(k)$ is not surjective. Then one has $|\mathbf{P}^1_k(k) \setminus f_k(\mathbf{P}^1_k(k))| = |k|$.*
ii. *Let $f \in k[x]$ such that the induced map $f_k \colon k \to k$ is not surjective. Then one has $|k \setminus f_k(k)| = |k|$.*

1.2. Part 2. Note that we can apply the above statement when k is an infinite algebraic extension of a finite field. This case was already conjectured in a talk 'How many values a polynomial map misses?' on the February 8th 2013 by D. Wan at the University of California Irvine. The conjecture was motivated by the study of the finite field case (see Chapter 4). In the second part of this chapter we study this specific case. We can say more about the 'size' of $k \setminus f(k)$ and one can view Theorem 1.2 as a special case of the following. Let C be a normal projective curve over an infinite algebraic extension k of a finite field. We will define the notion of the density of a subset $S \subseteq C(k)$ in Section 4.1. Finite subsets have density 0. Then we have the following theorem.

Theorem 1.4. *Let k be an infinite algebraic extension of a finite field. Let C, D be normal projective curves over k with $D(k)$ not empty. Let $f\colon C \to D$ be a finite morphism of such that the corresponding inclusion of function fields has separability degree n_{s} and let $f_k\colon C(k) \to D(k)$ be the induced map. Let $i \in \mathbf{Z}_{\geq 1}$ and set*

$$X_i = \left\{P \in D(k) : \#f_k^{-1}(P) = i\right\}$$

and

$$X_{\geq i} = \left\{P \in D(k) : \#f_k^{-1}(P) \geq i\right\}.$$

Then X_i and $X_{\geq i}$ have rational densities. Furthermore, the following hold:

i. $i > n_{\mathrm{s}} \implies X_i = X_{\geq i} = \emptyset$;
ii. $d(X_0) = 0 \implies X_0 = \emptyset$;
iii. $d(X_{\geq i}) = 0 \implies X_{\geq i} = \emptyset$.

The idea of the proof of Theorem 1.4 is the following. Our Galois theoretic approach to valuation theory as in Chapter 1 relates membership of X_i to having certain Frobenius element in a given Galois extension. Finally, one uses a new version of the Chebotarev density theorem together with the Hasse-Weil theorem to calculate how many points have a given Frobenius. The proof of Theorem 1.2 follows similar strategies.

1.3. Part 3. Let us discuss this new Chebotarev density theorem. Let K be a geometrically irreducible function field over a perfect field k with procyclic absolute Galois group with $F \in \mathrm{Gal}(k_{\mathrm{sep}}/k)$ as a topological generator (see Section 9 from Chapter 1, also for the definition of symbols like $(Q, M/K)$). Assume that k is the full constant field of K. Let M/K be a finite normal extension with automorphism group G. To an element $P \in \mathcal{P}_{K/k}$ with prime Q above it in M we associate a probability measure (P, M) on G which for $\gamma \in G$, with conjugacy class Γ, is defined by

$$(P, M)(\gamma) = \frac{\#\left((Q, M/K) \cap \Gamma\right)}{\#\Gamma \cdot \#(Q, M/K)}.$$

This is indeed well-defined since for a different choice Q' of a prime above P the elements $(Q, M/K)$ and $(Q', M/K)$ are conjugate. It is then easy to see that (P, M) is a probability measure on G. If $\mathrm{I}_{Q,K} = 0$, then the distribution is evenly divided over the whole Frobenius conjugacy class and zero outside.

Let k' be the full constant field of M. Let $N = \mathrm{Aut}(M/Kk')$, which is the geometric Galois group. Note that $G/N = \mathrm{Gal}(Kk'/K) = \mathrm{Gal}(k'/k) = \langle\overline{F}\rangle$, where $\overline{F}$ is the image of F under $\mathrm{Gal}(k_{\mathrm{sep}}/k) \to \mathrm{Gal}(k'/k)$. If $Q|_K$ is rational, one has $(Q, M/K) \subseteq \overline{F} \subseteq G$ (Lemma 3.2). We have the following theorem.

Theorem 1.5. *Assume that we are in the situation as described in this subsection. Let $\gamma \in \overline{F}$ and assume that $m = \mathrm{ord}(\gamma) | \mathrm{ord}(\mathrm{Gal}(k_{\mathrm{sep}}/k))$. Let k_m be the unique extension of degree m of k in some algebraic closure of K containing M. Let F' be the image of F under the maps $\mathrm{Gal}(k_{\mathrm{sep}}/k) \to \mathrm{Gal}(k_m/k) \cong \mathrm{Gal}(k_m K/K)$. Then the following hold:*

i. $\mathrm{Aut}(k_m M/K) = \mathrm{Gal}(k_m K/K) \times_{\mathrm{Gal}(k'K/K)} \mathrm{Aut}_K(M) \ni (F', \gamma)$;

ii. $M_\gamma = (k_m M)^{\langle (F',\gamma)\rangle}$ *is geometrically irreducible over* k *and satisfies* $k_m M_\gamma = k_m M$.

Furthermore, we have a natural map

$$\begin{aligned}\phi\colon \mathcal{P}^1_{M_\gamma/k} &\to \mathcal{P}^1_{K/k}\\ Q &\mapsto Q|_K\end{aligned}$$

with image $\{P \in \mathcal{P}^1_{K/k} : \gamma \in (P, M/K)\}$ *such that for* $P \in \mathcal{P}^1_{K/k}$ *we have* $\#\phi^{-1}(P) = \#N \cdot (P, M)(\gamma)$.

When k is an infinite algebraic extension of a finite field, one can calculate the density of $\{P \in \mathcal{P}^1_{K/k} : \gamma \in (P, L/K)\}$. See Theorem 4.7 for the calculation.

2. Proof of the first theorem

Definition 2.1. Let K be a geometrically irreducible function field over a field k and let $P \in \mathcal{P}^1_{K/k}$. Let $\overline{K}$ be an algebraic closure of K. Let M/K be a normal extension of K inside $\overline{K}$ with group $G = \mathrm{Aut}_K(M)$. Let $\overline{k}$ be the algebraic closure of k inside $\overline{K}$. Set $\Gamma = \mathrm{Aut}_k(\overline{k})$. Let Q be an extension of P to M. A *Frobenius* for Q/P is a continuous morphism $\Gamma \to G$ such that that the diagram, where ψ is the natural map,

$$\begin{array}{ccc}\Gamma & \xrightarrow{\quad\varphi\quad} & G\\ & \searrow^{\psi} & \downarrow{\scriptstyle \pi}\\ & & \mathrm{Aut}(\overline{k}\cap M/k) \cong \mathrm{Aut}((M\cap(\overline{k}K))/K) = G/N\end{array}$$

commutes and such that $\mathrm{im}(\varphi)\,\mathrm{I}_{Q,K} = \mathrm{D}_{Q,K}$. The set of all such Frobenius maps is denoted by $\mathrm{Frob}(Q/P)$.

For the next proposition and lemma let assume that M/K is a normal extension of function fields over a perfect field k inside $\overline{K}$. Let $G = \mathrm{Aut}_K(M)$. Let $P \in \mathcal{P}^1_{K/k}$ with Q above it in M.

Suppose $\varphi \in \mathrm{Frob}(Q/P)$. We use the notation as in the definition of a Frobenius. Consider $\mathrm{Graph}(\varphi) \subseteq \Gamma \times_{G/N} G = \mathrm{Gal}(\overline{k}M/K)$, which is a closed subgroup. Set $M^\varphi = (\overline{k}M)^{\mathrm{Graph}(\varphi)}$. Note that M^φ/K is a finite extension if M/K is finite. Furthermore, M^φ is geometrically irreducible over k since k is perfect. Finally, we have $\overline{k}M^\varphi = \overline{k}M$.

Proposition 2.2. *There is* $\varphi \in \mathrm{Frob}(Q/P)$ *such that* $\mathcal{P}^1_{M^\varphi/k}$ *is not empty.*

Proof. Let $\overline{Q}$ be an extension of Q to $\overline{k}M$. We have the following exact sequence (Theorem 3.6 from Chapter 1):

$$0 \to \mathrm{I}_{\overline{Q},K} \to \mathrm{D}_{\overline{Q},K} \to \Gamma \to 0.$$

This sequence is split (Theorem 3.8 from Chapter 1). Let $\varphi_0\colon \Gamma \to \mathrm{D}_{\overline{Q},K} \subseteq \Gamma \times_{G/N} G$ be such a splitting. Note that $\mathrm{im}(\varphi_0)$ is the graph of a function $\varphi\colon \Gamma \to \mathrm{D}_{Q,K}$. One has $\mathrm{im}(\varphi_0)\,\mathrm{I}_{\overline{Q},K} = \mathrm{D}_{\overline{Q},K}$. This gives $\mathrm{im}(\varphi)\,\mathrm{I}_{Q,K} = \mathrm{D}_{Q,K}$ as required (Theorem 3.6). The commutativity of the diagram follows since $\mathrm{Graph}(\varphi) = \mathrm{im}(\varphi_0) \subseteq \Gamma \times_{G/N} G$.

We will show $Q' = \overline{Q}|_{M^\varphi} \in \mathcal{P}^1_{M^\varphi/k}$. By construction we have $\mathrm{D}_{\overline{Q},K} \supseteq \mathrm{Graph}(\varphi)$. Hence we obtain $\mathrm{D}_{\overline{Q},M^\varphi} = \mathrm{D}_{\overline{Q},K} \cap \mathrm{Gal}(M/M^\varphi) = \mathrm{Gal}(M/M^\varphi)$ (Theorem 4.9 from Chapter 1). Hence $\overline{Q}$ is the unique prime above Q' in $\overline{k}M$ (Theorem 3.6 from Chapter 1) and Q' is rational (here we use that k is perfect, see [**Sti09**, Theorem 3.6.3]). □

Lemma 2.3. *Let $\varphi \in \mathrm{Frob}(Q/P)$. Consider the natural map $\psi\colon \mathcal{P}^1_{M^\varphi/k} \to \mathcal{P}^1_{K/k}$. Let $P \in \mathrm{im}(\psi) \cap \mathrm{unr}(M_{K,\mathrm{sep}}/K)$. Then there is a prime Q of M above P with $\mathrm{D}_{Q,K} = \mathrm{im}(\varphi)$.*

Proof. Let Q'' be a valuation on $\overline{k}M$ extending P such that $Q' = Q''|_{M^\varphi} \in \mathcal{P}^1_{M^\varphi/k}$ (Proposition 5.2 from Chapter 1). Note that $\mathrm{I}_{Q'',K} = 0$. Set $Q = Q''|_M$ and $P' = Q''_{\overline{k}K}$. As Q' is rational, the natural injective map

$$\mathrm{D}_{Q'',K} \cap \mathrm{Graph}(\varphi) = \mathrm{D}_{Q'',M^\varphi} \cong \mathrm{Aut}(k_{Q''}/k_{Q'}) \to \mathrm{D}_{Q'',K} \cong \mathrm{Aut}(k_{Q''}/k)$$

is surjective (Theorem 3.6 from Chapter 1). Hence we find $\mathrm{D}_{Q'',K} \subseteq \mathrm{Graph}(\varphi)$. The map $\mathrm{D}_{Q'',K} \to \mathrm{D}_{P',K} = \Gamma$ is surjective (Theorem 3.6 from Chapter 1, [**Sti09**, Theorem 3.6.3]). As $\mathrm{Graph}(\varphi)$ is a graph, this shows that $\mathrm{D}_{Q'',K} = \mathrm{Graph}(\varphi)$. We deduce $\mathrm{D}_{Q,K} = \mathrm{im}(\varphi)$ (Theorem 3.6 from Chapter 1). □

Proof of Theorem 1.2. With the help of Theorem 2.8 from Chapter 2 we see that equivalently we need to prove the following. Let L/K be a finite extension of function fields over k. Assume that the induced map $f_k\colon \mathcal{P}^1_{L/k} \to \mathcal{P}^1_{K/k}$ is not surjective. Show that $|\mathcal{P}^1_{K/k} \setminus \mathrm{im}(f_k)| = |k|$.

Let M be a finite normal extension of K such that $X = \mathrm{Hom}_K(L, M) \neq \emptyset$. Assume $P \in \mathcal{P}^1_{K/k}$, $P \notin \mathrm{im}(f_k)$. Let Q be an extension of P to M. Let $\varphi \in \mathrm{Frob}(Q/P)$ with $\mathcal{P}^1_{M^\varphi/k} \neq \emptyset$ (Proposition 2.2). Since k is a large field, one has $|\mathcal{P}^1_{M^\varphi/k}| = |k|$ ([**Jar11**, Proposition 5.4.3]). Note that we have $\mathrm{im}(\varphi)\,\mathrm{I}_{Q,K} = \mathrm{D}_{Q,K}$. As $P \notin \mathrm{im}(f_k)$ we conclude from Corollary 3.18 from Chapter 1 that $(\mathrm{I}_{Q,K} \setminus X)^{\mathrm{D}_{Q,K}\,/\,\mathrm{I}_{Q,K}} = \emptyset$. This implies $X^{\mathrm{im}(\varphi)} = \emptyset$. Consider the map $\psi\colon \mathcal{P}^1_{M^\varphi/k} \to \mathcal{P}^1_{K/k}$. The set $\mathrm{im}(\psi) \cap \mathrm{unr}(M_{K,\mathrm{sep}}/K)$ has cardinality $|k|$ as well. For $P' \in \mathrm{im}(\psi) \cap \mathrm{unr}(M_{K,\mathrm{sep}}/K)$ there is a prime Q' of M above P' with $\mathrm{im}(\varphi) = \mathrm{D}_{Q',K}$ (Lemma 2.3). We find $X^{\mathrm{D}_{Q',K}} = X^{\mathrm{im}(\varphi)} = \emptyset$. From Corollary 3.18 from Chapter 1 we conclude that $P' \notin \mathrm{im}(f_k)$. This finishes the proof. □

Proof of Corollary 1.3. i: The statement is true if f is constant ([**Jar11**, Proposition 5.4.3]). Assume $f = \frac{f_1}{f_2} \in k(x)$ is not constant with $f_1, f_2 \in k[x]$ coprime. Without loss of generality we may assume that f_1 is monic and that $\deg(f_1) \geq \deg(f_2)$. Let $y = f(x)$ and consider the extension $k(x)/k(y)$. Consider the induced map $\mathcal{P}^1_{k(x)/k} \to \mathcal{P}^1_{k(y)/k}$. Notice first that the minimal polynomial of x over $k(y)$ is $f_1(t) - f_2(t)y \in k(y)[t]$ of degree n. For $a \in k$ we find

$$\mathrm{Norm}_{k(x)/k(y)}(x - a) = (-1)^n(f_1(a) - f_2(a)y)$$

Looking at divisors, we see that $x - a$ lies above $y - f(a)$. A similar statement holds for the point at infinity. We see that the map exactly agrees with f_k. Hence the result follows from Theorem 1.2.

ii: This follows from i, since the map sends the point at infinity to the point at infinity. □

3. Chebotarev density theorem

In literature, one often finds the following version of the Chebotarev density theorem.

Theorem 3.1 (Chebotarev density theorem)**.** *Let M/K be a Galois extension of function fields over a finite field k, of cardinality q, with group G. Assume that the constant field of M is k. Let $C \subseteq G$ be a conjugacy class. Then for each positive integer n one has*

$$\#\{P \in \mathrm{unr}(M/K) : \deg_k(P) = n, (P, M/K) = C\} = \frac{\#C}{\#G}\frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

Proof. See [**Ros02**, Theorem 9.13B] □

The goal of this section is to prove Theorem 1.5. This is a generalization of the above theorem for $n = 1$. Our version does allow non-geometric extensions. Furthermore, in our statement k is quasi-cyclic field. See Section 9 from Chapter 1 for the definition of quasi-cyclic fields and the Frobenius formalism. A similar approach can be found in [**FJ05**, Section 6.4], but there only a density statement is deduced.

3.1. Proof of our Chebotarev density theorem. Let M/K be a finite normal extension of function fields over a quasi-cyclic field with $\overline{\langle F\rangle} = \mathrm{Gal}(k_{\mathrm{sep}}/k)$ and $\mathrm{Aut}_K(M) = G$. Let r be the order of $\mathrm{Gal}(k_{\mathrm{sep}}/k)$ (which is a Steinitz number). Assume that K is geometrically irreducible over k (otherwise enlarge k). Let k' be the full constant field of M and set $h = [k' : k]$. Let $N = \mathrm{Gal}(M/Kk')$, which is the geometric Galois group. Note that $G/N = \mathrm{Gal}(Kk'/K) = \mathrm{Gal}(k'/k) = \langle\overline{F}\rangle$, where $\overline{F}$ is the image of F under $\mathrm{Gal}(k_{\mathrm{sep}}/k) \to \mathrm{Gal}(k'/k)$. We call $\overline{F}$ the *global Frobenius class*.

Lemma 3.2. *Let $Q \in \mathcal{P}_{M/k}$. Then the following hold:*

i. *assume $\deg_k(Q|_K) = 1$, then $(Q, M/K) \subseteq \overline{F}$;*
ii. *consider $(Q, M/K)$ in $\mathrm{D}_{Q,K} / \mathrm{I}_{Q,K}$, then $\mathrm{ord}((Q, M/K))|r$.*

Proof. i. This follows easily from the definitions.
ii. We have $\mathrm{D}_{Q,K} / \mathrm{I}_{Q,K} \cong \mathrm{Gal}(\mathrm{k}_Q/\mathrm{k}_{Q|_K})$ and the result follows. □

Remark 3.3. The above phenomenon is not as weird as it looks. For example, if K is algebraically closed, the Frobenius element for an unramified prime is always the trivial element.

Hence in general not all elements of G will be realized as Frobenius elements.

Lemma 3.4. *Let $\gamma \in \overline{F}$ with $m = \mathrm{ord}(\gamma)|r$. Let k_m be the unique extension of degree m of k in some algebraic closure of K containing M. Let F' be the image of F under the maps $\mathrm{Gal}(k_{\mathrm{sep}}/k) \to \mathrm{Gal}(k_m/k) \cong \mathrm{Gal}(k_mK/K)$. Then the following hold:*

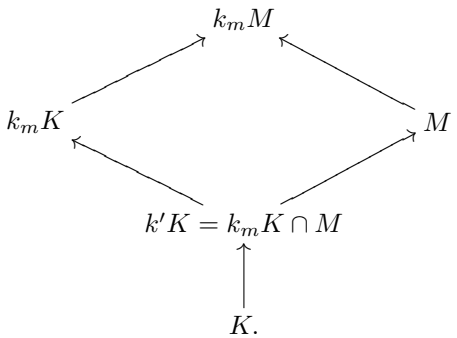
i. $\mathrm{Aut}_K(k_mM) = \mathrm{Gal}(k_mK/K) \times_{\mathrm{Gal}(k'K/K)} \mathrm{Aut}_K(M) \ni (F', \gamma)$;
ii. *$M_\gamma = (k_mM)^{\langle(F',\gamma)\rangle}$ is geometrically irreducible and satisfies $k_mM_\gamma = k_mM$.*

Furthermore, there is a map

$$\varphi\colon \mathcal{P}^1_{M_\gamma/k} \to S = \{Q \in \mathcal{P}_{M/k} : \deg_k(Q|_K) = 1,\ \gamma \in (Q, M/K)\}$$
$$Q'|_{M^\gamma} \mapsto Q'|_M,$$

where $Q' \in \mathcal{P}_{k_m M/k}$*, such that for* $Q \in S$ *we have* $\#\varphi^{-1}(Q) = \frac{\deg_k(Q)}{h}$.

Proof. Note first of all that $m \equiv 0 \pmod{\#G/N}$, by looking in the group G/N. This shows that $k_m K \cap M = k'K$. We have the following diagram:



Statement i follows directly. Note that $M_\gamma \cap k_m K = K$ and hence ii follows. Notice that $[k_m M : M_\gamma] = m$, and hence that $k_m M_\gamma = k_m M$. The natural restriction map $\mathrm{Gal}(k_m M/M_\gamma) \to \mathrm{Gal}(k_m K/K)$ is a bijection.

We claim that the following three statements are equivalent for $P' \in \mathcal{P}_{k_m M/k}$:

i. $\gamma \in (P'|_M, M/K)$ and $P'|_K$ is rational;
ii. $(F', \gamma) \in (P', k_m M/K)$ and $P'|_K$ is rational;
iii. $P'|_{M_\gamma}$ is rational.

i $\iff$ ii: Notice that $(P', k_m M/K) = (P'|_{k_m K}, k_m K/K) \times (P'|_M, M/K)$ (Lemma 9.4 from Chapter 1, as $k_m K/K$ is unramified). From the rationality of $P'|_K$ one obtains $(P'_{k_m K}, k_m K/K) = F'$ and the result follows.

Note that we have $(P', k_m M/M_\gamma)|_{k_m K} = (P'|_{k_m K}, k_m K/K)^{\mathrm{f}(P'|_{M_\gamma}/P'|_K)}$ (Corollary 9.3 from Chapter 1).

iii $\implies$ ii: If $P'|_{M_\gamma}$ is rational, then one has

$$(P', k_m M/M_\gamma)|_{k_m K} = (P'|_{k_m K}, k_m K/K) = F'.$$

As γ and F' have the same order, we obtain $(F', \gamma) \in (P', k_m M/M_\gamma)$. We have a natural inclusion $(P', k_m M/M_\gamma) \subseteq (P', k_m M/K)$ since $P'|_{M_\gamma}$ is rational. The result follows.

ii $\implies$ iii: We have $F' = (P'|_{k_m K}, k_m M/M_\gamma)^{\deg_k(P'|_{M_\gamma})}$. Note that ii implies that $\deg_k(P')|m$. Hence this can only happen if $(F', \gamma) = (P'|_{k_m K}, k_m M/M_\gamma)$. This shows that $P'|_{M_\gamma}$ is rational.

The above equivalences show that we have the map as described. We will calculate the sizes of the fibers.

For a rational prime $P \in \mathcal{P}_{M_\gamma/k}$ there is a unique prime above it in $k_m M$ (since it is just a constant field extension). Take a prime $P' \in \mathcal{P}_{M/k}$ such that $P'|_K$ is

rational with $\gamma \in (P'|_M, M/K)$. Notice that $[k_m M : M] = m/h$. In the extension $[k_m M : M]$, the residue field grows with a degree $m/\deg_k(P')$ and hence there are $\frac{m/h}{m/\deg_k(P')} = \frac{\deg_k(P')}{h}$ primes above it. □

Lemma 3.5. *Let $\gamma \in \overline{F}$ and let Γ be its conjugacy class in G. Consider the natural surjective map, where $S = \{Q \in \mathcal{P}_{M/K} : \deg_k(Q|_K) = 1,\ \gamma \in (Q, M/K)\}$,*

$$\psi \colon S \to T = \{P \in \mathcal{P}_{K/k} : \deg_k(P) = 1, \gamma \in (P, M/K)\}.$$

Then for $P \in T$ with prime $Q \in S$ above it we have

$$\#\psi^{-1}(P) = \frac{\#G}{\#\Gamma \cdot \#\,\mathrm{D}_{Q,K}} \cdot \#\left((Q, M/K) \cap \Gamma\right).$$

Proof. Let $Q \in S$ lie above P. Then we have $(Q, M/K) = \gamma\, \mathrm{I}_{Q,K}$. For $g \in G$ we have $(gQ, M/K) = g(Q, M/K)g^{-1}$. So $\gamma \in (gQ, M/K)$ iff $\gamma \in g(Q, M/K)g^{-1}$ iff $g^{-1}\gamma g \in (Q, M/K)$. Let G_γ be the stabilizer of γ under the conjugation action of G on itself. Then the number of $g \in G$ such that $\gamma \in (gQ, M/K)$ is equal to $\#G_\gamma \cdot \#\left((Q, M/K) \cap \Gamma\right) = \frac{\#G}{\#\Gamma} \cdot \#\left((Q, M/K) \cap \Gamma\right)$.

Furthermore, suppose that for $g, g' \in G$ we have $gQ = g'Q$. Then $g'^{-1}g \in \mathrm{D}_{Q,K}$. This shows that $\#\psi^{-1}(P) = \frac{\#G}{\#\Gamma \cdot \#\,\mathrm{D}_{Q,K}} \cdot \#\left((Q, M/K) \cap \Gamma\right)$. □

We can finally prove the new version of the Chebotarev density theorem.

Proof of Theorem 1.5. The first part directly follows from Lemma 3.4. The rest of the proof will follow from combining Lemma 3.4 and Lemma 3.5. We follow the notation from these lemmas. Note that $\phi = \psi \circ \varphi$. Let $P \in T$ and let $Q \in \psi^{-1}(P)$. Note that $\deg_k(Q)$ does not depend on the choice of Q. One has:

$$\begin{aligned}
\#\phi^{-1}(P) &= \#\varphi^{-1} \circ \psi^{-1}(P) \\
&= \frac{\deg_k(Q)}{h} \cdot \frac{\#G}{\#\Gamma \cdot \#\,\mathrm{D}_{Q,K}} \cdot \#\left((Q, M/K) \cap \Gamma\right) \\
&= \frac{\#N}{\#\Gamma} \cdot \frac{\deg_k(Q) \cdot \#\left((Q, M/K) \cap \Gamma\right)}{\#\,\mathrm{D}_{Q,K}} \\
&= \frac{\#N}{\#\Gamma} \cdot \frac{\deg_k(Q) \cdot \#\left((Q, M/K) \cap \Gamma\right)}{\#\,\mathrm{D}_{Q,K}} \cdot \frac{\#(Q, M/K)}{\#(Q, M/K)} \\
&= \#N \cdot (P, M)(\gamma) \cdot \deg_k(Q) \cdot \frac{\#(Q, M/K)}{\#\,\mathrm{D}_{Q,K}} \\
&= \#N \cdot (P, M)(\gamma).
\end{aligned}$$

Note that for $P \in \mathcal{P}^1_{K/k} \setminus T$ we have $(P, M)(\gamma) = 0 = \#\phi^{-1}(P)$.

□

3.2. Finite fields. In case k is finite we have control over the number of rational points of M_γ in Theorem 1.5 by Hasse-Weil. This gives us Theorem 3.1 when $n = 1$.

Corollary 3.6. *Assume that k is finite of cardinality q. Let $\gamma \in \overline{F}$. Then we have*

$$|\sum_{P \in \mathcal{P}_{K/k}} (P, M)(\gamma) - \frac{1}{\#N}(q+1)| \leq \frac{1}{\#N} 2g_{k'}(M)\sqrt{q}.$$

PROOF. We apply Theorem 1.5. By Hasse-Weil (Theorem 3.17 from Chapter 2) we have

$$|\{P \in \mathcal{P}_{M_\gamma/k} : \deg_k(P) = 1\} - (q+1)\}| \leq 2g_k(M_\gamma)\sqrt{q} = 2g_{k'}(M)\sqrt{q}.$$

This gives the required result. □

Remark 3.7. Let $n \in \mathbf{Z}_{\geq 1}$ be given. Using inclusion-exclusion one can prove a formula for $\sum_{P \in U_n}(P, M)(\Gamma)$ where $U_n = \{P \in \mathcal{P}_{K/k} : \deg_k(P) = n, \gamma \in (P, M/K)\}$ by using constant field extensions. The reason we do not provide this statement is that the formula becomes quite messy and that we only need the formula for the case $n = 1$.

4. Density theorem: infinite algebraic over a finite field

4.1. Density. Let f is a map between curves over a field k. We denote by f_k the map on the k-points.

Let C be a curve over k. Let k' be a subfield of k. A curve C' over k' together with an isomorphism $C' \times_{\mathrm{Spec}(k')} \mathrm{Spec}(k) \to C$ over $\mathrm{Spec}(k)$ is called a form of C over k'. We have a natural bijection $\pi \colon C(k) \to C'(k)$ coming from

$$C(k) \cong \mathrm{Hom}_{\mathrm{Spec}(k)}(\mathrm{Spec}(k), C' \times_{\mathrm{Spec}(k')} \mathrm{Spec}(k)) \cong \mathrm{Hom}_{\mathrm{Spec}(k')}(\mathrm{Spec}(k), C').$$

Let $S \subseteq C(k)$. Then we view S as a subset of $C'(k)$ by identifying S with $\pi(S)$. Note that for an intermediate field l of k/k' one has $C'(l) \subseteq C'(k)$.

Definition 4.1. Let k be an algebraic extension of a finite field and let C be a normal projective curve over k with $C(k) \neq \emptyset$. Let $S \subseteq C(k)$ and let $r \in \mathbf{R}$. Then we say that the *density* of S is equal to r if the following hold: for all $\epsilon > 0$ there exists $k' \subseteq k$ with k' finite and a form C' of C over k' with the following property: for all finite extensions $l \supseteq k'$ with $l \subseteq k$ we have

$$|\#(S \cap C'(l)) - r\#C'(l)| \leq \epsilon \cdot \#C'(l).$$

If S has a density and this density is equal to r, we write $d(S) = r$.

Lemma 4.2. *Let k be an infinite algebraic field extension of a finite field and let C be a normal projective geometrically irreducible curve over k. Then $C(k)$ is not finite.*

PROOF. This follows directly from Hasse-Weil (Corollary 3.17 from Chapter 2). □

Proposition 4.3. *Let k be an algebraic extension of a finite field and let C be a normal projective curve over k such that $C(k) \neq \emptyset$. Let $S, T \subseteq C(k)$. Then the following properties hold:*

i. *If S has a density, then its value is unique and $0 \leq d(S) \leq 1$.*
ii. *If S is finite and k is infinite, then $d(S) = 0$.*
iii. *If $(S \setminus T) \cup (T \setminus S)$ is finite, k is infinite and S has a density, then T has a density and $d(S) = d(T)$.*

iv. *If S and T have densities and $S \subseteq T$, then $d(S) \leq d(T)$ and $T \setminus S$ has density $d(T) - d(S)$.*
v. *If S and T have densities and $S \cap T = \emptyset$, then $d(S \cup T) = d(S) + d(T)$.*
vi. *If S has a density, then so does $S^c = C(k) \setminus S$ and $d(S^c) = 1 - d(S)$.*

PROOF. i. If C', C'' are forms of C over a finite field k'. Then there is a finite extension l of k' in k one has $C' \times_{\mathrm{Spec}(k')} \mathrm{Spec}(l) \cong C'' \times_{\mathrm{Spec}(k')} \mathrm{Spec}(l)$ over $\mathrm{Spec}(l)$ (use for example Proposition 2.4 from Chapter 2). Hence for the determination of the density, the choice of a form does not play a role. Fix a form C' over a finite field k'. Suppose that the density of S is r and r' and that the inequality holds for a given ϵ and all finite fields containing a field k'. Then there are two cases. If k is finite, one directly sees that $r = r'$. If k is infinite and if $C'(l) \neq \emptyset$ where $l \supseteq k'$ is finite, then if $\epsilon < 1/2(r - r')\#C'(l)$ we have a contradiction.

One obviously sees that the density is between 0 and 1.

ii: Note that $C(k)$ is an infinite set (Lemma 4.2). Then obviously the density of S is 0.

iii: This follows directly since $C(k)$ is an infinite set (Lemma 4.2).

iv, v, vi: Obvious. □

Remark 4.4. Let k be an algebraic field extension of a field k'. Let C be a normal projective geometrically irreducible curve over k. Let l be an intermediate extension of k/k'. Put $C_l = C \times_{\mathrm{Spec}(k)} \mathrm{Spec}(l)$. Put $K = k(C)$ and $lK = k(C_l)$. Note that $C_l(l) = C(l)$ and $C_l(l)$ can be identified with $\mathcal{P}_{lK/l}$ (Proposition 2.11 from Chapter 2). Set $A = \{l \text{ finite over } k' : \ k' \subseteq l \subseteq k\}$. We have

$$C(k) = \varinjlim_{l \in A} C(l) = \varinjlim_{l \in A} \mathcal{P}^1_{Kl/l}.$$

Hence we often study $C(k)$ by looking at the valuations.

4.2. Density theorem. Using limit arguments, we can deduce a density statement for infinite algebraic extensions of finite fields.

Let k be a finite field with $\mathrm{Gal}(k_{\mathrm{sep}}/k) = \overline{\langle F \rangle}$. Note that this group is isomorphic to $\hat{\mathbf{Z}}$. Let $s \in \hat{\mathbf{Z}}$ such that k_s/k is an infinite field extension (see Section 9 from Chapter 1 for the definitions). Then one has $\mathrm{Gal}(k_{\mathrm{sep}}/k_s) \cong s\hat{\mathbf{Z}}$. Observe that $s\hat{\mathbf{Z}} \cong \prod_{p \in S_s} \mathbf{Z}_p$ where $S_s = \{p : \mathrm{ord}_p(s) \neq \infty\}$ with ord_p is the composition $\hat{\mathbf{Z}} \to \mathbf{Z}_p \overset{\mathrm{ord}_p}{\to} \mathbf{Z}_{\geq 0} \sqcup \{\infty\}$.

Let M/K be a finite normal extension of function fields over k_s with group $G = \mathrm{Aut}_K(M)$. Assume that K is geometrically irreducible over k_s. Let k'_s be the full constant field of M. Let $N = \mathrm{Gal}(M/Kk'_s)$, which is the geometric Galois group. Note that $G/N = \mathrm{Gal}(Kk'_s/K) = \mathrm{Gal}(k'_s/k_s) = \langle F^s|_{k'_s} \rangle$.

Lemma 4.5. *Let H be a torsion group and let S be a set of primes. Define the Steinitz numbers $r_0 = \prod_{p \in S} p^\infty$ and $r_1 = \prod_{p \notin S} p^\infty$. Let $h \in H$. Then there are unique $h_0, h_1 \in H$ with $h_0 h_1 = h = h_1 h_0$ such that $\mathrm{ord}(h_0)|r_0$ and $\mathrm{ord}(h_1)|r_1$. The map*

$$\varphi_{H,S} \colon H \to H_S = \{h \in H : \mathrm{ord}(h)|r_0\}$$
$$h \mapsto h_0$$

is surjective and satisfies $\varphi_{H,S} \circ \varphi_{H,S} = \varphi_{H,S}$.

PROOF. First we prove that such a decomposition exists. Write $\operatorname{ord}(h) = s_0 \cdot s_1$ with $s_0 | r_0$ and $s_1 | r_1$. Then there exists integers a, b with $as_0 + bs_1 = 1$. Hence we find

$$h = h^1 = h^{as_0+bs_1} = h^{bs_1} \cdot h^{as_0}.$$

Then a decomposition of h is given by $h_0 = h^{bs_1}$ and $h_1 = h^{as_0}$.

We will prove uniqueness. If $h = h_0 h_1 = h_1 h_0$, then there exists integers a, b such that $a \operatorname{ord}(h_0) + b \operatorname{ord}(h_1) = 1$. Hence we obtain

$$h^{1-b \operatorname{ord}(h_1)} = h_0^{a \operatorname{ord}(h_0)} \cdot h_1^{1-b \operatorname{ord}(h_1)} = h_1.$$

It follows that $h_0, h_1 \in \langle h \rangle$. In the cyclic group $\langle h \rangle$ the result follows easily from the Chinese remainder theorem.

The properties of $\varphi_{H,S}$ follow directly. □

We will approximate M/K with extensions of function field over a finite fields.

Definition 4.6. A *finite approximation* of M/K is a triple (m, M_m, K_m) where $m \in \mathbf{Z}_{\geq 1}$, $m|s$, with K_m, M_m function fields over k_m with $K_m \subseteq M_m$, $K_m \subseteq K$ and $M_m \subset M$ such that the following hold.

i. If a prime p satisfies $p | \#G$ and $p \notin S_s$, one has $\operatorname{ord}_p(s) = \operatorname{ord}_p(m)$.
ii. One has $k_s K_m = K$ and $k_s M_m = M$.
iii. The extension M_m/K_m is Galois and the natural restriction map $G = \operatorname{Gal}(M/K) \to G' = \operatorname{Gal}(M_m/K_m)$ is an isomorphism;
iv. Let k'_s respectively k'_m be the full constant field of M respectively M_m. Then the natural map $N = \operatorname{Gal}(M/Kk'_s) \to N' = \operatorname{Gal}(M_m/Kk'_m)$ is an isomorphism.
v. The set $\mathcal{P}^1_{K_m/k_m}$ is not empty.

It is not hard to see that such finite approximations exist.

Recall that

$$F^s|_{k'_s} \in \operatorname{Gal}(k'_s/k_s) \cong G/N$$

and we can view $F^s|_{k'_s}$, the global Frobenius class, as a subset of G.

Theorem 4.7. *Let M/K be a finite normal extension with group G of function fields over k_s. Assume that K is geometrically irreducible. Write* $\operatorname{ord}(G) = s_0 \cdot s_1$ *where $s_0 | \prod_{p \in S_s} p^\infty = r$ and $s_1 | \prod_{p \notin S_s} p^\infty$. Let $a, b \in \mathbf{Z}$ with $as_0 + bs_1 = 1$.*

Then the map

$$\begin{aligned} \varphi_{G,S_s} : G \to G_{S_s} &= \Big\{ g \in G : \operatorname{ord}(g) | \prod_{p \in S_s} p^\infty \Big\} \\ x &\mapsto x^{bs_1} \end{aligned}$$

gives a map

$$\varphi \colon F^s|_{k'_s} \to G.$$

with image $F^s|_{k'_s} \cap G_{S_s}$. *Let* $\gamma \in G$ *with conjugacy class* Γ *and let* $T = \{P \in \mathcal{P}^1_{K/k} : \gamma \in (P, M/K, s)\}$. *Then* $d(T)$ *exists and is equal to*

$$d(T) = \frac{\#\varphi^{-1}(\Gamma)}{\#N}.$$

Furthermore, if $d(T)$ *is* 0, *then* S *is finite.*

PROOF. The description of φ_{G,S_s} follows from the uniqueness in Lemma 4.5. We claim that $\varphi_{G,S_s}(F^s|_{k'_s}) \subseteq F^s|_{k'_s}$. Take $h \in F^s|_{k'_s}$ and write it as $h = h_0h_1 = h_1h_0$ as in Lemma 4.5 with $S = S_s$. We reduce modulo N to obtain $F^s|_{k'_s} = \overline{h_0}\overline{h_1}$. We claim $\overline{h_1} = 1$. Indeed, the order of $\overline{h_1}$ divides $\#G/N|\prod_{p\in S_s} p^\infty$ and is also coprime to it and the result follows. We see that h_0 lies in $F^s|_{k'_s}$. As $\varphi_{G,S_s} \circ \varphi_{G,S_s} = \varphi_{G,S_s}$, it follows that the image is $F^s|_{k'_s} \cap G_{S_s}$.

