Heidelberg University
Department of Mathematics

Master's Thesis

Birational Anabelian Geometry of Curves over Algebraically Closed Fields

Martin W. Lüdtke

Thesis Advisor: Prof. Dr. Alexander Schmidt
Co-Advisor: Dr. Armin Holschbach

March 2015

Abstract

The fundamental question in birational anabelian geometry is whether a field is determined up to isomorphism by its absolute Galois group, provided that the group is "sufficiently non-abelian". The Neukirch-Uchida theorem (for global fields) and Pop's theorem (for finitely generated infinite fields) are examples of known cases. In the 1990s, Bogomolov initiated a programme that aims to prove birational anabelian conjectures for function fields of varieties of dimension ≥ 2 over algebraically closed fields. While it is impossible to recover a one-dimensional function field L over k from its absolute Galois group alone, we prove that L can be functorially recovered from an associated pair (G, U), consisting of the absolute Galois group U of L and a topological group G containing U as an open subgroup. It is defined by choosing an algebraic closure $\overline{L}$ of L and setting $(G, U) = (\mathrm{Aut}(\overline{L}|k), \mathrm{Aut}(\overline{L}|L))$, with a suitable topology on G. We also show a closely related theorem asserting that the algebraically closed ground field k can be functorially recovered from $\mathrm{Aut}(F|k)$ where $F|k$ is an algebraically closed extension of transcendence degree one.

Zusammenfassung

In der birationalen anabelschen Geometrie geht es um die Frage, inwieweit ein Körper bis auf Isomorphie durch seine absolute Galoisgruppe bestimmt ist, vorausgesetzt die Gruppe ist „ausreichend nicht-abelsch“. Die Sätze von Neukirch-Uchida (für globale Körper) und Pop (für endlich erzeugte unendliche Körper) stellen Beispiele von Fällen dar, in denen die Aussage bekannt ist. In den 1990er-Jahren begann Bogomolov ein Programm, das den Beweis von birationalen anabelschen Vermutungen für Funktionenkörper von Varietäten der Dimension ≥ 2 über algebraisch abgeschlossenen Körpern zum Ziel hat. Während es unmöglich ist, einen eindimensionalen Funktionenkörper L über k aus seiner absoluten Galoisgruppe alleine zurückzugewinnen, zeigen wir, dass L funktoriell aus einem zugeordneten Paar (G, U), bestehend aus der absoluten Galoisgruppe U von L und einer topologischen Gruppe G, welche U als offene Untergruppe enthält, rekonstruiert werden kann. Zur Definition dieses Paares wähle man einen algebraischen Abschluss $\overline{L}$ von L und setze $(G, U) = (\mathrm{Aut}(\overline{L}|k), \mathrm{Aut}(\overline{L}|L))$ mit einer geeigneten Topologie auf G. In diesem Zusammenhang beweisen wir auch die Aussage, dass der algebraisch abgeschlossene Grundkörper k funktoriell aus der Gruppe $\mathrm{Aut}(F|k)$ zurückgewonnen werden kann, wobei F einen algebraisch abgeschlossenen Erweiterungskörper vom Transzendenzgrad eins über k bezeichne.

Contents

1 Introduction

In anabelian geometry, one tries to recover information about a variety X from its étale fundamental group $\pi_1(X)$. It was conjectured by Grothendieck in his letter to Faltings [Gro97], that certain varieties are completely determined up to isomorphism by their étale fundamental group, as long as the involved fundamental groups are "sufficiently non-abelian", hence the term **anabelian geometry**. It is usually easier to prove birational versions of such statements. There one essentially replaces the variety X with its generic point $\operatorname{Spec} K(X)$, where $K(X)$ is the function field of X. The étale fundamental group $\pi_1(\operatorname{Spec} K(X))$ equals the absolute Galois group $\operatorname{Gal}(K(X)^{\mathrm{sep}}|K(X))$, with the choice of separable closure $K(X) \hookrightarrow K(X)^{\mathrm{sep}}$ corresponding to a "base point" of $\operatorname{Spec} K(X)$. The question then becomes:

> Can a field K be recovered (up to isomorphism) from its absolute Galois group?

This is false in general; for example, all finite fields have an absolute Galois group isomorphic to $\hat{\mathbb{Z}}$. On the other hand, there is the celebrated Neukirch-Uchida theorem (and its generalisation by Pop to finitely generated infinite fields [Pop00]), which states that global fields are functorially determined up to isomorphism by their absolute Galois groups ([NSW08], XII.2). Bogomolov [Bog91] conjectured that a similar result holds for function fields of varieties over algebraically closed fields, as long as the dimension is at least 2. ([Pop12a] proves such a result in the case that the base field is an algebraic closure of a finite field.) In dimension one, however, i. e. if X is a curve over an algebraically closed field k, Pop [Pop95] and Harbater [Har95] showed that the absolute Galois group of $K(X)$ is profinite free of rank the cardinality $|k|$ of the base field, so it contains no information whatsoever about X other than $|k|$. As a remedy for this situation, we prove in this thesis that X can be recovered up to birational equivalence from the pair (G, U), where

- $\overline{K(X)}$ is an algebraic closure of $K(X)$;
- $G = \mathrm{Aut}(\overline{K(X)}|k)$ is the group of field automorphisms of $\overline{K(X)}$ fixing k, endowed with the topology defined in section 2;
- $U = \mathrm{Aut}(\overline{K(X)}|K(X))$ is the open subgroup of G fixing $K(X)$.

Note that U is isomorphic to the absolute Galois group of $K(X)$ via the restriction

$$\mathrm{Aut}(\overline{K(X)}|K(X)) \to \mathrm{Gal}(K(X)^{\mathrm{sep}}|K(X)).$$

The precise statement we are going to prove is the following:

Theorem A. *Let k be an algebraically closed field, let $L|k$ be a one-dimensional function field with algebraic closure $F = \overline{L}$ and absolute Galois group $U = \mathrm{Aut}(F|L)$, and put $G = \mathrm{Aut}(F|k)$. If (k', L', F', G', U') is another such quintuple, then the natural map*

$$\mathrm{Isom}(F'|L'|k', F|L|k) \longrightarrow \mathrm{Isom}((G, U), (G', U'))$$

is a bijection.

By an isomorphism between two pairs (G, U) and (G', U'), each consisting of a topological group and an open subgroup, we mean an isomorphism of topological groups $G \cong G'$ which restricts to an isomorphism $U \cong U'$. As for the left hand side, an isomorphism between field towers $F'|L'|k'$ and $F|L|k$ is an isomorphism $F' \cong F$ that restricts to isomorphisms $L' \cong L$ and $k' \cong k$. The "natural map" in the theorem assigns to such an isomorphism σ the isomorphism $\sigma^* \in \mathrm{Isom}((G, U), (G', U'))$, given by

$$\sigma^*(\tau) = \sigma^{-1} \circ \tau \circ \sigma.$$

Theorem A can also be stated in a "base-point-free" way, following the idea that the absolute Galois group of a field is in a sense "determined up to conjugation" by the field alone, without the choice of an embedding into a separable closure. Define an **inner automorphism** of a pair (G, U) to be an automorphism which is given by conjugation with an element of U. The set of **outer isomorphisms** $\mathrm{OutIsom}((G, U), (G', U'))$ is defined as $\mathrm{Isom}((G, U), (G', U'))$ modulo the action of U' by post-composition with inner automorphisms. Given an isomorphism $\sigma : L'|k' \xrightarrow{\sim} L|k$, it extends non-canonically to $\tilde{\sigma} : F'|L'|k' \xrightarrow{\sim} F|L|k$, inducing $\tilde{\sigma}^* \in \mathrm{Isom}((G, U), (G', U'))$. The point is that any two extensions of σ differ only by pre-composition with an automorphism of $F'|L'$, thus inducing the same *outer* isomorphism $(G, U) \cong (G', U')$. We can therefore state the following variant of theorem A.

Theorem A′. *In the situation of theorem A, the natural map*

$$\mathrm{Isom}(L'|k', L|k) \longrightarrow \mathrm{OutIsom}((G,U),(G',U'))$$

is a bijection.

One notes that the bijection in theorem A is naturally an isomorphism of U'-sets and theorem A′ follows by simply modding out the U'-action on both sides.

Instead of proving theorem A directly, we will prove a related theorem that rather than focusing on a single one-dimensional function field over k, considers "all at once" by embedding them in a common algebraic closure F. The precise statement is the following:

Theorem B. *Let k be an algebraically closed field, let $F|k$ be an algebraically closed extension of transcendence degree one and let $G = \mathrm{Aut}(F|k)$ be the automorphism group with the topology defined in section 2. If (k', F', G') is another such triple, then the natural map*

$$\mathrm{Isom}^i(F'|k', F|k) \longrightarrow \mathrm{Isom}(G, G')$$

is a bijection.

Here, Isom^i means isomorphisms up to a power of the Frobenius in positive characteristic. More precisely, it means $\mathrm{Isom}(F'|k', F|k)$ modulo the equivalence relation that identifies σ_1 and σ_2 if $\mathrm{char}(k) = \mathrm{char}(k') = p > 0$ and $\sigma_2 = \sigma_1 \circ \mathrm{Frob}^n$ for some $n \in \mathbb{Z}$, where $\mathrm{Frob} \in \mathrm{Isom}(F'|k', F'|k')$ is the Frobenius automorphism $\mathrm{Frob}(x) = x^p$.

Theorem B says that the ground field k can be recovered from the topological group G, so it can be viewed as a Galois characterisation of k, with $G = \mathrm{Aut}(F|k)$ playing the role of an absolute Galois group of k. There is also a base-point-free version asserting the bijectivity of the natural map

$$\mathrm{Isom}^i(k', k) \longrightarrow \mathrm{OutIsom}(G, G'),$$

where the right hand sind consists of isomorphisms $G \cong G'$ modulo inner automorphisms of G'. In the special case $k = k'$ we obtain an isomorphism

$$\mathrm{Aut}^i(k) \cong \mathrm{Out}(G),$$

where $\mathrm{Aut}^i(k) = \mathrm{Aut}(k)$ in characteristic zero and $\mathrm{Aut}^i(k) = \mathrm{Aut}(k)/\langle \mathrm{Frob} \rangle$ in positive characteristic.

Outline of Proof

The rest of the thesis is concerned with the proof of theorem B, with the implication B ⇒ A proved at the end of section 2.

The difficult part is the surjectivity, so we start with an isomorphism of topological groups $\lambda : G \xrightarrow{\sim} G'$ and proceed in several steps to recover an isomorphism of field extensions $F'|k' \xrightarrow{\sim} F|k$ that induces λ.

Step 1: Detection of Function Fields. In section 2 we prove a generalised Galois correspondence for field extensions of finite transcendence degree, which implies that the one-dimensional function fields in $F|k$ correspond in G to the compact open subgroups. More precisely, to every one-dimensional function field $L|k$ in F there is an associated compact open subgroup $U_L := \mathrm{Aut}(F|L)$ in G, and L is determined by U_L up to "purely inseparable equivalence" (definition 2.2). Moreover, we show in section 4 that there is a group-theoretic criterion in terms of (G, U_L) to decide if the function field L is rational, i. e. isomorphic to $k(x)$.

Step 2: Local Theory. Following a common strategy in birational anabelian geometry, we prove a group-theoretic characterisation of decomposition subgroups. Given a function field L in $F|k$ with complete nonsingular model C, we have for every point on C an associated decomposition subgroup in $\mathrm{Gal}(L^{\mathrm{ab},\ell}|L) \cong U_L^{\mathrm{ab},\ell}$, where ℓ is a prime not equal to the characteristic of k, $L^{\mathrm{ab},\ell}$ is the maximal pro-ℓ abelian extension of L and $U_L^{\mathrm{ab},\ell}$ is the maximal pro-ℓ abelian quotient of U_L. The local theory entails the proof that for a pair (L, L') of function fields with $\lambda^{-1}(U_{L'}) = U_L$, the induced isomorphism

$$\lambda^{\mathrm{ab},\ell} : U_L^{\mathrm{ab},\ell} \xrightarrow{\sim} U_{L'}^{\mathrm{ab},\ell}$$

maps decomposition subgroups isomorphically to decomposition subgroups, thereby inducing a bijection $\lambda^* : C' \xrightarrow{\sim} C$ between complete nonsingular models. This is first done for rational function fields in section 7, by reducing the task to a group-theoretic characterisation of the stabiliser subgroups for the action of $\mathrm{PGL}(2, k)$ on $\mathbb{P}^1$ by Möbius transformations; then the general case is treated in section 8.

Step 3: Global Theory. In section 9, we use the local information from the previous step to reconstruct a field isomorphism $F'|k' \xrightarrow{\sim} F|k$ inducing λ. To this end, we show that for every pair (L, L') as above, the isomorphism of divisor groups

$$\lambda^* : \mathrm{Div}(C') \xrightarrow{\sim} \mathrm{Div}(C)$$

maps principal divisors to principal divisors, thus inducing an isomorphism

$$\lambda^* : L'^{\times}/k'^{\times} \xrightarrow{\sim} L^{\times}/k^{\times}.$$

Viewing both sides as projective spaces, this isomorphism is shown to be a collineation and the fundamental theorem of projective geometry implies that λ^* is induced by an isomorphism of field extensions $L'|k' \xrightarrow{\sim} L|k$. One then shows that they can be glued together to obtain the desired isomorphism $F'|k' \xrightarrow{\sim} F|k$.

Apart from the mentioned sections there are section 3, which summarises the theory of algebraic curves that is needed later, specifically invertible sheaves and linear systems; section 5 in which we recall Kummer theory; and section 6 which gives an alternative description of decomposition subgroups for function fields of curves in terms of "delta functions" and shows how decomposition subgroups behave with respect to morphisms between curves.