Fix a finite approximation (m, M_m, K_m) of M/K. Let $m' \in \mathbf{Z}_{\geq 1}$ with $mm'|s$. We have an approximation $(mm', M_{mm'} = M_mk_{mm'}, K_{mm'} = K_mk_{mm'})$. Let $k'_{mm'}$ be the full constant field of $M_{mm'}$. We have natural isomorphisms $G = \mathrm{Gal}(M/K) \to \mathrm{Gal}(M_{mm'}/K_{mm'})$ and similarly $N = \mathrm{Gal}(M/Kk'_s) \to \mathrm{Gal}(M_{mm'}/K_{mm'}k'_{mm'})$. Note that $G/N \cong \mathrm{Gal}(k'_{mm'}/k_{mm'}) \ni F^{mm'}|_{k'_{mm'}}$. Let $F^{mm'}|_{k'_{mm'}} \subseteq G$ be its lift to G. Consider the map

$$\begin{aligned} \varphi_{m'} \colon F^{mm'}|_{k'_{mm'}} &\to F^s|_{k'_s} \\ g &\mapsto g^{\frac{s}{mm'}}. \end{aligned}$$

We claim that there is $x_{m'} \in \hat{\mathbf{Z}}^*$ with

$$\frac{s}{mm'} \equiv x_{m'} \cdot bs_1 \pmod{\#G}.$$

Using the Chinese remainder theorem, it is enough to prove this statement primewise. Let p be a prime dividing $\#G$. And suppose $p \notin S_s$. Then we have $\frac{s}{mm'} \in \mathbf{Z}_p^*$ (assumption i of finite approximation) and furthermore $bs_1 = 1 - as_0 \in \mathbf{Z}_p^*$ and we can solve the problem at this prime. If $p \in S$, we have to solve $0 \equiv x \cdot 0$ and any unit will do the job. This gives us an injective map

$$\begin{aligned} \psi_{m'} \colon F^{mm'}|_{k'_{mm'}} &\to G. \\ g &\mapsto g^{x_{m'}}. \end{aligned}$$

We claim that its image lies in $F^s|_{k'_s}$, and by counting this will show that $\psi_{m'}$ induces a bijection between $\psi_{m'} \colon F^{mm'}|_{k'_{mm'}} \to F^s|_{k'_s}$. To see that this is true, it suffices to show that $x_{m'} \equiv \frac{s}{mm'} \pmod{\#G/N}$. This follows since $bs_1 \equiv 1 - as_0 \equiv 1 \pmod{\#G/N}$.

By construction we have the following commutative diagram:

$$\begin{array}{ccc} F^{mm'}|_{k'_{mm'}} & \xrightarrow{\varphi_{m'}} & F^s|_{k'_s} \\ \downarrow{\scriptstyle \psi_{m'}} & \nearrow{\scriptstyle \varphi} & \\ F^s|_{k'_s}. & & \end{array}$$

As $\psi_{m'}$ is bijection, this shows that the fibers of $\varphi_{m'}$ and φ have the same cardinality. This shows in particular that

$$d = \frac{\#\varphi^{-1}(\Gamma)}{\#N} = \frac{\#\varphi_{m'}^{-1}(\Gamma)}{\#N}.$$

Let us explain the importance of $\varphi_{m'}$. Put $W_{m'} = \mathcal{P}^1_{K_{mm'}/k_{mm'}}$. Let $P \in W_{m'}$ and let P' be the unique prime of $\mathcal{P}^1_{K/k_s}$ above it. Let Q' be a prime above P' in M and let Q be its restriction to $M_{mm'}$. Assume that P is unramified in $M_{mm'}$. Then we have the equality (Lemma 9.2 from Chapter 1)

$$(Q', M/K, s)|_{M_{mm'}} = \varphi_{m'}\left((Q, M_{mm'}/K_{mm'}, mm')\right).$$

Since $\varphi_{m'}$ maps a conjugacy class to a conjugacy class, we obtain

$$(P', M/K, s)|_{M_{mm'}} = \varphi_{m'}\left((P, M_{mm'}/K_{mm'}, mm')\right).$$

As $\mathcal{P}^1_{M/K} = \varinjlim_{m':\ mm'|s} W_{m'}$ (Remark 4.4), this allows us to calculate the Frobenius of primes of $\mathcal{P}^1_{M/K}$ by working over finite fields.

Let w be the number of rational prime of K which are ramified in M/K. Notice that w is at least the number of rational primes of $K_{mm'}$ which are ramified in $M_{mm'}/K_{mm'}$. We will calculate the density of $T' = T \cap \mathrm{unr}(M/K)$. This does not affect the density (Proposition 4.3 iii). Put $T'_{m'} = T' \cap W_{m'}$. We have

$$\begin{aligned}\#T'_{m'} &= \#\{P \in \mathrm{unr}^1(K_{mm'}/k_{mm'}) : (P, M_{mm'}/K_{mm'}) \subseteq \varphi_{m'}^{-1}(\Gamma)\} \\ &= \sum_{g \in \varphi_{m'}^{-1}(\Gamma)} \sum_{P \in \mathrm{unr}^1(K_{mm'}/k_{mm'})} (P, M_{mm'})(g).\end{aligned}$$

Note that $g_{k'_s}(M) = g_{k'_{mm'}}(M_{mm'})$ and $g_{k_s}(K) = g_{k_{mm'}}(K_{mm'})$ (Proposition 2.14 from Chapter 2). Set

$$c_{\pm,m'} = \#k_{mm'} + 1 \pm 2g_{k'_s}(M)\sqrt{\#k_{mm'}}.$$

and

$$e_{\pm,m'} = \#k_{mm'} + 1 \pm 2g_{k_s}(K)\sqrt{\#k_{mm'}}.$$

Corollary 3.6 gives us:

$$d \cdot c_{-,m'} - w \leq \#T'_{m'} \leq d \cdot c_{+,m'}.$$

Note that $e_{-,m'} \leq \#W_{m'} \leq e_{+,m'}$ by Hasse-Weil (Corollary 3.17 from Chapter 2). Hence we obtain

$$d \cdot \frac{c_{-,m'} - w}{e_{+,m'}} \leq \frac{\#T'_{m'}}{\#W_{m'}} \leq d \cdot \frac{c_{+,m'}}{e_{-,m'}}.$$

As m' goes to infinity, $\frac{c_{-,m'}-w}{e_{+,m'}}$ and $\frac{c_{+,m'}}{e_{-,m'}}$ go to 1. We obtain that $d(T) = d(T') = d$.

Suppose that $d(T) = 0$. Then it follows that $\gamma \notin \mathrm{im}(\varphi_m) = \{g \in F^s|_{k'_s} : \mathrm{ord}(g)|r\}$. Lemma 3.2 shows that all elements of T are ramified in M/K. This shows that T is finite. □

5. Proof of second theorem

Lemma 5.1. *Let H, H' be finite abelian groups and let $\varphi\colon H \to H'$ be a morphism of groups. Then there exists $n \in \mathbf{Z}_{\geq 1}$ such that for all $h \in H$ we have $\varphi(h^n) = \varphi(h)$ and such that $\operatorname{ord}(h^n)$ consists only of primes occurring in $\#H'$.*

PROOF. Write $\#H = n_1 \cdot n_2$ where n_1 consists of primes dividing $\#H'$ and n_2 consists of other primes. As $(n_1 \#H', n_2) = 1$, there are integers $a, b \in \mathbf{Z}$ with $an_1\#H' + bn_2 = 1$. Choose $n = bn_2$. For $h \in H$ we have

$$\varphi(h^n) = \varphi(h)^{bn_2} = \varphi(h)^{1-an_1\#H'} = \varphi(h)$$

and

$$(h^n)^{n_1} = h^{bn_1n_2} = 1.$$

□

Theorem 5.2. *Let k be an infinite algebraic extension of a finite field. Define the set of primes S by $\operatorname{Gal}(k_{\mathrm{sep}}/k) \cong \prod_{p\in S} \mathbf{Z}_p$. Let $L \supseteq K$ be a finite extension of function fields over k with separability degree n_{s}. Let $f_k\colon \mathcal{P}^1_{L/k} \to \mathcal{P}^1_{K/k}$ be the natural restriction map. Assume that $\mathcal{P}^1_{K/k}$ is not empty. Let M be a finite normal extension of K with group $G = \operatorname{Aut}_K(M)$ such that the G-set $X = \operatorname{Hom}_K(L, M)$ is not empty. Let k' be the full constant field of M and let $N = \operatorname{Gal}(M/Kk')$.*

Write $\operatorname{ord}(G) = s_0 \cdot s_1$ where $s_0 | \prod_{p\in S} p^\infty = r$ and $s_1 | \prod_{p\notin S} p^\infty = r$. Let $a, b \in \mathbf{Z}$ with $as_0 + bs_1 = 1$.

Pick a generator $F \subseteq G$ of G/N and consider the map

$$\varphi\colon F \to \{g \in F : \operatorname{ord}(g) | r\} \subseteq G$$
$$g \mapsto g^{bs_1}.$$

Let $i \in \mathbf{Z}_{\geq 1}$ and set

$$X_i = \{P \in \mathcal{P}^1_{K/k} : \#f_k^{-1}(P) = i\}.$$

Set $T_i = \{g \in G : \#X^g = i\}$. Then X_i has a density and it is equal to

$$d(X_i) = \frac{\#\varphi^{-1}(T_i)}{\#N}.$$

Furthermore, the following hold:

i. $i > n_{\mathrm{s}} \implies X_i = X_{\geq i} = \emptyset$;
ii. $d(X_0) = 0 \implies X_0 = \emptyset$;
iii. $d(X_{\geq i}) = 0 \implies X_{\geq i} = \emptyset$.

PROOF. Make k into a quasi-cyclic field such that it maps the generator under $\operatorname{Gal}(k_{\mathrm{sep}}/k) \to \operatorname{Gal}(G/N)$ to F (we suppress the choice of the generator later). Note that T_i is a union of conjugacy classes. Proposition 9.7 from Chapter 1 and Theorem 4.7 give us the values of $d(X_i)$.

i: Follows from Theorem 3.9 from Chapter 1 and Theorem 5.6 from Chapter 1.

ii. Let $P \in X_0$. Let P'' be a prime of M above P. It follows that $(P'', M/K) \subseteq T_0$ (Proposition 9.7 from Chapter 1). Lemma 5.1 show that there is $h \in (P'', M/K)$ with $\operatorname{ord}(h) | r$ (look at the map $\mathrm{D}_{P'',K} \to \mathrm{D}_{P'',K} / \mathrm{I}_{P'',K}$ and note $\#\,\mathrm{D}_{P'',K} / \mathrm{I}_{P'',K} \,| r$).

Then the set of unramified rational primes with h in the Frobenius has a positive density (Theorem 4.7). Proposition 9.7 from Chapter 1 implies that X_0 has a positive density.

iii. Let $P \in X_{\geq i}$. Let P'' be a prime above P in M. From Proposition 9.7 from Chapter 1 it follows that there is $g \in (P'', M/K)$ with $\#X^g \geq i$. From Lemma 5.1 it follows that there is a power of g, say h, with $h \in (P'', M/K)$ with $\mathrm{ord}(h)|r$. Notice that $\#X^h \geq \#X^g \geq i$. Theorem 4.7 give the result. □

Proof of Theorem 1.4. This follows from Theorem 5.2 in combination with Proposition 4.3v and the link between function fields and curves (Theorem 2.8 from Chapter 2). □

6. Examples of density calculations and lower bounds

6.1. Lower bounds for densities.

Lemma 6.1. *Let G be a finite group acting on a finite non-empty set X of cardinality d. Let N be a normal subgroup of G such that N acts transitively on X. Assume that G/N is cyclic with generator φ. Then we have:*

i. $\{\sigma \in \varphi : X^\sigma = \emptyset\} = \emptyset \iff \forall \sigma \in \varphi\text{: } \#X^\sigma = 1$;
ii. $\{\sigma \in \varphi : X^\sigma = \emptyset\} \neq \emptyset \iff \#\{\sigma \in \varphi : X^\sigma = \emptyset\} \geq \frac{\#\varphi}{d}$.

Proof. Consider the polynomial $g = (x-1)(x-d) \in \mathbf{R}[x]$. Then we have $g(0) = d$ and $g(x) \leq 0$ for $x \in [1, d]$. Put $\chi(\sigma) = \#X^\sigma$. Lemma 9.6 from Chapter 1 gives

$$\begin{aligned} d \cdot \#\{\sigma \in \varphi : X^\sigma = \emptyset\} &\geq \sum_{\sigma \in \varphi} g(\chi(\sigma)) \\ &= \sum_{\sigma \in \varphi} \chi(\sigma)^2 - (d+1) \sum_{\sigma \in \varphi} \chi(\sigma) + d\#\varphi \\ &= \#\varphi \#(N\backslash(X \times X))^{G/N} - \#\varphi \left((d+1)\#(N\backslash X)^{G/N} - d \right) \\ &= \#\varphi \cdot \#(N\backslash(X \times X))^{G/N} - \#\varphi \\ &= \#\varphi \cdot \#(N\backslash ((X \times X)\backslash\Delta(X)))^{G/N} \geq 0. \end{aligned}$$

From Lemma 9.6 from Chapter 1 we obtain

$$\#(N\backslash ((X \times X)\backslash\Delta(X)))^{G/N} = \frac{1}{\#N} \sum_{\sigma \in \varphi} \#\left((X \times X)\backslash\Delta(X)\right)^\sigma.$$

If there is $\tau \in \varphi$ with $\chi(\tau) \geq 2$, say with fixed points $x, y \in X$, we see that $(x, y) \in ((X \times X)\backslash\Delta(X))^\tau$ and we obtain $\#(N\backslash ((X \times X)\backslash\Delta(X)))^{G/N} > 0$

i: The implication from right to left is trivial. Consider the other implication. If $\{\sigma \in \varphi : X^\sigma = \emptyset\} = \emptyset$, then from the above we see that for all $\sigma \in \varphi$ we have $\chi(\sigma) < 2$. We conclude that $\chi(\sigma) = 1$ for all $\sigma \in \varphi$.

ii: The implications from right to left is trivial. Consider the other implication. If there is $\tau \in \varphi$ with $\chi(\tau) \geq 2$, then by the above we find

$$d \cdot \#\{\sigma \in \varphi : X^\sigma = \emptyset\} \geq \#\varphi.$$

Suppose that for all $\sigma \in \varphi$ we have $\chi(\sigma) \leq 1$. We then have (Lemma 9.6 from Chapter 1)

$$1 = \#(N\backslash X)^{G/N} = \frac{1}{\#N} \sum_{\sigma \in \varphi} \#X^{\sigma} < 1,$$

since there are elements without a fixed point. Contradiction. □

Proposition 6.2. *Let k be an infinite algebraic extension of a finite field. Let S be the set of primes such that $\mathrm{Gal}(k_{\mathrm{sep}}/k) \cong \prod_{s \in S} \mathbf{Z}_p$. Let L/K be an extension of function fields over k. Assume that K is geometrically irreducible. Assume that $\#G | \prod_{p \in S} p^{\infty}$. Define X_0 and X_1 as in Theorem 5.2. Then we have:*

i. *if $d(X_0) > 0$, then $d(X_0) \geq \frac{1}{[L:K]}$;*
ii. *$d(X_0) = 0 \iff d(X_1) = 1$.*

Proof. If L/K is not geometric, then $d(X_0) = 1$ and the results follow.

Assume that L/K is geometric. Take the notation from Theorem 5.2. The map φ is a bijection. Note that N acts transitively on X since L is geometrically irreducible. The result follows from Lemma 6.1. □

6.2. Examples. Let k be an infinite algebraic extension of a finite field and define S by $\mathrm{Gal}(k_{\mathrm{sep}}/k) \cong \prod_{p \in S} \mathbf{Z}_p$. Let L/K be a separable extension of function fields over a finite field k of degree n. Assume that $\mathcal{P}^1_{K/k} \neq \emptyset$. Let M be the Galois closure of L/K and assume that $G = \mathrm{Gal}(M/K) \cong S_n$ of order $n!$. Let k' be the full constant field of M and let $N = \mathrm{Gal}(M/Kk')$. We calculate the densities of the X_i using Theorem 5.2.

Assume that $n = 3$. Assume first that $G = N$.

$S \cap \{2,3\}$	t s.t. $\varphi_{G,S} = (g \mapsto g^t)$	$d(X_0)$	$d(X_1)$	$d(X_2)$	$d(X_3)$
$\emptyset$	0	0	0	0	1
$\{2\}$	3	0	$\frac{1}{2}$	0	$\frac{1}{2}$
$\{3\}$	-2	$\frac{1}{3}$	0	0	$\frac{2}{3}$
$\{2,3\}$	1	$\frac{1}{3}$	$\frac{1}{2}$	0	$\frac{1}{6}$.

The only non-trivial normal subgroup of S_3 with cyclic quotient is A_3. Assume that $G = S_3$, $N = A_3$. Then we have $2 \in S$ and we obtain the following

$S \cap \{2,3\}$	t s.t. $\varphi_{G,S} = (g \mapsto g^t)$	$d(X_0)$	$d(X_1)$	$d(X_2)$	$d(X_3)$
$\{2\}$	3	0	0	0	1
$\{2,3\}$	1	$\frac{2}{3}$	0	0	$\frac{1}{3}$.

Assume that $n = 4$. Assume first that $G = N$. We have the following table:

$S \cap \{2,3\}$	t s.t. $\varphi_{G,S} = (g \mapsto g^t)$	$d(X_0)$	$d(X_1)$	$d(X_2)$	$d(X_3)$	$d(X_4)$
$\emptyset$	0	0	0	0	0	1
$\{2\}$	9	$\frac{3}{8}$	0	$\frac{1}{4}$	0	$\frac{3}{8}$
$\{3\}$	4	0	$\frac{1}{4}$	0	0	$\frac{3}{4}$
$\{2,3\}$	1	$\frac{3}{8}$	$\frac{1}{3}$	$\frac{1}{4}$	0	$\frac{1}{24}$.

The only non-trivial normal subgroup of S_4 with cyclic quotient is A_4. Assume that $G = S_4$, $N = A_4$. Then we have $2 \in S$ and we obtain the following table:

$S \cap \{2,3\}$	t s.t. $\varphi_{G,S} = (g \mapsto g^t)$	$d(X_0)$	$d(X_1)$	$d(X_2)$	$d(X_3)$	$d(X_4)$
$\{2\}$	9	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0
$\{2,3\}$	1	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0.

Remark 6.3. One can approximate densities of the various X_i and obtain information about the Galois group.

Remark 6.4. Proposition 6.2 is false if $\#G \nmid \prod_{p \in S} p^\infty$. That ii is not true already follows from the above example calculations. Let k be an infinite extension of a finite field and define S by $\mathrm{Gal}(k_{\mathrm{sep}}/k) \cong \prod_{p \in S} \mathbf{Z}_p$. Assume furthermore that $2, 3 \in S$ and that $5 \notin S$. Let L/K be a separable extension of function fields over k of degree 5. Let M be a Galois closure of L/K. Assume that $[L : K] = 5$, $\mathrm{Gal}(M/K) \cong S_5$ and that M is geometric over k. As $-1 \cdot 24 + 5 \cdot 5 = 1$, we conclude that we have to consider the map $S_5 \to S_5$, $x \mapsto x^{25}$ in Theorem 5.2. Note that T_0 consists of the conjugacy classes of (12)(345) and (12345). It is not hard to see that the preimage of T_0 is precisely the conjugacy class (12)(345) of cardinality 20. Hence we find $d(X_0) = \frac{20}{120} = \frac{1}{6} < \frac{1}{5}$.

Chapter 4

Polynomial maps on vectors spaces over a finite field

1. Introduction

The main result of [**MWW12**] is the following theorem.

Theorem 1.1. *Let l be a finite field of cardinality q and let n be in $\mathbf{Z}_{\geq 1}$. Let $f_1, \ldots, f_n \in l[x_1, \ldots, x_n]$ not all constant and consider the map $f = (f_1, \ldots, f_n)\colon l^n \to l^n$. Set $\deg(f) = \max_i \deg(f_i)$. Assume that $l^n \setminus f(l^n)$ is not empty. Then we have*

$$|l^n \setminus f(l^n)| \geq \min\Big\{\frac{n(q-1)}{\deg(f)}, q\Big\}.$$

We refer to [**MWW12**] for a nice introduction to this problem including references and historical remarks. The proof in [**MWW12**] relies on p-adic liftings of such polynomial maps. We give a proof of a stronger statement using different techniques.

Theorem 1.2. *Under the assumptions of Theorem 1.1 we have*

$$|l^n \setminus f(l^n)| \geq \frac{n(q-1)}{\deg(f)}.$$

We deduce the result from the case $n = 1$ by putting a field structure k on l^n and relate the k-degree and the l-degree. We prove the result $n = 1$ in a similar way as in [**Tur95**].

2. Degrees

Let l be a finite field of cardinality q and let V be a finite dimensional l-vector space. By $V^\vee = \mathrm{Hom}(V, l)$ we denote the dual of V. Let $v_1, \ldots, v_f$ be a basis of V. By $x_1, \ldots, x_f$ we denote its dual basis in $V^\vee$, that is, x_i is the map which sends v_j to δ_{ij}. Denote by $\mathrm{Sym}_l(V^\vee)$ the symmetric algebra of $V^\vee$ over l. We have an isomorphism $l[x_1, \ldots, x_f] \to \mathrm{Sym}_l(V^\vee)$ mapping x_i to x_i. Note that $\mathrm{Map}(V, l) = l^V$ is a commutative ring under the coordinate wise addition and multiplication and it is a l-algebra. The linear map $V^\vee \to \mathrm{Map}(V, l)$ induces by the universal property of $\mathrm{Sym}_l(V^\vee)$ a ring morphism $\varphi\colon \mathrm{Sym}_l(V^\vee) \to \mathrm{Map}(V, l)$. When choosing a basis, we have the following commutative diagram, where the second horizontal map is the evaluation map and the vertical maps are the natural isomorphisms:

$$\begin{array}{ccc} \mathrm{Sym}(V^\vee) & \xrightarrow{\varphi} & \mathrm{Map}(V, l) \\ \uparrow & & \uparrow \\ l[x_1, \ldots, x_n] & \longrightarrow & \mathrm{Map}(l^n, l). \end{array}$$

Lemma 2.1. *The map φ is surjective. After a choice of a basis as above the kernel is equal to $(x_i^q - x_i : i = 1, \ldots, f)$ and every $f \in \mathrm{Map}(V, l)$ has a unique representative $\sum_{m=(m_1,\ldots,m_n):\ 0 \le m_i \le q-1} c_m x_1^{m_1} \cdots x_n^{m_n}$ with $c_m \in l$.*

Proof. After choosing a basis, we just consider the map

$$l[x_1, \ldots, x_f] \to \mathrm{Map}(l^n, l).$$

For $c = (c_1, \ldots, c_f) \in l^f$ set

$$f_c = \prod_i (1 - (x_i - c_i)^q).$$

For $c' \in l^f$ we have $f_c(c') = \delta_{cc'}$. With these building blocks one easily shows that φ is surjective.

For $i \in \{1, 2, \ldots, f\}$ the element $x_i^q - x_i$ is in the kernel of φ. This shows that modulo the kernel any $g \in l[x_1, \ldots, x_f]$ has a representative

$$f = \sum_{m=(m_1,\ldots,m_r):\ 0 \le m_i \le q-1} c_m x_1^{m_1} \cdots x_r^{m_n}.$$

The set of such elements has cardinality q^{q^r}. As $\#\,\mathrm{Map}(V, l) = q^{q^r}$, we see that the kernel is $(x_i^q - x_i : i = 1, \ldots, r)$. Furthermore, any element has a unique representative as described above. □

Note that $\mathrm{Sym}_l(V^\vee)$ is a graded l-algebra where we say that 0 has degree $-\infty$. For $f \in \mathrm{Map}(V, l)$ we set

$$\deg_l(f) = \min\left(\deg(g) : \varphi(g) = f\right).$$

Note that $\deg_l(f_1 + f_2) \le \max(\deg_l(f_1), \deg_l(f_2))$, with equality if the degrees are different. In practice, if $f \in l[x_1, \ldots, x_n]$, then $\deg_l(f)$ is calculated as follows: for all i replace x_i^q by x_i until $\deg_{x_i}(f) < q$. Then the degree is the total degree of the remaining polynomial.

Let W be a finite dimensional l-vector space. Then we have $\mathrm{Map}(V, W) = W \otimes_l \mathrm{Map}(V, l)$. For $f \in \mathrm{Map}(V, W)$ we set

$$\deg_l(f) = \max\left(\deg_l(g \circ f) : g \in W^\vee\right).$$

If $g_1, \ldots, g_n$ is a basis of $W^\vee$, then $\deg_l(f) = \max\left(\deg_l(g_i \circ f) : i = 1, \ldots, n\right)$. This follows from the identity $\deg_l(\sum_i c_i g_i) \le \max(\deg_l(g_i))$ for $c_i \in l$. Note that the degree is bounded above by $(q-1) \cdot \dim_l(V)$.

For $i \in \mathbf{Z}_{\ge 0}$ and a subset S of $\mathrm{Sym}_l(V^\vee)$ we set

$$S_l^i = \mathrm{Span}_l(s_1 \cdot \ldots \cdot s_i : s_i \in S) \in \mathrm{Sym}_l(V^\vee).$$

Lemma 2.2. *Let $f \in \mathrm{Map}(V, W)$. For $i \in \mathbf{Z}_{\ge 0}$ one has: $\deg_f \le i \iff f \in W \otimes_l (l + V^\vee)_l^i$.*

Proof. Suppose first that $W = l$. The proof comes down to showing the following identity for $i \in \mathbf{Z}_{\ge 0}$:

$$l + V^\vee + \ldots + (V^\vee)_l^i = (l + V^\vee)_l^i.$$

The general case follows easily. □

3. Relations between degrees

Let k be a finite field and let l be a subfield of cardinality q. Set $h = [k : l]$. Let V and W be finite dimension k-vector spaces. Let $f \in \mathrm{Map}(V, W)$. In this section we will describe the relation between the k-degree and the l-degree.

Let us first assume that $W = k$. Let $v_1, \ldots, v_r$ be a basis of V over k. Let $R = k[x_1, \ldots, x_r]/(x_1^{q^h} - x_1, \ldots, x_r^{q^h} - x_r)$. We have the following diagram where all morphisms are ring morphisms. Here ψ is the map discussed before, τ is the natural isomorphism, $\overline{\varphi}$ is the isomorphism discussed before, and σ is the isomorphism, depending on the basis, discussed above.

$$\begin{array}{ccc} k \otimes_l \mathrm{Map}(V,l) & \xrightarrow{\quad\tau\quad} & \mathrm{Map}(V,k) \\ \uparrow{\scriptstyle \psi} & & \uparrow{\scriptstyle \overline{\varphi}} \\ k \otimes_l \mathrm{Sym}_l(\mathrm{Hom}_l(V,l)) & & \mathrm{Sym}_k(\mathrm{Hom}_k(V,k))/\ker(\varphi) \xrightarrow{\sigma} R. \end{array}$$

Consider the ring morphism $\rho = \sigma \circ \overline{\varphi}^{-1} \circ \tau \circ \psi \colon k \otimes_l \mathrm{Sym}_l(\mathrm{Hom}_l(V,l)) \to R$. Lemma 2.2 suggest that to compare degrees, we need to find

$$\rho(k \otimes_l (l + \mathrm{Hom}_l(V,l))_l^i).$$

The following lemma says that it is enough to find $k + k \otimes_l \mathrm{Hom}_l(V,l)$.

Lemma 3.1. *For $i \in \mathbf{Z}_{\geq 0}$ we have the following equality in $k \otimes_l \mathrm{Sym}_l(V)$:*

$$k \otimes_l (l + \mathrm{Hom}_l(V,l))_l^i = (k + k \otimes_l \mathrm{Hom}_l(V,l))_k^i .$$

Proof. Both are k-vector spaces and the inclusions are not hard to see. □

The following lemma identifies $k + k \otimes_l \mathrm{Hom}_l(V,l)$.

Lemma 3.2. *One has*

$$\rho(k + k \otimes_l \mathrm{Hom}_l(V,l)) = \mathrm{Span}_k \left(\{ x_j^{q^s} : 1 \leq j \leq r,\ 0 \leq s < h \} \sqcup \{1\} \right).$$

Proof. Note that $\tau \circ \phi(k + k \otimes_l \mathrm{Hom}_l(V,l)) = k \oplus \mathrm{Hom}_l(V,k) \subseteq \mathrm{Map}(V,k)$. Note that

$$\sigma^{-1} \left(\mathrm{Span}_k \left(\{ x_j^{q^s} : 1 \leq j \leq r,\ 0 \leq s < h \} \right) \right) \subseteq \mathrm{Hom}_l(V,k).$$

As both sets have dimension $\dim_l(V) = r \cdot h$ over k, the result follows. □

For $m, n \in \mathbf{Z}_{\geq 1}$ we set $s_m(n)$ to be the sum of the digits of n in base m.

Lemma 3.3. *Let $m \in \mathbf{Z}_{\geq 2}$ and $n, n' \in \mathbf{Z}_{\geq 0}$. Then the following hold:*

i. $s_m(n + n') \leq s_m(n) + s_m(n')$;
ii. *Suppose $n = \sum_i c_i m^i$, $c_i \geq 0$. Then we have $\sum_i c_i \geq s_m(n)$ with equality iff for all i we have $c_i < m$.*

Proof. i. This is well-known and left to the reader.

ii. We give a proof by induction on n. For $n = 0$ the result is correct. Suppose first that $n = c_s m^s$ and assume that $c_s \geq m$. Then we have $n = (c_s - m)m^s + m^{s+1}$. By induction and i we have

$$c_s > c_s - m + 1 \geq s_m((c_s - m)m^s) + s_m(m^{s+1}) \geq s_m(c_s m^s).$$

In general, using i, we find

$$\sum_i c_i \geq \sum_i s_m(c_i m^i) \geq s_m(n).$$

Also, one easily sees that one has equality iff all c_i are smaller than m. □

Proposition 3.4. *Let $f \in k[x_1, \ldots, x_r]$ nonzero with the degree in all x_i of all the monomials less than q^h. Write $f = \sum_{s=(s_1,\ldots,s_r)} c_s x_1^{s_1} \cdots x_r^{s_r}$. Then the l-degree of $\tau^{-1} \circ \overline{\varphi}(\overline{f}) \in k \otimes_l \mathrm{Map}(V, l)$ is equal to*

$$\max\{s_q(s_1) + \ldots + s_q(s_r) : s = (s_1, \ldots, s_r) \text{ s.t. } c_s \neq 0\}.$$

Proof. Put $g = \tau^{-1} \circ \overline{\varphi} \circ \sigma^{-1}(\overline{f})$. From Lemma 2.2, Lemma 3.1 and Lemma 3.2 we obtain the following. Let $i \in \mathbf{Z}_{\geq 0}$. Then $\deg_l(g) \leq i$ iff

$$\begin{aligned} g \in \rho(k \otimes_l (l + \mathrm{Hom}_l(V, l))_l^i) &= \rho((k + k \otimes_l \mathrm{Hom}_l(V, l))_k^i) \\ &= \left(\mathrm{Span}_k\left(\{x_j^{q^s} : 1 \leq j \leq r,\ 0 \leq s < h\} \sqcup \{1\}\right)\right)_k^i. \end{aligned}$$

The result follows from Lemma 3.3. □

The case for a general W just follows by decomposing W into a direct sum of copies of k and then taking the maximum of the corresponding degrees.

4. Proof of main theorem

Lemma 4.1. *Let $m, q, h \in \mathbf{Z}_{>0}$ and suppose that $q^h - 1 | m$. Then we have: $s_q(m) \geq h(q-1)$.*

Proof. We do a proof by induction on m.

Suppose that $m < q^h$. Then $m = q^h - 1$ and we have $s_q(m) = h(q-1)$.

Suppose $m \geq q^h$. Write $m = m_0 q^h + m_1$ with $0 \leq m_1 < q^h$ and $m_0 \geq 1$. We claim that $q^h - 1 | m_0 + m_1$. Note that $m_0 + m_1 \equiv m_0 q^h + m_1 \equiv 0 \pmod{q^h - 1}$. Then by induction we find

$$s_q(m) = s_q(m_0) + s_q(m_1) \geq s_q(m_0 + m_1) \geq h(q-1).$$

□

Lemma 4.2. *Let k be a finite field of cardinality q'. Let $R = k[X_a : a \in k]$ and consider the action of k^* on R given by*

$$\begin{aligned} k^* &\mapsto \mathrm{Aut}_{k-\mathrm{alg}}(R) \\ c &\mapsto (X_a \mapsto X_{ca}). \end{aligned}$$

Let $F \in R$ fixed by the action of k^* with $F(0, \ldots, 0) = 0$ and such that the degree of no monomial of F is a multiple of $q' - 1$. Then for $w = (a)_a \in k^k$ we have $F(w) = 0$.

PROOF. We may assume that F is homogeneous with $d = \deg(F)$ which is not a multiple of $q' - 1$. Take $\lambda \in k^*$ a generator of the cyclic group. As F is fixed by k^* we find:

$$F(w) = F(\lambda w) = \lambda^d F(w).$$

As $\lambda^d \neq 1$, we have $F(w) = 0$ and the result follows. □

Finally we can state and prove a stronger version of Theorem 1.2.

Theorem 4.3. *Let k be a finite field. Let $l \subseteq k$ be a subfield with $[k : l] = h$ and let V be a finite dimensional k-vector space. Let $f \in \mathrm{Map}(V, V)$ be a non-constant and non-surjective map. Then f misses at least*

$$\frac{\dim_k(V) \cdot h \cdot (\#l - 1)}{\deg_l(f)}$$

values.

PROOF. Set $\#l = q$. Put a k-linear multiplication on V such that it becomes a field. This allows us reduce to the case where $V = k$. Assume $V = k$. After shifting we may assume $f(0) = 0$. Put an ordering $\leq$ on k. In $k[T]$ we have

$$\prod_{a \in k} (1 - f(a)T) = 1 - \sum_a f(a)T + \sum_{a<b} f(a)f(b)T^2 - \ldots = \sum_i a_i T^i.$$

For $1 \leq i < \frac{h(q-1)}{\deg_l(f)}$ we claim that $a_i = 0$. Put $f_0 \in k[x]$ a polynomial of degree at most $q^h - 1$ inducing $f \colon k \to k$. Consider $g_i = \prod_{a_1 < \ldots < a_i} f_0(X_{a_1}) \cdots f_0(X_{a_i})$ in $k[X_a : a \in k]$, which is fixed by k^*. We have a map

$$\varphi \colon k[X_a : a \in k] \to \mathrm{Map}(k^k, k).$$

Proposition 3.4 gives us that $\deg_l(\varphi(g_i)) = i \deg_l(f) < h(q-1)$. We claim that there is no monomial in g_i with degree a multiple of $q^h - 1$. Indeed, suppose that there is a monomial $cX_{a_1}^{r_1} \cdots X_{a_i}^{r_i}$ $(c \neq 0)$ in g_i (note that not all r_i are zero) and suppose that $q^h - 1 | \sum_i r_i$. Then by Lemma 4.1 and Proposition 3.4 we have

$$h(q-1) \leq s_q\Big(\sum_j r_j\Big) \leq \sum_j s_q(r_j) \leq i \cdot \deg_l(f) < h(q-1),$$

contradiction. Hence we can apply Lemma 4.2 to conclude that $a_i = 0$.

Hence we conclude

$$\prod_{a \in k} (1 - f(a)T) \equiv 1 \pmod{T^{\lceil \frac{h(q-1)}{\deg_l(f)} \rceil}}.$$

Similarly, for the identity function of l-degree 1, we conclude

$$\prod_{a \in k} (1 - aT) \equiv 1 \pmod{T^{\lceil \frac{h(q-1)}{\deg_l(f)} \rceil}}.$$

Combining this gives:

$$\begin{aligned}\prod_{a\in k\setminus f(k)}(1-aT) &= \frac{\prod_{a\in k}(1-aT)}{\prod_{b\in f(k)}(1-bT)}\\ &\equiv \frac{\prod_{a\in k}(1-aT)}{\prod_{b\in f(k)}(1-bT)}\cdot\prod_{c\in k}(1-f(c)T) \pmod{T^{\lceil\frac{h(q-1)}{\deg_l(f)}\rceil}}\\ &\equiv \prod_{b\in f(k)}(1-bT)^{\#f^{-1}(b)-1} \pmod{T^{\lceil\frac{h(q-1)}{\deg_l(f)}\rceil}}.\end{aligned}$$

Note that the polynomials $\prod_{a\in k\setminus f(k)}(1-aT)$ and $\prod_{b\in f(k)}(1-bT)^{\#f^{-1}(b)-1}$ have degree bounded by $s = k\setminus f(k)$ and are different since $s \geq 1$. But this implies that $s \geq \frac{h(q-1)}{\deg_l(f)}$. □

Remark 4.4. Different l in Theorem 4.3 may give different lower bounds.

5. Examples

In this section we will give examples which meet the bound from Theorem 1.2.

Example 5.1 ($n = \deg(f)$)**.** Let l be a finite field of cardinality q. In this example we will show that for $n, d \in \mathbf{Z}_{\geq 2}$ there are functions $f_1, \ldots, f_n \in l[x_1, \ldots, x_n]$ such that the maximum of the degrees is equal to d such that the induced map $f\colon l^n \to l^n$ satisfies $|l^n \setminus f(l^n)| = \frac{n(q-1)}{d} = q-1$. For $i = 1, \ldots, n-1$ set $f_i = x_i$. Let l_{n-1} be the unique extension of l of degree $n-1$. Let $v_1, \ldots, v_{n-1}$ be a basis of l_{n-1} over l. Then $g = \mathrm{Norm}_{l_{n-1}/l}(x_1v_1 + \ldots + x_{n-1}v_{n-1})$ is a homogeneous polynomial of degree $n-1$ in $x_1, \ldots, x_{n-1}$. Put $f_n = x_n \cdot g$. As the norm of a nonzero element is nonzero, one easily sees that $l^n \setminus f(l^n) = \{0\} \times \ldots \{0\} \times l^*$ has cardinality $q-1$.

Example 5.2 ($n = \frac{\deg(f)}{q-1}$)**.** Let l be a finite field and let $n \in \mathbf{Z}_{\geq 1}$. Let $f_1, \ldots, f_n \in l[x_1, \ldots, x_n]$ such that the combined map $f\colon l^n \to l^n$ satisfies $|l^n \setminus f(l^n)| = 1$ (Lemma 2.1). From Theorem 1.2 and the upper bound $n(q-1)$ for the degree we deduce that $\deg(f) = n(q-1)$.

Chapter 5

Subset sum problem

In this chapter we will give an application of character theory of finite abelian groups. This chapter has been published ([**Kos13**]). We have kept the article in its original form. This should make it readable without having read any other part of this thesis.

1. Introduction

In this article we fix an additively written finite abelian group G of size n. For a subset $D \subseteq G$, $g \in G$ and $i \in \mathbf{Z}_{\geq 0}$ we put

$$N(D, i, g) = \#\Big\{S \subseteq D : \#S = i,\ \sum_{s \in S} s = g\Big\},$$

the number of subsets of D of size i which sum up to g. Calculating these $N(D, i, g)$ in general is a hard problem, which comes up in coding theory and cryptography (see [**LW08**] and [**LW12**] for references).

In the case that D has more structure, one can sometimes find explicit formulas for the numbers $N(D, i, g)$. In this article, we will first prove and slightly improve an explicit formula for $N(G, i, g)$, due to Li and Wan in [**LW08**] and [**LW12**]. Before we can state the theorem, we need a bit of notation.

We let $\exp(G)$ be the exponent of G. For $g \in G$ we define

$$e(g) = \max\{d : d | \exp(G),\ g \in dG\}.$$

For an integer d let $G[d] = \{h \in G : dh = 0\}$, the d-torsion of G. We let μ be the Möbius function.

Theorem 1.1. *Let G be an abelian group of size n and let $g \in G$, $i \in \mathbf{Z}$ with $0 \leq i \leq n$. Then we have:*

$$N(G, i, g) = \frac{1}{n} \sum_{s | \gcd(\exp(G), i)} (-1)^{i + i/s} \binom{n/s}{i/s} \sum_{d | \gcd(e(g), s)} \mu\Big(\frac{s}{d}\Big) \#G[d].$$

The above theorem slightly improves [**LW12**, Theorem 1.1]. The main difference between this article and [**LW12**] is the way one proves this formula. In [**LW12**], the authors use a sieving technique, whereas our proof is based on the use of character theory of finite abelian groups.

From the above formula it is not obvious to see if $N(G, i, g) > 0$. We have the following theorem.

Theorem 1.2. *Let G be an abelian group of size n and let $i \in \mathbf{Z}$ with $0 \leq i \leq n$. Then $N(G, i, g) = 0$ if and only if one of the following holds:*

i. *$i = 0$ and $g \neq 0$;*
ii. *$i = 2$, $\exp(G) = 2$ and $g = 0$;*
iii. *$i = n - 2 \geq 2$, $\exp(G) = 2$ and $g = 0$;*
iv. *$i = n$ and $g \neq \sum_{h \in G[2]} h$.*

We will also prove a formula for $N(G \setminus \{0\}, i, g)$. This simplifies to the formula in [**LW08**, Theorem 1.2] if the exponent of G is prime.

Theorem 1.3. *Let G be an abelian group of size n and let $g \in G$, $i \in \mathbf{Z}$ with $0 \leq i \leq n - 1$. Then we have:*

$$N(G \setminus \{0\}, i, g) = \frac{1}{n} \sum_{s \mid \exp(G)} (-1)^{i + \lfloor i/s \rfloor} \binom{n/s - 1}{\lfloor i/s \rfloor} \sum_{d \mid \gcd(s, e(g))} \mu\Big(\frac{s}{d}\Big) \#G[d].$$

2. Proofs of the theorems

Let G be a finite abelian group of size n. We put $\hat{G} = \mathrm{Hom}(G, \mathbf{C}^*)$, the group of characters of G, and we denote its unit element by 1. This is a finite abelian group which is isomorphic to G. A good reference for character theory of finite abelian groups is [**Ser73**, Chapter 6.1]. We can extend a character χ to a $\mathbf{C}$-algebra morphism $\chi \colon \mathbf{C}[G] \to \mathbf{C}$ on the group ring $\mathbf{C}[G]$. For a character χ we put $\overline{\chi}$ for the conjugate character, which for all $g \in G$ satisfies $\overline{\chi}(g) = \overline{\chi(g)} = \chi(-g)$.

Lemma 2.1. *Let $\alpha = \sum_{g \in G} \alpha_g g \in \mathbf{C}[G]$. Then we have $\alpha_g = \frac{1}{n} \sum_{\chi \in \hat{G}} \overline{\chi}(g) \chi(\alpha)$.*

Proof. This follows from [**Ser73**, Chapter 6, corollary to Proposition 4]. □

Lemma 2.2. *Let $m \in \mathbf{Z}_{\geq 1}$ and $g \in G$. Then the following holds:*

$$\sum_{\chi \in \hat{G} \colon \chi^m = 1} \chi(g) = \begin{cases} \#G[m] & \text{if } g \in mG \\ 0 & \text{if } g \notin mG. \end{cases}$$

Proof. If $\chi^m = 1$, we know that the character factors through G/mG. A character on G/mG induces such a character on G. The rest follows from [**Ser73**, Chapter 6, Proposition 4]. □

Lemma 2.3. *Let $\chi \in \hat{G}$ be a character and m its order. Then we have*

$$\prod_{\sigma \in G} (1 - \chi(\sigma) Y) = (1 - Y^m)^{n/m}.$$

Proof. For an m-th root of unity $\zeta_m \in \mathbf{C}$ the identity $\prod_{i=0}^{m-1} (1 - \zeta_m^i Y) = 1 - Y^m$ holds. We consider n/m of such products. □

Lemma 2.4. *Let $g \in G$. The number $e(g)$ is equal to $\mathrm{lcm}\{d : d \mid \exp(G),\ g \in dG\}$. For $d \mid \exp(G)$ we have $g \in dG$ if and only if $d \mid e(g)$.*

PROOF. For the first statement, notice that if $g = d_1 g_1 = d_2 g_2$ with $g_1, g_2 \in G$ and $d_1, d_2 \in \mathbf{Z}$ with $\gcd(d_1, d_2) = 1$, then there are integers n_1, n_2 with $1 = n_1 d_1 + n_2 d_2$. Hence we have

$$g = (n_1 d_1 + n_2 d_2) g = d_1 d_2 (n_1 g_2 + n_2 g_1).$$

The second statement then follows directly. □

We will now prove the main theorem.

PROOF OF THEOREM 1.1. We make the following observation:

$$\sum_{i=0}^{n} \sum_{g \in G} N(G, i, g) g X^i = \prod_{\sigma \in G} (1 + \sigma X) \in \mathbf{C}[G][X].$$

Fix $g \in G$. Lemma 2.1 and the substitution $Y = -X$ give

$$\sum_{i=0}^{n} N(G, i, g)(-Y)^i = \frac{1}{n} \sum_{\chi \in \hat{G}} \overline{\chi}(g) \prod_{\sigma \in G} (1 - \chi(\sigma) Y).$$

Define $f \colon \mathbf{Z}_{\geq 0} \to \mathbf{C}$ by

$$f(s) = \sum_{\chi \in \hat{G} \colon \chi^s = 1} \overline{\chi}(g) = \sum_{d \mid s} \sum_{\chi \in \hat{G} \colon \operatorname{ord}(\chi) = d} \overline{\chi}(g).$$

By Lemma 2.2 we have $f(s) = \delta_{g \in sG} \# G[s]$. Using the Möbius inversion formula we find for $s \in \mathbf{Z}_{\geq 0}$

$$\sum_{\chi \in \hat{G} \colon \operatorname{ord}(\chi) = s} \overline{\chi}(g) = \sum_{d \mid s} \mu(s/d) \delta_{g \in dG} \# G[d].$$

Assume that $s \mid \exp(G)$. As $g \in sG$ if and only if $s \mid e(g)$ by Lemma 2.4, we find

$$\sum_{\chi \in \hat{G} \colon \operatorname{ord}(\chi) = s} \overline{\chi}(g) = \sum_{d \mid \gcd(s, e(g))} \mu(s/d) \# G[d].$$

Using Lemma 2.3 and the previous calculation, we obtain

$$\begin{aligned} \sum_{i=0}^{n} N(G, i, g)(-Y)^i &= \frac{1}{n} \sum_{s \mid \exp(G)} \sum_{\chi \in \hat{G} : \operatorname{ord}(\chi) = s} \overline{\chi}(g) \prod_{\sigma \in G} (1 - \chi(\sigma) Y) \\ &= \frac{1}{n} \sum_{s \mid \exp(G)} \sum_{d \mid \gcd(s, e(g))} \mu(s/d) \# G[d] (1 - Y^s)^{n/s}. \end{aligned} \tag{2}$$

We single out $N(G, i, g)$ and get:

$$(-1)^i N(G, i, g) = \frac{1}{n} \sum_{s \mid \gcd(\exp(G), i)} \sum_{d \mid \gcd(s, e(g))} \mu(s/d) \# G[d] (-1)^{i/s} \binom{n/s}{i/s}.$$

Hence we find

$$N(G, i, g) = \frac{1}{n} \sum_{s \mid \gcd(\exp(G), i)} (-1)^{i + i/s} \binom{n/s}{i/s} \sum_{d \mid \gcd(s, e(g))} \mu(s/d) \# G[d].$$

This finishes the proof of Theorem 1.1.

□

PROOF OF THEOREM 1.3. We have the following identity:

$$\sum_{i=0}^{n-1} \sum_{g \in G} N(G \setminus \{0\}, i, g) g X^i = \prod_{\sigma \in G, \sigma \neq 0} (1 + \sigma X) \in \mathbf{C}[G][X].$$

As all characters have value 1 on 0, we deduce the next result from Equation (2) by dividing by $1 - Y$:

$$\sum_{i=0}^{n-1} N(G \setminus \{0\}, i, g)(-Y)^i =$$

$$\frac{1}{n} \sum_{s \mid \exp(G)} \sum_{d \mid \gcd(s, e(g))} \mu(s/d) \#G[d] (1 - Y^s)^{n/s-1} (1 + Y + \ldots + Y^{s-1}).$$

Comparing the coefficients gives the result. □

We will now independently prove Theorem 1.2.

PROOF OF THEOREM 1.2. Let $g \in G$ and $0 \leq i \leq n$. If $i \in \{0, 1\}$, then the result is obvious. If $i = 2$, then any nonzero element g can be written as $g = g + 0$, and 0 cannot be written as the sum of two distinct elements if and only if $\exp(G) = 2$.

By considering complements we obtain

$$N(G, i, g) = N(G, n - i, \sum_{h \in G} h - g) = N(G, n - i, \sum_{h \in G[2]} h - g).$$

Note that if $\exp(G) = 2$ and $\#G \geq 4$, that $\sum_{h \in G} h = 0$. This handles the case $i = n - 2 \geq 4$. From now on assume that $i \leq \frac{n}{2}$.

Assume that $i \geq 3$. Take a subset $S' \subset G$ of size $i - 3$ and set $r = \sum_{h \in S'} h$. If n is even, take $s \in G \setminus S'$ such that $g - r - s \notin 2G$; such an s exists because $[G : 2G] \geq 2$ and $\#(G \setminus S') \geq \frac{n}{2} + 3 > \frac{n}{2}$. If n is odd, take $s \in G \setminus S'$. Let $T = G \setminus (S' \cup \{s\})$. There are at least 4 elements in $(g - r - s - T) \cap T$ and hence there are $t, t' \in T$ with $t = g - r - s - t'$. If $t = t'$ and n is even, then $g - r - s \in 2G$, a contradiction. If n is odd, then there is at most one t with $2t = g - r - s$. Hence we can write g as a sum of i distinct elements. □

Chapter 6

Shape parameter and some applications

1. Introduction

This chapter contains some prerequisites for the next chapter. Throughout this chapter let G be a finite abelian group, written multiplicatively.

Let $\mathbf{C}[G]$ be the group ring of G over $\mathbf{C}$. For $\chi \in G^\vee = \mathrm{Hom}(G, \mathbf{C}^*)$ and $f = \sum_{g\in G} c_g g \in \mathbf{C}[G]$ where $c_g \in \mathbf{C}$ we set

$$f_\chi = \sum_{g\in G} c_g \chi(g^{-1}).$$

For a subset $S \subseteq G$ we set $\mathbf{C}[S] = \{\sum_{s\in S} c_s s : c_s \in \mathbf{C}\} \subseteq \mathbf{C}[G]$, which is a $\mathbf{C}$-vector space. Let χ_0 be the identity element of $G^\vee$. We define the shape parameter of S, which we denote by $\mathrm{sh}_G(S)$, as follows:

$$\mathrm{sh}_G(S) = \frac{\#S}{\#G} \cdot \inf_{f\in\mathbf{C}[S]:f_{\chi_0}\neq 0} \frac{\sum_{\chi\in G^\vee} |f_\chi|}{|f_{\chi_0}|}.$$

In the first part of this chapter, we discuss some algebraic and analytic properties of the shape parameter. For example, $\#S \geq \mathrm{sh}_G(S) \geq 1$ with $\mathrm{sh}_G(S) = 1$ if and only if S is a coset of a subgroup (Proposition 3.3). We also give a large class of subsets with shape bounded by 2 (Lemma 3.6). These subsets are called 'intervals' and will be used in the next chapter to obtain generators of a certain Picard group. Intuitively a subset should have a small parameter if and only if it has a lot of structure with respect to the group structure.

In the last part, we discuss two applications of the shape parameter, which introduce the techniques used in the next chapter (Proposition 4.2 and Proposition 4.9).

Theorem 1.1. *Let k be a finite field of cardinality q. Let $S \subseteq k$ be nonempty with $\sqrt{q} \cdot \mathrm{sh}_{k^+}(S) < \#S$. Then $S \cap k^*$ generates k^* multiplicatively.*

Theorem 1.2. *Let k be a finite field of cardinality q. Let $D = \{l \text{ prime} : l|q-1\}$. Let $S \subseteq k$ be a subset such that*

$$\#S \geq \sqrt{q} \cdot 2^{\#D}\, \mathrm{sh}_{k^+}(S).$$

Then S contains a primitive root of k^*.

2. Fourier transform

Let $G^\vee = \mathrm{Hom}(G, \mathbf{C}^*)$ be the *character group* of G. We denote its unit element by χ_0. For $\chi \in G^\vee$ we denote by $\overline{\chi} \in G^\vee$ the character which for all $g \in G$ satisfies $\overline{\chi}(g) = \chi(g^{-1}) = \chi(g)^{-1}$.

Let $\mathbf{C}[G]$ denote the *group ring* of G over $\mathbf{C}$. This ring has an involution $^-$ defined by

$$\begin{aligned} {}^-\colon \mathbf{C}[G] &\to \mathbf{C}[G] \\ \sum_{g\in G} c_g g &\mapsto \sum_{g\in G} \overline{c_g} g^{-1}. \end{aligned}$$

As $\mathbf{C}[G]$ is a finite $\mathbf{C}$-algebra, we have a natural *trace map* $\mathrm{tr}_{\mathbf{C}[G]/\mathbf{C}}\colon \mathbf{C}[G] \to \mathbf{C}$. More explicitly, we have

$$\mathrm{tr}_{\mathbf{C}[G]/\mathbf{C}}(\sum_{g\in G} c_g g) = \#G \cdot c_1.$$

For $a = \sum_{g\in G} c_g g \in \mathbf{C}[G]$ we set

$$|a|^2 = \mathrm{tr}_{\mathbf{C}[G]/\mathbf{C}}(a\overline{a}) = \#G \cdot \sum_{g\in G} |c_g|^2.$$

Endow $\mathbf{C}^{G^\vee}$ with the structure of a $\mathbf{C}$-algebra where the multiplication and addition are componentwise. We have a ring involution $^-\colon \mathbf{C}^{G^\vee} \to \mathbf{C}^{G^\vee}, (c_\chi)_{\chi\in G^\vee} \mapsto (\overline{c_\chi})_{\chi\in G^\vee}$. The trace map $\mathrm{tr}_{\mathbf{C}^{G^\vee}/\mathbf{C}}\colon \mathbf{C}^{G^\vee} \to \mathbf{C}$ satisfies

$$\mathrm{tr}_{\mathbf{C}^{G^\vee}/\mathbf{C}}((c_\chi)_{\chi\in G^\vee}) = \sum_{\chi\in G^\vee} c_\chi$$

Similarly, for $b = (c_\chi)_{\chi\in G^\vee}$ we set

$$|b|^2 = \mathrm{tr}_{\mathbf{C}^{G^\vee}/\mathbf{C}}(b\overline{b}) = \sum_{\chi\in G^\vee} |c_\chi|^2.$$

We have an identification of sets $G^\vee = \mathrm{Hom}_{\mathbf{C}-\mathrm{alg}}(\mathbf{C}[G], \mathbf{C})$ given by

$$\chi \mapsto \left(\sum_{g\in G} c_g g \mapsto \sum_{g\in G} c_g \chi(g) \right).$$

For $f \in \mathbf{C}[G]$ and $\chi \in G^\vee$ we define

$$f_\chi = \overline{\chi}(f).$$

Lemma 2.1. *For $\chi \in G^\vee$ and $h \in G$ one has*

$$\sum_{g\in G} \chi(g) = \begin{cases} 0 & \text{if } \chi \neq \chi_0 \\ \#G & \text{if } \chi = \chi_0. \end{cases}$$

and

$$\sum_{\chi'\in G^\vee} \chi'(h) = \begin{cases} 0 & \text{if } h \neq 1 \\ \#G & \text{if } h = 1. \end{cases}$$

PROOF. For the first statement, the case $\chi = \chi_0$ is obvious. If $\chi \neq \chi_0$, then take $g \in G$ with $\chi(g) \neq 1$. For the sum S on the left one has $\chi(g)S = S$. Hence $S = 0$. The second statement follows from the first one from the canonical isomorphism $(G^\vee)^\vee = G$. □

With these conventions and definitions we can state the following *Fourier transform* statement.

Proposition 2.2 (Fourier transform)**.** *The map*

$$\begin{aligned} F_G \colon \mathbf{C}[G] &\to \mathbf{C}^{G^\vee} \\ f &\mapsto (f_\chi)_{\chi \in G^\vee} \end{aligned}$$

is an isomorphism of $\mathbf{C}$*-algebras. Its inverse is given by*

$$((c_\chi)_{\chi \in G^\vee}) \mapsto \frac{1}{\#G} \sum_{g \in G} \sum_{\chi \in G^\vee} c_\chi \chi(g) g.$$

One has:

i. *For a morphism* $s \colon G \to H$ *of finite abelian groups we have a natural commutative diagram of* $\mathbf{C}$*-algebras*

$$\begin{array}{ccc} \mathbf{C}[G] & \xrightarrow{F_G} & \mathbf{C}^{G^\vee} \\ \downarrow{\scriptstyle s_*} & & \downarrow{\scriptstyle s_*} \\ \mathbf{C}[H] & \xrightarrow{F_H} & \mathbf{C}^{H^\vee}. \end{array}$$

where

$$s_*\Big(\sum_{g \in G} c_g g\Big) = \sum_{g \in G} c_g s(g)$$

and

$$s_*((c_\chi)_{\chi \in G^\vee}) = (c_{\tau \circ s})_{\tau \in H^\vee}.$$

Furthermore, we have the following commutative diagram of $\mathbf{C}$*-vector spaces*

$$\begin{array}{ccc} \mathbf{C}[H] & \xrightarrow{F_H} & \mathbf{C}^{H^\vee} \\ \downarrow{\scriptstyle s^*} & & \downarrow{\scriptstyle s^*} \\ \mathbf{C}[G] & \xrightarrow{F_G} & \mathbf{C}^{G^\vee} \end{array}$$

where

$$s^*\Big(\sum_{h \in H} c_h h\Big) = \sum_{g \in G} c_{s(g)} g$$

and

$$s^*((c_\tau)_{\tau \in H^\vee}) = \frac{\#G}{\#H}\Big(\sum_{\tau \in H^\vee \colon \tau \circ s = \chi} c_\tau\Big)_{\chi \in G^\vee}.$$

ii. *If $G = G_1 \times G_2$, then we have a commutative diagram of $\mathbf{C}$-algebras where all maps are isomorphisms as follows:*

$$\begin{array}{ccc} \mathbf{C}[G] & \xrightarrow{\sim} & \mathbf{C}[G_1] \otimes_{\mathbf{C}} \mathbf{C}[G_2] \\ \downarrow{\scriptstyle F_G} & & \downarrow{\scriptstyle F_{G_1} \otimes F_{G_2}} \\ \mathbf{C}^{G^\vee} & \xrightarrow{\sim} & \mathbf{C}^{G_1^\vee} \otimes_{\mathbf{C}} \mathbf{C}^{G_2^\vee}. \end{array}$$

iii. *We have a commutative diagram of rings*

$$\begin{array}{ccc} \mathbf{C}[G] & \xrightarrow{F_G} & \mathbf{C}^{G^\vee} \\ \downarrow{\scriptstyle -} & & \downarrow{\scriptstyle -} \\ \mathbf{C}[G] & \xrightarrow{F_G} & \mathbf{C}^{G^\vee}. \end{array}$$

iv. *For $f \in \mathbf{C}[G]$ we have $|f|^2 = |F_G(f)|^2$.*

Proof. We will use Lemma 2.1 without referring to it.

The map F_G is a $\mathbf{C}$-algebra morphism, because its projections are $\mathbf{C}$-algebra morphisms. The well-known independence of characters theorem of Artin and Dedekind shows that the map is injective, and as $\#G = \#G^\vee$ we have an isomorphism of $\mathbf{C}$-algebras. That our formula T for the inverse is correct, follows from the following identity for $g \in G$:

$$T \circ F_G(g) = \frac{1}{\#G} \sum_{h \in G} \sum_{\chi \in G^\vee} \chi(g^{-1}h)h = g.$$

i. For the first diagram, the maps are as follows for $g \in G$:

$$\begin{array}{ccc} g & \longmapsto & (\overline{\chi}(g))_{\chi \in G^\vee} \\ \downarrow & & \downarrow \\ s(g) & \longmapsto & (\overline{\tau(s(g))})_{\tau \in H^\vee}. \end{array}$$

For the second diagram, it is easy to see that all morphisms are morphisms of $\mathbf{C}[G]$-modules.

We split up the proof in two cases, namely one where we assume that s is surjective, and one where s is assumed to be injective. As a morphism is a composition of a surjective one and an injective one, this will prove the claim. Assume that s is surjective

and let $h \in H$ and assume that $s(g_0) = h$. Then we have

$$\begin{aligned} F_G \circ s^*(h) &= \Big(\sum_{g\in G:\ s(g)=h} \overline{\chi}(g) \Big)_{\chi\in G^\vee} \\ &= \frac{\#G}{\#H} \left(\delta_{\chi|_{\ker s}=\chi_0} \cdot \overline{\chi}(g_0)\right)_{\chi\in G^\vee} \\ &= \frac{\#G}{\#H} \Big(\sum_{\tau\in H^\vee:\ \tau\circ s=\chi} \overline{\chi}(g_0) \Big)_{\chi\in G^\vee} \\ &= \frac{\#G}{\#H} \Big(\sum_{\tau\in H^\vee:\ \tau\circ s=\chi} \overline{\tau}(h) \Big)_{\chi\in G^\vee} \\ &= s^*((\overline{\tau}(h))_{\tau\in H^\vee}) \\ &= s^* \circ F_H(h). \end{aligned}$$

Assume that $G \to H$ is injective, view G as a subgroup of H. Let $\chi \in G^\vee$ and $h \in H$. Then we have exact sequence $0 \to (H/G)^\vee \to H^\vee \to G^\vee \to 0$. Take $\tau_1 \in H^\vee$ which maps to χ. Then one has

$$\begin{aligned} \sum_{\tau\in H^\vee:\tau\circ s=\chi} \overline{\tau}(h) &= \overline{\tau_1}(h) \sum_{\tau\in (H/G)^\vee} \overline{\tau}(h) \\ &= \begin{cases} 0 & \text{if } h \notin G \\ \#(H/G)\cdot\overline{\chi}(\overline{h}) & \text{if } h \in G. \end{cases} \end{aligned}$$

Hence we obtain:

$$\begin{aligned} F_G \circ s^*(h) &= (\sum_{g\in G:\ s(g)=h} \overline{\chi}(g))_{\chi\in G^\vee} \\ &= \delta_{h\in G}(\overline{\chi}(h))_{\chi\in G^\vee} \\ &= \frac{\#G}{\#H} \Big(\sum_{\tau\in H^\vee:\ \tau\circ s=\chi} \overline{\tau}(h) \Big)_{\chi\in G^\vee} \\ &= s^*((\overline{\chi}(h))_{\chi\in H^\vee}) \\ &= s^* \circ F_H(h). \end{aligned}$$

ii. We have natural inclusions $G_1 \to G$ and $G_2 \to G$. This induces maps $\mathbf{C}[G_i] \to \mathbf{C}[G]$ and by the definition of the tensor product we have a morphism $\mathbf{C}[G_1]\otimes_{\mathbf{C}}\mathbf{C}[G_2] \to \mathbf{C}[G]$ which is an isomorphism since it is surjective and since the dimensions agree. Similarly, we obtain an isomorphism $\mathbf{C}^{G_1^\vee} \otimes_{\mathbf{C}} \mathbf{C}^{G_2^\vee} \to \mathbf{C}^{G^\vee}$. As all maps are $\mathbf{C}$-linear, it is enough to check that a given g maps to the right element. One then checks easily that the maps go as follows for $g = (g_1, g_2) \in G$:

$$\begin{array}{ccc} g = (g_1, g_2) & \longmapsto & g_1 \otimes g_2 \\ \downarrow & & \downarrow \\ (\overline{\chi}(g))_{\chi\in G^\vee} & \longmapsto & (\overline{\tau}(g_1))_{\tau\in G_1^\vee} \otimes ((\overline{\tau'}(g_2))_{\tau'\in G_2^\vee}. \end{array}$$

iii. The maps are as follows for $c_g \in \mathbf{C}$ and $g \in G$:

$$\begin{array}{ccc} c_g g & \longmapsto & (c_g \overline{\chi}(g))_{\chi \in G^\vee} \\ \downarrow & & \downarrow \\ \overline{c_g} g^{-1} & \longmapsto & (\overline{c_g}\chi(g))_{\chi \in G^\vee}. \end{array}$$

iv. One has for $f \in \mathbf{C}[G]$

$$\begin{aligned} |f|^2 &= \mathrm{tr}_{\mathbf{C}[G]/\mathbf{C}}(f\overline{f}) = \mathrm{tr}_{\mathbf{C}^{G^\vee}/\mathbf{C}}(F_G(f\overline{f})) = \mathrm{tr}_{\mathbf{C}^{G^\vee}/\mathbf{C}}(F_G(f)F_G(\overline{f})) \\ &= \mathrm{tr}_{\mathbf{C}^{G^\vee}/\mathbf{C}}(F_G(f)\overline{F_G(f)}) = |F_G(f)|^2. \end{aligned}$$

□

Remark 2.3. Notice that $G^\vee$ acts on $\mathbf{C}^{G^\vee}$ as follows. For $\tau \in G^\vee$ we set

$$\tau((c_\chi)_{\chi \in G^\vee}) = (c_{\tau \cdot \chi})_{\chi \in G^\vee}.$$

By transport of structure using F_G^{-1} the group $G^\vee$ acts on $\mathbf{C}[G]$. For $\tau \in G^\vee$ and $f = \sum_{g \in G} c_g g \in \mathbf{C}[G]$ we have $\tau f = \sum_{g \in G} \overline{\tau}(g) c_g g$ (this follows easily from Proposition 2.2). From this action, we see in particular that $G^\vee$ acts on $\mathbf{C}[S] = \{\sum_{s \in S} c_s s : c_s \in \mathbf{C}\} \subseteq \mathbf{C}[G]$ where $S \subseteq G$ is a subset. Note that by definition we have $(\tau f)_\chi = f_{\tau\chi}$.

Conversely, G acts naturally on $\mathbf{C}[G]$. This induces an action on $\mathbf{C}^{G^\vee}$ given by

$$g((c_\chi)_{\chi \in G^\vee}) = (\overline{\chi}(g) c_\chi)_{\chi \in G^\vee}.$$

With these conventions all morphisms in the diagram for s^* in Theorem 2.2 become $\mathbf{C}[G]$-module maps.

3. Shape parameter

3.1. Definition. For a subset $S \subseteq G$ we set $\mathbf{C}[S] = \left\{ \sum_{s \in S} c_s s : c_s \in \mathbf{C} \right\} \subseteq \mathbf{C}[G]$, which is a $\mathbf{C}$-vector space. For $f \in \mathbf{C}[G]$ we define f_g by $f = \sum_{g \in G} f_g g$.

Definition 3.1. Let $f \in \mathbf{C}[G]$ such that $f_{\chi_0} \neq 0$. We define the *complexity* of f as

$$C_G(f) = \frac{\sum_{\chi \in G^\vee} |f_\chi|}{|f_{\chi_0}|}.$$

Note that for $c \in \mathbf{C}^*$ we have $C_G(f) = C_G(cf)$.

Let $S \subseteq G$ be non-empty. We define the *shape parameter* of S to be

$$\mathrm{sh}_G(S) = \frac{\#S}{\#G} \cdot \inf_{f \in \mathbf{C}[S] : f_{\chi_0} \neq 0} C_G(f) = \frac{\#S}{\#G} \cdot \inf_{f \in \mathbf{C}[S] : f_{\chi_0} \neq 0} \frac{\sum_{\chi \in G^\vee} |f_\chi|}{|f_{\chi_0}|}.$$

We will usually write $\mathrm{sh}(S)$ instead of $\mathrm{sh}_G(S)$ and $C(f)$ instead of $C_G(f)$, unless confusion arises.

Remark 3.2. First remark that this infimum in the above definition is in fact a minimum. For $c \in \mathbf{C}^*$ and $h \in \mathbf{C}[G]$ we have $C(ch) = C(h)$. Hence we only need to consider functions h with $h_{\chi_0} = 1$. Take a function $f \in \mathbf{C}[S]$ with $f_{\chi_0} = 1$. We have

$$\{h \in \mathbf{C}[S] : h_{\chi_0} = 1, C(h) \leq C(f)\} \subseteq \{h \in \mathbf{C}[G] : h_{\chi_0} = 1, C(h) \leq C(f)\}$$
$$\cong \Big\{(c_\chi)_{\chi \in G^\vee} \in \mathbf{C}^{G^\vee} : c_{\chi_0} = 1, \sum_{\chi \in G^\vee} |c_\chi| \leq C(f)\Big\}.$$

The first inclusion is as a closed set, and the isomorphism is as topological spaces (Proposition 2.2). The last set is obviously compact, and hence the first set is compact as well. It then easily follows that the infimum is obtained. In the rest of this chapter, we will often use this implicitly.

3.2. Properties of the shape parameter.

Proposition 3.3. *Let $S \subseteq G$ be non-empty. Then the following hold:*

i. *For $\alpha \in \mathrm{Aut}(G)$ and $b \in G$ we have $\mathrm{sh}(b \cdot \alpha(S)) = \mathrm{sh}(S)$.*
ii. *We have $1 \leq \mathrm{sh}(S) \leq \#S$. Furthermore we have $\mathrm{sh}(S) = 1$ if and only if S is a coset of a subgroup of G. We have $\mathrm{sh}(S) = \#S$ if and only if $\#S = 1$.*
iii. *For $S \subseteq S'$ we have $\mathrm{sh}(S') \leq \frac{\#S'}{\#S}\mathrm{sh}(S)$.*

Let G' be a finite abelian group and let $S' \subseteq G'$ be non-empty. Then the following hold:

iv. *Let $i\colon G \to G'$ be an injective group morphism. Then one has $\mathrm{sh}_G(S) = \mathrm{sh}_{G'}(i(S))$.*
v. *Let $\pi\colon G \to G'$ be a surjective morphism of groups. Then the equality $\mathrm{sh}_G(\pi^{-1}(S')) = \mathrm{sh}_{G'}(S')$ holds.*
vi. *We have $\mathrm{sh}_{G\times G'}(S \times S') \leq \mathrm{sh}_G(S) \times \mathrm{sh}_{G'}(S')$.*

Proof. iii: Follows easily from the definition.
iv: We identify G with the subgroup of $i(G)$ of G'. For $f \in \mathbf{C}[G] \subseteq \mathbf{C}[G']$ we have

$$C_{G'}(f) = \frac{\sum_{\chi \in G'^\vee} |f_\chi|}{|f_{\chi_0}|} = [G' : G] \cdot C_G(f),$$

because the map $G'^\vee \to G^\vee$ is $[G' : G]$-to-one. The result then follows from the definition.

v: Let $f' \in \mathbf{C}[S']$ with $f'_{\chi_0} = 1$. Then for $\pi^* f' \in \mathbf{C}[\pi^{-1}(S')]$ we obtain from Proposition 2.2ii

$$C_G(\pi^* f') = C_{G'}(f').$$

If we take f' such that $\mathrm{sh}_{G'}(S') = \frac{\#S}{\#G} C_{G'}(f')$ we find

$$\mathrm{sh}_G(\pi^{-1}(S')) \leq \frac{\#\pi^{-1}(S')}{\#G} C_G(\pi^* f') = \frac{\#S'}{\#G'} C_{G'}(f') = \mathrm{sh}_{G'}(S').$$

Conversely, let $f \in \mathbf{C}[\pi^{-1}(S')]$ with $f_{\chi_0} = 1$. Note that $\ker(\pi)$ acts on $\mathbf{C}[\pi^{-1}(S')]$ (see Remark 2.3). Consider

$$f'' = \frac{1}{\#\ker(\pi)} \sum_{g \in \ker(\pi)} g(f') \in \mathbf{C}[\pi^{-1}(S')].$$

By construction there exists an $f' \in \mathbf{C}[S']$ such that $\pi^* f' = f''$. From Remark 2.3 and the previous calculation one easily obtains $C_{G'}(f') = C_G(f'') \leq C_G(f)$. If we minimize over all possible f we obtain $\mathrm{sh}_G(\pi^{-1}(S')) \leq \mathrm{sh}_{G'}(S')$.

vi: Let $f \in \mathbf{C}[S] \subseteq \mathbf{C}[G]$ and $f' \in \mathbf{C}[S'] \subseteq \mathbf{C}[G']$. Then we have $f \otimes f' \in \mathbf{C}[G] \otimes_{\mathbf{C}} \mathbf{C}[G'] = \mathbf{C}[G \times G']$. For $(\chi, \chi') \in G^\vee \times G'^\vee$ we have by Proposition 2.2 ii the equality

$$(f \otimes f')_{(\chi,\chi')} = f_\chi \cdot f'_{\chi'}.$$

This gives

$$\frac{\#(S \times S')}{\#(G \times G')} C_{G\times G'}(f \otimes f') = \frac{\#S}{\#G} C_G(f) \cdot \frac{\#S'}{\#G'} C_{G'}(f')$$

and the result follows.

i. That it is invariant under automorphisms follows from iv. Hence we assume that $\alpha = \mathrm{id}_G$. We have a bijection $\varphi\colon \mathbf{C}[S] \to \mathbf{C}[\beta S]$ defined by $f \mapsto \beta \cdot f$. For $f \in \mathbf{C}[S]$ one has $(\varphi(f))_\chi = \chi(\beta) f_\chi$. As $\chi(\beta)$ is a root of unity, we see that $C(f) = C(\varphi(f))$.

ii. Let $f \in \mathbf{C}[S]$. We need to show that $|f_{\chi_0}| \leq \frac{\#S}{\#G} \sum_\chi |f_\chi|$. We have, using the inverse formula from Proposition 2.2,

$$|f_{\chi_0}| = |\sum_{s\in S} f_s| = |\frac{1}{\#G} \sum_{s\in S} \sum_\chi f_\chi \chi(s)| \leq \frac{\#S}{\#G} \sum_\chi |f_\chi|$$

Assume that we have an equality. By the translation property, i, we may assume that $1 \in S$ and we may assume that $f_{\chi_0} = 1$. We have $f_{\chi_0}\chi_0(1) = 1$. Hence we see that we have an equality if and only if $f_\chi \chi(s) \in \mathbf{R}_{\geq 0}$ for all $\chi \in G^\vee$ and $s \in S$. Using the case $s = 0$, one obtains $f_\chi \geq 0$. We see that if $f_\chi > 0$, then for any $s \in S$ we have $\chi(s) = 1$. We obtain that for any $t, t' \in \langle S \rangle$ and χ with $f_\chi > 0$ we see that $\chi(t) = 1$ and hence $f_t = \frac{1}{\#G} \sum_\chi f_\chi \chi(t) = \frac{1}{\#G} \sum_\chi f_\chi \chi(t') = f_{t'}$. Hence our function is constant on $\langle S \rangle$, and as it is nonzero ($f_{\chi_0} = 1$), it is non-negative. As f has support on S, we see that $S = \langle S \rangle$. Actually, we obtain $f = \frac{1}{\#S} \cdot 1_S$. For the converse, assume that $S = \langle S \rangle$. With the help of the function $f = \frac{1}{\#S} \cdot 1_S$ it is easy to see that $\mathrm{sh}(S) = 1$.

The upper bound directly follows from iii and the fact that $\mathrm{sh}(\{s\}) = 1$, which we have just shown. Assume that we reach the upper bound and that $\#S \geq 2$. After translation, we may assume that $\#S \supseteq \{e, g\}$ with $g \neq e$. Using iii and iv we can reduce to the case where $G = \langle g \rangle$ is of order n and $S = \{e, g\}$. Consider $f = \frac{1}{2}(e + g) \in \mathbf{C}[S]$. Then $C_G(f) = \frac{1}{2} \sum_{i=0}^{n-1} |1 + \zeta_n^i|$. This is strictly less than n. This shows that $\mathrm{sh}_G(S) < 2$ and the result follows. □

3.3. Bounds on the shape parameter. In this subsection we give an upper bound for the shape parameter of a specific type of set, the intervals. The usefulness of these sets comes from the fact that given a group there are intervals of many different cardinalities. If $S \subseteq G$ is non-empty, we set

$$SS^{-1} = \{st^{-1} : \ s, t \in S\}.$$

Lemma 3.4. *We have*

$$\mathrm{sh}(SS^{-1}) \leq \frac{\#(SS^{-1})}{\#S}.$$

PROOF. Let $f = 1_S = \sum_{s\in S} s \in \mathbf{C}[S]$. Note that $f \cdot \overline{f}$ has support in SS^{-1}. By Proposition 2.2 iii we have $(f \cdot \overline{f})_\chi = f_\chi \overline{f_\chi} = |f_\chi|^2$. From Proposition 2.2iv we obtain

$$\begin{aligned}\mathrm{sh}(SS^{-1}) &\leq \frac{\#(SS^{-1})}{\#G} C(f \cdot \overline{f}) \\ &= \frac{\#(SS^{-1})}{\#G} \frac{\sum_\chi |f_\chi|^2}{|f_{\chi_0}|^2} \\ &= \frac{\#(SS^{-1})}{\#G} \frac{\#G \sum_g |f_g|^2}{|f_{\chi_0}|^2} \\ &= \frac{\#(SS^{-1})}{\#G} \frac{\#G \cdot \#S}{\#S^2} \\ &= \frac{\#(SS^{-1})}{\#S}.\end{aligned}$$

□

Definition 3.5. An *interval* of $\mathbf{Z}$ is a non-empty set $S \subseteq \mathbf{Z}$ such that are $n, m \in \mathbf{R}$ with $S = [n, m] \cap \mathbf{Z}$.

Let $G = \mathbf{Z}/n\mathbf{Z}$. A *standard interval* of G is defined to be the image of an interval of $\mathbf{Z}$ under the natural map $\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$.

Let G be a finite abelian group. A subset $S \subseteq G$ is called a *full interval* if there exist $n \in \mathbf{Z}_{\geq 1}$, a surjective morphism $\pi\colon G \to \mathbf{Z}/n\mathbf{Z}$ and a standard interval T of $\mathbf{Z}/n\mathbf{Z}$ such that $\pi^{-1}(T) = S$. A full interval of a subgroup of G is called an *interval* of G.

Lemma 3.6. *For an interval $S \subseteq G$ we have* $\mathrm{sh}(S) \leq 2$.