Originality

Some comments are in order as to which parts of this thesis are original and which are to be attributed to other authors. Basically, the thesis is an expanded version of the 2001 article "On certain isomorphisms between absolute Galois groups" by M. Rovinsky [Rov03]. Apart from many details that had to be filled in, the main differences are the following:

- Rovinsky considers only fields of characteristic zero, while we treat the case of arbitrary characteristic. This makes it necessary to work with maximal pro-ℓ abelian quotients $U_L^{\mathrm{ab},\ell}$ instead of the full abelian quotients U_L^{ab}, and to always account for the indeterminacy arising from the phenomenon that purely inseparable extensions are not reflected in Galois groups. Only at one point (the reconstruction of ramification indices in lemma 9.3), an argument that works in characteristic zero breaks down and had to be replaced with a genuinely different argument to include the case of positive characteristic.

- Rather than working with two triples (k, F, G) and (k', F', G') and considering isomorphisms $G \xrightarrow{\sim} G'$, Rovinsky works with only one triple (k, F, G) and considers automorphisms of G. This restriction, however, seems unnecessary as everything works just as well with two triples.

- The group-theoretic characterisation of stabiliser subgroups in $\mathrm{Aut}(\mathbb{P}^1)$ requires a little more work than Rovinsky suggests, since he uses the notion of "parabolic subgroups" but this requires the language of algebraic groups which is not available in the context. A purely group-theoretic criterion (lemma 7.4) was suggested to me by A. Holschbach.

- The global theory (section 9) is treated differently here compared to Rovinsky's article. In order to recover a function field $L|k$ from its absolute Galois group U_L, he constructs a complete nonsingular model C from group-theoretic data, taking decomposition groups as closed points and recovering a scheme structure via an embedding of C as a closed subset into a projective space over k. However, the construction involves some non-canonical choices and it is not entirely clear how to make the choices compatible with morphisms between curves. Our approach, as sketched above, uses the same ingredients, namely linear systems and the fundamental theorem of projective geometry, but avoids any non-canonical choices. The idea to recover a field isomorphism $L'|k' \xrightarrow{\sim} L|k$ from a group isomorphism

  $$L'^{\times}/k'^{\times} \xrightarrow{\sim} L^{\times}/k^{\times}$$

  which is also a collineation of projective spaces, seems to be a standard method in birational anabelian geometry (see e. g. [Pop12b], [BT08]).

Finally, I wish to thank my advisor A. Schmidt and my co-advisor A. Holschbach for suggesting this topic to me, and for taking the time to discuss numerous technical questions.

2 A Galois-Type Correspondence for Transcendental Field Extensions

In this section we prove an analogue of the classical Galois correspondence for the case of transcendental field extensions. We consider an arbitrary ground field k and an algebraically closed field extension $F|k$ of finite transcendence degree. This situation is somewhat more general than necessary, since we eventually apply the theorem only in the case where the ground field k is also algebraically closed and the transcendence degree of $F|k$ is one. We denote by $G = \operatorname{Aut}(F|k)$ the group of field automorphisms of F that act trivially on k. Generalising the Krull topology, we consider the topology on G where the cosets $\sigma \operatorname{Aut}(F|L)$ for L a finitely generated subextension of $F|k$, form a basis of open neighbourhoods of $\sigma \in G$. Equivalently, G is endowed with the coarsest topology for which the action $G \times F \to F$ is continuous, F being equipped with the discrete topology.

Definition 2.1. For $L|k$ a finitely generated subextension of $F|k$, we define

$$U_L := \operatorname{Aut}(F|L).$$

Thus, the sets U_L form a basis of open neighbourhoods of the identity in G.

This topology was introduced in [PŠŠ66], where the authors also prove one part of the Galois-type correspondence (section 3, lemma 1). Rovinsky's article [Rov03] contains a statement (without proof) of the Galois-type correspondence, but our theorem 2.5 is more general in that it holds in arbitrary characteristic. (Rovinsky also assumes that the ground field k be algebraically closed and that the transcendence degree of $F|k$ be ≥ 1, but both is unnecessary.) In order to accomodate the case of positive characteristic, one has to deal with the phenomenon that purely inseparable extensions are not reflected in field automorphism groups. We therefore consider an equivalence relation on the set of subfields of $F|k$, which we call purely inseparable equivalence.

Definition 2.2. For a subfield K in $F|k$, its **purely inseparable closure** in F consists of all elements in F that are purely inseparable over K. If $\operatorname{char} k = p > 0$, then it is given by

$$K^i = K^{p^{-\infty}} = \left\{ x \in F : x^{p^n} \in K \text{ for some } n \in \mathbb{N} \right\}.$$

We call two subfields K_1, K_2 in $F|k$ **purely inseparably equivalent** if $K_1^i = K_2^i$.

While every algebraic field extension can be factored into a separable extension (namely the relative separable closure) followed by a purely inseparable extension, it is in general not possible to find a factorisation into a purely inseparable extension followed by a separable extension. However, if K is a subfield in $F|k$ such that $F|K$ is algebraic, then the fact that $F|K$ is normal implies that $F|K^i$ is separable ([Lan02], V.6.11).

Proposition 2.3. *The group G with the topology defined above is a Hausdorff, locally compact and totally disconnected topological group.*

Proof. Denote the multiplication and inversion in G by

$$\mu : G \times G \longrightarrow G, \quad \iota : G \longrightarrow G.$$

If $\sigma\tau = \rho$ and ρU_L is a basic open neighbourhood of ρ, then $\sigma U_{\tau L} \times \tau U_L \subseteq G \times G$ is an open neighbourhood of (σ, τ) contained in $\mu^{-1}(\rho U_L)$. Thus, μ is continuous. This implies in particular that the left ($\tau \mapsto \sigma\tau$) and right translations ($\tau \mapsto \tau\sigma$, for fixed $\sigma \in G$) are homeomorphisms on G. The continuity of ι now follows from $\iota^{-1}(\sigma U_L) = U_L \sigma^{-1}$.

G is Hausdorff: Suppose $\sigma, \tau \in G$ and $\sigma \neq \tau$. If $x \in F$ with $\sigma(x) \neq \tau(x)$, then σ and τ lie in different cosets of $U_{k(x)}$.

G is totally disconnected: In any topological group, the open subgroups and their cosets are also closed. If $\sigma, \tau \in G$ lie in different cosets of U_L, then σU_L and τU_L are open and closed sets separating the two elements. Therefore, no connected subset of G can contain two distinct elements.

G is locally compact: It suffices to show that every basic open neighbourhood U_L of the identity contains a compact neighbourhood. Let $x_1, \ldots, x_n$ be a transcendence basis (finite by assumption) of $F|L$, and put $M = L(x_1, \ldots, x_n)$. Then $F|M$ is algebraic, M is still finitely generated over k and we have $U_M \subseteq U_L$. The extension $F|M^i$ is Galois, we have $U_M = \mathrm{Gal}(F|M^i)$, and the induced topology on $U_M = \mathrm{Gal}(F|M^i)$ is the usual Krull topology which makes U_M a profinite and hence compact group. □

Lemma 2.4. *Let K_1, K_2 be subextensions of $F|k$ and let $\varphi : K_1 \xrightarrow{\sim} K_2$ be an isomorphism of fields over k. Then φ extends to an automorphism $\sigma \in G$ of F.*

$$\begin{tikzcd}
F \arrow[rr, dashed, "\sim", "\sigma"'] \arrow[d, dash] & & F \arrow[d, dash] \\
K_1 \arrow[rr, "\sim", "\varphi"'] \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\
& k &
\end{tikzcd}$$

Proof. Let X_i be a transcendence basis of $F|K_i$. The transcendence degrees are equal, so there exists a bijection between X_1 and X_2, by which we can extend φ to an isomorphism $\tilde{\varphi} : K_1(X_1) \xrightarrow{\sim} K_2(X_2)$. If $\iota_i : K_i(X_i) \hookrightarrow F$ denotes the canonical inclusion, then ι_1 and $\iota_2 \circ \tilde{\varphi}$ are two inclusions of $K_1(X_1)$ into its algebraic closure F. By basic field theory, they are conjugate under an automorphism of F, i. e. there exists $\sigma \in G$ with $\sigma \circ \iota_1 = \iota_2 \circ \tilde{\varphi}$. This is the desired extension of φ to F. □

Since in characteristic $p > 0$ the Frobenius map $x \mapsto x^p$ is injective, the image of $x \in F$ under an automorphism is uniquely determined by the image of x^{p^n}, for any $n \in \mathbb{N}_0$, hence we have $\mathrm{Aut}(F|K) = \mathrm{Aut}(F|K^i)$ for all subfields K in $F|k$. The automorphism group G is therefore "blind" towards purely inseparable extensions in the sense that purely inseparably equivalent subfields K_1 and K_2 satisfy $\mathrm{Aut}(F|K_1) = \mathrm{Aut}(F|K_2)$. However, the following Galois-type correspondence theorem shows that a subfield K of $F|k$ can be recovered from $\mathrm{Aut}(F|K)$ up to purely inseparable equivalence.

Theorem 2.5 (Galois-Type Correspondence)**.** *Let $F|k$ be an algebraically closed field extension of finite transcendence degree. Then the map $K \mapsto \operatorname{Aut}(F|K)$ is injective up to purely inseparable equivalence and induces bijections as follows:*

$$\begin{tikzcd}
\left\{\begin{array}{c}\textit{subfields } K \textit{ in } F|k\textit{, up to}\\ \textit{purely inseparable}\\ \textit{equivalence}\end{array}\right\} \arrow[r, hook] & \{\ \textit{closed subgroups of } G\ \} \\
\rotatebox{90}{$\subseteq$} & \rotatebox{90}{$\subseteq$} \\
\left\{\begin{array}{c}\textit{subfields } K \textit{ in } F|k \textit{ with}\\ \overline{K} = F\textit{, up to purely}\\ \textit{inseparable equivalence}\end{array}\right\} \arrow[r, "\sim"] & \{\ \textit{compact subgroups of } G\ \} \\
\rotatebox{90}{$\subseteq$} & \rotatebox{90}{$\subseteq$} \\
\left\{\begin{array}{c}\textit{finitely generated subfields}\\ K \textit{ in } F|k \textit{ with } \overline{K} = F\textit{, up}\\ \textit{to purely inseparable}\\ \textit{equivalence}\end{array}\right\} \arrow[r, "\sim"] & \left\{\begin{array}{c}\textit{compact open subgroups}\\ \textit{of } G\end{array}\right\}
\end{tikzcd}$$

We have $F^{\operatorname{Aut}(F|K)} = K^i$ for all subfields K of $F|k$.

Proof. For an arbitrary subextension K of $F|k$, we prove $F^{\operatorname{Aut}(F|K)} = K^i$. The inclusion $(\supseteq)$ is trivial. If $x \in F$, but $x \notin K^i$, there exists some $x' \in F \setminus \{x\}$ and an isomorphism $K(x) \cong K(x')$ over K, sending x to x'; take for example $x' = x + 1$ if x is transcendental over K, and any root $x' \neq x$ of the (not purely inseparable) minimal polynomial of x over K if x is algebraic over K. By lemma 2.4, the isomorphism $K(x) \cong K(x')$ extends to an automorphism σ of F. We have $\sigma \in \operatorname{Aut}(F|K)$, but $\sigma(x) \neq x$, therefore $x \notin F^{\operatorname{Aut}(F|K)}$.

The equality $F^{\operatorname{Aut}(F|K)} = K^i$ proves that $K \mapsto \operatorname{Aut}(F|K)$ is injective up to purely inseparable equivalence and that $H \mapsto F^H$ is a left-sided inverse. It is also clear that $\operatorname{Aut}(F|K) = \bigcap_{x \in K} U_{k(x)}$ is always a closed subgroup of G, that $\operatorname{Aut}(F|K) = \operatorname{Gal}(F|K^i)$ is compact if $\overline{K} = F$, and compact open if in addition K is finitely generated over k.

Let H be a compact subgroup of F. We will show that $F|F^H$ is algebraic and $\operatorname{Aut}(F|F^H) = H$. For $x \in F$, the group $U_{k(x)} \cap H$ is an open subgroup of the compact group H, hence it has finite index. If $\sigma_1, \ldots, \sigma_n \in H$ are representatives of the left cosets, then the H-orbit of x is the finite set $Hx = \{\sigma_1(x), \ldots, \sigma_n(x)\}$. The coefficients of the polynomial $f(X) = \prod_{i=1}^n (X - \sigma_i(x))$ are symmetric polynomials in the $\sigma_i(x)$ and are thus fixed by H. Therefore, x is algebraic over F^H. Since F^H is closed under purely inseparable extensions, $F|F^H$ is a Galois extension. Now H is a closed subgroup of $\operatorname{Gal}(F|F^H)$ and has the same fixed field $F^H = F^{\operatorname{Aut}(F|F^H)}$, therefore we conclude $H = \operatorname{Aut}(F|H)$ by classical Galois theory. This establishes the middle bijection.

It remains to show that if $H \leq G$ is a compact open subgroup, then there exists a finitely generated subfield K in $F|k$ with $H = \operatorname{Aut}(F|K)$. Since the sets U_L with $L|k$ finitely generated form a neighbourhood basis of the identity, there exists such an L with $U_L \subseteq H$. Looking at the fixed fields, we have $F^H \subseteq L^i$. Let T be a transcendence basis of $F^H|k$, which after raising to a p^n-th power if necessary, can be chosen to be contained in

L. Since H is compact, $F|F^H$ and thus $F|k(T)$ are algebraic extensions. Then $L|k(T)$ is algebraic and finitely generated, hence finite. The subextension $K := F^H \cap L$ is then also finite over $k(T)$, thus finitely generated over k. Moreover, since $F^H \subseteq L^i$, the extension $F^H|K$ is purely inseparable, so we have $\mathrm{Aut}(F|K) = \mathrm{Aut}(F|F^H) = H$. □

Remarks.