PROOF. Using Proposition 3.3iv and v, we reduce to the case where $G = \mathbf{Z}/n\mathbf{Z}$, for which we use additive notation, and where S is a standard interval. First of all assume that the size of S is odd, then we may assume (after shifting) $S = \{-\overline{m}, -\overline{m}+1, \ldots, 0, \ldots, \overline{m}-1, \overline{m}\}$ for some $m \in \mathbf{Z}_{\geq 0}$ with $m \leq \frac{n-1}{2}$. Let $T = \{0, 1, \ldots, \overline{m}\}$. Then $T - T = S$ and hence we find by Lemma 3.4

$$\mathrm{sh}(S) \leq \frac{\#S}{\#T} = \frac{2m+1}{m+1} < 2.$$

If $\#S$ is even of cardinality $2m+2$, we may assume that

$$S' = \{-\overline{m}, -\overline{m}+1, \ldots, 0, \ldots, \overline{m}-1, \overline{m}\} \subset S.$$

Hence from Proposition 3.3 and the previous result we deduce

$$\begin{aligned}\mathrm{sh}(S) &\leq \frac{2m+2}{2m+1} \mathrm{sh}(S') \\ &\leq \frac{2m+2}{2m+1} \frac{2m+1}{m+1} = 2.\end{aligned}$$

□

Lemma 3.7. *Let V be a vector space over $\mathbf{F}_p$ of dimension n. Let $c \in \{1, \ldots, p-1\}$ and $0 \leq i < n$ or $(c, i) = (1, n)$. Then there is an interval S in V with $\#S = cp^i$.*

PROOF. If $(c,i)=(1,n)$, the statement is obviously true. Assume $c\neq 0$ and let W be a subspace of dimension $i+1$ of V and consider a nonzero map $f\in W^\vee=\mathrm{Hom}(W,\mathbf{F}_p)$. Pick an interval S_0 of $\mathbf{F}_p$ of length c and set $S=f^{-1}(S_0)$. □

3.4. Shape and intersections.

Lemma 3.8. *Let G be a finite abelian group and let $S\subseteq G$ (respectively $S'\subseteq G$) be a coset of a subgroup H (respectively H'). Assume that $S\cap S'\neq\emptyset$. Then we have*

$$\frac{1}{[G:H']}\frac{\mathrm{sh}_G(S\cap S')}{\#(S\cap S')}\leq\frac{\mathrm{sh}_G(S)}{\#S}.$$

PROOF. One easily sees that $S\cap S'$ is a coset of $H\cap H'$. Hence we have $\mathrm{sh}_G(S)=\mathrm{sh}_G(S\cap S')=1$ (Proposition 3.3ii). The exact sequence $0\to H/(H\cap H')\to G/H'\to G/(HH')\to 0$ gives us

$$\#(S\cap S')=\#(H\cap H')\geq\frac{1}{[G:H']}\#H=\frac{1}{[G:H']}\#S.$$

The result follows. □

3.5. Questions concerning the shape parameter. We have the following open problems concerning the shape parameter.

Problem 2. Do we have equality in Proposition 3.3 statement vi?

Problem 3. What is the average shape parameter of a subset of a group? More precisely, what is (a good lower bound for)

$$\frac{1}{2^{\#G}-1}\sum_{S\subseteq G,\ S\neq\emptyset}\mathrm{sh}(S)?$$

What is the asymptotic behavior when $\#G\to\infty$? Given a group G, what is the maximum shape parameter of a subset? How does this grow with $\#G$? For a non-empty subset S of G we have $\mathrm{sh}(S)\leq\#S$. Can we find a better upper bound?

4. Applications of the shape parameter to finite fields

Let k be a finite field of characteristic p and let q be its cardinality.

4.1. Multiplicative versus additive group. For a subset U of k^* we denote by $\langle U\rangle$. the multiplicative subgroup of k^* generated by U. For a subset V of k we denote by $\langle V\rangle_+$ the additive subgroup of k^+ generated by V.

We will give on a subset $S\subseteq k$ such that $S\cap k^*$ generates k^* in a multiplicative way. Furthermore, we give conditions for $T\subseteq k^*$ such that T generates k as an additive group.

Lemma 4.1. *Let $\lambda\in(k^+)^\vee$, $\chi\in(k^*)^\vee$. Set*

$$c_{(\lambda,\chi)}=\sum_{a\in k^*}\lambda(a)\chi(a).$$

Then one has:

i. *$\lambda\neq\chi_0$, $\chi\neq\chi_0$: $|c_{(\lambda,\chi)}|=\sqrt{q}$;*
ii. *$\lambda\neq\chi_0$: $c_{(\lambda,\chi_0)}=-1$;*

iii. $\chi \neq \chi_0$: $c_{(\chi_0,\chi)} = 0$;
iv. $c_{(\chi_0,\chi_0)} = q - 1$.

PROOF. If $\lambda \neq \chi_0$, then we have $c_{(\lambda,\chi_0)} = -\lambda(0) = -1$. If $\chi \neq \chi_0$, then we have $c_{(\chi_0,\chi)} = 0$. We have $c_{(\chi_0,\chi_0)} = q - 1$. Finally, for $\lambda \neq \chi_0$, $\chi \neq \chi_0$, we have $|c_{\lambda,\chi}| = \sqrt{q}$. Indeed, one has

$$\begin{aligned}|\sum_{a\in k^*} \lambda(a)\chi(a)|^2 &= \sum_{a\in k^*} \lambda(a)\chi(a) \cdot \sum_{b\in k^*} \lambda(-b)\chi(1/b) = \sum_{a,b\in k^*} \lambda(a-b)\chi(a/b) \\ &= \sum_{a,b\in k^*} \lambda((a/b-1)b)\chi(a/b) = \sum_{\gamma,b\in k^*} \lambda((\gamma-1)b)\chi(\gamma) \\ &= \sum_{\gamma\in k^*} \chi(\gamma) \sum_{b\in k^*} \lambda((\gamma-1)b) = (*)\end{aligned}$$

Note that $\sum_{b\in k^*} \lambda((\gamma-1)b)$ is $q-1$ if $\gamma = 1$ and -1 if $\gamma \neq 1$ (here we use that the character λ is not trivial). Hence we have

$$(*) = -\sum_{\gamma\in k^*} \chi(\gamma) + q\chi(1) = q,$$

where we use that χ is not trivial. The result follows. □

Proposition 4.2. *The following hold:*

i. *Let $S \subseteq k$ be nonempty with $\sqrt{q} \cdot \mathrm{sh}_{k^+}(S) < \#S$. Then we have $\langle S \cap k^* \rangle_\cdot = k^*$*
ii. *Let $T \subseteq k^*$ be nonempty with $(\sqrt{q}-1) \cdot \mathrm{sh}_{k^*}(T) < \#T$. Then we have $\langle T \rangle_+ = k$.*

PROOF. i: Suppose that S has a shape given by the function $f \in \mathbf{C}[S] \subseteq \mathbf{C}[k]$, that is, $\mathrm{sh}_{k^+}(S) = \#S/q \cdot C_{k^+}(f)$ From Theorem 2.2 we have for $a \in k$ the equality $f_a = \frac{1}{\#k} f_\lambda \lambda(a)$. Suppose that $\langle S \cap k^* \rangle_\cdot \subsetneq k^*$. Then there exists a subgroup $H \subsetneq k^*$ of prime index l such that $S \cap k^* \subseteq H$. Let $\chi \in (k^*)^\vee$ be a character with kernel H.

By construction we have

$$\begin{aligned}0 &= \sum_{a\in k^*} f_a(\chi - 1)(a) = \frac{1}{\#k} \sum_{a\in k^*} \sum_{\lambda\in k^\vee} f_\lambda \lambda(a)(\chi-1)(a) \\ &= \frac{1}{\#k} \sum_{\lambda\in k^\vee} f_\lambda \left(c_{(\lambda,\chi)} - c_{(\lambda,1)}\right)\end{aligned}$$

Hence we have

$$f_1(q-1) = f_1\left(c_{(1,1)} - c_{(1,\chi)}\right) = \sum_{\lambda\in k^\vee, \lambda\neq 1} f_\lambda \left(c_{(\lambda,\chi)} - c_{(\lambda,1)}\right).$$

We take absolute values and we use the estimates (Lemma 4.1) to find:

$$|f_1|(q-1) \leq (\sqrt{q}+1) \sum_{\lambda\in k^\vee, \lambda\neq 1} |f_\lambda|.$$

This gives

$$\sqrt{q} \leq \frac{\sum_{\lambda \in k^\vee} |f_\lambda|}{|f_1|} = \frac{q}{\#S} \operatorname{sh}_{k^+}(S),$$

and this finishes the first case.

ii: Suppose that T has a shape given by the function $f \in \mathbf{C}[T] \subseteq \mathbf{C}[k^*]$, that is, $\operatorname{sh}_{k^*}(T) = \#T/(q-1) \cdot C_{k^*}(f)$. For $a \in k^*$ we have $f_a = \frac{1}{\#k^*} \sum_{\chi \in (k^*)^\vee} f_\chi \chi(a)$ (Theorem 2.2). Suppose that $\langle T \rangle_+ \subsetneq k$. Then there exists a subgroup $H \subsetneq k$ of index $p = \operatorname{char}(k)$ such that $T \cap k \subseteq H$. Let $\lambda \in k^\vee$ be a character with kernel H.

By construction we have

$$\begin{aligned} 0 &= \sum_{a \in k^*} (\lambda - 1)(a) f_a = \frac{1}{\#k^*} \sum_{a \in k^*} \sum_{\chi \in (k^*)^\vee} f_\chi (\lambda - 1)(a) \chi(a) \\ &= \frac{1}{\#k^*} \sum_{\chi \in (k^*)^\vee} f_\chi \left(c_{(\lambda,\chi)} - c_{(1,\chi)} \right). \end{aligned}$$

Hence we have

$$f_1 q = f_1 \left(c_{(1,1)} - c_{(\lambda,1)} \right) = \sum_{\chi \in (k^*)^\vee, \chi \neq 1} f_\chi \left(c_{(\lambda,\chi)} - c_{(1,\chi)} \right).$$

Putting absolute values and the other estimates (Lemma 4.1), we find:

$$|f_1| q \leq \sqrt{q} \sum_{\chi \in (k^*)^\vee, \chi \neq 1} |f_\chi|.$$

This gives

$$\sqrt{q} + 1 \leq \frac{\sum_{\lambda \in (k^*)^\vee} |f_\lambda|}{|f_1|} = \frac{q-1}{\#T} \operatorname{sh}(T),$$

and this finishes the proof. □

Remark 4.3. The character estimates above also follow from class field theory. In the next chapter we will use class field theory to estimate similar sums.

Remark 4.4. The statements in Proposition 4.2 are often sharp. Assume that q is a square and let k' be the subfield of k with $[k : k'] = 2$. Set $S = k'$ and $T = k'^*$. One has $\sqrt{q} \cdot \operatorname{sh}_{k^+}(S) = \#S$ and $(\sqrt{q} - 1) \cdot \operatorname{sh}_{k^*}(T) = \#T$. Note that $\langle S \cap k^* \rangle_\cdot = k'^* \subsetneq k^*$ and that $\langle T \rangle_+ = k' \subsetneq k$.

Corollary 4.5. *Let $S \subseteq k$ be an $\mathbf{F}_p$ vector space of size $> \sqrt{q}$. Then $k^* = \langle S \cap k^* \rangle_\cdot$.*.

Proof. Use Proposition 4.2 and the fact that $\operatorname{sh}(S) = 1$ (Proposition 3.3). □

Remark 4.6. For the subspace $\mathbf{F}_p \subseteq \mathbf{F}_{p^2} = k$ we have $\mathbf{F}_p^* = \langle \mathbf{F}_p^* \cap k^* \rangle_\cdot \subsetneq k^*$. Hence the result in Corollary 4.5 is sharp.

Corollary 4.7. *Let S be an interval of k of size $> 2\sqrt{q}$. Then $\langle S \cap k^* \rangle_\cdot = k^*$.*

Proof. From Lemma 3.6 we know that $\operatorname{sh}(S) \leq 2$. Now apply Proposition 4.2. □

One can use Proposition 4.2 for many other subsets, for example of product of subsets, of which one knows something about the shape.

Remark 4.8. Assume that q is odd. Let $S = k^{*2} \cup \{0\}$. As $\langle S \cap k^* \rangle_\cdot = k^{*2}$, we deduce from Proposition 4.2:

$$\mathrm{sh}_{k^+}(S) \geq \frac{(q+1)/2}{\sqrt{q}} > \frac{\sqrt{q}}{2}.$$

Hence S has quite a large shape and we see that sets can have arbitrarily large shape.

4.2. Primitive roots.

Proposition 4.9. *Let k be a finite field of cardinality q. Let $D = \{l \text{ prime} : l | q-1\}$. Let $S \subseteq k$ be a subset such that one of the following holds:*

i. $\#S \left(\sqrt{q} + 2^{\#D} - 1\right) > q^{1/2} \left(q^{1/2}(2^{\#D} - 1) + 1\right) \mathrm{sh}_{k^+}(S)$;

ii. $\#S \geq q^{1/2} 2^{\#D} \mathrm{sh}_{k^+}(S)$.

Then S contains a primitive root of k^*.

Proof. For every $l \in D$ let $\chi_l \in (k^*)^\vee$ be a character of order l. For $T \subseteq D$ put $\chi_T = \prod_{l \in T} \chi_l$ and put $\mu(T) = (-1)^{\#T}$. As k^* is cyclic, it follows that $a \in k$ is a primitive root iff $\prod_{l \in D}(1 - \chi_l)(a) \neq 0$. Suppose that S contains no primitive root. Let $f \in \mathbf{C}[S] \subseteq \mathbf{C}[k]$ with $C_k(f) = \frac{q}{\#S} \mathrm{sh}_{k^+}(S)$. Then we have (Theorem 2.2)

$$\begin{aligned} 0 &= \sum_{a \in k^*} f_a \prod_{l \in D} (1 - \chi_l)(a) \\ &= \frac{1}{\#k} \sum_{\lambda \in k^\vee} f_\lambda \sum_{a \in k^*} \lambda(a) \prod_{l \in D} (1 - \chi_l)(a) \\ &= \frac{1}{\#k} \sum_{\lambda \in k^\vee} f_\lambda \sum_{T \subseteq D} c_{(\lambda, \chi_T)} \mu(T). \end{aligned}$$

This gives, using our character estimates as in Lemma 4.1,

$$|f_1|(q + q^{1/2}(2^{\#D} - 1)) \leq \left(q^{1/2}(2^{\#D} - 1) + 1\right) \sum_{\lambda \in (k^+)^\vee} |f_\lambda|$$

The first result then follows, and the second one implies the first one after some estimates. □

Remark 4.10. One can show that $\#D = O(\log(q)/\log(\log(q)))$ ([**HW79**, page 355]), and hence the above theorem gives us a deterministic algorithm to find a generator of k^* which on average runs in time $O(q^{1/2+\epsilon})$ (by using for example an interval). One can actually do this in time $O(q^{1/4+\epsilon})$ as in [**Shp96**] by using special types of intervals.

5. Computing the shape parameter

In this section we discuss certain tricks for calculating the shape parameter in certain cases. We use the ideas in this section to calculate the shape parameter of all non-empty subsets of a cyclic group of order 6. This section is not needed in the rest of this thesis.

Let $S \subseteq G$ be non-empty. First note that the function $C_G \colon \mathbf{C}[S] \to \mathbf{R}$ is convex. Hence a local minimum is a global minimum.

Lemma 5.1. *There is $f \in \mathbf{R}[S]$ with $f_{\chi_0} = 1$ and $\mathrm{sh}(S) = \frac{\#S}{\#G} C_G(f)$.*

PROOF. Suppose $h = \sum h_g g \in \mathbf{C}[S]$ with $h_{\chi_0} = 1$ satisfies $\mathrm{sh}(S) = \frac{\#S}{\#G} C_G(h)$. Note that $h' = \sum \overline{h_g} g \in \mathbf{C}[S]$ satisfies $C_G(h) = C_G(h')$. Set $f = \frac{h+h'}{2} \in \mathbf{R}[S]$ and the result follows from convexity. □

Consider the hyperplane $D = \{h \in \mathbf{R}[S] : h_{\chi_0} = 1\}$ of $\mathbf{R}[S]$.

Lemma 5.2. *Let $\varphi = C_G|_D \colon D \to \mathbf{R}$. Let $f \in D$ such that the tangent map $d\varphi(f) \colon TD_f \to \mathbf{R}$ is 0 and such that for all $\chi \in G^\vee$ we have $f_\chi \neq 0$. Then we have*

$$\mathrm{sh}(S) = \frac{\#S}{\#G} C_G(f).$$

PROOF. By convexity a local optimum is a global optimum. The assumption that for all $\chi \in G^\vee$ we have $f_\chi \neq 0$ implies that φ is smooth at f. The function φ has a local minimum at the smooth point f if the gradient, $d\varphi(f)$, is zero. Apply Lemma 5.1. □

Remark 5.3. To find the approximate value of the shape parameter of S it might be useful to make $C_G|_D$ from the previous lemma smooth. This can be done as follows. Pick $\epsilon > 0$ and for $f \in D$ set

$$C_{G,\epsilon}(f) = \sum_\chi |f_\chi|_\epsilon,$$

where $|a + bi|_\epsilon = \sqrt{a^2 + b^2 + \epsilon}$. We will not discuss this strategy any further.

Note that the group $G' = G \rtimes \mathrm{Aut}(G)$ acts on $X = \{T \subseteq G : T \neq \emptyset\}$. From Proposition 3.3i we deduce that the shape is constant on G' orbits of X. Denote by G'_S the stabilizer of S under this action.

Lemma 5.4. *There is $f \in D$ which is constant on the orbits of the action of G'_S on S such that*

$$\mathrm{sh}(S) = \frac{\#S}{\#G} C_G(f).$$

PROOF. The group G' acts on $\mathbf{C}[G]$ as well. For $f' \in D$ set

$$f'' = \frac{1}{\#G'_S} \sum_{g' \in G'_S} g'(f') \in D.$$

Note that $C_G(f') = C_G(g'(f'))$. By convexity we have $C_G(f'') \leq C_G(f')$. The result follows since f'' is constant on the orbits of the action of G'_S on S. □

Remark 5.5. One can use Lemma 5.4 to calculate the shape parameter when G'_S acts transitively on S. In particular, when $\#S = 2$, say $S = \{x, y\}$ the element $g \mapsto xg^{-1}y$ of G'_S shows that

$$\mathrm{sh}(S) = \frac{2}{\#G} C_G\Big(\frac{1}{2}(x + y)\Big).$$

5.1. Example. Consider the cyclic group $C_6 = \langle\sigma\rangle$ of order 6. This group has 63 non-empty subsets. In this table we give an upper bound for the shape of their subsets. We look at the sets up to translation and up to isomorphism. Notice that $\mathrm{Aut}(C_6) = \{\pm 1\}$. The group $G \rtimes \mathrm{Aut}(G)$ acts on the set of non-empty subsets of G and the shape parameter is constant on such a subset. For a set $T \subseteq G$ we denote by $T^c = G \setminus T$. The orbits of this action are the following:

$$\{\{e\},\{\sigma\},\{\sigma^2\},\{\sigma^3\},\{\sigma^4\},\{\sigma^5\}\},$$
$$\{\{e,\sigma\},\{\sigma,\sigma^2\},\{\sigma^2,\sigma^3\},\{\sigma^3,\sigma^4\},\{\sigma^4,\sigma^5\},\{e,\sigma^5\}\},$$
$$\{\{e,\sigma^2\},\{\sigma,\sigma^3\},\{\sigma^2,\sigma^4\},\{\sigma^3,\sigma^5\},\{e,\sigma^4\},\{\sigma,\sigma^5\}\},$$
$$\{\{e,\sigma^3\},\{\sigma,\sigma^4\},\{\sigma^2,\sigma^5\}\},$$
$$\{\{e,\sigma,\sigma^2\},\{\sigma,\sigma^2,\sigma^3\},\{\sigma^2,\sigma^3,\sigma^4\},\{\sigma^3,\sigma^4,\sigma^5\},\{e,\sigma^4,\sigma^5\},\{e,\sigma,\sigma^5\}\},$$
$$\{\{e,\sigma^2,\sigma^4\},\{\sigma,\sigma^3,\sigma^5\}\},$$
$$\{\{e,\sigma^3\}^c,\{\sigma,\sigma^4\}^c,\{\sigma^2,\sigma^5\}^c\},$$
$$\{\{e,\sigma^2\}^c,\{\sigma,\sigma^3\}^c,\{\sigma^2,\sigma^4\}^c,\{\sigma^3,\sigma^5\}^c,\{e,\sigma^4\}^c,\{\sigma,\sigma^5\}^c\},$$
$$\{\{e,\sigma\}^c,\{\sigma,\sigma^2\}^c,\{\sigma^2,\sigma^3\}^c,\{\sigma^3,\sigma^4\}^c,\{\sigma^4,\sigma^5\}^c,\{e,\sigma^5\}^c\},$$
$$\{\{e\}^c,\{\sigma\}^c,\{\sigma^2\}^c,\{\sigma^3\}^c,\{\sigma^4\}^c,\{\sigma^5\}^c\},$$
$$\{G\}$$

and

$$\{\{e,\sigma,\sigma^3\},\{\sigma,\sigma^2,\sigma^4\},\{\sigma^2,\sigma^3,\sigma^5\},\{e,\sigma^3,\sigma^4\},\{\sigma,\sigma^4,\sigma^5\},\{e,\sigma^2,\sigma^5\},$$
$$\{e,\sigma^3,\sigma^5\},\{\sigma^2,\sigma^4,\sigma^5\},\{\sigma,\sigma^3,\sigma^4\},\{e,\sigma^2,\sigma^3\},\{\sigma,\sigma^2,\sigma^5\},\{e,\sigma,\sigma^4\}\}.$$

We take a representative of each class and calculate the shape parameter. Remark 5.5 directly gives the answer for 7 out of 12 orbits:

S	function	$\mathrm{sh}(S)$
$\{e\}$	e	1
$\{e,\sigma\}$	$\frac{1}{2}(e+\sigma)$	$1.244\ldots$
$\{e,\sigma^2\}$	$\frac{1}{2}(e+\sigma^2)$	$4/3$
$\{e,\sigma^3\}$	$\frac{1}{2}(e+\sigma^3)$	1
$\{e,\sigma^2,\sigma^4\}$	$\frac{1}{3}(e+\sigma^2+\sigma^4)$	1
$\{\sigma,\sigma^2,\sigma^4,\sigma^5\}$	$\frac{1}{4}(\sigma+\sigma^2+\sigma^4+\sigma^5)$	$4/3$
G	$\frac{1}{6}(e+\sigma+\sigma^2+\sigma^3+\sigma^4+\sigma^5)$	1.

In most remaining cases we find the following upper bounds:

S	function	$\mathrm{sh}(S)$
$\{e,\sigma,\sigma^2\}$	$\frac{1}{3}(e+\sigma+\sigma^2)$	$\leq 4/3$
$\{e,\sigma,\sigma^3\}$	$\frac{1}{2}(e+\sigma^3)$	$\leq 3/2$
$\{\sigma,\sigma^3,\sigma^4,\sigma^5\}$	$\frac{1}{3}(\sigma+\sigma^3+\sigma^5)$	$\leq 4/3$
$\{\sigma^2,\sigma^3,\sigma^4,\sigma^5\}$	$\frac{1}{6}(\sigma^2+\sigma^5)+\frac{1}{3}(\sigma^3+\sigma^4)$	$\leq 1.438.$

Finally, consider the set $S = \{\sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$. Consider the function

$$f = \frac{1}{5}\left(\sigma + \sigma^2 + \sigma^3 + \sigma^4 + \sigma^5\right).$$

Lemma 5.2 gives $\mathrm{sh}(S) = 5/3$.

Chapter 7

Deterministically generating Picard groups of hyperelliptic curves over finite fields

1. Introduction

1.1. Results. An algorithmic problem in arithmetic geometry is to explicitly find the group structure of the Picard group of a curve of genus g over a finite field of size $q = p^m$. A related problem is to find a generating set of this Picard group. In this chapter we describe a deterministic way of finding a generating set, when the curve is hyperelliptic, in time $O\big(g^{2+\epsilon}q^{1/2+\epsilon}\big)$ for any $\epsilon > 0$.

Let C be a hyperelliptic curve of genus g over a finite field k of cardinality q and characteristic p given by an equation $y^2 + h(x)y = f(x)$, satisfying the assumptions of Theorem 4.6 from Chapter 2 such that the natural projection map to the projective line by taking the x-coordinate is ramified at ∞. Call ∞' the point above ∞. Let $\varphi_C \colon C(k) \to \mathrm{Pic}^0_k(C)$ be the map given by $P \mapsto [P] - [\infty']$. Our main theorem is the following.

Theorem 1.1. *For any $\epsilon > 0$ there is a deterministic algorithm which on input a hyperelliptic curve C of genus g over a finite field k of cardinality q outputs a set of generators of $\mathrm{Pic}^0_k(C)$ in time $O\big(g^{2+\epsilon}q^{1/2+\epsilon}\big)$.*

Such a generating set can then be used in other algorithms to deterministically determine the group structure of $\mathrm{Pic}^0_k(C)$.

The above result is obtained from the following theorem. For a subset S of k put $C_S = \{P \in C(k) : x(P) \in S\}$. The following is a less precise version of Theorem 4.1 and Remark 4.2. An interval I of k is a subset of the form $B + \alpha[s, \ldots, s + r]$ where B is an additive subgroup of k, $\alpha \in k$ and $s, r \in \mathbf{Z}_{\geq 0}$ (or more precisely, see Definition 3.5 from Chapter 3).

Kohel and Shparlinksi ([**KS00**, Corollary 2]) have shown the following for $g = 1$. For S an interval of k of cardinality greater than $15(1 + \log(p))q^{1/2}$ they deduce that $\langle \varphi_C(C_S) \rangle = \mathrm{Pic}^0_k(C)$. We generalize and improve their result in the following ways.

Theorem 1.2. *Assume that $\#C(k) > (2g-2)\sqrt{q}$. Let $S \subseteq k$ be a coset of a subgroup or an interval. Put $s = 2$ if $p = 2$ and $s = 3$ if $p \neq 2$. Put $t = 1$ if S is a coset of a subgroup and $t = 2$ if S is an interval which is not a coset of a subgroup. Assume that*

$$\#S \geq 2t(2g - 2 + s)\sqrt{q}.$$

Assume that either $p \neq 2$ or $p = 2$ and $\deg(h) < g$. Then we have $\langle \varphi_C(C_S) \rangle = \mathrm{Pic}^0_k(C)$.

The above theorem improves the results of [**KS00**] in the following ways.

- We generalize by looking at hyperelliptic curves instead of only elliptic curves.
- We obtain similar theorems for subsets of $I \subseteq k$ or $I \subseteq k^*$ which have a small additive respectively multiplicative 'shape' (Theorem 4.6).
- Our constants tend to be a bit better. This improvement is already partially suggested in [**KS00**].
- We do not have a $(1 + \log p)$ factor. This improvement is also suggested in [**KS00**].
- We do look at the hard primes, such as $p = 2$ in the above theorem. These cases require more work and there are exceptional cases. In [**KS00**], this case is avoided by finding a similar theorem for the y-coordinate. In the end our estimates are better when $p = 2$, but there are exceptional sets coming from certain morphisms. Here is an example. Assume that E is an elliptic curve over a finite field k of characteristic 2 given by $y^2+a_1xy+a_3 = x^3+a_2x^2+a_4x+a_6$ with $a_1 \neq 0$. Then the map

$$\begin{aligned} \psi_E \colon E(k) &\to \mathbf{F}_2 \\ P &\mapsto \operatorname{tr}_{k/\mathbf{F}_2}\left((x(P)+a_2)/a_1^2\right) \\ \infty &\mapsto 0 \end{aligned}$$

  is a surjective morphism of groups with kernel $2E(k)$ (Proposition 5.4). Hence if we take $S = \{s \in k : \operatorname{tr}_{k/\mathbf{F}_2}((s+a_2)/a_1^2) = 0\}$, a coset of a subgroup of k of cardinality $q/2$, then $\langle P \in E(k) : x(P) \in S\rangle = 2E(k)$.

  In the multiplicative case, one has similar exceptional cases. Assume that E is an elliptic curve over a finite field k of odd characteristic given by $y^2 = x^3 + a_2x^2 + a_4x$. Then we have a surjective morphism

$$\begin{aligned} \phi_C \colon E(k) &\to k^*/k^{*2} \\ P &\mapsto \overline{x(P)} \\ \infty &\mapsto 1 \\ (0,0) &\mapsto \overline{a_4}. \end{aligned}$$

  (see Proposition 6.3).

In [**KS00**] the authors use the aforementioned corollary ([**KS00**, Corollary 2]) to give a deterministic algorithm to find the group structure of the set of rational points of an elliptic curve over a finite field of size q in $O(q^{1/2+\epsilon})$. By lack of good pairings, we use Theorem 1.2 just to find a generating set of the Picard group.

In [**KS00**] the authors give a deterministic algorithm to find the group structure of the set of rational points of an elliptic curve over a finite field of size q in $O(q^{1/2+\epsilon})$. In the end of their article, they discuss the possibility to generalize to hyperelliptic curves. We carry out this generalization and improve in the following ways.

Remark 1.3. Floris Hess has done similar calculations but he never published them. He remarked me that some of the tricks we use actually go back to Jean-Pierre Serre.

1.2. Strategy of the proofs. The strategy of the proof of Theorem 1.2 is the following. First we translate our problem to the calculation of certain character sums on the finite abelian group $k^+ \times \operatorname{Pic}^0_k(C)$. We then construct, using class field theory, a finite

geometric abelian extension of function fields IM of $k(C)$ with group $G = k^+ \times \mathrm{Pic}_k^0(C)$, which for a point $P \in C(k) \setminus \{\infty'\}$ satisfies $(P, M/k(C)) = (x(P), [P] - [\infty']) \in G$. Then using theorems from class field theory, we can estimate the character sums after we have calculated conductors of certain subextensions of $M/k(C)$. In certain exceptional cases, our proof does not work. The extension $M/k(C)$ we obtain either has Galois group which is smaller than $k^+ \times \mathrm{Pic}_k^0(C)$ or $M/k(C)$ is not geometric. With a bit more work, one can still work out these cases. The strategy for the multiplicative subset is similar.

2. Realizing Galois groups together with Frobenius elements

Let k be a finite field of cardinality $q = p^m$ of characteristic p. We want to realize k^+ and k^* as Galois groups of an extension of $K = k(x)$, the rational function field, with prescribed Frobenius elements.

There are two ways of approaching this problem. One is by means of non-explicit class field theory. The other approach is explicit class field theory. We use a mixture of both.

Let $P \neq \infty$ be a prime of $k(x)$, the function field of the projective line over k, corresponding to $f = \sum_{i=0}^{n} a_i x^i$ with $a_n = 1$. We put $\mathrm{N}(P) = (-1)^n a_0 \in k$. Furthermore, we put $\mathrm{T}(P) = -a_{n-1} \in k$.

Remark 2.1. We can interpret the definition above in the following way. Consider the points of $\mathbf{P}^1(\overline{k})$. Then $\mathrm{Gal}(\overline{k}/k)$ acts on $\mathbf{P}^1(\overline{k})$ and its orbits correspond to the primes of $k(x)$, the length of the orbit being the degree of the corresponding prime (Proposition 2.11 from Chapter 2). More precisely, an irreducible polynomial $f \in k[x]$ corresponding to a prime P corresponds to the set $Z(f) = \{\alpha \in \overline{k} : f(\alpha) = 0\} \subseteq \mathbf{A}^1(\overline{k}) \subseteq \mathbf{P}^1(\overline{k})$. Then one has for any $\beta \in Z(f)$ the equalities $\mathrm{T}(P) = \sum_{\alpha \in Z(f)} \alpha = \mathrm{tr}_{k(\beta)/k}(\beta)$. A similar statement holds for $\mathrm{N}(P)$.

We will first realize k^+ as a Galois group.

Proposition 2.2. *Let $K_+ = K[Y]/(Y^q - Y - x)$ and let $y = \overline{Y} \in K_+$. Then K_+/K is a Galois extension of fields for which the following hold:*

i. *the map $\varphi\colon k \to \mathrm{Gal}(K_+/K)$, $c \mapsto (y \mapsto y + c)$ is an isomorphism of groups;*
ii. *the extension is totally ramified at ∞, and is unramified at all other primes;*
iii. *the extension is geometric;*
iv. *for $P \in \mathcal{P}_{K/k} \setminus \{\infty\}$ we have $(P, K_+/K) = \varphi(\mathrm{T}(P)) \in \mathrm{Gal}(K_+/K)$;*
v. *$\mathfrak{f}(K_+/K) = 2\infty$, $\mathrm{disc}(K_+/K) = 2(q-1)\infty$; the conductor of any nontrivial subextension of K_+/K is 2∞;*
vi. *$g(K_+) = 0$.*

Proof. We will first show that $f = Y^q - Y - x \in k[x][Y]$ is irreducible. Let y' be a zero of this polynomial (in some algebraic closure) and consider $K' = K(y')$. Let ∞' be a prime of K' extending the prime ∞. It is easy to see that $v_{\infty'}(y) < 0$ and hence we have $-e(\infty'/\infty) = v_{\infty'}(x) = v_{\infty'}(y'^q - y') = v_{\infty'}(y'^q) = q v_{\infty'}(y')$. It follows that the ramification index is divisible by q and hence is equal to q. This proves that $K' = K_+$ is a field, that K_+/K is totally ramified at ∞ and statement iii.

One can easily prove statement i.

Consider a prime corresponding to a monic irreducible $f \in k[x]$ of degree n. Using Proposition 7.8 from Chapter 1 we see that the extension is unramified at this prime, and that the Frobenius can be found by looking at the action on $(k[x]/(f))\,[a]$ where $a \in \overline{k}$ is a root of $Y^q - Y - x \pmod f$. Note that $a^{q^n} = a + x + x^q + \ldots + x^{q^{n-1}} \pmod f = a + \mathrm{tr}_{k[x]/(f)/k}(x)$. This gives $(P, K_+/K) = \varphi(\mathrm{T}(P)) \in \mathrm{Gal}(K_+/K)$ and finishes the proof of ii and iv.

Note that $K_+ = k(y)$, and hence K_+ has genus 0 (statement vi). Using Riemann-Hurwitz (Theorem 2.22 from Chapter 2) we see that the degree of the discriminant is $2(q-1)$, and hence that the discriminant is $2(q-1)\infty$ (Proposition 2.21 from Chapter 2). Note that all nontrivial subextensions are wildly ramified and hence have conductor at least 2∞ (Corollary 3.6). Using the Führerdiskriminantenproduktformel (Theorem 3.7 from Chapter 2) we see that all non-trivial extensions have conductor 2∞.

□

Proposition 2.3. *Let K_+ be as in the previous proposition (Proposition 2.2). For $c \in k^*$ put $z_c = (cy) + (cy)^p + (cy)^{p^2} + \ldots + (cy)^{p^{m-1}}$. For $\overline{c} \in k^*/\mathbf{F}_p^*$ set $K_{\overline{c}} = K(z_c)$. Let $\tau_c \colon k \to \mathbf{F}_p$ be defined by $a \mapsto \mathrm{tr}_{k/\mathbf{F}_p}(ca)$. Then the following hold:*

i. *z_c is a zero of the irreducible polynomial $f_c = X^p - X - cx \in k(x)[X]$;*

ii. *$K_{\overline{c}}/K$ is Galois, the map $\varphi_c \colon \mathbf{F}_p \to \mathrm{Gal}(K_{\overline{c}}/K)$, $a \mapsto (z_c \mapsto z_c + a)$ is an isomorphism and the following diagram is commutative:*

$$\begin{array}{ccc} \mathrm{Gal}(K_+/K) & \xrightarrow{\sim} & k \\ \big\downarrow & & \big\downarrow{\scriptstyle \tau_c} \\ \mathrm{Gal}(K_{\overline{c}}/K) & \xrightarrow{\sim} & \mathbf{F}_p; \end{array}$$

iii. *for $P \in \mathcal{P}_{K/k} \setminus \{\infty\}$ we have*

$$(P, K_{\overline{c}}/K) = \varphi_c(\mathrm{tr}_{k/\mathbf{F}_p}(c\,\mathrm{T}(P))) \in \mathrm{Gal}(K_{\overline{c}}/K);$$

iv. *the map*

$$\begin{aligned} k^*/\mathbf{F}_p^* &\to \{L : K \subseteq L \subseteq K_+,\ [L:K] = p\} \\ \overline{c} &\mapsto K_{\overline{c}} \end{aligned}$$

is a bijection.

Proof. For $a \in k$ we have $\varphi(a)(z_c) = z_c + \mathrm{tr}_{k/\mathbf{F}_p}(ca)$. As $\mathrm{tr}_{k/\mathbf{F}_p}$ is surjective, it follows that $[K_{\overline{c}} : F] = p$. As z_c is a zero of $f_c = X^p - X - cx$, it follows that f_c the minimal polynomial of z_c over K. Hence statement i follows. Statement ii now follows easily. Statement iii follows directly from the definition of Frobenius elements, ii and Proposition 2.2 iv.

We will now prove statement iv. Both sets have the same size, hence it is enough to show that the map is injective. Using ii it is equivalent to show that for $c, c' \in k^*$ we have $\ker(\tau_c) = \ker(\tau_{c'})$ iff $c/c' \in \mathbf{F}_p^*$. But this follows easily from the fact that the trace form is non-degenerate. □

We will now realize k^* as a Galois group with specific Frobenius elements.

Proposition 2.4. *Let $K_* = K[Y]/(Y^{q-1} - x)$ and let y be the image of Y in K_*. Then K_*/K is a Galois extension of fields for which the following hold:*

i. *the map $\varphi\colon k^* \to \mathrm{Gal}(K_*/K)$, $c \mapsto (y \mapsto cy)$ is an isomorphism;*
ii. *the extension is totally ramified at (x) and ∞ and is unramified at all other primes;*
iii. *the extension is geometric;*
iv. *for $P \in \mathcal{P}_k(K) \setminus \{(x), \infty\}$ we have $(P, K_*/K) = \varphi(\mathrm{N}(P)) \in \mathrm{Gal}(K_*/K)$.*
v. *the conductor of K_*/K and any nontrivial subextension is $\infty + (x)$ and $\mathrm{disc}(K_*/K) = (q-2)(\infty + (x))$;*
vi. *for $d|(q-1)$, the unique subextension of degree d of K_*/K is given by $K(y^{(q-1)/d})$;*
vii. *$g(K_*) = 0$.*

Proof. The polynomial $f = Y^{q-1} - x$ is Eisenstein at x. This shows that K_*/K is a field extension which is totally ramified at (x). In a similar way, one can show that K_*/K is totally ramified at ∞. This proves the first part of ii and it proves iii.

One can easily prove i.

Let $f \in k[x]$, $f \neq x$, be an irreducible monic polynomial of degree n. Using Proposition 7.8 from Chapter 1, we see that this prime is unramified and that the Frobenius can be found by looking at the action of $(k[x]/(f))\,[a]$ where $a \in \overline{k}$ is a root of $Y^{q-1} - x \pmod f$. Note that $a^{q^n} = a \cdot \mathrm{Norm}_{k[x]/(f)/k}(x)$. This proves iv and the rest of ii.

Notice that our extension is tamely ramified and hence the conductor is just the sum of the ramifying primes (Corollary 3.6 from Chapter 2). Since the extension is tamely ramified, the discriminant is $(q-2)(\infty + (x))$ (Proposition 2.21 from Chapter 2).

Statement vi follows easily and statement vii follows since $K_* = k(y)$. □

3. A generic algorithm

Proposition 3.1. *Let C be a normal projective curve of genus $g \geq 1$ over a finite field k and let $D \in \mathrm{div}(k(C))$ satisfy $\deg_k(D) = 1$. Let $\varphi_D\colon \mathrm{div}(C) \to \mathrm{Pic}^0_k(C)$ given by $P \mapsto [P] - \deg_k(P)[D]$. Let $d \in \mathbf{Z}_{\geq 0}$ such that one of the following holds:*

i. *$\#C(k^d) > (2g-2)q^{d/2}$;*
ii. *$q^d \geq (4g-2)^2$.*

Then the images under φ_D of the primes of degree dividing d generate $\mathrm{Pic}^0_k(C)$.

Proof. Essentially this is done in [**MST99**, Theorem 2]: they prove more than what they claim.

The proof is the following. Put $L = k(C)$. Use Proposition 3.10 from Chapter 2 and consider the unramified extension L_D/L with group $\mathrm{Pic}^0_k(C)$. If the required group is not equal to $\mathrm{Pic}^0_k(C)$, then there is a non-trivial character $\chi \in \mathrm{Pic}^0_k(C)^\vee$ which is trivial on the primes of degree dividing d. It follows that

$$0 = \sum_{P \in \mathrm{unr}^d(L_D/L)} \deg_k(P) \left(\chi((P, L_D/L))^{d/\deg_k(P)} - 1((P, L_D/L))^{d/\deg_k(P)} \right).$$

By Proposition 2.11 from Chapter 2 we have

$$\sum_{P \in \mathrm{unr}^d(L_D/L)} \deg_k(P) = \#C(k^d).$$

Theorem 3.18 from Chapter 2 then gives us

$$\#C(k^d) \leq (2g-2)q^{d/2}.$$

Hasse-Weil (Corollary 3.17 from Chapter 2) gives us $q^d - 2gq^{d/2} < \#C(k^d)$ and the result follows after some rewriting. □

Remark 3.2. If $g = 1$, one has $C(k) \neq \emptyset$. Hence we can apply the above corollary (Proposition 3.1). This especially holds when C is an elliptic curve.

The above proposition provides a generic algorithm for finding generators of a Picard group of a normal projective curve of genus $g \geq 1$ over a finite field. First find $d \in \mathbf{Z}_{\geq 1}$ such that $q^d \geq (4g-2)^2$. Let k' be a field of cardinality q^d and consider the curve $C' = C_{k'}$ corresponding to the function field $k(C)k'$. By Hasse-Weil (Corollary 3.17 from Chapter 2) there is a rational point $D \in C'(k')$, which we view as a divisor of degree 1. Then the image of $\varphi_D \colon \mathrm{div}(C') \to \mathrm{Pic}^0_{k'}(C')$ of the points of $C'(k')$ generate $\mathrm{Pic}^0_{k'}(C')$ (Proposition 3.1). Then use the surjective norm map $\mathrm{Pic}^0_{k'}(C') \to \mathrm{Pic}^0_k(C)$ (Corollary 3.15 from Chapter 2) to find generators of $\mathrm{Pic}^0_k(C)$. If one can do all the steps efficiently, this should give an algorithm which runs in time $O(g^{2+\epsilon}q^{1+\epsilon})$ for any $\epsilon > 0$.

In this chapter we will reduce the running time to $O(g^{2+\epsilon}q^{1/2+\epsilon})$ in case C is a hyperelliptic curve (in a special form). The reason why we can do it faster in these cases is that we do not have to find the whole of $C'(k')$, but we can restrict to a smaller subset.

4. Hyperelliptic curves: statements of the results

Let k be a finite field of cardinality q and characteristic p. Let C be a hyperelliptic curve over k of genus g given by an equation $y^2 + h(x)y = f(x)$ where (f, h) satisfies i, ii, iii and iv of Theorem 4.6 from Chapter 2. We want to have a 'canonical' element in $C(k)$. We have an embedding $k(x) \subseteq k(C)$ and we assume that this map is ramified at ∞. Call ∞' the point of C above ∞. By Theorem 4.6 from Chapter 2 this happens exactly if the following holds:

- $\mathrm{char}(k) \neq 2$: $\deg(f) = 2g + 1$;
- $\mathrm{char}(k) = 2$: $1 \leq \deg(h) \leq g$.

We define f_i and h_j by $f = \sum_i f_i x^i$ and $h = \sum_j h_j x^j$.

Using this point ∞', there is a map $\varphi_C \colon C(k) \to \mathrm{Pic}^0_k(C)$, $P \mapsto [P] - [\infty']$. Notice that φ_C is injective. Indeed, otherwise we would have $[P] - [Q] = 0 \in \mathrm{Pic}^0_k(C)$, which implies that C would be a projective line of genus 0, contradiction ([**Sti09**, Theorem 1.4.11]).

First let S be a subset of k. Then we can associate to S a shape parameter with respect to k. Let $C_S = \{P \in C(k) : x(P) \in S\}$. Can one give conditions on $\#S$ and $\mathrm{sh}_{k^+}(S)$ such that $\mathrm{Pic}^0_k(C) = \langle \varphi_C(C_S) \rangle$? We can ask a similar question if $S \subseteq k^*$ and the shape parameter is taken with respect to k^*. We will study both cases separately.

4.1. Additive x-coordinate.

Theorem 4.1. *Let C over k be a hyperelliptic curve of genus g given according to our assumptions as above such that $\#C(k) > (2g-2)\sqrt{q}$. Put $s = 2$ if $p = 2$ and $s = 3$ if $p \neq 2$. Let $S \subseteq k^+$ such that*

$$q^{3/2} \cdot 2(2g-2+s) \cdot \mathrm{sh}_{k^+}(S) < (\#C(k) + (2g-2+2s)\sqrt{q}) \cdot \#S.$$

Then the following hold:

i. *Assume that either $p \neq 2$ or $p = 2$ and $\deg(h) < g$. Then we have $\langle \varphi_C(C_S) \rangle = \mathrm{Pic}^0_k(C)$.*

ii. *Assume that $p = 2$ and $\deg(h) = g$. Define the following:*

$$d_i = f_{2g+i} + \sqrt{f_{2g+2}} h_{g-1+i} \in k \text{ (for } i \in \{0,1\})$$
$$\epsilon_C = (-1)^{\mathrm{tr}_{k/\mathbf{F}_2}(d_0/h_g^2)} \in \mathbf{C}$$
$$\lambda_2 \in \mathrm{Hom}(k^+, \mathbf{C}^*), c \mapsto (-1)^{\mathrm{tr}_{k/\mathbf{F}_2}(cd_1/h_g^2)}$$
$$H_C = \{x \in k : \lambda_2(x) = -\epsilon_C\} \subseteq k,$$
$$\psi_C \in \mathrm{Hom}(\mathrm{Pic}^0_k(C), \mathbf{F}_2) \setminus \{0\} \text{ as in Proposition 5.4.}$$

Then we have:

(a) $\langle \varphi_C(C_S) \rangle \in \{\mathrm{Pic}^0_k(C), \ker(\psi_C)\}$;

(b) *if $S \cap H_C = \emptyset$, then $\langle \varphi_C(C_S) \rangle = \ker(\psi_C)$;*

(c) *if $S \cap H_C \neq \emptyset$ and if S is a coset of a subgroup of k, then $\langle \varphi_C(C_S) \rangle = \mathrm{Pic}^0_k(C)$;*

(d) *if $S \cap H_C \neq \emptyset$ and if*

$$q^{3/2}(2g-2+s)\,\mathrm{sh}_k(S \cap H_C) < (\#C(k) + (2g-2+2s)\sqrt{q}) \cdot \#(S \cap H_C),$$

then $\langle \varphi_C(C_S) \rangle = \mathrm{Pic}^0_k(C)$.

Remark 4.2. Theorem 4.1 depends on C because of the dependence on $\#C(k)$. One can get rid of this dependence by using the Hasse-Weil bound (Corollary 3.17 from Chapter 2). This theorem gives $\#C(k) \geq q + 1 - 2g\sqrt{q}$. For example, $\#C(k) > (2g-2)\sqrt{q}$ follows when $q \geq (4g-2)^2$.

Proof of Theorem 1.2. This follows from Theorem 4.1, Hasse-Weil (Corollary 3.17 from Chapter 2) and bounds on the shape (Proposition 3.3ii from Chapter 3 and Lemma 3.6 from Chapter 3). □

Example 4.3. Assume that $g = 1$ in Theorem 4.1. Then using some crude estimates, one sees that we can apply the theorem if $2s \cdot \mathrm{sh}_{k^+}(S) \leq \#S$. Furthermore, the exceptional case corresponds to ordinary elliptic curves in characteristic 2. In this case, there is a unique subgroup of $\mathrm{Pic}^0_k(E) \cong E(k)$ of index 2, namely $2E(k)$, which must be equal to $\ker(\psi_E)$.

Remark 4.4. If one puts $S = k$ in Theorem 4.1, one obtains a special case of Proposition 3.1.

Remark 4.5. Give a subset S of k^+, an upper bound on its shape can be obtained from picking a function $f \in \mathbf{C}[S] \subseteq \mathbf{C}[k]$ with $f_{\chi_0} \neq 0$. On the other hand, one can use Theorem 4.1 to give lower bounds for the shape of S.

4.2. Multiplicative x-coordinate.

Theorem 4.6. *Let C over k be a hyperelliptic curve of genus g given according to our assumptions as above. Put*

$$r = \#\{P \in C(k) \setminus \{\infty\} : x(P) = 0\} = \begin{cases} 2 & \text{if } p \neq 2,\ f_0 \in k^{*2} \\ 2 & \text{if } p = 2,\ h_0 \neq 0,\ \mathrm{tr}_{k/\mathbf{F}_2}(\frac{f_0}{h_0^2}) = 0 \\ 1 & \text{if } p \neq 2,\ f_0 = 0 \\ 1 & \text{if } p = 2,\ h_0 = 0 \\ 0 & \text{else} \end{cases}$$

and

$$s = \begin{cases} 2 & \text{if } p = 2, h_0 = 0 \\ 2 & \text{if } p \neq 2, f_0 = 0 \\ 3 & \text{else.} \end{cases}$$

Assume that $\#C(k) > (2g-2)\sqrt{q} + 2r$. Let $S \subseteq k^*$ such that

$$(q-1)\sqrt{q} \cdot 2(2g-2+s) \cdot \mathrm{sh}_{k^*}(S) < (\#C(k) + (2g-2+2s)\sqrt{q} - 2r) \cdot \#S.$$

Then the following hold:

i. *Assume that either $p = 2$ or $p \neq 2$ and $x \nmid f$. Then we have $\langle \varphi_C(C_S) \rangle = \mathrm{Pic}_k^0(C)$.*
ii. *Assume that $p \neq 2$ and $x | f_2$. Define the following:*

$$\lambda_2' \colon k^* \to k^*/k^{*2} \cong \{\pm 1\} \subseteq \mathbf{C}^*$$
$$\delta_C = \lambda_2'(f_{2g+1})$$
$$H_C' = \{x \in k : \lambda_2'(x) = -\delta_C\}$$
$$\phi_C \in \mathrm{Hom}(\mathrm{Pic}_k^0(C), k^*/k^{*2}) \setminus \{0\} \text{ (as in Proposition 6.3).}$$

Then we have:
(a) $\langle \varphi_C(C_S) \rangle \in \{\mathrm{Pic}_k^0(C), \ker(\phi_C)\}$;
(b) *if $S \cap H_C' = \emptyset$, then $\langle \varphi_C(C_S) \rangle = \ker(\phi_C)$;*
(c) *if $S \cap H_C' \neq \emptyset$ and if S is a coset of a subgroup of k^*, then $\langle \varphi_C(C_S) \rangle = \mathrm{Pic}_k^0(C)$;*
(d) *if $S \cap H_C' \neq \emptyset$ and if*

$$(q-1)\sqrt{q}(2g-2+s) \cdot \mathrm{sh}_{k^*}(S \cap H_C') < (\#C(k) + (2g-2+2s)\sqrt{q} - 2r)\,\#(S \cap H_C'),$$

then $\langle \varphi_C(C_S) \rangle = \mathrm{Pic}_k^0(C)$.

Corollary 4.7. *Let C over k be a hyperelliptic curve of genus g given according to our assumptions as above. Define r as in Theorem 4.6. Assume that one of the following hold:*

i. *$\#C(k) > \sqrt{q} \cdot (2g-2) + 2r$;*
ii. *$q + 1 - 2r \geq (4g-2)\sqrt{q}$.*

Then we have $\langle \varphi_C(k^*) \rangle = \mathrm{Pic}_k^0(k)$.

PROOF. Note that ii follows from i by Hasse-Weil (Corollary 3.17 from Chapter 2). Consider statement i. Put $S = k^*$ in Theorem 4.6. Note that $\mathrm{sh}_{k^*}(S) = 1$ (Proposition 3.3 from Chapter 3). The result follows from Theorem 4.1.

The second statement implies the first one if one puts $\#C(k) \geq q + 1 - 2g\sqrt{q}$ by the Hasse-Weil bound (Corollary 3.17 from Chapter 2). □

Remark 4.8. Corollary 4.7 is already interesting if $g = 1$. Then we need $\#C(k) > 2r$ to obtain the result. We will give three examples where $\#C(k) = 2r$, but with $\langle \varphi_C(k^*) \rangle \subsetneq \mathrm{Pic}^0_k(C)$

Consider the curve $y^2 + xy = x^3 + x^2 + 1$ over $\mathbf{F}_2$ with $C(k) = \{\infty', (0,1)\}$.

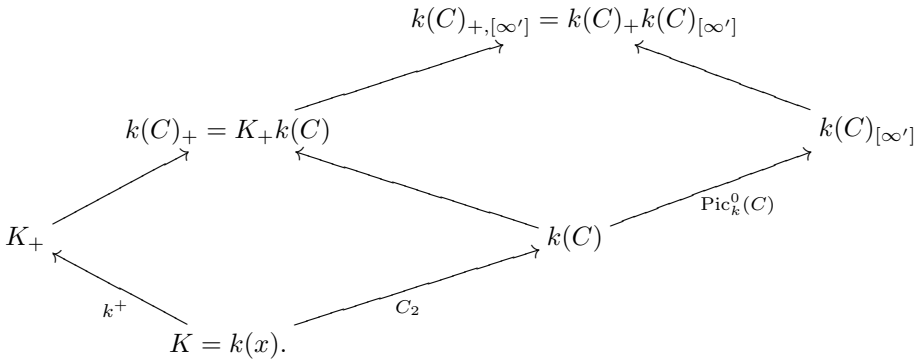
Consider the curve $y^2 = x^3 + 2x^2 + 2x$ over $\mathbf{F}_3$ with $C(k) = \{\infty', (0,0)\}$.

Consider the curve $y^2 = x^3 + x + 1$ over $\mathbf{F}_3$, with $C(k) = \{\infty', (0,1), (0,-1), (1,0)\}$ which is isomorphic to C_4.

5. Additive x-coordinate

Let C be a hyperelliptic curve of genus $g \geq 1$ over a finite field k of cardinality q and characteristic p given by an equation as in Section 4 with ∞' the point at infinity.

5.1. The diagram. Proposition 3.10 from Chapter 2 gives us an extension $k(C)_{[\infty']}/k(C)$ which is unramified with Galois group $\mathrm{Pic}^0_k(C)$ and the Frobenius at a rational point is $[P] - [\infty']$. Furthermore, we have an extension K_+ of $K = k(x)$ which has been studied in Proposition 2.2. Consider the following diagram of function fields:



The extension $k(C)/K$ has been studied in Theorem 4.6 from Chapter 2. It is geometric, Galois with group C_2 and totally ramified at ∞ and at some more points. The extension K_+/K is geometric and Galois with group k^+ and totally ramified at ∞. Consider the extension $k(C)_+/K$. As K_+ and $k(C)$ are linearly disjoint by genus considerations (Riemann-Hurwitz, Theorem 2.22 from Chapter 2), $k(C)_+/K$ is Galois with group $k^+ \times C_2$. Also $k(C)_+/k(C)$ is Galois with group k^+. We claim that $k(C)_+/K$ is geometric. If $\mathrm{char}(k) \neq 2$, then as $(\#k, 2) = 1$, the extension $k(C)_+/K$ is totally ramified at ∞. Assume that $\mathrm{char}(k) = 2$ and that $\deg(h) < g$. The conductor at ∞ of $k(C)/K$ is $2(g + 1 - \deg(h))\infty$, which is more than the conductor of K_+/K at ∞, which is 2∞. Hence $k(C)_+/K$ is totally ramified at ∞ and $k(C)_+/k(C)$ is totally ramified at ∞'. Assume that $\mathrm{char}(k) = 2$ and that $\deg(h) = g$. In this case, take a prime of K, not ∞, dividing h. Then $k(C)/K$ is ramified at this prime, but K_+/K is

not. Hence $k(C)_+/K_+$ is ramified at a prime above such a prime, and it cannot be a constant field extension. We conclude that $k(C)_+/K$ is always geometric.

The only possible ramification in $k(C)_+/k(C)$ is at ∞' (Corollary 3.11 from Chapter 1). We have already shown that it is totally ramified at ∞' if $\mathrm{char}(k) \neq 2$ or $\mathrm{char}(k) = 2$ and $\deg(h) = g$. One knows that the maximal abelian extension of K_∞, the completion of K at ∞, which is totally ramified of conductor 2∞ has degree q. Hence if $\mathrm{char}(k) = 2$ and $\deg(h) = g$, we see that $k(C)_+/K$ cannot be totally ramified at ∞. Hence in this case $k(C)_+/k(C)$ cannot be totally ramified. There is a unique field L with $k(C) \subseteq L \subseteq k(C)_+$ with $[L : k(C)] = 2$ which is unramified at ∞' (Corollary 3.15 from Chapter 1), and hence unramified.

Lemma 5.1. *Let k be a finite field of characteristic p and let $a \in k$. Then $f_a = x^p - x - a \in k[x]$ is irreducible if and only if $\mathrm{tr}_{k/\mathbf{F}_p}(a) \neq 0$.*

Proof. We claim that f_a is irreducible iff it has no roots. Indeed, if one adds a root of f_a to k, then the polynomial splits completely. Hence the degree of an irreducible factor does not depend on the factor, and since p is prime, the result follows.

$\Longrightarrow$: If $\alpha \in k$ is a root of f_a, then $\mathrm{tr}_{k/\mathbf{F}_p}(a) = \mathrm{tr}_{k/\mathbf{F}_p}(\alpha^p) - \mathrm{tr}_{k/\mathbf{F}_p}(\alpha) = 0$, because α and α^p are conjugates.

$\Longleftarrow$: Consider the map $\varphi\colon k \to k$, $x \mapsto x^p - x$. Then f_a is irreducible if and only if a is not in the image of φ. The kernel of this map is $\mathbf{F}_p$ and hence the image is exactly the kernel of the trace map. □

The following lemma explicitly describes L.

Lemma 5.2. *Assume that $p = 2$ and that $\deg(h) = g$. For $i = 0, 1$ put $d_i = f_{2g+i} + \sqrt{f_{2g+2}}h_{g-1+i}$. Then the unique unramified subextension L of $k(C)_+/k(C)$ comes from the subextension of K_+/K given by $z^2 - z - cx$ with $c = \frac{d_1}{h_g^2}$. This extension $L/k(C)$ is totally split at ∞' if and only if $\mathrm{tr}_{k/\mathbf{F}_2}\left(\frac{d_0}{h_g^2}\right) = 0$.*

Proof. Let v be the normalized valuation at ∞' of $k(C)$. Then $v(x) = -2$ as $k(C)/K$ is ramified. We have $\deg(f) \in \{2g+1, 2g+2\}$. Put $y' = y + \sqrt{f_{2g+2}}x^{g+1} \in k(C)$. Then we have $y'^2 + hy' = f_{\mathrm{new}}$ where $f_{\mathrm{new}} = f + f_{2g+2}x^{2g+2} + \sqrt{f_{2g+2}}hx^{g+1}$. Note that $f_{\mathrm{new},2g+1} = d_1$ is nonzero, as its square is nonzero by Theorem 4.6 iv(c) from Chapter 2. Hence f_{new} is of degree $2g + 1$. From the equation which y' satisfies, one easily obtains $v(y') = -(2g + 1)$.

Let z be an element of K_+ satisfying $z^2 - z - d_1x/h_g^2 = 0$ (Proposition 2.2 for the existence). Notice that $y'' = y'/(h_g x^g)$ satisfies

$$\begin{aligned} y''^2 + y'' &= \frac{f_{\mathrm{new}}(x) + (h(x) - h_g x^g)y'}{h_g^2 x^{2g}} \\ &= \frac{d_1 x}{h_g^2} + \frac{d_0}{h_g^2} + \frac{(f_{\mathrm{new}} - d_1 x^{2g+1} - d_0 x^{2g}) + (h(x) - h_g x^g)y'}{h_g^2 x^{2g}}. \end{aligned}$$

Hence we have

$$(y' + z)^2 + (y' + z) = \frac{d_0}{h_g^2} + \frac{(f_{\mathrm{new}}(x) - f_{2g+1}x^{2g+1} - f_{2g}x^{2g}) + (h(x) - h_g x^g)y'}{h_g^2 x^{2g}}.$$

The valuation of the right hand side at infinity is non-negative and the part in the fraction has a positive valuation. We use Proposition 7.8 from Chapter 1 to see that the extension $L/k(C)$ is unramified at infinity, and that the extension splits completely at infinity if and only if the polynomial $x^2 + x + \frac{d_0}{h_g^2}$ is not irreducible in $k[x]$. This happens if and only if $\mathrm{tr}_{k/\mathbf{F}_2}(\frac{d_0}{h_g^2}) = 0$ by Lemma 5.1. □

The following lemma gives us the conductor of subextensions of $k(C)_+/k(C)$.

Lemma 5.3. *Let L' be a subextension of degree p of $k(C)_+/k(C)$ which is totally ramified at ∞'. Then one has*

$$\mathfrak{f}(L'/k(C)) = \begin{cases} 2\infty' & \text{if } p = 2 \\ 3\infty' & \text{if } p \neq 2. \end{cases}$$

Proof. This follows from Lemma 3.19 from Chapter 2, Theorem 4.6 from Chapter 2, and Proposition 2.2. □

The next step is to study the extension $k(C)_{+,[\infty']}/k(C)$. If eiher $p \neq 2$ or $p = 2$ and $\deg(h) < g$, then we have seen above that $k(C)_+/k(C)$ is totally ramified at ∞'. As $k(C)_{[\infty']}/k(C)$ is unramified, it shows that $k(C)_+$ and $k(C)_{[\infty']}$ are disjoint over $k(C)$. In this case we have $\mathrm{Gal}(k(C)_{+,[\infty']}/k(C)) = k^+ \times \mathrm{Pic}_k^0(C)$.

Assume that $p = 2$ and that $\deg(h) = g$. We want to understand the Galois extension $k(C)_{+,[\infty']}/k(C)$. Using Lemma 5.2 and Proposition 3.10 from Chapter 2, we see that two things can happen: If $\mathrm{tr}_{k/\mathbf{F}_2}(\frac{d_0}{h_g^2}) = 0$, then one has $L \subseteq k(C)_{[\infty']}$ (there is a unique maximal extension where ∞' splits, see Corollary 3.15 from Chapter 1). This means that there is a surjective homomorphism $\mathrm{Pic}_k^0(C) \to \mathrm{Gal}(L/k(C))$. One has $\mathrm{Gal}(k(C)_{+,[\infty']}/k(C)) = k^+ \times_{\mathrm{Gal}(L/k(C))} \mathrm{Pic}_k^0(C)$. If $\mathrm{tr}_{k/\mathbf{F}_2}(\frac{d_0}{h_g^2}) = 1$, then $k(C)_+$ and $k(C)_{[\infty']}$ are disjoint, and $\mathrm{Gal}(k(C)_{+,[\infty']}/k(C)) = k^+ \times \mathrm{Pic}_k^0(C)$. Unfortunately, the extension is not geometric. There is a degree 2 extension of k inside $k(C)_{+,[\infty']}$ (Proposition 3.10 from Chapter 2). Also in this case one can produce a surjective homomorphism $\mathrm{Pic}_k^0(C) \to \mathrm{Gal}(L/k(C))$.

Recall the definition of T from Page 105.

Proposition 5.4. *Assume that $p = 2$ and that $\deg(h) = g$. Then we have a surjective morphism of groups*

$$\psi_C \colon \mathrm{Pic}_k^0(C) \to \mathbf{F}_2$$

defined as follows: Let $P \neq \infty'$ be a prime of $k(C)$. Then we have:

$$\psi_C([P] - \deg_k(P)[\infty']) = \mathrm{tr}_{k/\mathbf{F}_2}\left(\frac{\mathrm{f}(P/P|_K)\,\mathrm{T}(P|_K)d_1 + \deg_k(P)d_0}{h_g^2}\right) \in \mathbf{F}_2.$$

Proof. Assume first $\mathrm{tr}_{k/\mathbf{F}_2}(\frac{d_0}{h_g^2}) = 0$. Then $L \subseteq k(C)_{[\infty']}$ and this gives a surjective map ψ_C on the Galois groups. To see what it does, we look at the Frobenius elements. Let P be a prime of degree n in $k(C)$. One has $(P, k(C)_{[\infty']}/k(C)) = [P] - n[\infty'] \in \mathrm{Pic}_k^0(C)$ (Proposition 3.10 from Chapter 2). This Frobenius maps to

$(P, L/k(C)) = \mathrm{tr}_{k/\mathbf{F}_2}(\frac{\mathrm{f}(P/P|_K)\,\mathrm{T}(P|_K)d_1}{h_g^2}) = \mathrm{tr}_{k/\mathbf{F}_2}(\frac{\mathrm{f}(P/P|_K)\,\mathrm{T}(P|_K)d_1+\deg_k(P)d_0}{h_g^2})$ (Corollary 9.3 from Chapter 1, Proposition 2.3 and Lemma 5.2).

Assume $\mathrm{tr}_{k/\mathbf{F}_2}(\frac{d_0}{h_g^2}) = 1$. Let L' be the third degree 2 extension in the V_4 extension Lk' over $k(C)$ where k' is the unique degree 2 extension of k. Then we have a natural map $\mathrm{Pic}_k^0(C) \to \mathrm{Gal}(L'/k(C)) = \mathbf{F}_2$ (Proposition 3.10 from Chapter 2). Let P be a prime of $k(C)$ of degree n. Note that there is a unique maximal extension in $Lk'/k(C)$ where P is totally split (Corollary 3.15 from Chapter 1). Assume that n is even. Then P splits in $L'/k(C)$ iff it splits in $L/k(C)$ (Proposition 2.15 from Chapter 2). If n is odd, then P splits in $L'/k(C)$ iff it does not split in $L/k(C)$. This gives the required map. □

Remark 5.5. Assume that E is an elliptic curve over a finite field k of characteristic 2 given by $y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$ with $a_1 \neq 0$. Then the above map simplifies to

$$\begin{aligned}\psi_E\colon E(k) &\to \mathbf{F}_2\\ P &\mapsto \mathrm{tr}_{k/\mathbf{F}_2}((x(P) + a_2)/a_1^2)\\ \infty &\mapsto 0.\end{aligned}$$

As $E(k)$ has a unique subgroup of index 2, namely $2E(k)$, this is also the kernel of the map. It is actually quite easy to see that the map is a morphism in this case. Suppose that the points (x_i, y_i) $(i = 1, 2, 3)$ lie on a line $y = \lambda x + \mu$. This gives the equation $\lambda^2 + a_1\lambda + a_2 = x_1 + x_2 + x_3$. If we divide by a_1^2 we obtain $\frac{x_1+a_2}{a_1^2} + \frac{x_2+a_2}{a_1^2} + \frac{x_2+a_2}{a_1^2} = \left(\frac{\lambda}{a_1}\right)^2 + \frac{\lambda}{a_1}$. Notice that $\mathrm{tr}_{k/\mathbf{F}_2}(\left(\frac{\lambda}{a_1}\right)^2) = \mathrm{tr}_{k/\mathbf{F}_2}(\frac{\lambda}{a_1})$ and hence this relation is preserved. One then checks that it is also correct if some of the points are the point at infinity, and one concludes that the map is a morphism.

5.2. Character sum estimates. Put

$$C(k)^* = C(k) \setminus \{\infty'\} = \mathrm{unr}^1(k(C)_{+,[\infty']}/k(C)).$$

Let $\lambda \in k^\vee$ and $\chi \in \mathrm{Pic}_k^0(C)^\vee$. Since we have a natural map $\mathrm{Gal}(k(C)_{+,[\infty']}/k(C)) \to k^+ \times \mathrm{Pic}_k^0(C)$, we can view (λ, χ) as a character of $\mathrm{Gal}(k(C)_{+,[\infty']}/k(C))$ by taking the product. We put

$$c_{(\lambda,\chi)} = \sum_{P\in C(k)^*} (\lambda, \chi)(P, k(C)_{+,[\infty']}/k(C)) = \sum_{P\in C(k)^*} \lambda(x(P))\chi(\varphi_C(P))$$

(see Lemma 9.4 from Chapter 1, we avoid the only ramification at ∞'). Our goal is to estimate these $c_{(\lambda,\chi)}$. Put $s = 2$ if $p = 2$ and $s = 3$ if $p \neq 2$.

5.2.1. *Case 1.* Assume that either $p \neq 2$ or $p = 2$ and $\deg(h) < g$.

Lemma 5.6. *The following hold for $\lambda \in k^\vee$ and $\chi \in \mathrm{Pic}_k^0(C)^\vee$.*

i. *if $\lambda \neq \chi_0$, then $|c_{(\lambda,\chi)}| \leq (2g - 2 + s)\sqrt{q}$;*
ii. *$c_{\chi_0,\chi_0} = \#C(k) - 1$;*
iii. *if $\chi \neq \chi_0$, then $|c_{(\chi_0,\chi)} + 1| \leq (2g - 2)\sqrt{q}$.*

PROOF. i: The degree of the conductor of the corresponding extension is s (see Lemma 5.3 and Lemma 3.20 from Chapter 2). Hence the result follows from Theorem 3.18 from Chapter 2.

ii: Obvious.

iii: The degree of the conductor of the corresponding extension is 0 (Lemma 5.3, Lemma 3.20 from Chapter 2). Hence the result follows from Theorem 3.18 from Chapter 2. □

5.2.2. *Case 2.* Assume that $p = 2$ and $\deg(h) = g$. Let λ_2 be the special character of k^+ corresponding to the unramified subextension of $L/k(C)$ of degree 2. More explicitly, we define $\lambda_2 \in k^\vee$, $c \mapsto (-1)^{\mathrm{tr}_{k/\mathbf{F}_2}(cd_1/h_g^2)} \in \mathbf{C}^*$ (Lemma 5.2 and Proposition 2.3). Put $\epsilon_C = (-1)^{\mathrm{tr}_{k/\mathbf{F}_2}(d_0/h_g^2)}$ (it is -1 if there is a constant field extension). Let $\chi_2 = (-1)^{\psi_C} \in \mathrm{Pic}_k^0(C)^\vee$.

Lemma 5.7. *The following hold for $\lambda \in k^\vee$ and $\chi \in \mathrm{Pic}_k^0(C)^\vee$.*

i. $c_{(\lambda,\chi)\cdot(\lambda_2,\chi_2)} = \epsilon_C c_{(\lambda,\chi)}$;
ii. *if* $\lambda \neq \chi_0, \lambda_2$, *then* $|c_{(\lambda,\chi)}| \leq (2g-2+s)\sqrt{q}$;
iii. $c_{(\chi_0,\chi_0)} = \#C(k) - 1$;
iv. $c_{(\lambda_2,\chi_2)} = \epsilon_C\,(\#C(k) - 1)$;
v. *if* $\chi \neq \chi_0$, *then* $|c_{(\chi_0,\chi)} + 1| \leq (2g-2)\sqrt{q}$;
vi. *if* $\chi \neq \chi_2$, *then* $|c_{(\lambda_2,\chi)} + \epsilon_C| \leq (2g-2)\sqrt{q}$.

PROOF. i: Let $P \in C(k)^*$. We have $\lambda_2(x(P))\chi_2(\varphi_C(P)) = \epsilon_C$ by construction. Indeed, if $\epsilon_C = 1$, $\lambda_2(x(P))$ and $\chi_2(\varphi_C(P))$ are equal. If $\epsilon_C = -1$, then a rational point splits in one extension iff it does not split in the other one, and hence they differ by a sign. The result follows.

ii: The degree of the conductor of the corresponding extension is s (Lemma 5.3, Lemma 3.20 from Chapter 2). Hence the result follows from Theorem 3.18 from Chapter 2.

iii: Obvious.

iv: Follows from ii and i.

v: The degree of the conductor of the corresponding extension is 0 (Lemma 5.3, Lemma 3.20 from Chapter 2). Hence the result follows from Theorem 3.18 from Chapter 2.

vi: Follows from v and i. □

5.3. Proof of theorem.

PROOF OF THEOREM 4.1. Suppose $\langle \varphi_C(C_S) \rangle \subsetneq \mathrm{Pic}_k^0(C)$. Then there exists a subgroup $H \subseteq \mathrm{Pic}_k^0(k)$ of prime index l such that $\varphi_C(C_S) \subseteq H$. Let $\chi \in \mathrm{Pic}_k^0(C)^\vee$ be a character with kernel H. Let $f \in \mathbf{C}[S] \subseteq \mathbf{C}[k]$. Then for $a \in k$ we have $f_a = \frac{1}{q}\sum_{\lambda \in k^\vee} f_\lambda \lambda(a)$ (Proposition 2.2 from Chapter 3).

By construction we have

$$0 = \sum_{P\in C(k)^*} f(x(P))(\chi-1)(\varphi_C(P)) = \frac{1}{q}\sum_{P\in C(k)^*}\sum_{\lambda\in k^\vee} f_\lambda \lambda(x(P))(\chi-1)(P)$$
$$= \frac{1}{q}\sum_{\lambda\in k^\vee} f_\lambda \left(c_{(\lambda,\chi)} - c_{(\lambda,1)}\right).$$

Assume that $\chi \neq \chi_2$ if $p = 2$ and $\deg(h) = g$. Choose f such that $\mathrm{sh}_k(S) = \#S/q \cdot C_k(f)$. Rewrite our equation in the following way:

$$f_1(c_{(1,1)} - c_{(1,\chi)}) = \sum_{\lambda\in k^\vee,\lambda\neq 1} f_\lambda \left(c_{(\lambda,\chi)} - c_{(\lambda,1)}\right).$$

We will now put in the estimates of Lemma 5.7. Notice first

$$|c_{(1,1)} - c_{(1,\chi)}| = |(c_{(1,1)}+1) - (c_{(1,\chi)}+1)| = |\#C(k) - (c_{(1,\chi)}+1)|$$
$$\geq \#C(k) - (2g-2)\sqrt{q} > 0.$$

Taking absolute values gives

$$|f_1|(\#C(k) + (2g-2+2s)\sqrt{q}) \leq 2(2g-2+s)\sqrt{q}\sum_{\lambda\in k^\vee}|f_\lambda|.$$

Pick f such that $C(f) = q/\#S \cdot \mathrm{sh}_k(S)$. Then we obtain

$$\frac{q}{\#S}\cdot \mathrm{sh}_k(S) = C(f) \geq \frac{\#C(k) + (2g-2+2s)\sqrt{q}}{2(2g-2+s)\sqrt{q}}$$

and this gives us the required result.

Assume that $p = 2$, $\deg(h) = g$ and that $\chi = \chi_2$. Then one has

$$0 = \sum_{\lambda\in k^\vee} f_\lambda \left(c_{(\lambda,\chi_2)} - c_{(\lambda,1)}\right) = \sum_{\lambda \pmod{\langle\lambda_2\rangle}} (f_\lambda - \epsilon_C f_{\lambda\lambda_2})\left(c_{(\lambda,\chi_2)} - c_{(\lambda,1)}\right).$$

Hence we have

$$(f_1 - \epsilon_C f_{\lambda_2})\left(c_{(1,1)} - c_{(1,\chi_2)}\right) = 1/2 \sum_{\lambda\in k^\vee,\lambda\neq 1,\lambda_2} (f_\lambda - \epsilon_C f_{\lambda\lambda_2})\left(c_{(\lambda,\chi_2)} - c_{(\lambda,1)}\right).$$

The estimates of Lemma 5.7 give

$$|f_1 - \epsilon_C f_{\lambda_2}|(\#C(k) + (2g-2+2s)\sqrt{q}) \leq (2g-2+s)\sqrt{q}\sum_{\lambda\in k^\vee}|f_\lambda - \epsilon_C f_{\lambda\lambda_2}|.$$

Notice that $f_\lambda - \epsilon_C f_{\lambda\lambda_2} = (f - \epsilon_C\lambda_2 f)_\lambda = ((1-\epsilon_C\lambda_2)f)_\lambda$ by Remark 2.3 from Chapter 3 (and because λ_2 has order 2). Notice that the image of the map $\mathbf{C}[S] \to \mathbf{C}[S]$, $f \mapsto (1-\epsilon_C\lambda_2)f$ is $\mathbf{C}[H_C \cap S]$ where $H_C = \{x \in k : \lambda_2(x) = -\epsilon_C\}$. If $H_C \cap S = \emptyset$, then we have $C_S \subseteq \ker(\psi_C) \overset{2}{\subseteq} \mathrm{Pic}^0_k(C)$ (Proposition 5.4). We can interpret our equation as a shape of $H_C \cap S$ and by choosing the function which obtains the shape of $H_C \cap S$ we obtain:

$$\frac{\#C(k) + (2g-2+2s)\sqrt{q}}{(2g-2+s)\sqrt{q}} \leq \frac{q}{\#(S\cap H_C)}\cdot \mathrm{sh}_k(S\cap H_C).$$

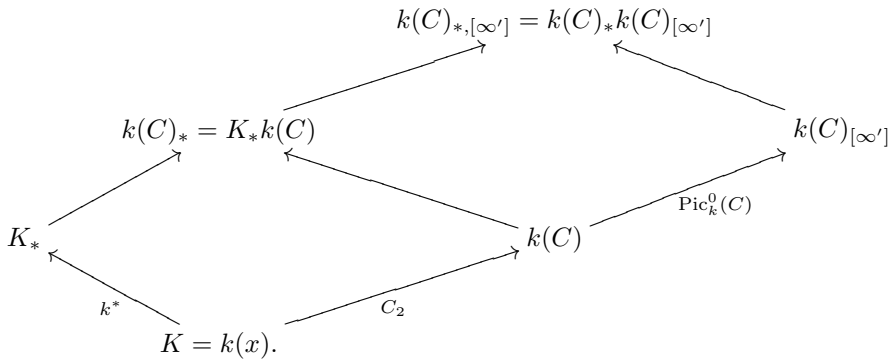
The final result follows after applying Lemma 3.8 from Chapter 3.

□

6. Multiplicative x-coordinate

Let C be a hyperelliptic curve of genus $g \geq 1$ over a finite field k of cardinality q and characteristic p given by an equation as in Section 4.