(a) The association $K \mapsto \mathrm{Aut}(F|K)$ is compatible with the G-actions in the sense that

$$\mathrm{Aut}(F|\sigma K) = \sigma\,\mathrm{Aut}(F|K)\sigma^{-1} \tag{2.1}$$

for all subextensions K of $F|k$ and all $\sigma \in G$. Moreover, the G-action on the set of subextensions of $F|k$ is compatible with purely inseparable equivalence since $\sigma(K)^i = \sigma(K^i)$.

(b) The Galois correspondence is inclusion-reversing in the sense that

$$K_1^i \subseteq K_2^i \;\Leftrightarrow\; \mathrm{Aut}(F|K_2) \subseteq \mathrm{Aut}(F|K_1)$$

for all subfields K_1 and K_2 of $F|k$.

(c) If $K_1 \subseteq K_2$ is an algebraic extension of subfields of $F|k$, then the left cosets of $\mathrm{Aut}(F|K_2) \subseteq \mathrm{Aut}(F|K_1)$ are in bijection with the K_1-embeddings $K_2 \hookrightarrow \overline{K_1}$, therefore the index $(\mathrm{Aut}(F|K_1) : \mathrm{Aut}(F|K_2))$ equals the degree of separability $[K_2 : K_1]_s$.

(d) In general, there exist closed subgroups of G that do not arise as $\mathrm{Aut}(F|K)$ for some subfield K of $F|k$. A subgroup $H \leq G$ arises in this way if and only if $\mathrm{Aut}(F|F^H) = H$. However, we have for example the closed subgroup $G^\circ \subseteq G$ which is generated by all the compact open subgroups U_L with $L|k$ finitely generated, whose fixed field is k, but one can show that G° is a proper subgroup of G unless $F|k$ is algebraic.

Now let us apply the Galois-type correspondence to the situation we are interested in, i. e. k algebraically closed and $F|k$ of transcendence degree one. We use the term **function field in** F to refer to a finitely generated subextension of $F|k$ of transcendence degree one. The Galois-type correspondence shows that the function fields $L|k$ in F are encoded in G via the compact open subgroups U_L, at least up to purely inseparable equivalence.

Corollary 2.6. *Let k be an algebraically closed field, $F|k$ algebraically closed of transcendence degree one and $G = \mathrm{Aut}(F|k)$. Let (k', F', G') be another such triple and let $\lambda : G \xrightarrow{\sim} G'$ be an isomorphism of topological groups. Then λ induces a bijection*

$$\left\{\begin{array}{c}\textit{function fields } L'|k' \textit{ in } F',\\ \textit{up to purely inseparable}\\ \textit{equivalence}\end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{c}\textit{function fields } L|k \textit{ in } F,\\ \textit{up to purely inseparable}\\ \textit{equivalence}\end{array}\right\}$$

given by $L' \mapsto L$ whenever $\lambda^{-1}(U_{L'}) = U_L$.

Proof. The sets are in bijection with the compact open subgroups of G and G', respectively. □

The following proposition gives an explicit description of purely inseparable equivalence for one-dimensional function fields.

Proposition 2.7. *Let k be an algebraically closed ground field of characteristic $p > 0$, let $F|k$ be an algebraically closed extension and let $L|k$ be a finitely generated subextension of transcendence degree 1. Then for each $n \in \mathbb{N}_0$, the extension $L^{p^{-n}}|L$, obtained by adjoining the p^n-th roots of all elements in L, is the unique purely inseparable extension of L in F of degree p^n. Moreover, the finitely generated subextensions of $F|k$ which are purely inseparably equivalent to L are precisely those of the form L^{p^n} with $n \in \mathbb{Z}$. In particular, they form an infinite field tower*

$$\ldots \subset L^{p^2} \subset L^p \subset L \subset L^{p^{-1}} \subset L^{p^{-2}} \subset \ldots.$$

Proof. Let $x \in L \setminus k$ be a transcendence basis, so that $L|k(x)$ is finitely generated and algebraic, hence finite. Consider the following field diagram:

$$\begin{tikzcd}
 & L^{p^{-n}} \\
k(x)^{p^{-n}} \arrow[ur, dash] & \\
 & L \arrow[uu, dash] \\
k(x) \arrow[uu, dash] \arrow[ur, dash] &
\end{tikzcd}$$

We have $[L^{p^{-n}} : k(x)^{p^{-n}}] = [L : k(x)]$ since the two extensions are isomorphic under the n-th power of the Frobenius automorphism. Moreover, since k is algebraically closed, we have $k(x)^{p^{-n}} = k(x^{p^{-n}})$ which is a simple extension of degree p^n over $k(x)$. Thus we see from the field diagram that $[L^{p^{-n}} : L] = p^n$.

If $M|L$ is another purely inseparable extension of degree p^n, we have $x^{p^n} \in L$ for all $x \in M$, thus $M \subseteq L^{p^{-n}}$. By comparing degrees, the last inclusion is in fact an equality, hence $M = L^{p^{-n}}$.

Clearly, the fields of the form $L^{p^{-n}}$ with $n \in \mathbb{Z}$ are finitely generated over k and purely inseparably equivalent to L. For the converse, let $M|k$ be finitely generated with $M^i = L^i$. Then for every element $x \in M$ there exists $n \in \mathbb{N}$ with $x^{p^n} \in L$. Since M is finitely generated we find a single $n \in \mathbb{N}$ that works for all x, hence $M^{p^n} \subseteq L$. Similarly, for each $y \in L$, there exists $m \in \mathbb{N}$ such that $y^{p^m} \in M^{p^n}$. Therefore, L is purely inseparable over M^{p^n}. Since M^{p^n} is finitely generated over k and of transcendence degree 1, there exists $m \in \mathbb{N}_0$ such that $L = (M^{p^n})^{p^{-m}} = M^{p^{n-m}}$, hence $M = L^{p^{m-n}}$. □

Now we show how the main result A follows from theorem B. In the situation of theorem A, we have an isomorphism $\lambda : (G, U) \xrightarrow{\sim} (G', U')$ and prove that it is induced by a unique isomorphism of field extensions $F'|L'|k' \xrightarrow{\sim} F|L|k$.

Proof of Theorem B $\Rightarrow$ Theorem A. By theorem B, there exists $\sigma : F'|k' \xrightarrow{\sim} F|k$ such that $\lambda = \sigma^*$, and σ is unique up to a power of the Frobenius in positive characteristic. Since $(\sigma^*)^{-1}(U_{L'}) = U_{\sigma L'}$, we have $U_{\sigma L'} = U_L$, thus the fields L and $\sigma L'$ are purely inseparably equivalent. The description of purely inseparable equivalence in proposition 2.7 shows that after composing σ with a (unique) suitable power of the Frobenius we have $\sigma L' = L$, so that σ is an isomorphism $F'|L'|k' \xrightarrow{\sim} F|L|k$. □

3 Algebraic Curves

Throughout, let k be a fixed algebraically closed ground field. If $L|k$ is a one-dimensional function field, i. e. a finitely generated extension of transcendence degree 1, then L has an interpretation as the field of rational functions on an algebraic curve C over k. Thus we are naturally led to use the language of algebraic geometry, such as morphisms, divisors and invertible sheaves, and to study how the geometry of the curves C is reflected in the absolute Galois groups $\mathrm{Gal}(L^{\mathrm{sep}}|L)$ of their function fields. In this section, we review definitions and collect statements from the theory of algebraic curves that will be needed later. Our main references are [Har77] (I.6, II.7 and IV.) and [GW10] (Chapter 15). We will make free use of the language of schemes.

Algebraic Curves, Rational Maps and Complete Nonsingular Models

By an **algebraic curve** (or simply **curve**) over k we mean a one-dimensional integral separated scheme of finite type over k. If we speak of a **point** on a curve, we mean a closed point, unless stated otherwise. A point $P \in C$ is **nonsingular** if the local ring $\mathcal{O}_P$ is regular (or equivalently normal). The curve C is **nonsingular** if it is nonsingular at every point. We say that C is **complete** if it is proper over k, which is equivalent to being projective. The **function field** $K(C)$ of a curve C is the local ring at the generic point. It is a finitely generated field extension over k of transcendence degree 1 and its elements are called **rational functions** on C.

For every point $P \in C$, the natural map $\mathcal{O}_P \to K(C)$ is injective and realises $K(C)$ as the field of fractions of $\mathcal{O}_P$. Suppose that $P \in C$ is nonsingular. Then the local ring $\mathcal{O}_P$ is a discrete valuation ring and there is an associated normalised discrete valuation ord_P on $K(C)$ which is trivial on k (we say ord_P is a valuation on $K(C)|k$). For $f \in K(C)^\times$, the integer $\mathrm{ord}_P(f)$ is called the **order** of f at P. We say that

f is **regular** at P if $\mathrm{ord}_P(f) \geq 0$;
f has a **zero** at P if $\mathrm{ord}_P(f) > 0$;
f has a **pole** at P if $\mathrm{ord}_P(f) < 0$.

If C is complete and nonsingular, the map $P \mapsto \mathrm{ord}_P$ defines a bijective correspondence between the points on C and the normalised discrete valuations on $K(C)|k$.

A **rational map** between two curves $\phi : C_2 \dashrightarrow C_1$ is represented by a pair (U, f) where U is a non-empty open subset of C_2 (which is automatically dense) and f is a morphism $f : U \to C_1$. Two such pairs (U, f) and (U', f') define the same rational map if f and f' agree on a non-empty open subset of $U \cap U'$. A rational map is **dominant** if the image $f(U)$ is dense (this does not depend on the choice of the representing pair (U, f)). Dominant rational maps can be composed, so the curves over k with dominant rational maps form a category. Two curves C_2 and C_1 are **birational** if they are isomorphic in this category. A dominant rational map $\phi : C_2 \dashrightarrow C_1$ maps the generic point of C_2 to the generic point of C_1, therefore it defines a finite extension of function fields $\phi^* : K(C_1) \hookrightarrow K(C_2)$ over k. It turns out that the map

$$\{\text{dominant rational maps } C_2 \dashrightarrow C_1\} \longrightarrow \mathrm{Hom}_k(K(C_1), K(C_2))$$

is bijective. In other words, the contravariant functor

$$\begin{pmatrix} \text{curves over } k \text{ with} \\ \text{dominant rational maps} \end{pmatrix} \longrightarrow \begin{pmatrix} \text{one-dimensional function} \\ \text{fields over } k \text{ with} \\ k\text{-homomorphisms} \end{pmatrix}$$

given by $C \mapsto K(C)$, is fully faithful; in fact, it is part of an equivalence of categories (see below). In particular, two curves are birational if and only if their function fields are isomorphic over k. A curve C is called a **rational curve** if it is birational to the projective line $\mathbb{P}^1$, or equivalently if its function field $K(C)$ is isomorphic over k to the purely transcendental function field $k(x)$.

Every dominant morphism $C_2 \to C_1$ determines a dominant rational map $C_2 \dashrightarrow C_1$, therefore isomorphic curves are birational. However, the converse can fail in two ways: First, singular curves can be birational to nonsingular curves (e. g. the singular cubic $y^2 = x^3$ is birational to the affine line); second, non-complete curves can be birational to complete curves (e. g. the affine line $\mathbb{A}^1$ is birational to the projective line $\mathbb{P}^1$). However, if C_1 is complete and C_2 is nonsingular, then every rational map $C_2 \dashrightarrow C_1$ extends uniquely to a morphism $C_2 \to C_1$. Therefore, we have fully faithful functors $(a) \to (b)$ and $(b) \to (c)$ as follows:

(a) complete nonsingular curves over k with dominant morphisms;

(b) curves over k with dominant rational maps;

(c) (one-dimensional function fields over k with k-homomorphisms)$^{\mathrm{op}}$.

There is also a functor $(c) \to (a)$ that assigns to every one-dimensional function field $L|k$ a complete nonsingular curve C_L with function field naturally isomorphic to L, thereby establishing an equivalence between the three categories. The construction is as follows:

- As a set, C_L consists of one point for each normalised discrete valuation on $L|k$, together with a generic point η.
- C_L is endowed with the topology in which the closed subsets are finite sets of non-generic points and the whole space.
- For each closed (= non-generic) point $P \in C_L$, its local ring $\mathcal{O}_P$ is by definition the valuation ring of the associated valuation ord_P. The local ring at the generic point is L.

- A sheaf of k-algebras on C_L is defined by the rule

  $$\mathcal{O}(U) := \bigcap_{P \in U} \mathcal{O}_P$$

  for every non-empty open subset U, the intersection being taken inside L. The restriction homomorphisms are simply inclusions between subrings of L.

One then checks that this defines indeed a complete nonsingular curve over k (cf. [Har77], Ch. I.6). Given an inclusion $L_1 \hookrightarrow L_2$ of one-dimensional function fields over k, one obtains a morphism $\phi : C_{L_2} \to C_{L_1}$ as follows: Given a point $P \in C_{L_2}$, corresponding to the discrete valuation ord_P on L_2, the restriction of ord_P to L_1 is a discrete valuation on L_1, thus equivalent to ord_Q for a unique point $Q \in C_{L_1}$. Setting $\phi(P) := Q$ defines ϕ as a map between sets. Given a non-empty open subset $U \subseteq C_{L_1}$, the inclusion $L_1 \hookrightarrow L_2$ restricts to a homomorphism $\mathcal{O}(U) \hookrightarrow \mathcal{O}(\phi^{-1}(U))$. This defines ϕ as a morphism between schemes over k and makes $L \mapsto C_L$ into a functor. By construction, the function field of C_L is isomorphic to L, so we call C_L a **complete nonsingular model** of $L|k$.

Divisors

From now on, all curves are assumed to be complete and nonsingular. A **Weil divisor** (or simply **divisor**) on a curve C is an element of the free abelian group over the points of C. A divisor is written as a formal sum $D = \sum_{P \in C} n_P\, P$ with $n_P \in \mathbb{Z}$ such that only finitely many coefficients are nonzero. The group of divisors on C is denoted by $\mathrm{Div}(C)$. A divisor is called **effective** (written $D \geq 0$) if $n_P \geq 0$ for all P. The **degree** of a divisor is an integer, defined as

$$\deg\Bigl(\sum_P n_P\, P\Bigr) := \sum_P n_P.$$

The divisors of degree zero form a subgroup $\mathrm{Div}^0(C)$ of $\mathrm{Div}(C)$.

A rational function $f \in K(C)^\times$ has only finitely many poles and zeroes, so there is an associated divisor $\mathrm{div}(f)$, defined by

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)\, P.$$

A divisor is called a **principal divisor** if it is equal to $\mathrm{div}(f)$ for some $f \in K(C)^\times$. The principal divisors form a subgroup $\mathrm{PDiv}(C)$ of $\mathrm{Div}(C)$. The quotient

$$\mathrm{Pic}(C) := \mathrm{Div}(C) / \mathrm{PDiv}(C)$$

is called the **Picard group** of C. Divisors that differ by a principal divisor are also called **linearly equivalent**. Principal divisors have degree zero, reflecting the fact that a rational function has the same number of zeroes and poles when counted with multiplicities. The quotient $\mathrm{Div}^0(C)/\mathrm{PDiv}(C)$ is denoted by $\mathrm{Pic}^0(C)$. A rational function without zeroes and poles is necessarily constant, i. e. contained in k, showing that there is an exact sequence of abelian groups

$$1 \longrightarrow k^\times \longrightarrow K(C)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \longrightarrow \mathrm{Pic}^0(C) \longrightarrow 0. \tag{3.1}$$

Ramification, Pullback and Pushforward of Divisors

Let $\phi : C_2 \to C_1$ be a dominant morphism between complete nonsingular curves and let $\phi^* : K(C_1) \hookrightarrow K(C_2)$ be the associated extension of function fields. The **degree** $\deg(\phi)$ of ϕ is defined as the degree of $K(C_2)|K(C_1)$. The degree of inseparability is defined similarly. The morphism ϕ is **separable** (resp. **purely inseparable**) if the extension $K(C_2)|K(C_1)$ has this property. For $P \in C_2$ and $Q = \phi(P) \in C_2$, there is an associated extension of discrete valuation rings $\phi^* : \mathcal{O}_Q \hookrightarrow \mathcal{O}_P$. The **ramification index** $e(P|Q)$ of ϕ at P is defined as the valuation

$$e(P|Q) = \operatorname{ord}_P(\phi^*(\pi_Q)),$$

where π_Q is a uniformising parameter of $\mathcal{O}_Q$, i. e. an element with $\operatorname{ord}_Q(\pi_Q) = 1$. As a consequence, we have

$$\operatorname{ord}_P(\phi^*(x)) = e(P|Q) \operatorname{ord}_Q(x) \quad \text{for all } x \in L_1^\times. \tag{3.2}$$

We say that ϕ is **ramified at** P if $e(P|Q) > 1$, and **unramified** otherwise. At all but finitely many points, the ramification index equals the degree of inseparability of ϕ. In particular, a separable morphism is unramified almost everywhere. Every point $Q \in C_1$ has only finitely many preimages, and their number equals $\deg(\phi)$ when each point is counted with its ramification index as multiplicity:

$$\sum_{P \in \phi^{-1}(Q)} e(P|Q) = \deg(\phi) \quad \text{for all } Q \in C_1. \tag{3.3}$$

The **inverse image divisor** of $Q \in C_1$ is by definition

$$\phi^*(Q) = \sum_{P \in \phi^{-1}(Q)} e(P|Q)\, P.$$

This defines by linear extension a homomorphism $\phi^* : \operatorname{Div}(C_1) \to \operatorname{Div}(C_2)$, called **pullback of divisors**. Formula 3.2 implies

$$\operatorname{div}(\phi^*(x)) = \phi^* \operatorname{div}(x) \quad \text{for all } x \in L_1^\times. \tag{3.4}$$

There is also a **pushforward of divisors** $\phi_* : \operatorname{Div}(C_2) \to \operatorname{Div}(C_1)$, uniquely defined by $\phi_*(P) = \phi(P)$ for $P \in C_2$. It follows from formula 3.3 that the composite $\phi_* \circ \phi^*$ is just multiplication by $\deg(\phi)$.

For a complete nonsingular curve C, the equivalence of categories between curves and function fields implies that dominant morphisms $\phi : C \to \mathbb{P}^1$ correspond bijectively to rational functions $f \in K(C) \setminus k$. The zeroes of f are the preimages of $0 \in \mathbb{P}^1$ under ϕ, the poles are preimages of $\infty \in \mathbb{P}^1$ and the orders are given by the respective ramification indices (or their negative in the case of a pole). The inverse image divisors $\phi^*(0)$ and $\phi^*(\infty)$ are called the **divisor of zeroes** and **divisor of poles**, respectively. Their difference is the divisor of f:

$$\operatorname{div}(f) = \phi^*(0) - \phi^*(\infty).$$

Invertible Sheaves

Let C be a complete nonsingular curve. An **invertible sheaf** $\mathcal{L}$ on C is a locally free sheaf of $\mathcal{O}_C$-modules of rank one. The isomorphism classes of invertible sheaves on C form a group with respect to the tensor product, the identity being $\mathcal{O}_C$ and the inverse of $\mathcal{L}$ being given by the sheaf hom

$$\mathcal{L}^\vee := \mathcal{H}om_{\mathcal{O}_C}(\mathcal{L}, \mathcal{O}_C).$$

The fact that C is proper over k implies that the space of global sections $\Gamma(C, \mathcal{L})$ of an invertible sheaf is a finite-dimensional k-vector space. Every divisor $D = \sum_P n_P P$ defines an invertible sheaf $\mathcal{O}_C(D)$ by the rule

$$\mathcal{O}_C(D)(U) = \big\{ f \in K(C)^\times : \operatorname{ord}_P(f) + n_P \geq 0 \text{ for all } P \in U \big\} \cup \{0\}.$$

The correspondence $D \mapsto \mathcal{O}_C(D)$ defines an isomorphism between the Picard group $\operatorname{Div}(C)/\operatorname{PDiv}(C)$ and the group of isomorphism classes of invertible sheaves. In particular, every invertible sheaf $\mathcal{L}$ has a well-defined degree $\deg(\mathcal{L})$.

There is a distinguished invertible sheaf on C, called the **canonical sheaf** ω, which plays the role of a dualising sheaf for Serre duality. The dimension of its space of global sections $g := \dim_k \Gamma(C, \omega)$ serves as one of several equivalent definitions of an important invariant of C, the **genus**. Curves of genus 0 are rational; curves of genus 1 are elliptic curves. The genus also appears in the Riemann-Roch theorem, which allows to compute the Euler characteristic of an invertible sheaf in terms of its degree.

Theorem 3.1 (Riemann-Roch Theorem). *Let $\mathcal{L}$ be an invertible sheaf on a complete nonsingular curve C of genus g. Then*

$$\dim_k H^0(C, \mathcal{L}) - \dim_k H^1(C, \mathcal{L}) = \deg(\mathcal{L}) + 1 - g.$$

It is a consequence of Serre duality that an invertible sheaf of degree $\geq 2g - 1$ has vanishing first cohomology, so in this case the Riemann-Roch theorem computes the dimension of the space of global sections:

$$\text{if } \deg(\mathcal{L}) \geq 2g - 1 \text{ then } \dim_k \Gamma(C, \mathcal{L}) = \deg(\mathcal{L}) + 1 - g.$$

Linear Systems

Let $\mathcal{L}$ be an invertible sheaf on a complete nonsingular curve C. The **order** of a non-zero global section $s \in \Gamma(C, \mathcal{L})$ at a point $P \in C$ is defined by choosing an isomorphism $\varphi_U : \mathcal{L}|_U \xrightarrow{\sim} \mathcal{O}_C|_U$ in a neighbourhood of P and setting $\operatorname{ord}_P(s) := \operatorname{ord}_P(\varphi_U(s|_U))$. This is well-defined because any two such isomorphisms φ_U differ only by multiplication with a unit in $\mathcal{O}_C(U)$. The **divisor of zeroes** of $s \in \Gamma(C, \mathcal{L}) \setminus \{0\}$ is the effective divisor

$$(s)_0 := \sum_{P \in C} \operatorname{ord}_P(s) P.$$

In the case $\mathcal{L} = \mathcal{O}_C(D)$, it is given by $(s)_0 = \operatorname{div}(s) + D$. The **complete linear system** of $\mathcal{L}$ is the set of all divisors of zeroes $(s)_0$ for $s \in \Gamma(C, \mathcal{L}) \setminus \{0\}$. It equals the set of effective divisors in the linear equivalence class defined by $\mathcal{L}$ and the association $s \mapsto (s)_0$ defines a bijection

$$\mathbb{P}\Gamma(C, \mathcal{L}) \xrightarrow{\sim} |\mathcal{L}|,$$

where for a k-vector space V, we denote by $\mathbb{P}V := (V \setminus \{0\})/k^\times$ its **projectivisation**. This gives $|\mathcal{L}|$ the structure of a projective space over k. Since the definition of a divisor of zeroes is invariant under isomorphisms, any invertible sheaf $\mathcal{L}'$ isomorphic to $\mathcal{L}$ defines the same complete linear system and the projective structures coincide in the sense that a subset of $|\mathcal{L}|$ is a projective subspace iff it is a projective subspace in $|\mathcal{L}'|$. For a divisor D on C, we write $|D|$ instead of $|\mathcal{O}_C(D)|$.

A **linear system** on C is defined as a projective subspace of a complete linear system. In other words, a subset $\mathfrak{d} \subseteq \operatorname{Div}(C)$ is a linear system if there exists an invertible sheaf $\mathcal{L}$ and a subspace $V \subseteq \Gamma(C, \mathcal{L})$ such that $\mathfrak{d}$ consists of the set of divisors of zeroes

$$\mathfrak{d} = \big\{(s)_0 : s \in V \setminus \{0\}\big\}.$$

The **dimension** of a linear system $\mathfrak{d}$ is defined as $\dim \mathfrak{d} = \dim V - 1$. To give a more explicit description, $\mathfrak{d}$ is a linear system of dimension n if and only if there exists a divisor D and linearly independent global sections $s_0, \ldots, s_n$ of $\mathcal{O}_C(D)$ such that

$$\mathfrak{d} = \big\{\operatorname{div}(a_0 s_0 + \ldots + a_n s_n) + D : (a_0, \ldots, a_n) \in k^{n+1}, \text{ not all } a_i = 0\big\}.$$

A **base point** of a linear system $\mathfrak{d}$ is a point $P \in C$ such that $n_P > 0$ for all $D = \sum_Q n_Q Q$ in $\mathfrak{d}$. A linear system is **base-point-free** if it has no base points. If $\mathcal{L}$ is an invertible sheaf and $V \subseteq \Gamma(C, \mathcal{L})$ a subspace defining $\mathfrak{d}$, then $\mathfrak{d}$ is base-point-free if and only if $\mathcal{L}$ is **generated by the global sections** in V, i. e. for all $P \in C$ there exists $s \in V$ such that $s_P \notin \mathfrak{m}_P \mathcal{L}_P$. An invertible sheaf $\mathcal{L}$ is called **base-point-free** if the associated complete linear system, consisting of the divisors of zeroes of its global sections, is base-point-free.

Proposition 3.2. *Let $\mathcal{L}$ be an invertible sheaf on a complete nonsingular curve C of genus g. If $\deg(\mathcal{L}) \geq 2g$, then $\mathcal{L}$ is base-point-free.*

Proof. We may assume $\mathcal{L} = \mathcal{O}_C(D)$ for a divisor D of degree $\geq 2g$. For every $P \in C$, there is a map $|D - P| \to |D|$, given by addition of P. It is surjective if and only if P is a base point of $|D|$. The map corresponds to the inclusion of invertible sheaves $\mathcal{O}_C(D - P) \subseteq \mathcal{O}_C(D)$. By the Riemann-Roch theorem, $\dim |D - P| = \dim |D| - 1$, therefore the map is not surjective. □

We will also need an alternative description of base-point-free lines in terms of inverse image divisors of morphisms to $\mathbb{P}^1$. There is a more general statement for higher-dimensional base-point-free linear systems involving morphisms to $\mathbb{P}^n$ and hyperplane divisors, but we will content ourselves with the case $n = 1$.