6.1. The diagram. Consider the following diagram (see Proposition 3.10 from Chapter 2 and Proposition 2.4)



The extension $k(C)_+/K$ has Galois group $k^* \times C_2$ and is geometric by genus considerations.

If $p = 2$, then $k(C)_+/k(C)$ is totally ramified at ∞ and at the the points of $k(C)$ above (x) of K, because $(2, q-1) = 1$. Hence $k(C)_{*,[\infty']}/k(C)$ is Galois with group $k^* \times \mathrm{Pic}^0_k(C)$ and geometric.

Assume $p \neq 2$. Assume that $k(C)/K$ is not ramified at (x), equivalently, $x \nmid f$ (Theorem 4.6 from Chapter 2). Then $k(C)_*/k(C)$ is totally ramified at the primes above (x) of $k(C)$. This shows that $k(C)_{*,[\infty']}/k(C)$ is Galois with group $k^* \times \mathrm{Pic}^0_k(C)$ and geometric

Lemma 6.1. *Let M' be a subextension of $k(C)_*/k(C)$ with $M' \neq k(C)$. Let M be the unique degree 2 subextension of $k(C)_*/k(C)$ if $p \neq 2$. Let $R = \{P \in \mathcal{P}_{k(C)/k} : P|_K = (x)\}$. Then we have:*

	$\mathfrak{f}(M'/k(C))$	$\deg_k(\mathfrak{f}(M'/k(C)))$
$p = 2,\ x \nmid h$	$\infty' + \sum_{P \in R} P$	3
$p = 2,\ x \mid h$	$\infty' + \sum_{P \in R} P$	2
$p \neq 2,\ x \nmid f,\ M' \neq M$	$\infty' + \sum_{P \in R} P$	3
$p \neq 2,\ x \mid f,\ M' \neq M$	$\infty' + \sum_{P \in R} P$	2
$p \neq 2,\ x \nmid f,\ M' = M$	$\sum_{P \in R} P$	2
$p \neq 2,\ x \mid f,\ M' = M$	0	0.

Proof. Note that the ramification in $M'/k(C)$ is always tame, and hence the conductor is the sum of the ramifying primes.

Assume that $p = 2$. As $(q-1, 2) = 1$, we see that $M'/k(C)$ is totally ramified above ∞' and the primes in R.

Assume that $p \neq 2$. It follows from local class field theory that a maximal abelian totally ramified extension of conductor ∞ or (x) of K_∞ has degree $q-1$. Hence we see that all extensions except $M/k(C)$ are ramified at ∞'. If (x) is ramified in $k(C)/K$, then all extensions $M'/k(C)$, except $M/k(C)$, are ramified at the primes of R. If (x) is unramified in $k(C)/K$, then all $M/k(C)$ are totally ramified at the primes of R.

Apply Theorem 4.6 from Chapter 2 and Theorem 3.7 to fill in the second column of the table. If (x) is not ramified at $k(C)/K$, then $\sum_{P\in R} \deg_k(P) = 2$. If (x) is ramified, then $\sum_{P\in R} \deg_k(P) = 1$. The third column now follows from the second one. □

Lemma 6.2. *Consider the extension $k(C)/K$. Assume $p \neq 2$. Then we have:*

- *(x) is ramified $\iff$ $f_0 = 0$;*
- *(x) is split $\iff$ $f_0 \in k^{*2}$;*
- *(x) is inert $\iff$ $f_0 \in k^* \setminus k^{*2}$.*

Assume $p = 2$. Then we have:

- *(x) is ramified $\iff$ $h_0 = 0$;*
- *(x) is split $\iff$ $h_0 \neq 0$ and $\mathrm{tr}_{k/\mathbf{F}_2}(\frac{f_0}{h_0^2}) = 0$*
- *(x) is inert $\iff$ $h_0 \neq 0$ and $\mathrm{tr}_{k/\mathbf{F}_2}(\frac{f_0}{h_0^2}) \neq 0$*

Proof. Assume $p \neq 2$. The first case we know by Theorem 4.6 from Chapter 2. The other two parts follow from Proposition 7.8 from Chapter 1.

Assume $p = 2$. The first case follows from Theorem 4.6 from Chapter 2. The other two parts follow from from Proposition 7.8 from Chapter 1 and Lemma 5.1. □

Assume $p \neq 2$ and $x|f$. Then the extension $M/k(C)$ is unramified. Notice that $M = k(C)k(\sqrt{x})$ (Proposition 2.4). We want to determine when ∞' splits in this extension. The prime ∞' splits completely in $M/k(C)$ iff ∞ splits completely in the extension $k(z)[y]/(y^2 - f(z^2))$ over $k(z)$, where $z = \sqrt{x}$. Put $y' = \frac{y}{z^{2g+1}}$. Then y' satisfies $y'^2 - \frac{f(z^2)}{z^{2(2g+1)}}$. The right hand side is integral at ∞, and reducing modulo this prime gives the equation $y'^2 - f_{2g+1}$. We see that it splits at ∞ iff f_{2g+1} is a square (Proposition 7.8 from Chapter 1). Hence $M \subseteq k(C)_{[\infty']}$ iff f_{2g+1} is a square. Recall the notation N from Page 105. We obtain an analogue of Proposition 5.4:

Proposition 6.3. *Assume that $p \neq 2$ and that $x|f$. Let x' be the unique prime above (x) in $k(C)$. We have a surjective morphism of groups*

$$\phi_C \colon \mathrm{Pic}_k^0(C) \to k^*/k^{*2}$$

defined as follows. Let P be a prime of $k(C)$ with $P \neq \infty', x'$. Then we have $\phi_C([P] - \deg_k(P)[\infty']) = \overline{\mathrm{N}(P|_K)^{\mathrm{f}(P/P|_K)} f_{2g+1}^{\deg_k(P)}}$. Furthermore, we have $\phi_C([x'] - [\infty']) = \overline{f_1 f_{2g+1}}$.

Proof. We use Proposition 2.4. Most parts are similar to the proof of Proposition 5.4. We just need to calculate when P splits completely in $M/k(C)$. From Corollary 9.3 from Chapter 1 and Proposition 2.4 we deduce the formula. For the prime x' we need to do a special calculation. But x' splits in $M/k(C)$ iff it splits completely in $k(z)[y]/(y^2 - f(z^2))$. Put $y'' = \frac{y}{z}$. Then after the reduction at 0 it satisfies $y''^2 - f_1$.

Note that $f_1 \neq 0$ by our assumptions, and the extension is totally split by Proposition 7.8 from Chapter 1 iff f_1 is a square. The result follows. □

Remark 6.4. The map ϕ_C has been studied in [**BPS12**], where one takes $n = 2$, $\Delta = \mathrm{Spec}(k)$ and $\beta = ([P] - [\infty'], \mathrm{Spec}(k))$ where P is the unique point with $x = 0$ of $C(k)$. This point $[P] - [\infty']$ is 2-torsion, as $(x) = 2P - 2\infty'$.

Remark 6.5. Assume that E is an elliptic curve over a finite field k of odd characteristic given by $y^2 = x^3 + a_2x^2 + a_4x$. Then the above morphism becomes

$$\begin{aligned} \phi_C \colon E(k) &\to k^*/k^{*2} \\ P &\mapsto \overline{x(P)} \\ \infty &\mapsto 1 \\ (0,0) &\mapsto \overline{a_4}. \end{aligned}$$

As a matter of fact, it is not hard to see the following: Suppose points $P_1, P_2, P_3 \in E(k)$ lie on the line $y = \lambda x + \mu$. The constant term gives $x(P_1)x(P_2)x(P_3) = \mu^2$.

6.2. Character sum estimates. Let $R = \{P \in \mathcal{P}_{k(C)/k} : P|_K = (x)\}$. Put $C(k)^{**} = C(k)\backslash(R \cup \{\infty'\}) = \mathrm{unr}^1(k(C)_{*,[\infty']}/k(C))$. Let $\lambda \in (k^*)^\vee$ and $\chi \in \mathrm{Pic}^0_k(C)^\vee$. Since we have a natural map $\mathrm{Gal}(k(C)_{*,[\infty']}/k(C)) \to k^* \times \mathrm{Pic}^0_k(C)$, we can view (λ, χ), using the product, as a character of $\mathrm{Gal}(k(C)_{*,[\infty']}/k(C))$. We put

$$c_{(\lambda,\chi)} = \sum_{P \in C(k)^{**}} (\lambda,\chi)((P, k(C)_{*,[\infty']}/k(C))) = \sum_{P \in C(k)^{**}} \lambda(x(P))\chi(\varphi_C(P))$$

(see Lemma 9.4 from Chapter 1, we avoid the possible ramification here). Put $s = 2$ if (x) is ramified in $k(C)/K$ and $s = 3$ if not.

If $p \neq 2$, put $\lambda_2' \colon k^* \to k^*/k^{*2} \cong \{\pm 1\} \subseteq \mathbf{C}^*$. If $p \neq 2$, and $x|f$, put $\delta_C = \lambda_2'(f_{2g+1})$ and put χ_2' for the compositum of ϕ_C with the isomorphism $k^*/k^{*2} \cong \{\pm 1\} \subseteq \mathbf{C}^*$.

Lemma 6.6. *Let $\lambda \in k^\vee$, $\chi \in \mathrm{Pic}^0_k(C)^\vee$. Then the following hold.*

i. $c_{\chi_0,\chi_0} = \#C(k) - \#R - 1$;
ii. *if $\lambda \neq \chi_0$, and if $\lambda \neq \lambda_2'$, $\chi \neq \chi_2'$ if $p = 2$ and $x|f$, then $|c_{\lambda,\chi}| \leq (2g-2+s)\sqrt{q}$;*
iii. *if $\chi \neq \chi_0$, then $|c_{(\chi_0,\chi)} + 1 + \sum_{P \in R} \chi((P, k(C)_*/k(C)))| \leq (2g-2)\sqrt{q}$;*
iv. *if $p = 2$ and $x|f$, then $c_{(\lambda,\chi)\cdot(\lambda_2',\chi_2')} = \delta_C c_{(\lambda,\chi)}$.*

Proof. i: Obvious.

ii, iii: Follow from Lemma 6.1, Theorem 3.18 from Chapter 2 and Lemma 3.20 from Chapter 2. We still need to do the case when $\lambda = \lambda_2'$. We obtain directly $|c_{(\lambda_2',\chi)} + 1 + 1_{s=2} \cdot (\sum_{P \in R}(\lambda_2', \chi)((P, k(C)_{*,[\infty']}/k(C))))| \leq (2g - 2 + 2(s-2))\sqrt{q}$. The result then follows since

$$(4-s)\sqrt{q} \geq \begin{cases} 1 & \text{if } s = 3 \\ 2 & \text{if } s = 2. \end{cases}$$

iv: Let $P \in C(k)^{**}$. We claim: $\lambda_2'(x(P))\chi_2'(P) = \delta_C$. Indeed, if $\delta_C = 1$, then $\lambda_2'(x(P)) = \chi_2'(P)$ by construction. If $\delta_C = -1$, then a rational point splits in one extension iff it does not split in the other one. This gives a sign. The result follows. □

6.3. Proof of theorem.

Proof of Theorem 4.6. Notice that $\#R = r$ by Lemma 6.2.

Suppose $\langle \varphi_C(C_S) \rangle \subsetneq \mathrm{Pic}^0_k$. Then there exists a subgroup $H \subseteq \mathrm{Pic}^0_k$ of index l (prime) such that $\varphi_C(C_S) \subseteq H$. Let $\chi \in \mathrm{Pic}^0(k)^\vee$ be a character with kernel H. Let $f \in \mathbf{C}[S] \subseteq \mathbf{C}[k^*]$. Write $f = \frac{1}{q-1} \sum_{\lambda \in (k^*)^\vee} f_\lambda \lambda$.

By construction we have

$$0 = \sum_{P \in C(k)^{**}} f(x(P))(\chi - 1)(P) = \frac{1}{q-1} \sum_{P \in C(k)^{**}} \sum_{\lambda \in (k^*)^\vee} f_\lambda \lambda(x(P))(\chi - 1)(P)$$
$$= \frac{1}{q-1} \sum_{\lambda \in (k^*)^\vee} f_\lambda \left(c_{(\lambda,\chi)} - c_{(\lambda,1)} \right).$$

Assume that $\chi \neq \chi_2'$ if $p \neq 2$ and $x | f_2$. Choose f such that $\mathrm{sh}_{k^*}(S) = \#S/(q-1) \cdot C(f)$. Rewrite our equation in the following way:

$$f_1(c_{(1,1)} - c_{(1,\chi)}) = \sum_{\lambda \in (k^*)^\vee, \lambda \neq 1} f_\lambda \left(c_{(\lambda,\chi)} - c_{(\lambda,1)} \right).$$

Putting in the estimates of Lemma 6.6, we obtain first

$$|c_{(1,1)} - c_{(1,\chi)}| = |(c_{(1,1)} + 1) - (c_{(1,\chi)} + 1)| = |\#C(k) - (c_{(1,\chi)} + 1)|$$
$$\geq \#C(k) - (2g-2)\sqrt{q} - 2r > 0.$$

This gives us

$$|f_1|(\#C(k) + (2g - 2 + 2s)\sqrt{q} - 2r) \leq 2(2g - 2 + s)\sqrt{q} \sum_{\lambda \in (k^*)^\vee} |f_\lambda|.$$

Hence we have

$$\frac{q-1}{\#S} \cdot \mathrm{sh}_{k^*}(S) = C(f) \geq \frac{\#C(k) + (2g - 2 + 2s)\sqrt{q} - 2r}{2(2g - 2 + s)\sqrt{q}}$$

and this gives us the required result.

Assume that $p \neq 2$, $x | f$ and that $\chi = \chi_2'$. Then one has

$$0 = \sum_{\lambda \in (k^*)^\vee} f_\lambda \left(c_{(\lambda,\chi_2')} - c_{(\lambda,1)} \right) = \sum_{\lambda \pmod{\langle \lambda_2' \rangle}} (f_\lambda - \delta_C f_{\lambda\lambda_2}) \left(c_{(\lambda,\chi_2')} - c_{(\lambda,1)} \right).$$

Hence we have

$$(f_1 - \delta_C f_{\lambda_2'}) \left(c_{(1,1)} - c_{(1,\chi_2')} \right) = 1/2 \sum_{\lambda \in (k^*)^\vee, \lambda \neq 1, \lambda_2'} \left(f_\lambda - \delta_C f_{\lambda\lambda_2'} \right) \left(c_{(\lambda,\chi_2')} - c_{(\lambda,1)} \right).$$

The estimates of Lemma 6.6 give

$$|f_1 - \delta_C f_{\lambda_2'}|(\#C(k) + (2g - 2 + 2s)\sqrt{q} - 2r) \leq (2g - 2 + s)\sqrt{q} \sum_{\lambda \in (k^*)^\vee} |f_\lambda - \delta_C f_{\lambda\lambda_2'}|.$$

Notice that $f_\lambda - \delta_C f_{\lambda\lambda_2'} = (f - \delta_C \lambda_2' f)_\lambda = ((1 - \delta_C \lambda_2')f)_\lambda$ by Remark 2.3 from Chapter 3 (and because λ_2' has order 2). Notice that the image of the map $\mathbf{C}[S] \to \mathbf{C}[S]$, $f \mapsto (1 - \epsilon_C \lambda_2) f$ is $\mathbf{C}[H_C' \cap S]$ where $H_C' = \{x \in k : \lambda_2'(x) = -\delta_C\}$. If $H_C' \cap S = \emptyset$, then we have $C_S \subseteq \ker(\phi_C) \overset{2}{\subseteq} \mathrm{Pic}^0_k(C)$ (Proposition 5.4). We can interpret our equation as

a shape of $H'_C \cap S$ and by choosing the function which obtains the shape of $H'_C \cap S$ we obtain:

$$\frac{\#C(k) + (2g-2+2s)\sqrt{q} - 2r}{(2g-2+s)\sqrt{q}} \leq \frac{q-1}{\#(S \cap H'_C)} \cdot \mathrm{sh}_{k^*}(S \cap H'_C).$$

The result follows after using Lemma 3.8 from Chapter 3. □

7. The algorithm

In this section we will describe how to find generators for $\mathrm{Pic}^0_k(C)$, that is, we give the proof of Theorem 1.1. We make a few assumptions:

i. We can do operations in k, a finite field of cardinality q, as addition and multiplication in time polynomial in $\log(q)$.
ii. Our hyperelliptic curve C is given as in Theorem 4.6 from Chapter 2 such that $k(C)/k(x)$ is totally ramified at ∞.
iii. Divisors on $\mathrm{Pic}^0_k(C)$ are represented as Galois-invariant divisors of $\mathrm{div}^0_{\overline{k}}(C_{\overline{k}})$, where divisors on $\mathrm{div}^0_{\overline{k}}(C_{\overline{k}})$ are represented in $\mathbf{Z}^{(C(\overline{k}))}$.

Proof of Theorem 1.1. Put $t = \left(2^4(2g+1)+2^2\right)^2$. Deterministically construct k', a finite field extension of k of cardinality q^i where $tq > q^i \geq t$. This can be done in time $O(q^{1/2}i^4)$ ([**Sho90**]), which is in $O(q^{1/2}g^2)$. Addition and multiplication can then be done in k' in time polynomial in $\log(g)$ and $\log(q)$.

Construct an interval S of k' with the following properties:

i. $\#S \geq \lceil 4(2g+1)q^{i/2} \rceil = r$;
ii. $\#S = O(g^2 q^{1/2})$;
iii. if $p = 2$ and $\deg(h) = g$, then $S \subseteq H_C$.

This can be done for the following reason. We claim that there are intervals of length between r and $2r$. Indeed, write r in basis $p = \mathrm{char}(k)$, say with main term $a_s p^s$. We claim that there is an interval of cardinality $r' = 2a_s p^s$. Note that $r \leq r' \leq 2r$. We want to apply Lemma 3.7 from Chapter 3 (for H_C in the special case), and for this it is enough to show that $4r \leq q^i$. Indeed, we have

$$q^i \geq q^{i/2} t^{1/2} = q^{i/2}\left(2^4(2g+1)+2^2\right) \geq 4(4(2g+1)q^{i/2}+1) \geq 4r.$$

We claim that $\#S = O(g^2 q^{1/2})$. Indeed, $gq^{i/2} \leq gt^{1/2}q^{1/2}$, which is of order $O(g^2 q^{1/2})$ and the result follows.

We will apply Theorem 4.1 with our interval S. We have $\mathrm{sh}_{k^+}(S) \leq 2$ (Lemma 3.6 from Chapter 3) and $q^i \geq (4g-2)^2$ and hence $\#S \geq 2\,\mathrm{sh}_{k^+}(S)(2g-2+s)q^{i/2}$. Theorem 4.1 (see Remark 4.2) gives $\langle \varphi_{C_{k'}}(C_{k',S}) \rangle = \mathrm{Pic}^0_{k'}(C_{k'})$.

We will construct $C_{k',S}$. For all $x \in S$ we look at the equation $y^2 + h(x)y = f(x)$ and we have to solve this in y (Theorem 4.6 from Chapter 2 tells us that this is a smooth model).

Assume that $p = 2$. Note that $h \neq 0$. If x is fixed, we need to find y with

$$\left(\frac{y}{h(x)}\right)^2 - \frac{y}{h(x)} = \left(\frac{f(x)}{h(x)}\right)^2.$$

This is an Artin-Schreier equation and solutions can easily be obtained by linear algebra. Each step here can be done in polynomial time in $\log(q^i)$, hence polynomial time in $\log(g)$ and $\log(q)$. Hence the total cost of this is $O(g^{2+\epsilon}q^{1/2+\epsilon})$.

Assume that $p \neq 2$. Then for $x \in S$ we need to solve $y^2 = f(x)$. First calculate a quadratic non-residue in time $O(q^{i/4+\delta})$, that is, in time $O(\log(g)^{1/2}q^{1/4+\delta})$ (see [**Shp96**]). Then we apply Tonelli-Shanks to solve the equation for a fixed x in time polynomial in $\log(q)$ ([**vdW06**, Lemma 3.4]). Hence in total the cost of this step is again $O(g^{2+\epsilon}q^{1/2+\epsilon})$.

Hence we have calculated $C_{k',S}$. Let ∞'' be the point at infinity of $C_{k'}$. The image of $C_{k',S}$ under $\varphi_{C_{k'}}(k')\colon C_{k'} \to \mathrm{Pic}^0_k(C_{k'})$ generates the group $\mathrm{Pic}^0_k(C_{k'})$. It maps P to $[P] - [\infty'']$. Since the norm map $\mathrm{Norm}_{k'k(C)/k(C)}\colon \mathrm{Pic}^0_k(C_{k'}) \to \mathrm{Pic}^0_k(C)$ is surjective (Corollary 3.15 from Chapter 2), a generating set of $\mathrm{Pic}^0_k(C)$ is given by

$$\mathrm{Norm}_{k'k(C)/k(C)}\left(\varphi_{C_{k'}}(C_{k',S})\right).$$

More explicitly, for $P \in C_{k',S}$ we have

$$\mathrm{Norm}_{k'k(C)/k(C)}(\varphi_{C_{k'}}(P)) = -[k' : k][\infty'] + \sum_{g \in \mathrm{Gal}(k'/k)} [g(P)].$$

□

Remark 7.1. In the proof above, we made some bad estimates, especially for t. We chose for these bad estimates because it allows for a shorter and more uniform proof.

Chapter 8

Automorphism groups of fields

1. Introduction

In this chapter we study automorphism groups of fields. Let Ω be an algebraically closed field and let k be a subfield such that the transcendence degree of Ω over k is finite but not zero. Our goal is to study $\mathrm{Aut}_k(\Omega)$, the automorphisms of Ω which are the identity on k, and $\mathrm{Aut}(k \to \Omega)$, the automorphism of Ω which induce an automorphism on k. All these groups are topological groups where we view them as subsets of Ω^Ω, where Ω has the discrete topology and Ω^Ω the product topology. These groups are quite mysterious and our goal is to gain an understanding for them. In this introduction we will discuss the three main theorems of this chapter. Let us drop any of the assumptions above.

The first theorem gives a splitting of an exact sequence (see Subsection 3.4).

Theorem 1.1. *Let Ω be an algebraically closed field with subfield k. Then we have an exact sequence of topological groups*

$$1 \to \mathrm{Aut}_k(\Omega) \to \mathrm{Aut}(k \to \Omega) \to \mathrm{Aut}(k) \to 1.$$

If k is algebraically closed, there is a continuous morphism $\mathrm{Aut}(k) \to \mathrm{Aut}(k \to \Omega)$ which splits the sequence.

The second theorem main theorem is as follows (see Subsection 5.4).

Theorem 1.2. *Let Ω be an algebraically closed field and let k be a subfield such that the transcendence degree of Ω over k is finite but not zero. Then there are surjective continuous group morphisms from $\mathrm{Aut}_k(\Omega)$ and $\mathrm{Aut}(k \to \Omega)$ to a not finitely generated free abelian group with the discrete topology.*

Finally, we have the following theorem (see Section 6).

Theorem 1.3. *Let Ω be an algebraically closed field and let k be an algebraically closed field such that the transcendence degree of Ω over k is one. Then the action of $\mathrm{Aut}(k \to \Omega)$ on $\mathcal{P}_{\Omega/k}$, the set of valuations of Ω which are trivial on k but not trivial, is transitive and the kernel of this action is $\langle x \to x^p \rangle$ if $p > 0$ and trivial if $p = 0$.*

2. Prerequisites

2.1. Category of arrows. Let $\mathcal{C}$ be a category. Then we define the *category of arrows* of $\mathcal{C}$ to be the following category. The objects in this category are morphisms $s\colon A \to B$ in the category $\mathcal{C}$. A morphism between $s\colon A \to B$ and $s'\colon A' \to B'$ is a pair (t, t') with $t : A \to A'$ and $t' : B \to B'$ which satisfies $s't = t's$. We denote the set of homomorphisms between s and s' by $\mathrm{Hom}(s, s')$.

2.2. Topology. Let Ω be a field. We will endow Ω with the discrete topology. We give Ω^Ω the product topology. This means that a subset $A \subseteq \Omega^\Omega$ is open iff for every $f \in A$ there exists a finite $S \subseteq \Omega$ such that $U_{S,f} = \{g \in \Omega^\Omega : g|_S = f|_S\} \subseteq A$. Notice that Ω^Ω is a Hausdorff space.

Lemma 2.1. *Let H be a subgroup of $\mathrm{Sym}(\Omega) \subseteq \Omega^\Omega$. Then H is compact $\iff$ H is closed in $\mathrm{Sym}(\Omega)$ and for all $a \in \Omega$ the set $Ha = \{h(a) : h \in H\}$ is finite.*

Proof. $\Longrightarrow$: For $a \in \Omega$, the map $H \to \Omega$, $f \mapsto f(a)$, where Ω has the discrete topology, is continuous. By compactness it follows that Ha is finite. As Ω^Ω is a Hausdorff space, it follows that H is closed in Ω^Ω. Hence it is closed in $\mathrm{Sym}(\Omega)$.

$\Longleftarrow$: We can view $\mathrm{Sym}(\Omega)$ as a closed subset of $\Omega^\Omega \times \Omega^\Omega$ by sending σ to (σ, σ^{-1}). The induced topology on $\mathrm{Sym}(\Omega)$ agrees with its topology from Ω^Ω. Using this embedding we have $H \subseteq \prod_{a\in\Omega} Ha \times \prod_{a\in\Omega} Ha = T$. The latter is a compact space by Tychonov. As $\mathrm{Sym}(\Omega)$ is closed in $\Omega^\Omega \times \Omega^\Omega$ and H is closed in $\mathrm{Sym}(\Omega)$, it follows that H is closed in T. It follows that H is compact. □

Automorphism groups will be specific subgroups of Ω^Ω and they are endowed with the induced topology. Let $k \subseteq \Omega$ be a subfield. We will put $\mathrm{Aut}_k(\Omega)$ to be the set of automorphism of Ω which are the identity on k. Consider $\mathrm{Aut}(k \to \Omega)$, that is, the set of automorphisms $\Omega \to \Omega$ which induce an automorphism $k \to k$. Note that $\mathrm{Aut}(k \to \Omega)$ is a subset Ω^Ω which contains $\mathrm{Aut}_k(\Omega)$. We will also consider $\mathrm{Aut}(\Omega)$. These three groups become topological groups with their induced topology.

Note that $\mathrm{Aut}_k(\Omega) \subseteq \mathrm{Aut}(k \to \Omega) \subseteq \mathrm{Aut}(\Omega)$. If k' is an intermediate field of Ω/k, then we have natural morphism $\mathrm{Aut}_{k'}(\Omega) \subseteq \mathrm{Aut}_k(\Omega)$. We also have a natural morphism $\mathrm{Aut}(k \to \Omega) \to \mathrm{Aut}(k)$.

Remark 2.2. Assume that Ω/k is algebraic. Let S be the set of finite Galois extensions of k in Ω. Then one has $\mathrm{Aut}_k(\Omega) = \varprojlim_{l\in S} \mathrm{Aut}_k(l)$. This is a subset of $\prod_{l\in S} \mathrm{Aut}_k(l)$. We endow the finite sets $\mathrm{Aut}_k(l)$ with the discrete topology and $\prod_{l\in S} \mathrm{Aut}_k(l)$ with the product topology. Let $\mathfrak{T}$ be the subspace topology on $\mathrm{Aut}_k(\Omega)$. One can easily show that $\mathfrak{T}$ agrees with the other topology on $\mathrm{Aut}_k(\Omega)$.

2.3. Transcendence degree. Here are some basic facts about the transcendence degree of an extension of fields. See [**Lan02**, Chapter VIII] for some details. Let L/K be a field extension. Then a set $S \subseteq L$ is *algebraically independent* if the K-algebra morphism $K[x_s : s \in S] \to L$ sending x_s to s is injective. A maximal S is called a *transcendence basis* of L/K. If S is a transcendence basis, then $L/K(S)$ is algebraic. Note that any algebraically independent set can be extended to a transcendental basis. We define the *transcendence degree* of L/K, which is a cardinal number, by $\mathrm{trdeg}_K(L) = |S|$. This degree does not depend on the choice of a transcendence basis. Notice that for a morphism $\sigma\colon L \to L'$ we have $\mathrm{trdeg}_K(L) = \mathrm{trdeg}_{\sigma(K)}(\sigma(L))$. If M is an extension of L, then we have the identity $\mathrm{trdeg}_K(M) = \mathrm{trdeg}_L(M) + \mathrm{trdeg}_K(L)$ (as cardinal numbers). In fact, the union of transcendence bases of M/L and L/K is a transcendence basis of M/K.

3. Properties of the automorphism groups

3.1. Extension of morphisms. We begin with a theorem which shows that automorphism groups are 'big' if the top field is algebraically closed.

Proposition 3.1. *Let Ω be an algebraically closed field and let k be a subfield. Let E be an intermediate field of Ω/k. Suppose $\sigma \in \mathrm{Hom}(k \to E, k \to \Omega)$. Then there is $\sigma' \in \mathrm{Aut}(k \to \Omega)$ with $\sigma'|_E = \sigma \iff \mathrm{trdeg}_E(\Omega) = \mathrm{trdeg}_{\sigma(E)}(\Omega)$. The latter condition holds if $\mathrm{trdeg}_k(E) < \mathrm{trdeg}_k(\Omega)$ or $\mathrm{trdeg}_k(\Omega) < \infty$.*

Proof. $\Longrightarrow$: We have $\mathrm{trdeg}_E(\Omega) = \mathrm{trdeg}_{\sigma'(E)}(\sigma'(\Omega)) = \mathrm{trdeg}_{\sigma'(E)}(\Omega)$.

$\Longleftarrow$: Let S be a transcendence basis of Ω/E and S' be one for $\Omega/\sigma(E)$. Let $\tau\colon S \to S'$ be a bijection. Define the isomorphism $\sigma''\colon E(S) \to \sigma'(E)(S')$ to be σ' on E and τ on S. As Ω is algebraically closed and Ω is algebraic over $E(S)$ and $\sigma'(E)(S')$, we can extend this to an element $\sigma' \in \mathrm{Aut}(k \to \Omega)$ as required.

We have the identity

$$\begin{aligned}\mathrm{trdeg}_k(E) + \mathrm{trdeg}_E(\Omega) &= \mathrm{trdeg}_k(\Omega) = \mathrm{trdeg}_k(\sigma(E)) + \mathrm{trdeg}_{\sigma(E)}(\Omega)\\ &= \mathrm{trdeg}_k(E) + \mathrm{trdeg}_{\sigma(E)}(\Omega).\end{aligned}$$

If $\mathrm{trdeg}_k(\Omega) < \infty$, the statement follows easily. Otherwise, it follows from the fact that for infinite cardinal numbers A and B we have $A + B = \max(A, B)$. □

Remark 3.2. From the above proposition, a very similar statement follows for $\mathrm{Aut}_k(\Omega)$.

Remark 3.3. Let Ω be an algebraically closed field and let k be a subfield. Let $\overline{k}$ be the algebraic closure of k in Ω. Then we have a commutative diagram of topological groups with exact rows (Proposition 3.1) and where all vertical maps are injective as follows:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Aut}_{\overline{k}}(\Omega) & \longrightarrow & \mathrm{Aut}_k(\Omega) & \longrightarrow & \mathrm{Aut}_k(\overline{k}) & \longrightarrow & 1\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{Aut}_{\overline{k}}(\Omega) & \longrightarrow & \mathrm{Aut}(k \to \Omega) & \longrightarrow & \mathrm{Aut}(k \to \overline{k}) & \longrightarrow & 1.
\end{array}$$

3.2. Topological statements.

Lemma 3.4. *Let Ω/k be a field extension with $\mathrm{trdeg}(\Omega/k) \geq 1$. Let T be the set of elements in Ω which are transcendental over k. Then one has $\Omega = k(T)$.*

Proof. The set of algebraic elements in Ω/k is a subgroup of Ω^+. If $H \subsetneq G$ are groups, then $\langle G \setminus H \rangle = G$. Indeed, for $h \in H$ and $g \in G \setminus H$ we have $h = g^{-1} \cdot (gh)$. □

We say that an extension L/K of fields is *purely inseparable* if it is algebraic and for all intermediate fields M of L/K with $[M : K] < \infty$ we have $[M : K] = [M : K]_{\mathrm{i}}$. Hence if $\mathrm{char}(K) = 0$, then the only purely inseparable extension is K itself. We say that an extension fields L/K is *almost finitely generated* if there exists a finitely generated extension K' of K in L such that L/K' is purely inseparable.

Proposition 3.5. *Let Ω be a field and let $E \subseteq E'$ and E'' be intermediate fields. Let (P) be the property that Ω is algebraically closed and* $\mathrm{trdeg}_E(\Omega) < \infty$. *Then the following statements hold:*

i. $\mathrm{Aut}_E(\Omega) \subseteq \mathrm{Aut}(E \to \Omega)$, $\mathrm{Aut}_{E'}(\Omega) \subseteq \mathrm{Aut}_E(\Omega)$ *and* $\mathrm{Aut}_{E'}(\Omega) \subseteq \mathrm{Aut}(E \to \Omega)$ *are closed;*

ii. $\mathrm{Aut}_E(\Omega)$ *is compact* $\overset{(P)}{\underset{\Longleftarrow}{\Longrightarrow}}$ Ω/E *is algebraic;*

iii. $\mathrm{Aut}_E(\Omega) \subseteq \mathrm{Aut}_{E''}(\Omega)$ $\overset{(P)}{\underset{\Longleftarrow}{\Longrightarrow}}$ EE''/E *is purely inseparable;*

iv. $\mathrm{Aut}(E \to \Omega) \subseteq \mathrm{Aut}(E' \to \Omega)$ $\overset{(P)}{\underset{\Longleftarrow}{\Longrightarrow}}$ $E' = \Omega$ *or* E'/E *is normal;*

v. $\mathrm{Aut}_{E'}(\Omega) \subseteq \mathrm{Aut}_E(\Omega)$ *is open* $\overset{(P)}{\underset{\Longleftarrow}{\Longrightarrow}}$ E'/E *is almost finitely generated in* Ω*;*

vi. $\mathrm{Aut}_{E'}(\Omega) \subseteq \mathrm{Aut}_E(\Omega)$ *is normal* $\Longleftarrow$ E'/E *is normal algebraic or* Ω/E' *is purely inseparable.*

PROOF. i. All statements follow easily.

ii. $\Longrightarrow$: Suppose that Ω/E is not algebraic and let $t \in \Omega$ be transcendental over E. Then for each $i \in \mathbf{Z}_{\geq 1}$ we have a morphism $\sigma_i \in \mathrm{Hom}_E(E(t), \Omega)$ mapping t to t^i. Using Proposition 3.1 we can extend this to an element of $\mathrm{Aut}_E(\Omega)$. Hence the orbit of t under $\mathrm{Aut}_E(\Omega)$ is not finite. Hence $\mathrm{Aut}_E(\Omega)$ is not compact.

$\Longleftarrow$: One easily shows that $\mathrm{Aut}_E(\Omega)$ is closed in $\mathrm{Sym}(\Omega)$. The result then follows from Lemma 2.1.

iii. $\Longrightarrow$: Suppose that EE''/E is not purely inseparable. Assume first that $t \in E''$ is transcendental over E. Then we can consider the E-linear map $E(t) \to E(t^2)$ mapping t to t^2. Using Proposition 3.1 we can extend this to an element of $\mathrm{Aut}_E(\Omega)$. This shows that $\mathrm{Aut}_E(\Omega) \not\subset \mathrm{Aut}_{E''}(\Omega)$. Suppose that there exists $e \in E'' \setminus E$ which is separable over E. As Ω is algebraically closed, we can extend id_E to an element of $\mathrm{Hom}_E(E(e), \Omega)$ which does not fix e. This map can be extended to an element of $\mathrm{Aut}_E(\Omega)$ by Proposition 3.1. This shows that $\mathrm{Aut}_E(\Omega) \not\subset \mathrm{Aut}_{E''}(\Omega)$.

$\Longleftarrow$: Put $p = \mathrm{char}(k)$. If $p = 0$, then we have $E'' \subseteq E$ and the statement obviously follows. If $p \neq 0$, then for every $e \in E''$, there is $i \in \mathbf{Z}_{\geq 0}$ with $e^{p^i} \in E$. Hence if an automorphism is the identity on E, it also the identity on E''.

iv. $\Longrightarrow$: Assume $E' \neq \Omega$. Assume that E'/E is not algebraic. Say that $t \in E'$ is transcendental over E. Let t' be an element in $\Omega \setminus E'$ which is transcendental over E (Lemma 3.4). Then by Proposition 3.1 and Lemma 3.4 there is a morphism in $\mathrm{Hom}(E \to \Omega)$ which maps t to t'. Hence $\mathrm{Hom}(E \to \Omega) \not\subset \mathrm{Hom}(E' \to \Omega)$. Assume that E'/E is algebraic, but not normal. Then take $e' \in E'$ such that one of its conjugates e'' over E does not lie in E'. There is an element of $\mathrm{Hom}(E \to \Omega)$ which maps e' to e'' which is the identity on E (Theorem 3.1).

$\Longleftarrow$: If $E' = \Omega$, the statement is obvious. If E'/E is normal, then any element of $\mathrm{Aut}(E \to \Omega)$ maps E' into E'.

v. By iii one has: E'/E is almost finitely generated $\iff$ there is a finite subset $S \subseteq E'$ such that $E'/E(S)$ is purely inseparable $\underset{\underset{(P)}{\Longleftarrow}}{\overset{\Longrightarrow}{}}$ $\exists S \subseteq E'$ finite such that $\mathrm{Aut}_E(\Omega) \cap U_{S,\mathrm{id}_\Omega} = \mathrm{Aut}_{E(S)}(\Omega) = \mathrm{Aut}_{E'}(\Omega)$.

vi. If Ω/E' is purely inseparable, then $\mathrm{Aut}_{E'}(\Omega) = \mathrm{Aut}_\Omega(\Omega)$ by i, and hence the subgroup is normal. Suppose that E'/E is normal algebraic. Let $\tau \in \mathrm{Aut}_{E'}(\Omega)$ and $\sigma \in \mathrm{Aut}_E(\Omega)$. For $\alpha \in E'$ we have $\sigma(\alpha) \in E'$. Hence we have $\sigma^{-1}\tau\sigma(\alpha) = \alpha$ and hence $\sigma^{-1}\tau\sigma \in \mathrm{Aut}_{E'}(\Omega)$ as required. □

Remark 3.6. We cannot drop the assumption that Ω is algebraically closed and that $\mathrm{trdeg}(\Omega/E) < \infty$ in the implications where we put a *(P)*. Here are examples.

ii, iii, v: Let $\Omega = E' = E'' = \mathbf{R}$ and $E = \mathbf{Q}$. It is easy to see that $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{R}) = \mathrm{Aut}_{\mathbf{R}}(\mathbf{R}) = 1$.

We have $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{R})$ is compact, but $\mathbf{R}/\mathbf{Q}$ is not algebraic (ii).

We have $\mathrm{Aut}_{\mathbf{R}}(\mathbf{R}) \subseteq \mathrm{Aut}_{\mathbf{Q}}(\mathbf{R})$, but $\mathbf{R}/\mathbf{Q}$ is not purely inseparable (iii).