Lemma 3.3. *A set $\mathfrak{d} \subseteq \operatorname{Div}(C)$ of divisors on a complete nonsingular curve is a base-point-free line if and only if there exists a dominant morphism $\phi : C \to \mathbb{P}^1$ such that $\mathfrak{d}$ is the set of inverse image divisors*

$$\mathfrak{d} = \big\{\phi^*(Q) : Q \in \mathbb{P}^1\big\}.$$

Proof. Let $\phi : C \to \mathbb{P}^1$ be a dominant morphism, corresponding to the rational function $f \in K(C)$. With $D := \phi^*(\infty)$ the divisor of poles, two linearly independent global sections of $\mathcal{O}_C(D)$ are given by 1 and f. The corresponding base-point-free line consists of the divisors $D + \operatorname{div}(f - a)$ for $a \in k$, together with D itself. Identifying $\mathbb{P}^1 = k \cup \{\infty\}$, we have

$$D + \operatorname{div}(f - a) = D + \phi^*(a) - \phi^*(\infty) = \phi^*(a),$$

thus the base-point-free line consists indeed of the inverse image divisors of ϕ.

Conversely, let $\mathfrak{d}$ be a base-point-free line in $\operatorname{Div}(C)$. Then there exists a divisor D and two linearly independent global sections $s_0, s_1 \in \Gamma(C, \mathcal{O}_C(D))$ such that

$$\mathfrak{d} = \{D + \operatorname{div}(\lambda s_0 + \mu s_1) : \lambda, \mu \in k, \text{ not both zero}\}.$$

After replacing D with the linearly equivalent divisor $D + \operatorname{div}(s_0)$, we may assume $(s_0, s_1) = (1, f)$ for some $f \in K(C) \setminus k$. Then it is clear from the discussion above that $\mathfrak{d}$ will be the set of inverse image divisors of the dominant morphism $\phi : C \to \mathbb{P}^1$ that corresponds to the rational function f. □

Lemma 3.4. *Consider the set of principal divisors on a complete nonsingular curve C as a projective space over k via $K(C)^\times/k^\times \xrightarrow{\sim} \operatorname{PDiv}(C)$. Then a subset $S \subseteq \operatorname{PDiv}(C)$ is a finite-dimensional projective subspace if and only if there exists $D \in \operatorname{Div}(C)$ such that $S + D$ is a base-point-free linear system in $|D|$.*

Proof. Suppose $S \subseteq \operatorname{PDiv}(C)$ is a finite-dimensional projective subspace, so it is given by

$$S = \big\{\operatorname{div}(f) : f \in W \setminus \{0\}\big\}$$

for some finite-dimensional subspace $W \subseteq K(C)$. The divisor $D := \sum n_P P$ with

$$n_P := -\min\big\{\operatorname{ord}_P(f) : f \in W \setminus \{0\}\big\}$$

is well-defined by finite-dimensionality. We have $\operatorname{div}(f) + D \geq 0$ for all $f \in W \setminus \{0\}$, and at each point equality is achieved for some f, thus $S + D \subseteq |D|$ has no base points. The rest follows from the commutativity of the square

$$\begin{tikzcd}
\mathbb{P}\Gamma(C, \mathcal{O}_C(D)) \arrow[r, hook] \arrow[d, "(-)_0"'] & K(C)^\times/k^\times \arrow[d, "\operatorname{div}"] \\
{|D|} \arrow[r, hook, "-D"] & \operatorname{PDiv}(C)
\end{tikzcd}$$

□

An invertible sheaf $\mathcal{L}$ on a complete nonsingular curve C is called **very ample** if it is isomorphic to $i^*\mathcal{O}(1)$ for some (necessarily closed) immersion $i : C \hookrightarrow \mathbb{P}^r$ and $r \in \mathbb{N}$. This is equivalent to $\mathcal{L}$ satisfying all of the following three conditions:

(a) $\mathcal{L}$ has no base points;

(b) $\mathcal{L}$ separates points;

(c) $\mathcal{L}$ separates tangent vectors.

Having no base points implies that for all $P \in C$, the subspace

$$H_P := \{s \in \Gamma(C, \mathcal{L}) : s_P \in \mathfrak{m}_P \mathcal{L}_P\}$$

is a hyperplane, $\mathcal{L}$ **separating points** means that distinct points $P \neq Q$ have distinct hyperplanes $H_P \neq H_Q$, and **separating tangent vectors** means the subspaces

$$\{s \in \Gamma(C, \mathcal{L}) : s_P \in \mathfrak{m}_P^2 \mathcal{L}_P\}$$

have codimension 2. A Riemann-Roch argument shows that every invertible sheaf of degree $\geq 2g + 1$ satisfies these conditions, thereby proving the following proposition.

Proposition 3.5. *On a complete nonsingular curve of genus g, every invertible sheaf of degree $\geq 2g + 1$ is very ample.* □

4 Detecting the Rationality of Function Fields

We return to the situation of theorem B: k is an algebraically closed field, $F|k$ an algebraically closed extension of transcendence degree one and $G = \mathrm{Aut}(F|k)$. The aim of this section is to prove the following refinement of corollary 2.6.

Proposition 4.1. *Let (k', F', G') and $\lambda : G \xrightarrow{\sim} G'$ as in theorem B. Then the bijection from corollary 2.6, given by $L' \mapsto L$ if $\lambda^{-1}(U_{L'}) = U_L$, restricts to a bijection between sets of rational function fields as follows:*

$$\begin{tikzcd}
\left\{\begin{array}{c}\text{function fields } L'|k' \text{ in } F',\\ \text{up to purely inseparable}\\ \text{equivalence}\end{array}\right\} \arrow[r, "\sim"] & \left\{\begin{array}{c}\text{function fields } L|k \text{ in } F,\\ \text{up to purely inseparable}\\ \text{equivalence}\end{array}\right\} \\
\left\{\begin{array}{c}\text{rational function fields}\\ k'(x')|k' \text{ in } F', \text{ up to purely}\\ \text{inseparable equivalence}\end{array}\right\} \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, "\sim"] & \left\{\begin{array}{c}\text{rational function fields}\\ k(x)|k \text{ in } F, \text{ up to purely}\\ \text{inseparable equivalence}\end{array}\right\} \arrow[u, phantom, sloped, "\subseteq"]
\end{tikzcd}$$

Moreover, we have $\mathrm{char}(k) = \mathrm{char}(k')$.

Note that the property of a function field to be rational depends only on its purely inseparable equivalence class, for the function fields purely inseparably equivalent to $k(x)$ are given by $k(x)^{p^n} = k(x^{p^n})$ for $n \in \mathbb{Z}$, if $\mathrm{char}(k) = p > 0$.

Lemma 4.2. *Let K be a subextension of $F|k$ and $H = \operatorname{Aut}(F|K)$. Then the normaliser of H in G is given by*

$$N_G(H) = \left\{\sigma \in G \;\middle|\; \sigma K^i = K^i\right\}$$

and the restriction homomorphism $N_G(H) \to \operatorname{Aut}(K^i|k)$ induces an isomorphism

$$N_G(H)/H \cong \operatorname{Aut}(K^i|k).$$

Proof.

$$\begin{aligned} N_G(H) &= \left\{\sigma \in G \;\middle|\; \sigma \operatorname{Aut}(F|K)\sigma^{-1} = \operatorname{Aut}(F|K)\right\} \\ &= \{\sigma \in G \mid \operatorname{Aut}(F|\sigma K) = \operatorname{Aut}(F|K)\} && \text{by (2.1)} \\ &= \left\{\sigma \in G \;\middle|\; \sigma K^i = K^i\right\} && \text{by theorem 2.5.} \end{aligned}$$

This shows that every element of the normaliser $N_G(H)$ gives rise to an automorphism of $K^i|k$ by restriction. The map $N_G(H) \to \operatorname{Aut}(K^i|k)$ is surjective by lemma 2.4 and its kernel is given by $\operatorname{Aut}(F|K^i) = \operatorname{Aut}(F|K)$. □

For a one-dimensional function field $L|k$ in F, we can recover the automorphism group $\operatorname{Aut}(L^i|k)$ from (G, U_L) as the quotient $N_G(U_L)/U_L$. We are, however, more interested in $\operatorname{Aut}(L|k)$ because it is via the category equivalence from section 3 interpreted as (the opposite group of) the automorphism group of a complete nonsingular model C of $L|k$ and therefore contains geometric information. The following lemma shows how $\operatorname{Aut}(L^i|k)$ and $\operatorname{Aut}(L|k)$ are related.

Lemma 4.3. *Let $L|k$ be a one-dimensional function field and $L^i|L$ its purely inseparable closure. Then there is a canonical exact sequence*

$$1 \longrightarrow \operatorname{Aut}(L|k) \longrightarrow \operatorname{Aut}(L^i|k) \longrightarrow \mathbb{Z}.$$

In particular, $\operatorname{Aut}(L^i|k)$ *is a semidirect product*

$$\operatorname{Aut}(L^i|k) \cong \operatorname{Aut}(L|k) \rtimes Z$$

where Z is either trivial or isomorphic to $\mathbb{Z}$.

Proof. The statement is trivial in characteristic zero, so assume $\operatorname{char}(k) = p > 0$. Every automorphism of $L|k$ extends uniquely to $L^i|k$, defining an injective homomorphism $\operatorname{Aut}(L|k) \hookrightarrow \operatorname{Aut}(L^i|k)$. To define the second map, let $\sigma \in \operatorname{Aut}(L^i|k)$ be given. Since the extensions $L^i|L$ and $L^i|\sigma L$ are isomorphic via σ, the field L^i is also the purely inseparable closure of σL. By proposition 2.7, there exists a unique $\varphi(\sigma) = n \in \mathbb{Z}$ such that $\sigma L = L^{p^n}$. This defines a group homomorphism $\varphi : \operatorname{Aut}(L^i|k) \to \mathbb{Z}$. An automorphism σ belongs to $\ker(\varphi)$ if and only if $\sigma L = L$, in which case it is in the image of the first homomorphism. This proves the exactness of the sequence. The image $Z := \operatorname{im}(\varphi) \subseteq \mathbb{Z}$ of φ is either trivial or isomorphic to $\mathbb{Z}$. In either case, the exact sequence

$$1 \longrightarrow \operatorname{Aut}(L|k) \longrightarrow \operatorname{Aut}(L^i|k) \longrightarrow Z \longrightarrow 1$$

is split by a section $Z \to \operatorname{Aut}(L^i|k)$, hence $\operatorname{Aut}(L^i|k)$ is isomorphic to a semidirect product $\operatorname{Aut}(L|k) \rtimes Z$. □

Definition 4.4. Let G be an arbitrary group and let $n \in \mathbb{N}$. An element $x \in G$ is called n**-divisible** if $y^n = x$ for some $y \in G$. It is called **infinitely** n**-divisible** if there exists a sequence $(x_1, x_2, \ldots)$ in G with $x_1 = x$ and $x_i = x_{i+1}^n$ for all $i \in \mathbb{N}$. We say the group G is n**-divisible** if every element is n-divisible.

Clearly, in an n-divisible group, every element is infinitely n-divisible.

Lemma 4.5. *Let $L|k$ be a function field in F with purely inseparable closure L^i, let $\sigma \in \mathrm{Aut}(L^i|k)$ and $n \in \mathbb{N}$, $n \geq 2$. Then σ is infinitely n-divisible in $\mathrm{Aut}(L^i|k)$ if and only if $\sigma L = L$ and σ is also infinitely n-divisible in $\mathrm{Aut}(L|k)$.*

Proof. By lemma 4.3, $\mathrm{Aut}(L^i|k)$ fits into an exact sequence

$$1 \longrightarrow \mathrm{Aut}(L|k) \longrightarrow \mathrm{Aut}(L^i|k) \xrightarrow{\varphi} \mathbb{Z}.$$

If σ is infinitely n-divisible in $\mathrm{Aut}(L^i|k)$, then $\varphi(\sigma)$ is infinitely n-divisible in $\mathbb{Z}$, hence $\varphi(\sigma) = 0$ and by exactness $\sigma \in \mathrm{Aut}(L|k)$.

If $(\sigma_1, \sigma_2, \ldots)$ is a sequence in $\mathrm{Aut}(L^i|k)$ with $\sigma_1 = \sigma$ and $\sigma_i = \sigma_{i+1}^n$ for all i, then the σ_i are infinitely n-divisible themselves, hence contained in $\mathrm{Aut}(L|k)$, so that σ is already infinitely n-divisible as an element of $\mathrm{Aut}(L|k)$. □

Lemma 4.6. *The automorphism group $\mathrm{Aut}_k(\mathbb{P}^1)$ is ℓ-divisible for every prime number $\ell \neq \mathrm{char}(k)$.*

Proof. The automorphisms of $\mathbb{P}^1$ are the Möbius transformations, i. e. they are of the form $(x : y) \mapsto (ax+by : cx+dy)$ with $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,k)$. This gives an isomorphism between $\mathrm{Aut}(\mathbb{P}^1)$ and the projective linear group $\mathrm{PGL}(2,k) = \mathrm{GL}(2,k)/k^\times$, hence it is enough to show that $\mathrm{GL}(2,k)$ is ℓ-divisible. Let $A \in \mathrm{GL}(2,k)$ be given. We may assume that A is in Jordan normal form

$$A = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \quad \text{or} \quad A = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

Then a matrix $B \in \mathrm{GL}(2,k)$ with $B^\ell = A$ is respectively given by

$$B = \begin{pmatrix} \lambda^{1/\ell} & 0 \\ 0 & \mu^{1/\ell} \end{pmatrix} \quad \text{or} \quad B = \lambda^{1/\ell} \begin{pmatrix} 1 & \lambda^{-1}/\ell \\ 0 & 1 \end{pmatrix}.$$ □

Lemma 4.7. *Let $L|k$ be a function field in F with purely inseparable closure L^i and let $\ell \neq \mathrm{char}(k)$ be a prime number. Then L is rational if and only if the subgroup of $\mathrm{Aut}(L^i|k)$ generated by the infinitely ℓ-divisible elements is infinite and contains no abelian subgroup of finite index.*

Proof. Let C be a complete nonsingular model of $L|k$, let g be its genus and let H be the subgroup of $\mathrm{Aut}(L^i|k)$ generated by the infinitely ℓ-divisible elements. By lemma 4.5, H is in fact isomorphic to the similarly defined subgroup of $\mathrm{Aut}(L|k)$. By the equivalence of categories between curves and function fields, we have isomorphisms

$$\mathrm{Aut}(L|k) \cong \mathrm{Aut}(C)^{\mathrm{op}} \cong \mathrm{Aut}(C),$$

thus we may identify H with the subgroup of $\mathrm{Aut}(C)$ that is generated by the infinitely ℓ-divisible elements.

Now assume that C is rational, i. e. $C \cong \mathbb{P}^1$. By lemma 4.6, we have $H = \mathrm{Aut}(\mathbb{P}^1)$. It is clear that this group is infinite as it contains all the translations $z \mapsto z + b$ for $b \in k$. (We identify $\mathbb{P}^1$ with $k \cup \{\infty\}$ and use the notation $\frac{az+b}{cz+d}$ rather than $(az + b : cz + d)$.) Assume $N \leq \mathrm{Aut}(\mathbb{P}^1)$ is a subgroup of finite index. By the pigeonhole principle, N contains a non-trivial translation $\phi(z) = z + b$ with $b \neq 0$ and a non-trivial homothety $\psi(z) = az$ with $a \neq 1$. They do not commute with each other since

$$\begin{aligned}\psi \circ \phi(z) &= az + ab,\\ \phi \circ \psi(z) &= az + b,\end{aligned}$$

but $ab \neq b$. Thus, N is not abelian.

For the converse, assume that C is not rational, so C has genus $g \geq 1$. If $g \geq 2$, then $\mathrm{Aut}(C)$ and hence its subgroup H are finite (Ex. V.1.11 in [Har77]). (The Hurwitz bound $\# \mathrm{Aut}(C) \leq 84(g-1)$ may be violated in positive characteristic, but finiteness still holds.) If $g = 1$, then C is an elliptic curve and after choosing a point $O \in C$, it carries a group law with identity O. The group T of translations $\tau_P(Q) = P + Q$ forms an abelian subgroup of $\mathrm{Aut}(C)$, and its index equals the order of the stabiliser of O, which is one of $\{2, 4, 6, 12, 24\}$ (Thm. III.10.1 in [Sil09]). Since multiplication by ℓ is surjective on C, the group T is ℓ-divisible, hence contained in H, so that H has an abelian subgroup of finite index. □

Now we can prove the main result of this section.

Proof of proposition 4.1. Let $L|k$ and $L'|k'$ be function fields with $\lambda^{-1}(U_{L'}) = U_L$. Then λ induces an isomorphism $N_G(U_L)/U_L \xrightarrow{\sim} N_{G'}(U_{L'})/U_{L'}$, thus $\mathrm{Aut}(L^i|k) \cong \mathrm{Aut}(L'^i|k')$ by lemma 4.2. With ℓ a prime not equal to either of $\mathrm{char}(k)$ and $\mathrm{char}(k')$, lemma 4.7 shows that the property of L (resp. L') being a rational function field is encoded in the group structure of $\mathrm{Aut}(L^i|k)$ (resp. $\mathrm{Aut}(L'^i|k')$), which shows the first part of the proposition.

To prove $\mathrm{char}(k) = \mathrm{char}(k')$, choose an arbitrary rational function field $L|k$ in F and choose L' with $\lambda^{-1}(U_{L'}) = U_L$. We have an isomorphism $\mathrm{Aut}(L^i|k) \cong \mathrm{Aut}(L'^i|k')$ as above. Passing to the subgroups generated by the infinitely ℓ-divisible elements, we find $\mathrm{Aut}(\mathbb{P}^1_k) \cong \mathrm{Aut}(\mathbb{P}^1_{k'})$. We claim that the characteristic of k is the unique prime p for which $\mathrm{Aut}(\mathbb{P}^1_k)$ is not p-divisible, or zero if no such prime exists. We already proved the ℓ-divisibility for all primes $\ell \neq \mathrm{char}(k)$, so suppose $\mathrm{char}(k) = p > 0$ and assume for contradiction that there exists $\psi \in \mathrm{Aut}(\mathbb{P}^1_k)$ such that $\psi^p = z + 1$. If $P \in \mathbb{P}^1_k$ is a fixed point of ψ, it is also a fixed point of ψ^p, hence $P = \infty$. As a Möbius transformation with ∞ as its only fixed point, ψ is necessarily a translation, $\psi = z + a$ for some $a \in k$. But then $\psi^p = z + pa = z \neq z + 1$, contradiction! □

5 Kummer Theory

In this section we review standard facts from Kummer theory and apply it to the situation at hand, i. e. for function fields of algebraic curves over an algebraically closed field. Specifically, we define the ℓ-adic Tate module $\mathbb{T}_\ell$ and use Kummer theory to describe the Galois group of the maximal pro-ℓ abelian extension of a function field.

First consider an arbitrary field L and a natural number $n \in \mathbb{N}$ such that L contains a primitive n-th root of unity. Let $\overline{L}$ be a fixed algebraic (or separable) closure of L. For a subgroup A of $L^\times$ containing $L^{\times n}$, let $L(\sqrt[n]{A})$ be the subfield of $\overline{L}$ obtained by adjoining the n-th roots of all elements of A. It is always an abelian extension of exponent n, which is to say that $L(\sqrt[n]{A})|L$ is a Galois extension with abelian Galois group, in which $\sigma^n = 1$ for all $\sigma \in \mathrm{Gal}(L(\sqrt[n]{A})|L)$. The main theorem of Kummer theory states that there is a inclusion-reversing correspondence:

$$\begin{tikzcd}
\left\{ \begin{matrix} \text{subgroups } A \text{ of } L^\times \\ \text{containing } L^{\times n} \end{matrix} \right\} \arrow[r, shift left] & \left\{ \begin{matrix} \text{abelian extensions } E|L \text{ of} \\ \text{exponent } n \text{ inside } \overline{L} \end{matrix} \right\} \arrow[l, shift left] \\
A \arrow[r, mapsto] & L(\sqrt[n]{A}) \\
E^{\times n} \cap L^\times & E \arrow[l, mapsto]
\end{tikzcd}$$

Moreover, there is a non-degenerate bilinear pairing

$$\begin{aligned} \mathrm{Gal}(L(\sqrt[n]{A})|L) \times A/L^{\times n} &\longrightarrow \mu_n \\ (\sigma, a \bmod L^{\times n}) &\longmapsto \sigma(\sqrt[n]{a})/\sqrt[n]{a} \end{aligned}$$

taking values in the group μ_n of n-th roots of unity. The pairing yields isomorphisms

$$\begin{aligned} \mathrm{Gal}(L(\sqrt[n]{A})|L) &\xrightarrow{\sim} \mathrm{Hom}(A/L^{\times n}, \mu_n), \\ A/L^{\times n} &\xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(L(\sqrt[n]{A})|L), \mu_n). \end{aligned}$$

Now let k be an algebraically closed field, ℓ a prime number not equal to the characteristic of k, and L a finitely generated extension of k. Let $L^{\mathrm{ab},\ell}$ be the maximal pro-ℓ abelian extension of L, i. e. L is obtained by adjoining all the roots $\sqrt[\ell^n]{x}$ for $x \in L^\times$ and $n \in \mathbb{N}$. For every $n \in \mathbb{N}$ we have a bilinear pairing

$$\begin{aligned} \langle \cdot, \cdot \rangle_n : \mathrm{Gal}(L^{\mathrm{ab},\ell}|L) \times L^\times &\longrightarrow \mu_{\ell^n}, \\ \langle \sigma, x \rangle_n &:= \sigma(\sqrt[\ell^n]{x})/\sqrt[\ell^n]{x}. \end{aligned} \tag{5.1}$$

The elements $\omega_n = \langle \sigma, x \rangle_n$ form a compatible system of roots of unity in the sense that $\omega_n = \omega_{n+1}^\ell$ for all $n \in \mathbb{N}$. In other words, they define an element of the projective limit $\varprojlim_{n \in \mathbb{N}} \mu_{\ell^n}$ with respect to the transition maps $\mu_{\ell^{n+1}} \to \mu_{\ell^n}, \omega \mapsto \omega^\ell$ for $n \in \mathbb{N}$.

Definition 5.1. We call $\mathbb{T}_\ell := \varprojlim_{n \in \mathbb{N}} \mu_{\ell^n}$ the **ℓ-adic Tate module** of $k^\times$.

$\mathbb{T}_\ell$ is an abelian topological group carrying a natural module structure over the ring $\mathbb{Z}_\ell$ of ℓ-adic integers, which makes it a free $\mathbb{Z}_\ell$-module of rank one. It is generated over $\mathbb{Z}_\ell$ by any compatible system of primitive roots of unity, but it does not come with a canonical generator. We write $\mathbb{T}_\ell$ additively.

Lemma 5.2. *Let k be an algebraically closed field, $L|k$ a finitely generated extension and $\ell \neq \operatorname{char}(k)$ a prime number. Then an element $x \in L^\times$ is infinitely ℓ-divisible if and only if $x \in k^\times$.*

Proof. One implication is clear because k is algebraically closed, so suppose $x \in L^\times$ is infinitely ℓ-divisible. Let T be a transcendence basis of $L|k$. Then $L|k(T)$ is a finite extension. We have $k(T)(\sqrt[\ell^n]{x}) \subseteq L$ for all $n \in \mathbb{N}$, thus $[k(T)(\sqrt[\ell^n]{x}) : k(T)]$ divides $[L : k(T)]$. This degree equals the order of x in $k(T)^\times / k(T)^{\times \ell^n}$, thus $x^{[L:k(T)]}$ is an ℓ^n-th power in $k(T)$ for all $n \in \mathbb{N}$. But $k(T)$ is the field of fractions of the polynomial ring $k[T]$, a unique factorisation domain, so we must have $x^{[L:k(T)]} \in k^\times$ and hence $x \in k^\times$. □

Proposition 5.3 (The Kummer isomorphism)**.** *Let k be an algebraically closed field and let $L|k$ be a finitely generated extension. Then the Kummer pairings* (5.1) *define a non-degenerate bilinear pairing*

$$\langle \cdot, \cdot \rangle : \operatorname{Gal}(L^{\mathrm{ab},\ell}|L) \times L^\times / k^\times \longrightarrow \mathbb{T}_\ell.$$

The pairing induces an isomorphism of topological groups

$$\operatorname{Gal}(L^{\mathrm{ab},\ell}|L) \cong \operatorname{Hom}(L^\times, \mathbb{T}_\ell)$$

where $L^\times$ is discrete and $\operatorname{Hom}(L^\times, \mathbb{T}_\ell)$ *is equipped with the compact-open topology.*

Explicitly, a homomorphism $f : L^\times \to \mathbb{T}_\ell, x \mapsto (f_n(x))_{n \in \mathbb{N}}$ corresponds under the Kummer isomorphism to the unique automorphism $\sigma \in \operatorname{Gal}(L^{\mathrm{ab},\ell}|L)$ with

$$\sigma(\sqrt[\ell^n]{x}) / \sqrt[\ell^n]{x} = f_n(x) \quad \text{for all } x \in L^\times \text{ and } n \in \mathbb{N}.$$

Let us also remark that as an abelian pro-ℓ group, $\operatorname{Gal}(L^{\mathrm{ab},\ell}|L)$ has a canonical structure of a $\mathbb{Z}_\ell$-module, and the Kummer isomorphism respects the $\mathbb{Z}_\ell$-action.

Proof. Non-degeneracy on the left: If $\langle \sigma, x \rangle = 0$ for all $x \in L^\times$, then σ fixes $\sqrt[\ell^n]{x}$ for all $x \in L^\times$ and $n \in \mathbb{N}$, thus σ acts trivially on all of $L^{\mathrm{ab},\ell}$.

Non-degeneracy on the right: If $\langle \sigma, x \rangle = 0$ for all $\sigma \in \operatorname{Gal}(L^{\mathrm{ab},\ell}|L)$, then $\sqrt[\ell^n]{x} \in L^\times$ for all $n \in \mathbb{N}$, thus x is infinitely ℓ-divisible in $L^\times$. By lemma 5.2, $x \in k^\times$.