Furthermore, $\mathrm{Aut}_{\mathbf{R}}(\mathbf{R}) \subseteq \mathrm{Aut}_{\mathbf{Q}}(\mathbf{R})$ is open, but $\mathbf{R}/\mathbf{Q}$ is not almost finitely generated (v).

iv: Put $\Omega = \mathbf{R}$, $E' = \mathbf{Q}(\sqrt[3]{2})$ and $E = \mathbf{Q}$.

Note that $\mathrm{Aut}(\mathbf{Q} \to \mathbf{R}) = \mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2}) \to \mathbf{R}) = 1$. But $\mathbf{Q}(\sqrt[3]{2}) \neq \mathbf{R}$ and $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ is not normal (iv).

Problem 4. We have the following problems.

- When is $\mathrm{Aut}(E \to \Omega)$ compact or finite?
- When is $\mathrm{Aut}_E(\Omega)$ finite?

3.3. Galois theory. Let us recall the classical theorem of Galois theory. We say that Ω/k is Galois if it is algebraic, normal and separable.

Theorem 3.7. *Let Ω/k be an extension of fields. Set*

$$S = \{E : k \subseteq E \subseteq \Omega : \Omega/E \text{ Galois}\}.$$

Then we have a bijection

$$\varphi\colon \{H \subseteq \mathrm{Aut}_k(\Omega) \text{ compact subgroups}\} \to S$$
$$H \mapsto \Omega^H.$$

with inverse given by $E \mapsto \mathrm{Aut}_E(\Omega)$.

Proof. See for example [**Mor96**, Theorem 17.8]. □

Proposition 3.8. *Let Ω be an algebraically closed field and let k be a subfield such that $\mathrm{trdeg}(\Omega/k) < \infty$. Set*

$$S' = \{E : k \subseteq E \subseteq \Omega : \Omega/E \text{ Galois}, E/k \text{ almost f.g.}\}.$$

Then we have a bijection

$$\varphi\colon \{H \subseteq \mathrm{Aut}_k(\Omega) \text{ open compact subgroups}\} \to S'$$
$$H \mapsto \Omega^H.$$

with inverse given by $E \mapsto \mathrm{Aut}_E(\Omega)$.

PROOF. This follows from Theorem 3.7 and Proposition 3.5 v. □

3.4. A short exact sequence.

Definition 3.9. Let G be an ordered abelian group and let k be a field. We use multiplicative notation for G. Then we set $k((G))$ to be the set of formal sums $\alpha = \sum_{g\in G} a_g g$, where $a_g \in k$ such that $\operatorname{supp}(\alpha) = \{g : a_g \neq 0\}$ is well-ordered. For $\beta = \sum_{g\in G} b_g g$ we set

$$\alpha + \beta = \sum_{g\in G} (a_g + b_g)g$$

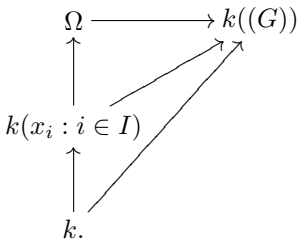
$$\alpha \cdot \beta = \sum_{g\in G} \left(\sum_{h_1,h_2\in G:\ h_1\cdot h_2 = g} \alpha_{h_1}\beta_{h_2} \right) g.$$

One can show that these operations are well-defined and that these operations make $k((G))$ into a field ([**Poo93**, Corollary 2]), which is algebraically closed if k is algebraically closed and G is divisible ([**Poo93**, Corollary 4]). Furthermore, it is a valued field where we put $v(\alpha) = \min(\operatorname{supp}(\alpha))$ with value group G and residue field k. Such ordered fields are called *Malcev fields*.

PROOF OF THEOREM 1.1. It is easy to see that all maps are continuous. The only non-trivial part is the surjectivity of the last map, and Proposition 3.1 takes care of this.

Assume that k is algebraically closed. Let $(x_i)_{i\in I}$ be a transcendence basis of Ω/k. Put a total ordering $\leq$ on I using the axiom of choice. Consider the ordered abelian group $G = \bigoplus_{i\in I} \mathbf{Q}$ which is ordered by saying $a = (a_i)_{i\in I} \leq b = (b_i)_{i\in I}$ if $\min(\operatorname{supp}(a)) < \min(\operatorname{supp}(b))$, or $i = \min(\operatorname{supp}(a)) = \min(\operatorname{supp}(b))$ and $a_i \leq b_i$. Consider the field $k((G))$.

It is quite obvious from the definition that the elements $(\delta_{ij})_j \in k((G))$ for $i \in I$ are algebraically independent. Hence we have an induced map $k(x_i : i \in I) \to k((G))$ which sends x_i to $(\delta_{ij})_j$. As $k((G))$ is algebraically closed, we can take an inclusion $\Omega \subseteq k((G))$ making the following diagram commute:



This gives us a splitting $\operatorname{Aut}(k) \to \operatorname{Aut}(k \to \Omega)$ defined as follows:

$$\varphi\colon \operatorname{Aut}(k) \to \operatorname{Aut}(k \to \Omega)$$

$$\sigma \mapsto \left(\sum_{g\in G} a_g g \in \Omega \mapsto \sum_{g\in G} \sigma(a_g)g \right).$$

We will show that this map is continuous. Take $\tau \in \mathrm{Aut}(k \to \Omega)$, $a \in \Omega$ and consider the set $U = \{h \in H : h(a) = \tau(a)\}$. It suffices to show that $\varphi^{-1}(U)$ is open. Take $\tau' \in \varphi^{-1}(U)$. Consider the minimal polynomial $f = f^a_{k(x_i : i \in I)} \in k(x_i : i \in I)[x]$ of x over $k(x_i : i \in I)$. Let $a_1 = a, a_2, \ldots, a_n$ be the different zeros of f in $k((G))$. Write $a_i = \sum_{g \in G} c_{ig} g$. For $i = 2, \ldots, n$, as $a_1 \neq a_i$, there exist $g_i \in G$ such that $c_{1g_i} \neq c_{ig_i}$. Let $S = \{c_{1g_i} : i = 2, \ldots, n\}$. Let $S' \subset k$ be the finite set of elements of k which occur in the expressions of f. Let $T = S \cup S'$ and consider the open set $V = \{h' \in \mathrm{Aut}(k) : \forall t \in T : h'(t) = \tau'(t)\}$. We claim: $\varphi(V) \subseteq U$. For $h \in \varphi(V)$ we have $h(f) = f$ (where h acts only on the coefficients). This means that h maps a to one of the a_i. By construction it maps a to a and the result follows. □

Remark 3.10. If k is not algebraically closed, then the sequence is not necessarily split. Assume that $\mathrm{Aut}(k)$ has an element σ of finite order $n > 2$ and let Ω be any algebraically closed field containing k. It follows from the famous Artin-Schreier theorem ([**Lan02**, Corollary 9.3, Chapter VI)]) that $\mathrm{Aut}(\Omega)$ has no element of order n. Hence the sequence does not split.

For example, take k_0 a field and let $k = k_0(x)$. Let Ω be an algebraic closure of k. Let $\sigma \in \mathrm{Aut}_{k_0}(k)$ be the automorphism which sends x to $\frac{-1}{1+x}$ of order 3.

4. Degree map of categories

4.1. General categorical notions.

Definition 4.1. Let $\mathcal{C}$ be a category. Then $\mathcal{C}$ is called *filtered* if the following conditions are satisfied:

i. $\mathcal{C}$ is not empty;
ii. for every $A, B \in \mathrm{Ob}(\mathcal{C})$ there exists $C \in \mathrm{Ob}(\mathcal{C})$ such that $\mathrm{Hom}_{\mathcal{C}}(A, C)$, $\mathrm{Hom}_{\mathcal{C}}(B, C) \neq \emptyset$;
iii. for every $A, B \in \mathrm{Ob}(\mathcal{C})$ and $f, g \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ there is $C \in \mathrm{Ob}(\mathcal{C})$ and $h \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ such that $h \circ f = h \circ g$.

Let G be a group. Then we define the category $C(G)$ to be the following. The object set is $\{\mathrm{pt}\}$ and $\mathrm{Hom}(\mathrm{pt}, \mathrm{pt}) = G$, with composition coming from the composition law of G. Notice that any $\sigma \in \mathrm{Aut}(G)$ induces an automorphism of $C(G)$ which maps the arrow g to $\sigma(g)$. We denote this automorphism by σ as well. If H is a group as well, then one easily gets $C(G \times H) \cong C(G) \times C(H)$.

Let $\mathcal{C}$ be any category. We set $\mathrm{Simp}(\mathcal{C})$ to be the following category. The set of objects is the same as that of $\mathcal{C}$ and between any two objects there is a unique arrow. There is a functor $F_{\mathcal{C}} \colon \mathcal{C} \to \mathrm{Simp}(\mathcal{C})$ which sends an object to the object itself, and maps a morphism to the unique morphism connecting the source and the target. Note that an automorphism of $\mathcal{C}$ induces an automorphism of $\mathrm{Simp}(\mathcal{C})$.

4.2. Degree.

Definition 4.2. Let $\mathcal{C}$ be a category, let $G \to \mathrm{Aut}(\mathcal{C})$ be a morphism of groups and let H be a G-group, that is, we have a morphism $G \to \mathrm{Aut}(H)$. For $\sigma \in G$, $h \in H$ we write ${}^{\sigma}h$ for this action. A *G-pre-degree d to H* is a functor

$$d \colon \mathcal{C} \to C(H)$$

which respects the G-actions (for any $\sigma \in G$ we have $\sigma \circ d = d \circ \sigma$). A *$G$-degree* d to H is a functor

$$d\colon \operatorname{Simp}(\mathcal{C}) \to C(H)$$

which respects the G-actions.

If G is trivial, we will call such functors a pre-degree respectively degree.

Remark 4.3. More concretely, in the above definition, a G-pre-degree is an association $d\colon \operatorname{Hom}(\mathcal{C}) \to H$ satisfying the following for all $A, B, C \in \operatorname{Ob}(\mathcal{C})$, $f \in \operatorname{Hom}(A, B)$, $g \in \operatorname{Hom}(B, C)$ and $\sigma \in G$:

i. $d(g \circ f) = d(g) \cdot d(f)$;
ii. $d(\sigma(f)) = {}^{\sigma}d(f)$.

Furthermore, a G-degree is a rule $d\colon \operatorname{Ob}(\mathcal{C}) \times \operatorname{Ob}(\mathcal{C}) \to H$, denoted by $d((A, B)) = d(B/A)$, satisfying for all $A, B, C \in \operatorname{Ob}(\mathcal{C})$ and $\sigma \in G$:

i. $d(C/A) = d(C/B) \cdot d(B/A)$;
ii. $d(\sigma(B)/\sigma(A)) = {}^{\sigma}d(B/A)$.

Instead of working with a functor, we will often just check that the above relations hold.

Remark 4.4. We can generalize the definition of a pre-degree or degree by allowing monoids instead of groups for H.

Proposition 4.5. *Let $\mathcal{C}$ be a category. Then the following hold.*

i. *Let $d\colon \operatorname{Simp}(\mathcal{C}) \to C(H)$ be a G-degree. Then $d \circ F_{\mathcal{C}}$ is a G-pre-degree.*
ii. *Assume $\mathcal{C}$ is filtered and let $d'\colon \mathcal{C} \to C(H)$ be a G-pre-degree. Then there is a unique degree $d\colon \operatorname{Simp}(\mathcal{C}) \to C(H)$ such that $d' = d \circ F_{\mathcal{C}}$.*

Proof. i. Follows easily from the definitions.

ii. Let $A, B \in \operatorname{Ob}(\mathcal{C})$. Take $C \in \operatorname{Ob}(\mathcal{C})$ with $f \in \operatorname{Hom}(A, C)$ and $g \in \operatorname{Hom}(B, C)$. We put

$$d(B/A) = d'(g)^{-1} \cdot d'(f).$$

We need to show that this definition does not depend on the choice of C and f and g. Let $C' \in \operatorname{Ob}(\mathcal{C})$ with $f' \in \operatorname{Hom}(A, C')$ and $g \in \operatorname{Hom}(B, C')$. Without loss of generality we may assume that there is a map $h \in \operatorname{Hom}(C, C')$ (property ii of a filtered category). After extending (property iii of a filtered category), we may assume that $h \circ f = f'$ and $h \circ g = g'$. But then we have

$$d'(g')^{-1} \cdot d'(f') = d'(g)^{-1} d'(h)^{-1} d'(h) d'(f) = d'(g)^{-1} d'(f)$$

as required.

We will show that $d' = d \circ F_{\mathcal{C}}$. For an identity map $\mathrm{id}_B \in \operatorname{Hom}(B, B)$ we have $d'(\mathrm{id}_B) = 1$. Furthermore, if $f \in \operatorname{Hom}(A, B)$ we have

$$d(B/A) = d'(\mathrm{id}_B)^{-1} d'(f) = d'(f)$$

as required.

We will show that i and ii hold for d. Let $A, B, C \in \mathrm{Ob}(\mathcal{C})$ and let $D \in \mathrm{Ob}(\mathcal{C})$ with $f \in \mathrm{Hom}(A, D)$, $g \in \mathrm{Hom}(B, D)$ and $h \in \mathrm{Hom}(C, D)$. Then we have

$$d(C/A) = d'(h)^{-1}d'(f) = \big(d'(h)^{-1}d'(g)\big) \cdot \big(d'(g)^{-1}d'(f)\big) = d(C/B) \cdot c(B/A).$$

Furthermore, we have for $\sigma \in G$

$$d(\sigma(B)/\sigma(A)) = d'(\sigma(g))^{-1}d'(\sigma(f)) = {}^{\sigma}d'(g)^{-1} \cdot {}^{\sigma}d'(f) = {}^{\sigma}d(B/A).$$

Finally, we will prove uniqueness. Let $A, B \in \mathrm{Ob}(\mathcal{C})$ and let $C \in \mathrm{Ob}(\mathcal{C})$ with $f \in \mathrm{Hom}(A, C)$ and $g \in \mathrm{Hom}(B, C)$. Then for any other possible extension d'' we would have

$$d''(C/B)d''(B/A) = d''(C/A)$$

and $d''(C/B) = d(g)$ and $d''(C/A) = d(f)$. Hence $d''(B/A) = d(g)^{-1}d(f)$ as required. □

Remark 4.6. If a degree corresponds to a pre-degree, we will often use the same notation for both functors.

Lemma 4.7. *Let $\mathcal{C}$ be a category, let $G \subseteq \mathrm{Aut}(\mathcal{C})$ be a subgroup and let H be a G-group. Let $S \subseteq \mathrm{Hom}(\mathcal{C})$ be a collection which satisfies for all $A, B, C, C' \in \mathrm{Ob}(\mathcal{C})$ and $f, t, t' \in \mathrm{Hom}(\mathcal{C})$:*

i. *there exists $g \in \mathrm{Hom}(\mathcal{C})$ such that $g \circ f \in S$;*
ii. *if $g \circ f \in S$ and $g' \circ f \in S$, then there there exists $h, h' \in \mathrm{Ob}(\mathcal{C})$ with $h \circ g \circ f \in S$ and $h \circ g = h' \circ g'$;*
iii. *if $s \in S$ and $\sigma \in G$, then $\sigma(s) \in S$;*
iv. *if $t \circ t' \in S$, then $t \in S$.*

Furthermore, assume we have a map $d\colon S \to H$ satisfying

v. *if $s, t \in S$ and $st \in S$ we have $d(st) = d(s)d(t)$;*
vi. *if $s \in S$ and $\sigma \in G$, then $d(\sigma(s)) = {}^{\sigma}d(s)$.*

Then there is a unique G-pre-degree d' on $\mathcal{C}$ to H extending d defined as follows. Let $f \in \mathrm{Hom}(\mathcal{C})$ and $g \in S$ such that $g \circ f \in S$ (property i). Then $g \in S$ (property iv). Set

$$d'(f) = d(g)^{-1} \cdot d(g \circ f).$$

Proof. If such an extension exists, then one directly sees that it is equal to d' (uniqueness). We first show that the extension is well-defined. Let $g' \in S$ such that $g' \circ f \in S$. Then there are $h, h' \in \mathrm{Hom}(\mathcal{C})$ such that $h \circ g \circ f \in S$ and $h \circ g = h' \circ g'$ (property ii). By property iv we have $h \circ g, h' \circ g', h, h' \in S$. We find, using property v,

$$\begin{aligned} d(g)^{-1}d(g \circ f) &= d(g)^{-1}d(h)^{-1}d(h \circ g \circ f) = d(h \circ g)^{-1}d(h' \circ g' \circ f) \\ &= d(h' \circ g')^{-1}d(h' \circ g' \circ f) = d(g')^{-1}d(h')^{-1}d(h' \circ g' \circ f) \\ &= d(g')^{-1}d(g' \circ f). \end{aligned}$$

We will show that d' satisfies the two required properties.

Consider $f \circ f'$. Then there is a $g \in S$ such that $g \circ f \circ f' \in S$ (property i). Hence we have $g, g \circ f \in S$ (property iv) and this gives:

$$\begin{aligned} d'(f \circ f') &= d(g)^{-1} d(g \circ f \circ f') = \left(d(g)^{-1} d(g \circ f)\right) \left(d(g \circ f)^{-1} d(g \circ f \circ f')\right) \\ &= d'(f) \circ d'(f'). \end{aligned}$$

Furthermore, we have (property iii and vi)

$$d'(\sigma(f)) = d(\sigma(g))^{-1} \cdot d(\sigma(g \circ f)) = {}^{\sigma}d(g)^{-1} \cdot {}^{\sigma}d(g \circ f) = {}^{\sigma}d'(f).$$

□

4.3. Functorial properties. Here are some functorial properties of pre-degrees and degrees.

Lemma 4.8. *Let $\mathcal{C}$ be a category. Let $G \subseteq \mathrm{Aut}(\mathcal{C})$ and let H be a G-group. Let $f\colon H \to H'$ be a G-morphism. Then the following hold:*

i. *Let $d\colon \mathcal{C} \to C(H)$ be a G-pre-degree. Then the map $f \circ d\colon \mathrm{Hom}(\mathcal{C}) \to H'$ given by $(f \circ d)(g) = f(d(g))$ gives a G-pre-degree.*
ii. *Let $d\colon \mathrm{Simp}(\mathcal{C}) \to C(H)$ be a G-pre-degree. Then the map $f \circ d\colon \mathrm{Ob}(\mathcal{C}) \times \mathrm{Ob}(\mathcal{C}) \to H'$ given by $(f \circ d)((A, B)) = f(d((A, B)))$ is a G-degree.*

Proof. i. We have:

$$\begin{aligned} (f \circ d)(g \circ g') &= f(d(g \circ g')) \\ &= f(d(g) \cdot d(g')) \\ &= f(d(g)) \cdot f(d(g')) \\ &= (f \circ d)(g) \cdot (f \circ d)(g') \end{aligned}$$

and

$$(f \circ d)(\sigma(g)) = f(d(\sigma(g))) = f({}^{\sigma}d(g)) = {}^{\sigma}(f \circ d)(g).$$

ii. The proof is very similar to the proof of i. □

Remark 4.9. Let d be a G-(pre-)degree to H. Let $G' \subseteq G$ be a subgroup. Then d is a G'-(pre-)degree.

Remark 4.10. Let d and d' be G-pre-degrees (respectively G-degrees) to H respectively H'. Then $d \times d'$ is also a G-pre-degree (respectively G-degree) to $H \times H'$.

If d is a G-degree (respectively G-pre-degree) on $\mathcal{C}$ and $\mathcal{C}'$ is a G-stable subcategory of $\mathcal{C}$, then d is automatically a G-degree (respectively G-pre-degree). But it might give a degree (respectively pre-degree) with respect to a larger or different group than G.

4.4. Cohomology associated to a degree map. We will very briefly discuss cohomology (see [**Ser79**, Appendix Non-abelian Cohomology]). Let G be a group acting on a group H on the left. A cocycle is a map $c\colon G \to H$ which satisfies for all $g, g' \in G$ the identity $c(gg') = c(g)g(c(g'))$. We define an equivalence relation on the set of cocycles by $c \sim c'$ iff there exists $h \in H$ with $c'(s) = h^{-1}c(s)s(h)$. The set $H^1(G, H)$ of equivalence classes forms a pointed set with as chosen point the class of the zero cocycle. If the action of G on H is trivial, then $H^1(G, H) = \mathrm{Hom}(G, H)$.

Lemma 4.11. *Let $\mathcal{C}$ be a category, let G be a group and H be a G-group. Let d be a G-degree to H. Let $A \in \mathrm{Ob}(\mathcal{C})$. Then we can associate an element $c_d \in H^1(G,H)$ to d defined by*

$$\begin{aligned} c_d \colon G &\to H \\ \sigma &\mapsto d(A/\sigma(A)), \end{aligned}$$

which does not depend on the choice of A.

Proof. We will first show that $c_d \in H^1(G,H)$. Indeed, for $\sigma, \tau \in G$ we have

$$c_d(\sigma\tau) = d(A/\sigma\tau(A)) = d(A/\sigma(A)) \cdot d(\sigma(A)/\sigma\tau(A)) = c_d(\sigma) \cdot {}^{\sigma}c_d(\tau).$$

For $A, B \in \mathrm{Ob}(\mathcal{C})$ we have

$$d(B/\sigma(B)) = d(B/A)d(A/\sigma(A))d(\sigma(A)/\sigma(B)) = d(A/B)^{-1}d(A/\sigma(A))^{\sigma}d(A/B).$$

which shows that c_d does not depend on A. □

Let G be a group acting on a group H, let $\overline{c} \in H^1(G,H)$ represented by a cocycle c and let $N \lhd G$ contained in $\ker(G \to \mathrm{Aut}(H))$. Then we have a map

$$\begin{aligned} c_N \colon G &\to H \rtimes (G/N) \\ \sigma &\mapsto (c(\sigma), \sigma N)\,. \end{aligned}$$

This is a group morphism. Indeed, we have

$$\begin{aligned} c_N(\sigma\tau) &= (c(\sigma\tau), \sigma\tau N) = (c(\sigma) \cdot {}^{\sigma}c(\tau), \sigma N \cdot \tau N) \\ &= (c(\sigma), \sigma N)(c(\tau), \tau N) = c_N(\sigma)c_N(\tau). \end{aligned}$$

This morphism depends on the choice of c, but different choices give isomorphic images. Indeed, for $a \in H$ we have an isomorphism

$$\begin{aligned} \varphi_a \colon H \rtimes (G/N) &\to H \rtimes (G/N) \\ (h, \overline{g}) &\mapsto (a^{-1}hg(a), \overline{g}). \end{aligned}$$

This shows that $c \sim c'$ implies that the images of c_N and c'_N are isomorphic.

Remark 4.12. Let us explain why degrees can be useful. Suppose we want to understand a group G. Then we hope to get a map $G \to H \rtimes (G/N)$ for which we understand H and G/N. This gives us information about G.

5. Examples of degrees and an application

In this section we will give some examples of degrees we will use. Later we will deduce properties of the various degrees.

5.1. Pre-degrees on $\mathcal{C}_p$. Let p be a prime number or 0 and let $\mathcal{C}_p$ be the category of fields of characteristic p with finite morphisms. That is, $\varphi\colon K \to L$ where $[L : \varphi(K)] < \infty$. As morphisms on fields are injective, we will usually identify K with $\varphi(K)$.

The *Grothendieck group* $\mathfrak{H}$ of finite groups is the free abelian group on the collection of finite groups (written multiplicatively), where we quotient out by the relations coming from $[G] = [G'] \cdot [G'']$ where $0 \to G' \to G \to G'' \to 0$ is an exact sequence of finite groups. In fact, it is a free abelian group on the isomorphy classes of finite simple groups. Hence it is not finitely generated.

For convenience we put we put $p^{\mathbf{Z}} = \{1\}$ if $p = 0$.

Proposition 5.1. *Consider the category $\mathcal{C}_p$. We have the following pre-degrees, defined as follows on a morphism $\varphi\colon K \to L$:*

i. $d_{\mathrm{d}}(\varphi) = [L : \varphi(K)] \in \mathbf{Q}_{>0}$ *(standard pre-degree)*
ii. $d_{\mathrm{i}}(\varphi) = [L : \varphi(K)]_{\mathrm{i}} \in p^{\mathbf{Z}}$ *(inseparability pre-degree)*
iii. $d_{\mathrm{s}}(\varphi) = [L : \varphi(K)]_{\mathrm{s}} \in \mathbf{Q}_{>0}$ *(separability pre-degree)*
iv. $d_{\mathrm{g}}(\varphi) = \frac{[\mathrm{Aut}_K(M)]}{[\mathrm{Aut}_L(M)]} \in \mathfrak{H}$ *(if M/K is finite normal containing L; group pre-degree).*
v. $d_{\mathrm{t}}(\varphi) = d_{\mathrm{g}}(\varphi) \times d_{\mathrm{i}}(\varphi) \in \mathfrak{H} \times p^{\mathbf{Z}}$ *(total pre-degree).*

Proof. It is obvious that d_{d}, d_{i}, d_{s} are pre-degrees. Once we show that d_{g} is a pre-degree, then d_{t} is automatically a pre-degree.

Let S be the collection of normal morphisms. For a normal extension $\varphi\colon K \to L$ we set $d_{\mathrm{g}}(\varphi) = [\mathrm{Aut}_K(L)] \in \mathfrak{H}$. We will check that the assumptions of Lemma 4.7 are satisfied. Trivially iii and vi are satisfied. Assumption i follows from taking a normal closure, ii follows from the fact that a compositum of normal fields is again normal. Assumption iv is a standard property of normal morphisms. Finally, if $K \subseteq L \subseteq M$ with L/K and M/L normal in $\mathcal{C}_p$, then we have a well-known short exact sequence

$$0 \to \mathrm{Aut}_L(M) \to \mathrm{Aut}_K(M) \to \mathrm{Aut}_K(L) \to 0.$$

This shows that v holds. □

Remark 5.2. Note that we have a morphism of groups $f\colon \mathfrak{H} \to \mathbf{Q}_{>0}$, $[H] \mapsto \#H$. Then we have $d_{\mathrm{s}} = f \circ d_{\mathrm{g}}$.

5.2. Degrees on $\mathrm{Sub}(\Omega, [K])$. We want to turn the pre-degrees of the previous section into degrees by restricting to a filtered category.

Let Ω be a field of characteristic $p \geq 0$. We define the category $\mathrm{Sub}(\Omega)$ which has as objects the set of subfields of Ω. The set of homorphisms between two subfields K and K' is the empty set unless $K \subseteq K'$, and in that case, it consists of this inclusion only. The composition of morphisms is the natural one.

Definition 5.3. Two fields $K, L \subseteq \Omega$ are called *commensurable* if there is a field $M \subseteq \Omega$ which is finite over K and L.

Lemma 5.4. *Commensurability is an equivalence relation on* $\mathrm{Sub}(\Omega)$.

Proof. The only part which needs proof is the transitivity, and this is an easy exercise. □

The commensurability class of K is denoted by $[K]$.

For any subfield K of Ω we set $\mathrm{Sub}(\Omega, [K])$ to be the full subcategory of $\mathrm{Sub}(\Omega)$ which has as objects the fields which are commensurable with K. Note that this category is filtered.

Note that $\mathrm{Aut}(\Omega)$ acts on $\mathrm{Sub}(\Omega)$, and an automorphism $\sigma \in \mathrm{Aut}(\Omega)$ induces a functor $\mathrm{Sub}(\Omega, [K]) \to \mathrm{Sub}(\Omega, [\sigma(K)])$. We put $\mathrm{Aut}_{[K]}(\Omega) \subseteq \mathrm{Aut}(\Omega)$ to be the set of morphisms such that $[K] = [\sigma(K)]$. Note that $\mathrm{Aut}_{[K]}(\Omega)$ acts on $\mathrm{Sub}(\Omega, [K])$.

Let G be a group and let $G \to \mathrm{Aut}_{[K]}(\Omega)$ be a morphism. Let H be a group with trivial G-action. Let d be a pre-degree on $\mathcal{C}_p$ to H. Then d induces a pre-degree on $\mathrm{Sub}(\Omega, [K])$ and in certain cases a G-pre-degree. As $\mathrm{Sub}(\Omega, [K])$ is filtered, this induces a G-degree (Proposition 4.5).

It is very easy to see that we have the following G-degrees (where the action on the image groups is trivial): d_{d}, d_{i}, d_{s}, d_{g} and d_{t}.

Such a degree induces an element $c_d \in H^1(G, H)$ (Lemma 4.11). The kernel of c_d is defined to be the set of elements mapping to the special element.

Lemma 5.5. *Let the situation be as above. Then one has* $\mathrm{Aut}_K(\Omega) \subseteq \mathrm{Aut}(K \to \Omega) \subseteq \mathrm{Aut}_{[K]}(\Omega) \cap \ker(c_d)$.

Proof. This follows directly. □

5.3. Finite transcendence degree.

5.3.1. *Finite transcendence degree.* We will shrink our category even more. Let Ω be a field of characteristic $p \geq 0$ and let $k \subseteq \Omega$ be a subfield such that $\mathrm{trdeg}_k(\Omega) < \infty$.

Put $\mathfrak{C}_k = \{E : k \subseteq E \subseteq \Omega,\ E/k \text{ f.g.},\ \Omega/E \text{ algebraic}\}$, which is non-empty. We claim that $\mathfrak{C}_k$ is an equivalence class under commensurability.

Proposition 5.6. *Let $K \subseteq L \subseteq M$ be a tower of fields where M is finitely generated over K. Then L is finitely generated over K.*

Proof. Let $x_1, \ldots, x_s$ be a transcendence basis of L/K and extend it to a transcendence basis $x_1, \ldots, x_r$ of M/K. Consider the following diagram

$$\begin{array}{ccccc} K & \longrightarrow & L & \longrightarrow & M \\ \uparrow & & \uparrow & & \uparrow{\scriptstyle <\infty} \\ K & \longrightarrow & K' = K(x_1, \ldots, x_s) & \longrightarrow & E = K(x_1, \ldots, x_r), \end{array}$$

Consider the natural map $L \otimes_K E \to LE$ with image N. We claim that this map is injective. Indeed, one easily sees that it is injective if and only if it is injective when restricted to $L \otimes_K K[x_{s+1}, \ldots, x_r]$. But $x_{s+1}, \ldots, x_r$ remain transcendental over the algebraic extension L of K. Hence $\dim_{K'}(L) = \dim_E(N) \leq \dim_E(M) < \infty$. □

Remark 5.7. A statement as in Proposition 5.6 is false for rings. For any field k, the chain $k[x, y] \supset k[xy^i : i \in \mathbf{Z}_{\geq 0}] \supset k$ gives a counterexample.

We can now show that $\mathfrak{C}_k$ is an equivalence class. Indeed, if $E, E' \in \mathfrak{C}_k$, then EE' is finite over both E an E' and hence E and E' are commensurable. Suppose that $E \in \mathfrak{C}$ is commensurable with E'. Then we have $[EE' : E] < \infty$. It follows that EE' is finitely generated over k, and by Proposition 5.6 it follows that E' is finitely generated

over k. If $\mathrm{trdeg}(E'/k) \neq \mathrm{trdeg}(E/k) = \mathrm{trdeg}(\Omega/k)$, then EE'/E' is not algebraic and hence not finite.

The category we will be working in is $\mathrm{Sub}(\Omega, \mathfrak{C}_k)$. Put $G = \mathrm{Aut}(k \to \Omega) \subseteq \mathrm{Aut}_{\mathfrak{C}_k}(\Omega)$. On this category we have the natural degrees G-degrees d_d, d_i, d_s, d_g and d_t, for which the action on the target group is trivial. Put p equal to $\mathrm{char}(k)$ if nonzero and 1 otherwise. The degree d_t gives a cocyle

$$c'_k\colon \mathrm{Aut}(k \to \Omega) \to \mathfrak{h} \times p^{\mathbf{Z}}$$

with restriction

$$c_k\colon \mathrm{Aut}_k(\Omega) \to \mathfrak{h} \times p^{\mathbf{Z}}.$$

5.4. Main theorem. Let k be a field of characteristic p and let Ω be a field extension of k of finite transcendence degree $r \in \mathbf{Z}_{\geq 1}$ which is algebraically closed.

We can finally state the main theorem of this section.

Theorem 5.8. *Let Ω be an algebraically closed field and let k be a subfield such that $1 \leq \mathrm{trdeg}_k(\Omega) < \infty$. Define c_k and c'_k as in the previous subsection. Then one has:*

i. *c_k and c'_k are surjective;*
ii. *c_k and c'_k are continuous if $\mathfrak{h} \times p^{\mathbf{Z}}$ is endowed with the discrete topology;*
iii. *the kernels of c_k and c'_k contain all morphisms which induce an automorphism on an element of $\mathfrak{C}_k$;*
iv. *$\ker(c_k)$ and $\ker(c'_k)$ are open and not compact.*

Most of the statements in the theorem above follow quite easily. The hardest statement is the surjectivity of c_k and c'_k. For the proof of the surjectivity we need a couple of lemmas which reduce to the case of transcendence degree 1 and k algebraically closed.

Proof of Theorem 1.2. Follows directly from Theorem 5.8. □

Lemma 5.9 (Approximation lemma)**.** *Let Ω be a field and let $K, L, M \subseteq \Omega$ be subfields. Assume that L and K are commensurable. Then there is a finite set $B \subseteq M$ such that for all $B' \subseteq M$ with $B \subseteq B'$ we have $d_t(L(B')/K(B')) = d_t(LM/KM)$.*

Proof. Using the multiplicativity of d_t, we see that it is enough to prove the case for an inclusion $K \subseteq L$.

Let N be a finite normal extension of K containing L. Let $S = \{b_1, \ldots, b_s\}$ be a basis of N/K and let $T \subseteq S$ be a basis of NM/KM. For $s \in S \setminus T$ we have a relation $s = \sum_{t \in T} b_{s,t} t$ where $b_{s,t} \in KM$. Let $B = \{b_{s,t} : s \in S \setminus T, t \in T\}$. Let $B' \subseteq M$ satisfy $B \subseteq B'$. Then we have have $\#T \geq [N(B') : K(B')] \geq [NM : KM] = \#T$ and hence $[N(B') : K(B')] = [NM : KM]$. As the usual degree is multiplicative, a similar statement holds for all subextensions. As a separable extension of $K(B')$ remains separable over KM, we deduce $[N(B') : K(B')]_i = [NM : KM]_i$ and $[N(B') : K(B')]_s = [NM : KM]_s$. After possibly enlarging B, we may assume that similar statements hold for K replaced by L. Consider the natural injective map $\mathrm{Aut}_{KM}(NM) \to \mathrm{Aut}_{K(B')}(N(B'))$, which is surjective since both have size $[N(B') : K(B')]_s = [NM : LM]_s$. Similarly, the map $\mathrm{Aut}_{KM}(LM) \to \mathrm{Aut}_{L(B')}(N(B'))$ is an isomorphism. Hence $d_t(L(B')/K(B')) = d_t(LM/KM)$. □

Lemma 5.10. *Let k' be a subextension of Ω/k where Ω/k' is not algebraic. Then the diagram*

$$\begin{array}{ccc} \mathrm{Aut}_k(\Omega) & \xrightarrow{c_k} & \mathfrak{h} \times p^{\mathbf{Z}} \\ \uparrow & \nearrow_{c_{k'}} & \\ \mathrm{Aut}_{k'}(\Omega) & & \end{array}$$

is commutative.

PROOF. Let $\sigma \in \mathrm{Aut}_{k'}(\Omega)$. Let $L \in \mathfrak{C}_k$. Let $B' \subseteq k'$ be a finite set such that $d_t(L(B')/\sigma(L)(B')) = d_t(k'L/k'\sigma(L))$ (Lemma 5.9). Note that $L(B') \in \mathfrak{C}_k$ and $Lk' \in \mathfrak{C}_{k'}$. Hence we find, as σ fixes k',

$$c_k(\sigma) = d_t(L(B')/\sigma(L)(B')) = d_t(k'L/k'\sigma(L)) = c_{k'}(\sigma).$$

□

Lemma 5.11. *Let K be a function field over an algebraically closed field k. Let $D \geq 0$ be an effective divisor of K with $\deg_k(D) \geq 2g(K)$. Then there exists $x \in K$ with $(x)_\infty = D$.*

PROOF. For all $v \in \mathcal{P}_{K/k}$ with $v \leq D$ we have $\mathfrak{L}(D - v) \subsetneq \mathfrak{L}(D)$ (Riemann-Roch, Theorem 2.13 from Chapter 2). As k is infinite, it follows that $\bigcup_{v \in \mathcal{P}_{K/k}:\ v \leq D} \mathfrak{L}(D-P) \subsetneq \mathfrak{L}(D)$ and the result follows. □

Let $n \in \mathbf{Z}_{\geq 1}$ be an integer. By S_n we denote the symmetric group on n elements.

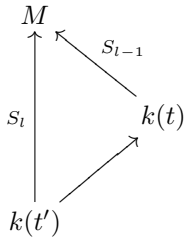
Lemma 5.12. *Let $l \in \mathbf{Z}_{\geq 3}$ be prime and let K be a function field over an algebraically closed field k. Suppose that $x \in K^*$ satisfies $(x)_\infty = 2P_1 + \sum_{i=2}^{l-1} P_i$ for primes P_i of K which are pairwise different. Then $K/k(x)$ is separable of degree l. If M is a Galois closure of $K/k(x)$, then $\mathrm{Gal}(M/k(x)) \cong S_l$ and $\mathrm{Gal}(M/K) \cong S_{l-1}$.*

PROOF. One has $[K : k(x)] = \deg((x)_\infty)$ according to Lemma 2.12 from Chapter 2. The prime ∞ of $k(x)$ splits into $l-2$ unramified prime and one prime which has ramification index 2. If the extension is inseparable, then it is purely inseparable as l is prime and hence every prime has a unique extension (Theorem 5.6 from Chapter 1). Hence our extension is separable (here we need $l \geq 3$). From Proposition 9.8ii from Chapter 1 (and from Proposition 8.3 from Chapter 1) follows that $\mathrm{Gal}(M/k(t)) \subseteq S_l$ contains a 2-cycle. Notice that $\mathrm{Gal}(M/k(t))$ has an element of order l as l is prime, which is necessarily an l-cycle. One can easily see that a 2-cycle and an l-cycle generate S_l as l is prime (as l is prime, one can assume that these cycles are (12) and $(12 \ldots l)$ in S_l and then use [**Lan02**, Chapter 1, Exercise 38]). Note that $[M : K] = (l-1)!$ and hence we have $\mathrm{Gal}(M/K) \cong S_{l-1}$. □

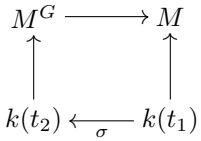
PROOF OF THEOREM 5.8. i. It is enough to show that c_k is surjective. We may assume $k = \overline{k}$ and Ω/k has transcendence degree 1 (Lemma 5.10), say with t a transcendent. As c_k is a morphism, it is enough to show that the image of c_k contains $([G], 1)$ for any finite group G and $([0], p)$ if $p = \mathrm{char}(k) > 0$.