The isomorphism: For $n \in \mathbb{N}$, let $L_n = L(\sqrt[\ell^n]{L^\times})$ be the maximal abelian extension of exponent ℓ^n. We have $L^{\mathrm{ab},\ell} = \bigcup_{n \in \mathbb{N}} L_n$, and for each $n \in \mathbb{N}$ the pairing $\langle \cdot, \cdot \rangle_n$ defines an isomorphism $\mathrm{Gal}(L_n|L) \cong \mathrm{Hom}(L^\times/L^{\times \ell^n}, \mu_{\ell^n})$. We therefore have isomorphisms

$$\begin{aligned}\mathrm{Gal}(L^{\mathrm{ab},\ell}|L) &\cong \varprojlim_{n\in\mathbb{N}} \mathrm{Gal}(L_n|L)\\ &\cong \varprojlim_{n\in\mathbb{N}} \mathrm{Hom}(L^\times/L^{\times \ell^n}, \mu_{\ell^n})\\ &\cong \varprojlim_{n\in\mathbb{N}} \mathrm{Hom}(L^\times, \mu_{\ell^n})\\ &\cong \mathrm{Hom}(L^\times, \varprojlim_{n\in\mathbb{N}} \mu_{\ell^n})\\ &= \mathrm{Hom}(L^\times, \mathbb{T}_\ell).\end{aligned}$$

Now we show that the profinite topology on $\mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$ corresponds to the compact-open topology on $\mathrm{Hom}(L^\times, \mathbb{T}_\ell)$. Recall that for topological groups G and H, a subbase for the compact-open topology on $\mathrm{Hom}_{\mathrm{cts}}(G,H)$ consists of the sets

$$\mathcal{U}(K,V) := \{f \in \mathrm{Hom}_{\mathrm{cts}}(G,H) \mid f(K) \subseteq V\}$$

with $K \subseteq G$ compact and $V \subseteq H$ open. Let $\mathrm{Gal}(L^{\mathrm{ab},\ell}|E)$ be a basic open neighbourhood of the identity in $\mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$ where E is finite over L. By Kummer theory, we have $E = L(\sqrt[\ell^n]{x_1}, \ldots, \sqrt[\ell^n]{x_r})$ for some $n \in \mathbb{N}$ and finitely many elements $x_1, \ldots, x_r \in L^\times$. For $\sigma \in \mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$, we have

$$\begin{aligned}\sigma \in \mathrm{Gal}(L^{\mathrm{ab},\ell}|E) &\Leftrightarrow \sigma(\sqrt[\ell^n]{x_i}) = \sqrt[\ell^n]{x_i} \text{ for } i = 1, \ldots, r\\ &\Leftrightarrow \langle \sigma, x_i\rangle_n = 1 \text{ for } i = 1, \ldots, r\\ &\Leftrightarrow \langle \sigma, x_i\rangle \in \ker\left[\mathbb{T}_\ell \xrightarrow{\pi_n} \mu_{\ell^n}\right] \text{ for } i = 1, \ldots, r,\end{aligned}$$

thus $\mathrm{Gal}(L^{\mathrm{ab},\ell}|E)$ corresponds in $\mathrm{Hom}(L^\times, \mathbb{T}_\ell)$ to the subgroup $\mathcal{U}(\{x_1, \ldots, x_r\}, \ker \pi_n)$, which is open in the compact-open topology. Conversely, every open neighbourhood of the identity in $\mathrm{Hom}(L^\times, \mathbb{T}_\ell)$ contains a neighbourhood of the form $\mathcal{U}(\{x_1, \ldots, x_r\}, \ker \pi_n)$ for finitely many elements $x_1, \ldots, x_r \in L^\times$ and some $n \in \mathbb{N}$, and we have seen that this corresponds in $\mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$ to the open subgroup $\mathrm{Gal}(L^{\mathrm{ab},\ell}|L(\sqrt[\ell^n]{x_1}, \ldots, \sqrt[\ell^n]{x_r}))$. □

6 Decomposition Subgroups

In this section we quickly review the concept of decomposition subgroups in a Galois extension of discretely valued fields before we turn to the case of function fields of curves, where we find a description of decomposition subgroups in terms of "delta functions" and see how they behave with respect to morphisms between curves. A treatment of the theory of discretely valued fields can be found in [Neu07], chapter II.

Consider a Galois extension $L|K$ with a discrete valuation v on K and a discrete valuation w on L that extends v, i. e. w "lies over" v. The Galois group $\mathrm{Gal}(L|K)$ acts transitively from the right on the set of valuations lying over v by the rule $w.\sigma = w \circ \sigma$. The **decomposition subgroup** of w is defined as the stabiliser

$$\mathrm{Gal}(L|K)_w := \{\sigma \in \mathrm{Gal}(L|K) \mid w \circ \sigma = w\}.$$

Since the action is transitive, the decomposition subgroups of any two valuations lying over v are conjugate. In particular, if $L|K$ is an abelian extension, we have without fixing an extension of v to L a well-defined decomposition subgroup $\mathrm{Gal}(L|K)_v$.

Completions

A discrete valuation v on K defines an absolute value $|x|_v = q^{-v(x)}$ on K, with a fixed real number $q > 1$. This defines a metric $d_v(x, y) = |x - y|_v$ on K and consequently a topology, which depends only on the equivalence class of v and not on the choice of q. There is a field extension $K_v|K$ together with a discrete valuation extending v (which we also denote by v), such that K_v is complete with respect to the metric d_v and such that K is dense in K_v. It is called the **completion** of K with respect to v, and is unique up to unique isomorphism of valued fields over K. It is also characterised by the universal property that every embedding of K into a field which is complete with respect to a valuation extending v factors uniquely over K_v. The valuation v on K_v extends uniquely to any algebraic extension $E|K_v$. If the field extension is finite, the extended valuation is again discrete and in this case E is also complete.

Let $L|K$ be a finite Galois extension and w a discrete valuation on L lying over v. Then the inclusion $K \hookrightarrow L \hookrightarrow L_w$ induces a natural embedding $K_v \hookrightarrow L_w$. The extension $L_w|K_v$ is again a finite Galois extension and there is a restriction homomorphism $\mathrm{Gal}(L_w|K_v) \to \mathrm{Gal}(L|K)$. It is injective because L is dense in L_w and the automorphisms in $\mathrm{Gal}(L_w|K_v)$ are continuous with respect to the w-adic topology. Its image is precisely the decomposition subgroup $\mathrm{Gal}(L|K)_w$:

$$\mathrm{Gal}(L_w|K_v) \cong \mathrm{Gal}(L|K)_w.$$

The same is true if $L|K$ is an arbitrary (not necessarily finite) Galois extension, provided one replaces the completion L_w with the **localisation** of L at w, which is the direct limit of the completions of all finite subextensions of $L|K$.

Decomposition Subgroups for Function Fields of Curves

Let k be an algebraically closed field, ℓ a prime number not equal to the characteristic of k and $L|k$ the function field of a complete nonsingular curve C over k. Since the (closed) points of C are in a natural correspondence to the set of normalised discrete valuations on L that are trivial on k, we may speak of the decomposition subgroup in $\mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$ of a point $P \in C$.

Every map $f : C \to \mathbb{T}_\ell$ induces an automorphism in $\mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$ in the following way: First f is extended by linearity to define a homomorphism $\mathrm{Div}^0(C) \to \mathbb{T}_\ell$. This is pulled back via $\mathrm{div} : L^\times \to \mathrm{Div}^0(C)$ to obtain a homomorphism $L^\times \to \mathbb{T}_\ell$. Finally, this defines by Kummer theory an automorphism in $\mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$. Altogether, the automorphism $\sigma \in \mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$ associated to the map $f : C \to \mathbb{T}_\ell$ is uniquely defined by

$$\langle \sigma, x \rangle = \sum_{P \in C} \mathrm{ord}_P(x) f(P) \quad \text{for all } x \in L^\times. \tag{6.1}$$

Definition 6.1. We denote by $\Phi_L \subseteq \mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$ the subgroup of all automorphisms coming from a map $C \to \mathbb{T}_\ell$.

Proposition 6.2. *The kernel of* $\mathrm{Map}(C, \mathbb{T}_\ell) \twoheadrightarrow \Phi_L$ *consists precisely of the constant maps,* Φ_L *is a closed subgroup of* $\mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$ *and we have two isomorphisms of topological groups*

$$\mathrm{Map}(C, \mathbb{T}_\ell)/\mathbb{T}_\ell \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Div}^0(C), \mathbb{T}_\ell) \xrightarrow{\sim} \Phi_L$$

where $\mathrm{Map}(C, \mathbb{T}_\ell)$ *and* $\mathrm{Hom}(\mathrm{Div}^0(C), \mathbb{T}_\ell)$ *are equipped with the compact-open topology.*

Proof. Applying the functor $\mathrm{Hom}(-, \mathbb{T}_\ell)$ to the exact sequence

$$0 \longrightarrow \mathrm{Div}^0(C) \longrightarrow \mathrm{Div}(C) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0$$

yields another exact sequence

$$0 \longrightarrow \mathrm{Hom}(\mathbb{Z}, \mathbb{T}_\ell) \longrightarrow \mathrm{Hom}(\mathrm{Div}(C), \mathbb{T}_\ell) \longrightarrow \mathrm{Hom}(\mathrm{Div}^0(C), \mathbb{T}_\ell) \longrightarrow 0,$$

with the rightmost 0 following from the freeness of $\mathbb{Z}$. We obtain an isomorphism

$$\varphi : \mathrm{Map}(C, \mathbb{T}_\ell)/\mathbb{T}_\ell \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Div}^0(C), \mathbb{T}_\ell)$$

where on the left hand side, $\mathbb{T}_\ell$ is identified with the constant maps on C. The sets

$$\mathcal{U}(\{P_1, \ldots, P_r\}, U) \bmod \mathbb{T}_\ell \quad \text{resp.} \quad \mathcal{U}(\{D_1, \ldots, D_r\}, U)$$

with $D_i \in \mathrm{Div}^0(C)$, $P_i \in C$ and $U \subseteq \mathbb{T}_\ell$ an open subgroup form a neighbourhood basis of the identity in $\mathrm{Map}(C, \mathbb{T}_\ell)/\mathbb{T}_\ell$ resp. $\mathrm{Hom}(\mathrm{Div}^0(C), \mathbb{T}_\ell)$. The continuity of φ follows from

$$\mathcal{U}(\mathrm{Supp}\, D, U) \bmod \mathbb{T}_\ell \subseteq \varphi^{-1}\big(\mathcal{U}(\{D\}, U)\big)$$

for $D \in \mathrm{Div}^0(C)$, and the openness from

$$\varphi^{-1}\big(\mathcal{U}(\{P_1 - Q, \ldots, P_r - Q\}, U)\big) \subseteq \mathcal{U}(\{P_1, \ldots, P_r\}, U) \bmod \mathbb{T}_\ell$$

with an arbitrary point $Q \in C$. Thus, φ is a homeomorphism.

Now apply $\mathrm{Hom}(-, \mathbb{T}_\ell)$ to the exact sequence (3.1)

$$1 \longrightarrow L^\times/k^\times \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \longrightarrow \mathrm{Pic}^0(C) \longrightarrow 0$$

to obtain an exact sequence

$$0 \longrightarrow \mathrm{Hom}(\mathrm{Pic}^0(C), \mathbb{T}_\ell) \longrightarrow \mathrm{Hom}(\mathrm{Div}^0(C), \mathbb{T}_\ell) \xrightarrow{\psi} \mathrm{Hom}(L^\times, \mathbb{T}_\ell)$$

(where $\mathrm{Hom}(L^\times/k^\times, \mathbb{T}_\ell) = \mathrm{Hom}(L^\times, \mathbb{T}_\ell)$ because $k^\times$ is ℓ-divisible). There exists an abelian variety, the **Jacobian variety** of C, whose underlying group of closed points is $\mathrm{Pic}^0(C)$, which implies that this group is also ℓ-divisible ([Mum74], II.4). Hence $\mathrm{Hom}(\mathrm{Pic}^0(C), \mathbb{T}_\ell) = 0$ and ψ is injective. Since $\mathrm{Hom}(L^\times, \mathbb{T}_\ell) \cong \mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$ via Kummer theory (5.3), we have to show that the compact-open topology on $\mathrm{Hom}(\mathrm{Div}^0(C), \mathbb{T}_\ell)$ coincides with the subspace topology induced by ψ. The continuity of ψ follows from

$$\psi^{-1}\big(\mathcal{U}(\{x_1, \dots, x_r\}, U)\big) = \mathcal{U}(\{\mathrm{div}(x_1), \dots, \mathrm{div}(x_r)\}, U)$$

for $x_i \in L^\times$ and $U \subseteq \mathbb{T}_\ell$ open. To see that every open subset of $\mathrm{Hom}(\mathrm{Div}^0(C), \mathbb{T}_\ell)$ is also open in the induced topology, it suffices to consider neighbourhoods of the identity of the form $\mathcal{U}(\{D_1, \dots, D_r\}, \ell^n\mathbb{T}_\ell)$ with $D_i \in \mathrm{Div}^0(C)$ and $n \in \mathbb{N}_0$. Since $\mathrm{Pic}^0(C)$ is ℓ-divisible, there exist divisors $E_i \in \mathrm{Div}^0(C)$ and rational functions $x_i \in L^\times$ with $D_i = \mathrm{div}(x_i) + \ell^n E_i$. Then for $f \in \mathrm{Hom}(\mathrm{Div}^0(C), \mathbb{T}_\ell)$ we have

$$f(D_i) \in \ell^n\mathbb{T}_\ell \;\Leftrightarrow\; f(\mathrm{div}(x_i)) \in \ell^n\mathbb{T}_\ell,$$

hence

$$\mathcal{U}(\{D_1, \dots, D_r\}, \ell^n\mathbb{T}_\ell) = \psi^{-1}\big(\mathcal{U}(\{x_1, \dots, x_r\}, \ell^n\mathbb{T}_\ell)\big).$$

Finally, the claim that $\Phi_L \subseteq \mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$ is a closed subgroup follows from the fact that Φ_L is a continuous image of the compact group $\mathrm{Map}(C, \mathbb{T}_\ell)$. □

Definition 6.3. A map $f : C \to \mathbb{T}_\ell$ is called a **delta function** at $P \in C$ if it is constant on $C \setminus \{P\}$. A delta function f at P is **normalised** if it vanishes outside P.