If $p > 0$, we have a morphism $k(t) \to k(t^p)$, $t \mapsto t^p$. Extend it to $\sigma \in \mathrm{Aut}_k(\Omega)$ with Proposition 3.1. We then have $c_k(\sigma) = ([0], p)$.

Let G be a finite group. We will show that $([G], 1) \in \mathrm{im}(c_k)$. Take a prime $l \in \mathbf{Z}_{\geq 3}$ big enough such that we have an embedding $G \subseteq S_l$. Use Lemma 5.12 and Lemma 5.11 with $k(t)$ to obtain the following diagram for a certain field M and an element $t' \in k(t)$:



Hence this gives us a field extension M/M^G with group G. Pick l' prime with $l' \geq \max(3, 2g(M), 2g(M^G))$ and again using Lemma 5.12 and Lemma 5.11 construct subfields $k(t_2)$ and $k(t_1)$ of M^G respectively M which satisfy $d_t(M^G/k(t_2)) = d_t(M/k(t_1)) = (\frac{[S_{l'}]}{[S_{l'-1}]}, 1)$. Pick an isomorphism $\sigma\colon k(t_1) \to k(t_2)$ and extend it to an element $\sigma \in \mathrm{Aut}_k(\Omega)$ (Proposition 3.1). We have the following diagram:



Then using the multiplicativity of d_t we have

$$\begin{aligned} c_k(\sigma) &= d_t(k(t_1)/\sigma(k(t_1))) = d_t(k(t_1)/k(t_2)) \\ &= \frac{d_t(M/M^G)d_t(M^G/k(t_2))}{d_t(M/k(t_1))} = d_t(M/M^G) = ([G], 1). \end{aligned}$$

This finishes the first part of the proof.

ii. Let T be a transcendence basis of Ω/k and $f \in \mathrm{Aut}(k \to \Omega)$. Note that c_k is constant on $U_{T,f} \cap \mathrm{Aut}(k \to \Omega)$.

iii. This follows from the construction.

iv. Suppose the kernel of c_k is compact. Then so is the kernel of c'_k, as $\mathrm{Aut}_k(\Omega) \subseteq \mathrm{Aut}(k \to \Omega)$ is closed (Proposition 3.5i). Hence we look at the kernel of c_k.

The kernel is an normal open (by continuity) subgroup. Assume that it is compact. Then from Proposition 3.8 we see that $\ker(c_k) = \mathrm{Aut}_E(\Omega)$ for some subextension E of Ω/k such that Ω/E is algebraic. Let $\sigma \in \mathrm{Aut}_k(\Omega)$. Then one has $\mathrm{Aut}_E(\Omega) = \sigma\,\mathrm{Aut}_E(\Omega)\sigma^{-1} = \mathrm{Aut}_{\sigma(E)}(\Omega)$. From Proposition 3.1 and Lemma 3.4 it follows that for $T = \bigcup_{\sigma \in \mathrm{Aut}_k(\Omega)} \sigma(E)$ we have that $k(T) = \Omega$. Hence we obtain $\mathrm{Aut}_E(\Omega) = \mathrm{Aut}_\Omega(\Omega) = \{\mathrm{id}_\Omega\}$. This contradicts iii. □

Remark 5.13. We do not know exactly what the kernel is of c_k or c'_k. We do not know if it is generated by the subgroups of $\mathrm{Aut}_k(\Omega)$ which are both open and compact.

6. Faithful actions on the set of valuations

Let Ω/k be a field extension where Ω is algebraically closed and $\mathrm{trdeg}_k(\Omega) = 1$. Consider the set $\mathcal{P}_{\Omega/k}$ of valuation rings of Ω which contain k. Let $\mathfrak{C}$ be the subfields of Ω/k which are finitely generated and of transcendence 1 over k with their natural inclusions. This set is equal to $\varprojlim_{K\in\mathfrak{C}} \mathcal{P}_{K/k}$. The sets $\mathcal{P}_{K/k}$ are endowed with the co-finite topology and this limit is a subset of $\prod_{K\in\mathfrak{C}} \mathcal{P}_{K/k}$, which is endowed with the product topology. For $K \in \mathfrak{C}$ and $S \subseteq \mathcal{P}_{K/k}$ finite and we put

$$U(S,K) = \{v \in \mathcal{P}_{\Omega/k} : v|_K \notin S\}.$$

These $U(S,K)$ form a basis for the topology.

Lemma 6.1. *The actions of $G = \mathrm{Aut}(k \to \Omega)$ and $\mathrm{Aut}_k(\Omega)$ on $\mathcal{P}_{\Omega/k}$ are continuous.*

Proof. As the inclusion $\mathrm{Aut}_k(\Omega) \subseteq G$ is continuous, it is enough to prove the statement for G.

For $\sigma \in G$, the map $\sigma\colon \mathcal{P}_{\Omega/k} \to \mathcal{P}_{\Omega/k}$ is a homeomorphism. Indeed, it sends $U(S,K)$ to $U(\sigma(S),\sigma(K))$.

Consider the map $\mathrm{Aut}(k \to \Omega) \times \mathcal{P}_{\Omega/k} \to \mathcal{P}_{\Omega/k}$. Pick a basis element $U(S,K) \subseteq \mathcal{P}_{\Omega/k}$ and suppose $\sigma \in \mathrm{Aut}(k \to \Omega)$ and $x \in \mathcal{P}_{\Omega/k}$ satisfy $\sigma(x) \in U(S,K)$. We have the following commutative diagram, where the horizontal map is a homeomorphism of topological spaces and the other maps are the multiplication maps:

$$\begin{array}{ccc} \mathrm{Aut}(k\to\Omega)\times\mathcal{P}_{\Omega/k} & \xrightarrow{(\tau,x)\mapsto(\tau\sigma^{-1},\sigma(x))} & \mathrm{Aut}(k\to\Omega)\times\mathcal{P}_{\Omega/k} \\ & \searrow \quad \swarrow & \\ & \mathcal{P}_{\Omega/k} & \end{array}.$$

Hence we may assume that $\sigma = \mathrm{id}_\Omega$. For every $s \in S$ take $x_s \in K$ with the property that s is the only pole of x_s (Lemma 2.24 from Chapter 2). Put $T = \{x_s : s \in S\}$ and let $V = U_{T,\mathrm{id}_\Omega} \cap \mathrm{Aut}(k \to \Omega)$. But then we have $V \cdot U(S,K) \subseteq U(S,K)$. This shows that the action is continuous. □

Lemma 6.2. *Let k be a field and let $k(x)$ be the rational function field. Put $p = \mathrm{char}(k)$ if positive and 1 otherwise. Let $m \in \mathbf{Z}_{\geq 1}$, $n \in p^{\mathbf{Z}_{\geq 0}}$. Then one has:*

i. *there is $y \in k(x)$ such that $[k(x) : k(y)]_s = m$, $[k(x) : k(y)]_i = n$, such that if $v \in \mathcal{P}_{k(x)/k}$ satisfies $v(x) > 0$, then $v(y) = m \cdot n \cdot v(x) > 0$;*
ii. *there is $z \in \overline{k(x)}$ such that $k(z) \supseteq k(x)$, $[k(z) : k(x)]_s = m$, $[k(z) : k(x)]_i = n$, such that if $v \in \mathcal{P}_{k(z)/k}$ satisfies $v(z) > 0$, then $v(x) = m \cdot n \cdot v(z) > 0$.*

Proof. We only prove i. The proof of ii is similar.

Since the various degrees are multiplicative, it is enough to prove the cases $(n,m) = (p,1), (l,1), (1,p)$ where l is a prime different from p.

The case $(l,1)$: take $y = x^l$. The properties obviously hold.

The case $(p,1)$: take $y = \frac{x^p}{1-x^{p-1}}$. We first claim that $k(x)/k(y)$ has the right degrees. Consider this extension. Let v be a valuation with $v(x) > 0$. Then one has $v(y) = pv(x) - v(1 - x^{p-1}) = pv(x)$. As x is a zero of $f = X^p + X^{p-1}y - y \in k(y)[X]$, it follows that $k(x)/k(y)$ is a degree p extension. We still need to prove that this

extension is separable. We differentiate f and obtain $-X^{p-2}y$. This has zero only 0, and this is not a zero of f. Hence the polynomial is separable and $k(x)/k(y)$ is separable.

The case $(1,p)$: take $y = x^p$. The properties obviously hold. □

Proposition 6.3. *Let Ω/k be a field extension where Ω is algebraically closed and* $\mathrm{trdeg}_k(\Omega) = 1$. *Then* $\ker(c_{d_s \times d_i} \colon \mathrm{Aut}_k(\Omega) \to \mathbf{Q}^* \times \mathbf{Q}^*)$ *acts transitively on $\mathcal{P}_{\Omega/k}$.*

Proof. Let $v_0, v_1 \in P_{\Omega/k}$. Let $x \in \Omega$ be transcendental over k and put $K = k(x)$. Let $x_i \in K$ with $v_i(x_i) > 0$. Now find $x_i' \in k(x_i)$ using Lemma 6.2 with the property that $[k(x_i) : k(x_i')]_i = [K : k(x_{1-i})]_i$, $[k(x_i) : k(x_i')]_s = [K : k(x_{1-i})]_s$ and $v_i(x_i') > 0$. Notice that the restriction of v_i to $k_i(x_i')$ corresponds to the valuation from the polynomial x_i' (with valuation ring $k[x_i']_{(x_i')}$). Let $\sigma \in \mathrm{Aut}_k(\Omega)$ such that $\sigma(x_0') = x_1'$ (Propsition 3.1). We have

$$\begin{aligned} c_{d_s}(\sigma) &= d_s(k(x_0')/k(x_1')) \\ &= d_s(k(x_0')/k(x_0)) \cdot d_s(k(x_0)/k(x_1)) \cdot d_s(k(x_1)/k(x_1')) \\ &= d_s(k(x_1)/K) \cdot d_s(k(x_0)/k(x_1)) \cdot d_s(K/k(x_0)) \\ &= d_s(K/K) = 1. \end{aligned}$$

Similarly, we obtain $c_{d_s \times d_i}(\sigma) = (1,1)$.

Consider the valuation $\sigma(v_0)$ and v_1, which both restrict to the same valuation on $k(x_1')$. Hence by Theorem 3.6 from Chapter 1 there is a $\tau \in \mathrm{Aut}_{k(x_1')}(\Omega)$ such that $\tau\sigma(v_0) = v_1$. Notice that $c_{d_s \times d_i}(\tau) = (1,1)$ (since it fixes a transcendental). Hence $c_{d_s \times d_i}(\tau\sigma) = (1,1)$ as required. □

Lemma 6.4. *Let $L \supseteq K$ be a separable extension of function fields over a field k. Then there is a valuation of K which totally splits in L.*

Proof. We may assume that L/K is Galois. Let $z \in K$ be transcendental over k and let $R = \overline{k[z]}$, the integral closure of $k[z]$ in K. Take $f \in R[x]$ monic such that $L = K[x]/(f)$ (here we use that L/K is separable). Consider the integral extension $R[x]/(f) \supseteq R$. Consider the finite set $S \subset \mathcal{P}_{K/k}$ consisting of

- primes which ramify in L/K;
- primes above ∞ of $k(z)$;
- primes dividing the discriminant of f (here we use separability).

Take an element $h \in K$ which has poles in S such that $f(h) \in K$ has poles precisely at S (Lemma 2.24 from Chapter 2). Since the divisor of $f(h)$ has degree 0, there must exist a valuation $v \in P_{K/k}$, $v \notin S$, such that $v(f(h)) > 0$. Notice that $v(h) \geq 0$ by construction. Furthermore $\overline{f} \in k_v[x]$ is separable and has a simple zero $\overline{h}$. We conclude from Proposition 7.8 from Chapter 1 that v extends to a valuation w on L such that $k_w = k_v$. As $e(w/v) = f(w/v) = 1$, and the extension is Galois, the prime v totally splits (Theorem 3.6 from Chapter 1). □

Proposition 6.5. *Let K/k be a function field. Then the action of* $\mathrm{Aut}_k(K)$ *on $\mathcal{P}_{K/k}$ is faithful.*

PROOF. Suppose $\sigma \in \mathrm{Aut}_k(K)$ acts trivially on $\mathcal{P}_{K/k}$. Let k' be the integral closure of k in K.

Assume first that σ has finite order n. Suppose $n > 1$. Consider the finite Galois extension K/K^σ, which has a prime which totally splits according to Lemma 6.4. As $\langle\sigma\rangle$ acts transitively on the set of primes above this prime (Theorem 3.6 from Chapter 1), we conclude that σ does not act as the identity on $\mathcal{P}_{K/k}$, contradiction. Hence $n = 1$ and σ is the identity.

Assume that σ has infinite order and is the identity on k'. Then we may replace k by its integral closure and hence we may assume that K is geometrically irreducible. This implies that we have an injective map $\mathrm{Aut}_k(K) \to \mathrm{Aut}_{\overline{k}}(\overline{k}K)$. It is enough to show that any $\tau \in \mathrm{Aut}_{\overline{k}}(\overline{k}K)$ of infinite order has an infinite orbit under the action on $C(\overline{k})$ where C is the normal projective curve over $\overline{k}$ corresponding to $\overline{k}K$ (Proposition 2.11 from Chapter 2).

Assume that $g(C) = 0$. Then $C \cong \mathbf{P}^1$ with automorphism group $\mathrm{PGL}_2(\overline{k})$. Take an element $M \in \mathrm{PGL}_2(\overline{k})$ of infinite order. If M is diagonalizable, after scaling, we may assume that $M = \mathrm{diag}(1, r)$ where $r \in \overline{k}^*$ is not a root of unity. It is obvious that there are infinite orbits in this case. Otherwise, M is of the form

$$\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$$

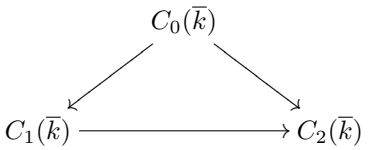
for some $r \in \overline{k}$. This has finite order, unless $\mathrm{char}(k) = 0$, and if $\mathrm{char}(k) = 0$, there are orbits of infinite length.

Assume that $g(C) = 1$. Then after the choice of a base point C is an elliptic curve. The automorphism group of the curve is $C(\overline{k}) \rtimes T$ where T is a finite group ([**Sil09**, Theorem 10.1]). Since we want to show that a morphism has infinite orbits, this reduces to the case where the morphism is a translation by a point. If this point has finite order, then the automorphism would have finite order. If the point has infinite order, then all orbits have infinite length.

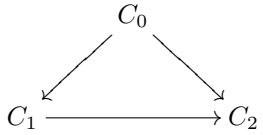
Assume that $g(C) \geq 2$. Then the automorphism group is finite ([**Sin74**]), and hence no elements of infinite order exist.

We will now do the general case. As k' is finite over k, there is an $n \in \mathbf{Z}_{\geq 1}$ such that σ^n is the identity on k'. From the above discussions, we conclude $\sigma^n = \mathrm{id}|_K$. Hence σ has finite order and the first part shows that σ is the identity. □

Proposition 6.6. *Let C_0, C_1, C_2 be normal projective curves over a field k. Suppose we have dominant morphisms $\varphi_1 \colon C_0 \to C_1$ and $\varphi_2 \colon C_0 \to C_2$ where $C_0 \to C_1$ is separable. Assume that we have a unique map of sets $C_1(\overline{k}) \to C_2(\overline{k})$ such that*



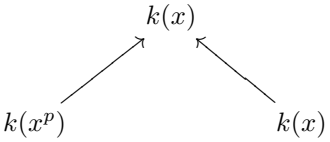
commutes. Then there is a unique dominant morphism of curves $C_1 \to C_2$ such that the diagram



commutes.

PROOF. We may assume that $C_0 \to C_1$ is Galois with group G. Then by assumptions for any $\sigma \in \mathrm{Aut}_{C_1}(C_0)$ the morphism $\varphi_2 \circ \sigma \colon C_0 \to C_2$ induces the same map $C_0(\overline{k}) \to C_2(\overline{k})$. From Proposition 2.4 from Chapter 2 we conclude that $\varphi_2 \circ \sigma = \varphi_2$ for any $\sigma \in \mathrm{Aut}_{C_1}(C_0)$. If we look at function field (Theorem 2.8 from Chapter 2), we conclude that $k(C_2) \subseteq k(C_0)^{\mathrm{Aut}_{k(C_1)}(k(C_0))} = k(C_1)$. This gives us the required morphism $C_1 \to C_2$. □

Remark 6.7. The assumption that φ_1 is separable, is needed. For example for $k = \mathbf{F}_p$, the diagram

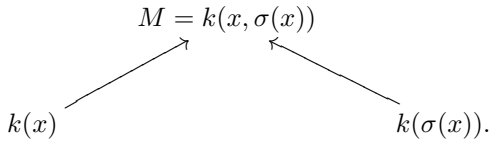


where x is transcendental over k and all the arrows are the natural inclusions, gives a counterexample.

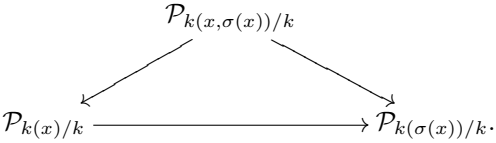
Theorem 6.8. *Let Ω be an algebraically closed field of characteristic $p \geq 0$. Let k be an algebraically closed subfield of Ω with $\mathrm{trdeg}_k(\Omega) = 1$. Then the kernel of the action of $\mathrm{Aut}(k \to \Omega)$ on $\mathcal{P}_{\Omega/k}$ is $\langle x \mapsto x^p \rangle$ if $p > 0$ and trivial if $p = 0$.*

PROOF. For simplicity, if $p = 0$, replace p by 1. It is obvious that $\mathrm{Aut}(k \to \Omega)$ acts on $\mathcal{P}_{\Omega/k}$ and that $\langle x \mapsto x^p \rangle$ is in the kernel.

Suppose $\sigma \in \mathrm{Aut}(k \to \Omega)$ acts trivially. We will show that $\sigma \in \langle x \mapsto x^p \rangle$. Let d be the inseparability degree. Then there exists a power τ of $x \mapsto x^p$ such that $d(\tau \circ \sigma) = 1$. Hence we assume that $d(\sigma) = 1$. Let $x \in \Omega$ be transcendental over k. Consider the following diagram of fields:

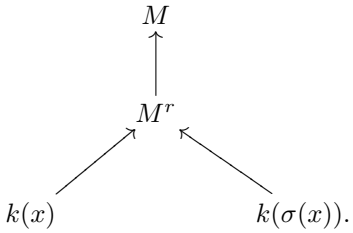


We first claim that there is a unique $\mathcal{P}_{k(x)/k} \to \mathcal{P}_{k(\sigma(x))/k}$ making the following diagram commute:



Indeed, take $f \in k[x]$ irreducible or $f = 1/x \in k[1/x]$. Then for a valuation $v \in \mathcal{P}_{\Omega/k}$ we have $v(f) > 0$ iff $v(\sigma(f)) > 0$. This shows that there is a unique map making the diagram commute.

By construction, the inseparability degree of $k(x, \sigma(x))/k(x)$ and the one of $k(x, \sigma(x))/k(\sigma(x))$ are the same, say that this degree is r. From Proposition 2.14 from Chapter 1, where we use that k is perfect, we conclude that we have a diagram



We apply Proposition 2.11 from Chapter 2 and Propostion 6.6 to obtain unique inclusions $k(x) \subseteq k(\sigma(x))$ and $k(\sigma(x)) \subseteq k(x)$. But this shows that $\sigma(x) = \frac{ax+b}{cx+d}$ for some $a, b, c, d \in k$ with $ad - bc \neq 0$. But if $\sigma(x) \neq x$, then σ does not act as the identity on $\mathcal{P}_{k(x)/k}$, and by Theorem 5.2 from Chapter 1 it does not act as the identity on $\mathcal{P}_{\Omega/k}$. □

Proof of Theorem 1.3. Follows directly from Proposition 6.3 and Theorem 6.8. □

Bibliography

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[AT09] Emil Artin and John Tate. *Class field theory*. AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original.

[Bir09] Peter Birkner. Efficient arithmetic on low-genus curves. *Technische Universiteit Eindhoven*, 2009. Phd thesis.

[BPS12] Nils Bruin, Bjorn Poonen, and Michael Stoll. Generalized explicit descent and its application to curves of genus 3. `http://arxiv.org/abs/1205.4456`, 2012. preprint.

[CAS67] *Algebraic number theory*. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich. Academic Press, London, 1967.

[CFA+06] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[Cor01] Gunther Cornelissen. Two-torsion in the Jacobian of hyperelliptic curves over finite fields. *Arch. Math. (Basel)*, 77(3):241–246, 2001.

[Efr06] Ido Efrat. *Valuations, orderings, and Milnor K-theory*, volume 124 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2006.

[End72] Otto Endler. *Valuation theory*. Springer-Verlag, New York, 1972. To the memory of Wolfgang Krull (26 August 1899–12 April 1971), Universitext.

[EP05] Antonio J. Engler and Alexander Prestel. *Valued fields*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005.

[FJ05] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 2005.

[HW79] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[Jar11] Moshe Jarden. *Algebraic patching*. Springer Monographs in Mathematics. Springer, Heidelberg, 2011.

[Kos13] Michiel Kosters. The subset sum problem for finite abelian groups. *J. Combin. Theory Ser. A*, 120(3):527–530, 2013.

[KS00] David R. Kohel and Igor E. Shparlinski. On exponential sums and group generators for elliptic curves over finite fields. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 395–404. Springer, Berlin, 2000.

[Kuh] Franz-Viktor Kuhlman. *Book on Valuation Theory (in preparation)*. `http://math.usask.ca/~fvk/Fvkbook.htm`.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[LW08] Jiyou Li and Daqing Wan. On the subset sum problem over finite fields. *Finite Fields Appl.*, 14(4):911–929, 2008.

[LW12] Jiyou Li and Daqing Wan. Counting subset sums of finite abelian groups. *J. Combin. Theory Ser. A*, 119(1):170–182, 2012.

[Mor96] Patrick Morandi. *Field and Galois theory*, volume 167 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[MST99] Volker Müller, Andreas Stein, and Christoph Thiel. Computing discrete logarithms in real quadratic congruence function fields of large genus. *Math. Comp.*, 68(226):807–822, 1999.

[MWW12] Gary L. Mullen, Daqing Wan, and Qiang Wang. Value sets of polynomial maps over finite fields. `http://arxiv.org/abs/1210.8119`, 2012. preprint.

[Poo93] Bjorn Poonen. Maximally complete fields. *Enseign. Math. (2)*, 39(1-2):87–106, 1993.

[Pop13] Florian Pop. Little survey on large fields. 2013.

[Ros02] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[RV99] Dinakar Ramakrishnan and Robert J. Valenza. *Fourier analysis on number fields*, volume 186 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.

[Sch77] A. Schinzel. Abelian binomials, power residues and exponential congruences. *Acta Arith.*, 32(3):245–274, 1977.

[Ser73] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[Ser02] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002. Translated from French to English by Patrick Ion and revised by the author.

[Sho90] Victor Shoup. New algorithms for finding irreducible polynomials over finite fields. *Math. Comp.*, 54(189):435–447, 1990.

[Shp96] Igor Shparlinski. On finding primitive roots in finite fields. *Theoret. Comput. Sci.*, 157(2):273–275, 1996.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Sin74] Balwant Singh. On the group of automorphisms of a function field of genus at least two. *J. Pure Appl. Algebra*, 4:205–229, 1974.

[Ste88] Peter Stevenhagen. Class groups and governing fields. *University of California, Berkeley*, 1988. Phd thesis.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[Tur95] Gerhard Turnwald. A new criterion for permutation polynomials. *Finite Fields Appl.*, 1(1):64–82, 1995.

[vdW06] Christiaan van de Woestijne. Deterministic equation solving over finite fields. *Universiteit Leiden*, 2006. Phd thesis.

Samenvatting

De Nederlandse vertaling van de titel van dit proefschrift is *Groepen en lichamen in de aritmetiek*. Bij het maken van een samenvatting van dit proefschrift heb ik de volgende keuze gemaakt. Om de samenvatting dicht bij de werkelijke inhoud van dit proefschrift te houden, heb ik besloten slechts een samenvatting te geven van Hoofdstuk 3, Hoofdstuk 4 en Hoofdstuk 7. Ik hoop hiermee toch een goede afspiegeling te kunnen geven van de inhoud van dit proefschrift zonder dat het te technisch wordt.

Hoofdstuk 3 en Hoofdstuk 4

6.1. Polynomen over R. De *reële getallen*, $\mathbf{R}$, zijn alle getallen op de getallenlijn waarbij alle gaten zijn opgevuld (de precieze definitie zal ik achterwege laten). Zo zijn $2, 0, -1/3, \sqrt{2}$ en π allemaal reële getallen. Zij f een *polynoom* met coëfficiënten in de reële getallen. Dit betekent dat we f kunnen schrijven als $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ voor een zekere n waarbij alle a_i reële getallen zijn. De *graad* van zo'n polynoom is de grootste i zodat a_i niet nul is. Een voorbeeld van een polynoom van graad 3 is $f = 3x^3 + x^2 - \sqrt{2}$. Stel dat we zo'n polynoom f hebben. Dan kunnen we een reëel getal r invullen in f en dan krijgen we weer een reëel getal, en dit noteren we met $f(r)$. Als $f = 3x^3 + x^2 - \sqrt{2}$, dan vinden we bijvoorbeeld $f(\sqrt{2}) = 3\sqrt{2}^3 + \sqrt{2}^2 - \sqrt{2} = 5\sqrt{2} + 2$. Dit geeft ons een *afbeelding* van $\mathbf{R}$ naar $\mathbf{R}$: aan een getal r uit $\mathbf{R}$ kennen we $f(r)$ toe. Het *beeld* van deze afbeelding zijn alle waardes $f(r)$ waarbij r loopt over $\mathbf{R}$.

In hoofdstuk 4 heb ik het volgende bewezen: als het beeld van zo'n afbeelding niet heel $\mathbf{R}$ is, dan zijn er oneindig veel reële getallen die niet in het beeld zitten. Het kan dus niet zo zijn dat het beeld slechts één punt mist. In het bovenstaande geval is het bewijs niet heel moeilijk. In mijn proefschrift heb ik een sterkere stelling bewezen die een dergelijke uitspraak geeft over polynomiale afbeeldingen over "perfecte grote lichamen". In het volgende stukje zal ik kort uitleggen wat een lichaam is.

6.2. Lichamen. Een *lichaam* is een verzameling K met twee bewerkingen $K \times K \to K$, die we voor $x, y \in K$ noteren met $x + y$ respectievelijk $x \cdot y$, en die voldoen aan de volgende eigenschappen:

i. er is een element 0 in K zodat voor alle x in K geldt $0 + x = x$;
ii. voor alle x, y in K geldt $x + y = y + x$;
iii. voor alle x in K bestaat er een y in K met $x + y = 0$;
iv. voor alle x, y, z in K geldt $(x + y) + z = x + (y + z)$;
v. er is een element 1 in K zodat voor alle x in K geldt $1 \cdot x = x$;
vi. voor alle x, y in K geldt $x \cdot y = y \cdot x$;

vii. voor alle x in K behalve 0 bestaat er een y in K met $x \cdot y = 1$;
viii. voor alle x, y, z in K geldt $x(y + z) = x \cdot y + x \cdot z$.

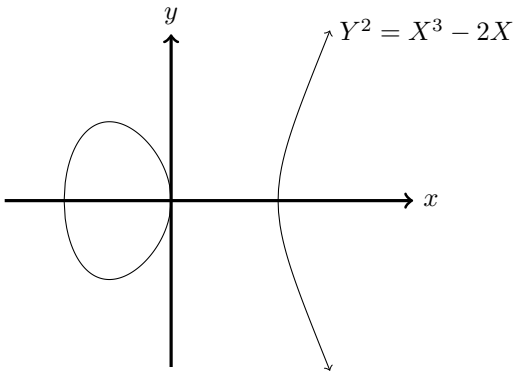
Ik hoop dat ik de lezer nu niet heb afgeschrikt. Het komt er op neer dat een lichaam een verzameling (een collectie dingen) is waar je kan optellen, aftrekken, vermenigvuldigen en door een niet nul-element kan delen. Zo vormen de reële getallen $\mathbf{R}$ een lichaam.

6.3. Polynomen over eindige lichamen. Er zijn oneindig veel reële getallen. Een lichaam waarvan de onderliggende verzameling eindig is, wordt een *eindig lichaam* genoemd. De reële getallen zijn dus geen eindig lichaam. Een voorbeeld van een eindig lichaam is $\mathbf{F}_2$, de verzameling die bestaat uit 0 en 1, met de volgende bewerkingen: $0 + 0 = 1 + 1 = 0$, $1 + 0 = 0 + 1 = 1$, $1 \cdot 1 = 1$ en $1 \cdot 0 = 0 \cdot 1 = 0 \cdot 0 = 0$.

Zij $\mathbf{F}$ een eindig lichaam. Dan kunnen we polynomen bekijken met coëfficiënten in $\mathbf{F}$. Zo'n polynoom geeft een afbeelding van $\mathbf{F}$ naar $\mathbf{F}$. In Hoofdstuk 4 heb ik het volgende bewezen: als het beeld onder zo'n polynomiale afbeelding niet heel $\mathbf{F}$ is en maar weinig punten mist, dan is de graad van het polynoom groot.

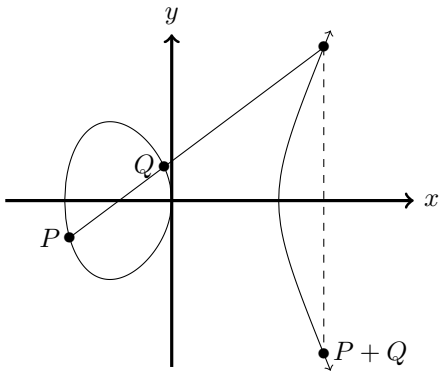
Hoofdstuk 7

Bekijk de vergelijking $Y^2 = X^3 - 2X$. We zoeken oplossingen in het platte vlak van deze vergelijking, dat wil zeggen, we zoeken reële getallen x, y die voldoen aan $y^2 = x^3 - 2x$. Bijvoorbeeld $x = y = 0$ is een oplossing, en dit punt noteren we als $(0, 0)$. Ook $(x, y) = (\sqrt{2}, 0)$ is een oplossing. Er zijn oneindig veel oplossingen voor deze vergelijking en je krijgt het volgende plaatje als je de oplossingen in het platte vlak tekent.



De kromme, de oplossing van de vergelijking in het vlak samen met een extra punt O, wordt een *elliptische kromme* genoemd. We noteren de kromme met E. De theorie van de elliptische krommen valt onder de *arithmetische meetkunde*. Het bijzondere is dat de elliptische kromme een *abelse groep* is als we een bepaalde bewerking beschouwen. Dat wil zeggen, aan elk tweetal punten P, Q van E kennen we een derde punt $P + Q$ op de kromme toe, en deze bewerking voldoet aan een aantal regels. Laat mij eerst de bewerking uitleggen. Stel dat we twee verschillende punten P en Q op de kromme hebben in het vlak. Dan moeten we $P + Q$, een derde punt op de kromme, definiëren. Het plaatje hieronder legt uit hoe dat werkt. Trek een lijn door P en Q. Neem aan dat de lijn de kromme in een derde punt in het vlak snijdt. Dan is $P + Q$ gedefinieerd

als de spiegeling van dit derde punt in de x-as. Als er niet zo'n derde punt is, dan zeggen we dat $P + Q = O$. Als we een punt P bij zichzelf optellen, dan trekken we de raaklijn aan P in plaats van de lijn door P en Q als hierboven en volgen we verder bovenstaande constructie. Verder definiëren we $P + O = O + P = P$ voor een punt P op de kromme.



Deze optelling voldoet aan de volgende regels voor P, Q, R in E:

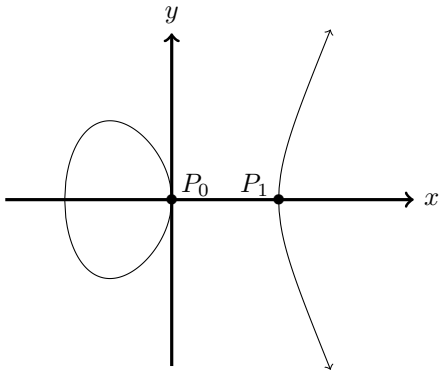
i. $P + Q = Q + P$;
ii. $(P + Q) + R = P + (Q + R)$;
iii. $P + O = O + P = P$;
iv. er bestaat een punt $-P$ op E met $P + (-P) = O$.

Het is niet moeilijk om in te zien dat aan i, iii en iv voldaan zijn. Inderdaad, i volgt uit de constructie. De lijn tussen P en Q is hetzelfde als de lijn tussen Q en P. Aan de derde eigenschap is per definitie voldaan. We gaan nu de vierde eigenschap bewijzen. Neem een punt P uit het vlak op de kromme, en spiegel dit punt in de x-as. Dan is het gevonden punt $-P$ en aan eigenschap iv is voldaan. Het is overigens niet eenvoudig om te laten zien dat aan eigenschap ii voldaan is (er is een andere aanpak die dat vrij direct geeft).

De regels hierboven zeggen precies dat E een *abelse groep* is met de bewerking die we hebben gedefinieerd. We schrijven overigens $P + (-Q)$ als $P - Q$ en we zeggen dat we Q van P aftrekken.

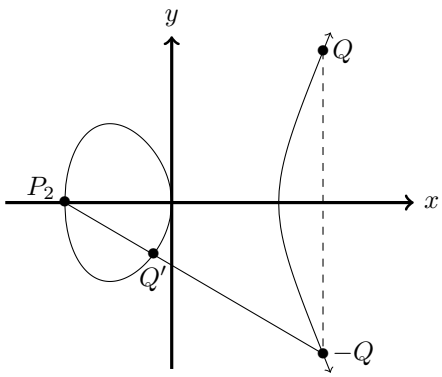
Beschouw de natuurlijke projectie van E zonder O op de x-as. Een punt (x, y) op de kromme in het vlak wordt naar het punt x gestuurd. Het probleem dat ik bestudeerd heb, in een net iets andere context, is het volgende. Neem een stuk (deelverzameling) van de x-as en bekijk alle punten op E waarvoor de x-coördinaat in deze verzameling valt. Is het zo dat we met behulp van optellen en aftrekken alle punten van E uit deze punten kunnen krijgen?

Ik geef twee voorbeelden. Bekijk eerst alle punten met x-coördinaat tussen 0 en $\sqrt{2}$, dat wil zeggen, in het gesloten interval $[0, \sqrt{2}]$. Het is niet heel moeilijk om in te zien dat we slechts twee punten vinden: $P_0 = (0, 0)$ en $P_1 = (\sqrt{2}, 0)$. In een plaatje ziet dit er als volgt uit.



We gaan nu kijken welke punten we allemaal kunnen maken. Merk op dat $P_1 + P_1 = P_0 + P_0 = O$, omdat zowel de raaklijn door P_0 als de raaklijn door P_1 verticaal is en geen derde snijpunt heeft met de kromme in het vlak. We vinden verder $P_0 + P_1 = (-\sqrt{2}, 0)$, het derde punt met y-coordinaat 0. We noemen dit punt P_2. Om eenzelfde reden is $P_0 + P_2 = P_1$ en $P_1 + P_2 = P_0$. Verder volgt uit bovenstaandat dat $-P_0 = P_0$, $-P_1 = P_1$ en $-P_2 = P_2$. We concluderen dat we alleen de punten O, P_0, P_1, P_2 krijgen (voor de wiskundigen: dit is de 2-torsie van de elliptische kromme).

Stel nu dat we beginnen met alle punten met x-coordinaat kleiner dan of gelijk aan 0. Dan beginnen we dus met de gesloten contour aan de linkerkant van onze plaatjes. We gaan nu bewijzen dat we elk punt van de kromme kunnen krijgen door optellen en aftrekken uit deze verzameling. Net als hierboven kunnen we $O = P_0 + P_0$ maken (een wiskundige zou zeggen dat we O al kunnen maken door de lege som te nemen). Neem nu een punt uit het vlak op de kromme buiten de contour, zeg Q. Spiegel dit punt in de x-as en krijg $-Q$. Trek dan de lijn door P_2 en $-Q$. We krijgen een derde snijpunt met de contour, zeg Q'. Maar dan geldt $P_2 + Q' = Q$. In een plaatje ziet dit er als volgt uit.



Kortom, we kunnen alle punten op de elliptische kromme maken op deze manier.

In dit proefschrift heb ik naar eenzelfde probleem gekeken voor elliptische krommes over eindige lichamen (ze worden ook gedefinieerd als de oplossingsverzameling van een vergelijking). Het grote verschil met het bovenstaande stuk is dat je eigenlijk

geen plaatjes meer kunt tekenen. Nog steeds vormen de punten van de kromme een abelse groep en hebben we een projectie op een x-as. Neem nu een stuk van de x-as. Dan kunnen we ons nog steeds afvragen of de punten met x-coördinaat in deze deelverzameling alle punten voortbrengen. Dit laatste is precies wat ik heb bestudeerd in Hoofdstuk 7.

Dankwoord

Ik wil graag mijn promotor Hendrik Lenstra bedanken voor de goede en inspirerende begeleiding. Ook wil ik de promotiecommissie bedanken voor hun werk.

Ik wil de medewerkers van het Mathematisch Insituut bedanken, met name van de afdeling algebra, getaltheorie en meetkunde. Ik heb van allen zeer veel geleerd en de goede sfeer op het instituut is mijn onderzoek zeker ten goede gekomen.

Zonder namen te noemen wil ik al mijn vrienden bedanken: de andere promovendi in mijn groep, mijn studievrienden, mijn Haagse vrienden van de Amberhorst en Kornalijnhorst, mijn klaverjasvrienden, mijn hardloopvrienden, mijn bordspellenvrienden en mijn pubquizvrienden.

Als laatste wil ik mijn familie bedanken.

Curriculum Vitae

Op 4 juni 1987 werd Michiel Kosters geboren in Leidschendam. In 2005 haalde hij cum laude zijn diploma aan het Christelijk Gymnasium Sorghvliet te Den Haag. Vanwege de goede examenresultaten kreeg hij de Diligentiaprijs voor natuurkunde, een prijs voor scheikunde en een prijs voor Latijn. In dat jaar begon hij met het studeren van wiskunde en natuurkunde aan de Universiteit Leiden. Hoewel hij in zijn eerste jaar winnaar was voor de aanmoedigingsprijs in de natuurkunde, besloot hij zich volledig te richten op de studie wiskunde. In 2008 haalde hij cum laude zijn bachelor wiskunde en vervolgens in 2010 cum laude zijn master wiskunde. Tijdens zijn studie won hij zowel de teamwedstrijden LIMO (Landelijke Interuniversitaire Mathematische Olympiade) als de PION (Project Interuniversitaire Oympiade Natuurkunde). Zijn masterscriptie werd begeleid door professor Hendrik Lenstra, die hem tijdens het schrijven een promotieplek op het Mathematisch Instituut van de Universiteit Leiden aanbood. In september 2010 begon hij met zijn promotieonderzoek bij professor Hendrik Lenstra waarvan dit proefschrift het resultaat is.

Na zijn promotie zal Michiel verder gaan als postdoctoraal onderzoeker aan de Nanyang Technological University in Singapore.

Index