Despite the terminology, a delta function at P is allowed to be constant on all of C. The notion of a delta function is still well-defined if f is only defined up to addition of a constant, therefore the delta functions at P form a subgroup of $\mathrm{Map}(C, \mathbb{T}_\ell)/\mathbb{T}_\ell$. Clearly, every delta function at P is equivalent modulo constants to a unique *normalised* delta function at P. Under the isomorphism $\mathrm{Map}(C, \mathbb{T}_\ell)/\mathbb{T}_\ell \cong \Phi_L$, the normalised delta function $f(Q) = \delta_{PQ}\,\omega$ at P corresponds to the automorphism $\sigma \in \mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$ satisfying

$$\langle \sigma, x\rangle = \mathrm{ord}_P(x)\omega \quad \text{for all } x \in L^\times.$$

Thus, an automorphism $\sigma \in \mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$ is induced by a delta function at P if and only if $\langle \sigma, \cdot\rangle : L^\times \to \mathbb{T}_\ell$ factors over $\mathrm{ord}_P : L^\times \to \mathbb{Z}$.

Proposition 6.4. *Let C be a complete nonsingular curve over k and L its function field. Then the decomposition subgroup in $\mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$ of a point $P \in C$ consists precisely of those automorphisms that are induced by a delta function at P.*

Proof. Let L_P be the completion of L at the discrete valuation ord_P and let $L_P^{\mathrm{ab},\ell}$ be its maximal pro-ℓ abelian extension, endowed with the unique valuation extending ord_P. Choose an L-embedding $L^{\mathrm{ab},\ell} \hookrightarrow L_P^{\mathrm{ab},\ell}$ to obtain a valuation on $L^{\mathrm{ab},\ell}$ extending ord_P:

$$\begin{tikzcd}
& L_P^{\mathrm{ab},\ell} \arrow[dd, dash] \\
L^{\mathrm{ab},\ell} \arrow[ur, dash] \arrow[dd, dash] & \\
& L_P \\
L \arrow[ur, dash] &
\end{tikzcd}$$

Let $\hat{\mathcal{O}}_P \subseteq L_P$ be the valuation ring of L_P and let $\pi \in L^\times$ be a uniformising parameter at P (i. e. $\operatorname{ord}_P(\pi) = 1$). We claim

$$L_P^{\mathrm{ab},\ell} = \bigcup_{n\in\mathbb{N}} L_P(\pi^{1/\ell^n}),$$

so that $L_P^{\mathrm{ab},\ell}$ is seen to be the localisation (i. e. union of the completions of all finite subextensions) of $L^{\mathrm{ab},\ell}$. Indeed, $L_P^{\mathrm{ab},\ell}$ is the union of all fields $L_P(x^{1/\ell^n})$ with $x \in L_P^\times$ and $n \in \mathbb{N}$. We can write $x = \pi^m u$ with $m \in \mathbb{Z}$ and $u \in \hat{\mathcal{O}}_P^\times$. The polynomial $X^{\ell^n} - u$ splits into distinct linear factors over $\hat{\mathcal{O}}_P/(\pi) \cong k$, hence over L_P by Hensel's lemma. Thus $L_P(x^{1/\ell^n}) = L_P(\pi^{m/\ell^n})$, which proves the claim.

Now the decomposition subgroup of P is the image of the restriction homomorphism

$$\operatorname{Gal}(L_P^{\mathrm{ab},\ell}|L_P) \longrightarrow \operatorname{Gal}(L^{\mathrm{ab},\ell}|L).$$

Under the Kummer isomorphism, this corresponds to the restriction of functions $L_P^\times \to \mathbb{T}_\ell$ to $L^\times$, so we have to show that a homomorphism $f : L^\times \to \mathbb{T}_\ell$ extends to $L_P^\times$ if and only if it factors over $\operatorname{ord}_P : L^\times \to \mathbb{Z}$. One implication is easy, so suppose that f extends to a homomorphism $\tilde{f} : L_P^\times \to \mathbb{T}_\ell$. Since $\hat{\mathcal{O}}_P^\times$ is ℓ-divisible, $\tilde{f}$ is trivial on $\hat{\mathcal{O}}_P^\times$, hence factors over $\operatorname{ord}_P : L_P^\times \to \mathbb{Z}$. Then f factors also over $\operatorname{ord}_P : L^\times \to \mathbb{Z}$. □

Definition 6.5. Let C be a complete nonsingular curve over k and L its function field. For a point P on C, we define $\underline{P} \subseteq \operatorname{Gal}(L^{\mathrm{ab},\ell}|L)$ to be the decomposition subgroup of the discrete valuation ord_P on L. We think of $\underline{P}$ as the point P encoded in the Galois group of $L^{\mathrm{ab},\ell}|L$.

Proposition 6.6. *Let C be a complete nonsingular curve over k with function field L. Then the decompositition subgroups $\underline{P}$ for $P \in C$ are $\mathbb{Z}_\ell$-linearly disjoint in* $\operatorname{Gal}(L^{\mathrm{ab},\ell}|L)$*, i. e. the natural homomorphism*

$$\bigoplus_{P\in C} \underline{P} \longrightarrow \operatorname{Gal}(L^{\mathrm{ab},\ell}|L)$$

is injective. In particular, if $\sigma \in \operatorname{Gal}(L^{\mathrm{ab},\ell}|L)$ is contained in the decomposition subgroups of two distinct points, then $\sigma = 1$.

Proof. Let $P_1, \ldots, P_r \in C$ be distinct points and $\sigma_i \in \underline{P_i}$ such that $\sigma_1 \cdots \sigma_r = 1$. Then the σ_i correspond to normalised delta functions $f_i : C \to \mathbb{T}_\ell$ at P_i such that $f_1 + \ldots + f_r$ is constant. Since the f_i vanish almost everywhere, we have in fact $f_1 + \ldots + f_r = 0$. Evaluating at P_i, we see $f_i(P_i) = 0$, thus all f_i are zero and $\sigma_1 = \ldots = \sigma_r = 1$. □

Proposition 6.7. *Let C be a complete nonsingular curve over k with function field L. Then Φ_L is the closed subgroup of* $\operatorname{Gal}(L^{\mathrm{ab},\ell}|L)$ *topologically generated by the decomposition subgroups $\underline{P}$ for $P \in C$.*

Proof. Φ_L is closed in $\mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$ by proposition 6.2. It suffices to show that $\mathrm{Map}(C, \mathbb{T}_\ell)$ is topologically spanned by the delta functions. The delta functions generate the maps with finite support and we prove that these are dense in $\mathrm{Map}(C, \mathbb{T}_\ell)$. We have to show that every non-empty open subset V of $\mathrm{Map}(C, \mathbb{T}_\ell)$ contains a map with finite support. We may assume that V is of the form $V = \mathcal{U}(K_1, U_1) \cap \ldots \cap \mathcal{U}(K_r, U_r)$ with $K_i \subseteq C$ finite and $U_i \subseteq \mathbb{T}_\ell$ open. Let f be an element in V. Then the function

$$\tilde{f}(P) = \begin{cases} f(P), & P \in K_1 \cup \ldots \cup K_r, \\ 0, & P \notin K_1 \cup \ldots \cup K_r \end{cases}$$

is in V and has finite support. □

Behaviour of Decomposition Subgroups under Morphisms of Curves

For the remainder of the section, let k be an algebraically closed ground field, ℓ a prime number not equal to the characteristic of k, and $F|k$ an algebraically closed extension of transcendence degree one. We keep the notation $G = \mathrm{Aut}(F|k)$ and $U_L = \mathrm{Aut}(F|L)$ from section 2. Recall that U_L is isomorphic to the absolute Galois group of L via the restriction $\mathrm{Aut}(F|L) \to \mathrm{Gal}(L^{\mathrm{sep}}|L)$, so that we have an isomorphism $U_L^{\mathrm{ab},\ell} \cong \mathrm{Gal}(L^{\mathrm{ab},\ell}|L)$, where $U_L^{\mathrm{ab},\ell}$ denotes the maximal pro-ℓ abelian quotient of U_L, i. e. the projective limit of all quotients U_L/N with N an open normal subgroup such that U_L/N is an abelian ℓ-group.

Lemma 6.8. *Let $L|k$ be a function field in F, let $\sigma \in G$ be an automorphism of $F|k$ and define $L' = \sigma L$. Let C and C' be complete nonsingular models of L and L', respectively, and let $\phi_\sigma : C' \xrightarrow{\sim} C$ be the isomorphism induced by σ. Denote by $\mathrm{ad}(\sigma) : U_L^{\mathrm{ab},\ell} \xrightarrow{\sim} U_{L'}^{\mathrm{ab},\ell}$ the isomorphism induced by conjugation with σ. Then the following square is commutative:*

$$\begin{tikzcd}
\mathrm{Map}(C, \mathbb{T}_\ell) \arrow[r] \arrow[d, "-\circ\phi_\sigma"] & U_L^{\mathrm{ab},\ell} \arrow[d, "\mathrm{ad}(\sigma)"] \\
\mathrm{Map}(C', \mathbb{T}_\ell) \arrow[r] & U_{L'}^{\mathrm{ab},\ell}
\end{tikzcd}$$

Proof. It suffices to show that both squares in the following diagram commute:

$$\begin{tikzcd}
\mathrm{Hom}(\mathrm{Div}^0(C), \mathbb{T}_\ell) \arrow[r, "-\circ\mathrm{div}"] \arrow[d, "-\circ(\phi_\sigma)_*"] & \mathrm{Hom}(L^\times, \mathbb{T}_\ell) \arrow[r] \arrow[d, "-\circ\sigma^{-1}"] & U_L^{\mathrm{ab},\ell} \arrow[d, "\mathrm{ad}(\sigma)"] \\
\mathrm{Hom}(\mathrm{Div}^0(C'), \mathbb{T}_\ell) \arrow[r, "-\circ\mathrm{div}"] & \mathrm{Hom}(L'^\times, \mathbb{T}_\ell) \arrow[r] & U_{L'}^{\mathrm{ab},\ell}
\end{tikzcd}$$

The commutativity of the left square follows from the commutativity of

$$\begin{tikzcd}
L'^{\times} \arrow[r, "\mathrm{div}"] \arrow[d, "\sigma^{-1}"] & \mathrm{Div}^0(C') \arrow[d, "(\phi_\sigma)_*"] \\
L^{\times} \arrow[r, "\mathrm{div}"] & \mathrm{Div}^0(C)
\end{tikzcd}$$

which in turn follows from $\mathrm{ord}_{P'} \circ \sigma = \mathrm{ord}_{\phi_\sigma(P')}$ for $P' \in C'$.

For the right square, let $\tau \in U_L$ and $x \in L^{\times}$. Then we have

$$\begin{aligned}
\langle \sigma\tau\sigma^{-1}, x\rangle_n &= \frac{\sigma\tau\sigma^{-1}(\sqrt[\ell^n]{x})}{\sqrt[\ell^n]{x}} \\
&= \sigma\Big(\frac{\tau(\sqrt[\ell^n]{\sigma^{-1}(x)})}{\sqrt[\ell^n]{\sigma^{-1}(x)}}\Big) \\
&= \sigma\big(\langle \tau, \sigma^{-1}(x)\rangle_n\big) \\
&= \langle \tau, \sigma^{-1}(x)\rangle_n,
\end{aligned}$$

which implies the commutativity. □

Given an inclusion $L_1 \subseteq L_2$ of function fields in F, we have an inclusion $U_{L_2} \subseteq U_{L_1}$ between the corresponding automorphism groups. This induces two homomorphisms between their maximal pro-ℓ abelian quotients: The first, $\mathrm{res} : U_{L_2}^{\mathrm{ab},\ell} \to U_{L_1}^{\mathrm{ab},\ell}$, comes from the functoriality of passing to the maximal pro-ℓ abelian quotient and can also be regarded as the restriction homomorphism $\mathrm{Gal}(L_2^{\mathrm{ab},\ell}|L_2) \to \mathrm{Gal}(L_1^{\mathrm{ab},\ell}|L_1)$. The second is the pro-$\ell$ **transfer homomorphism** $\mathrm{Ver} : U_{L_1}^{\mathrm{ab},\ell} \to U_{L_2}^{\mathrm{ab},\ell}$ (*Verlagerung* in German) from group cohomology (see the discussion above Prop. 1.5.9 in [NSW08] for a definition). The following proposition relates these two homomorphisms with the pullback and pushforward map of divisors.

Proposition 6.9. *Let $L_1 \subseteq L_2$ be an inclusion of function fields in F, let C_1, C_2 be complete nonsingular models, let $\phi : C_2 \to C_1$ be the dominant morphism corresponding to $L_1 \hookrightarrow L_2$ and let $\deg_i(\phi) = [L_2 : L_1]_i$ be its degree of inseparability. Let $\alpha_j : \mathrm{Hom}(\mathrm{Div}^0(C_j), \mathbb{T}_\ell) \to U_{L_j}^{\mathrm{ab},\ell}$ be the injective homomorphism with image Φ_{L_j} for $j = 1, 2$. Then the following squares commute:*

$$\begin{tikzcd}
\mathrm{Hom}(\mathrm{Div}^0(C_2), \mathbb{T}_\ell) \arrow[r, "\alpha_2"] \arrow[d, "-\circ\phi^*"] & U_{L_2}^{\mathrm{ab},\ell} \arrow[d, "\mathrm{res}"] \\
\mathrm{Hom}(\mathrm{Div}^0(C_1), \mathbb{T}_\ell) \arrow[r, "\alpha_1"] & U_{L_1}^{\mathrm{ab},\ell}
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathrm{Hom}(\mathrm{Div}^0(C_2), \mathbb{T}_\ell) \arrow[r, "\alpha_2"] & U_{L_2}^{\mathrm{ab},\ell} \\
\mathrm{Hom}(\mathrm{Div}^0(C_1), \mathbb{T}_\ell) \arrow[r, "\alpha_1"] \arrow[u, "\deg_i(\phi)^{-1}\cdot(-\circ\phi_*)"] & U_{L_1}^{\mathrm{ab},\ell} \arrow[u, "\mathrm{Ver}"']
\end{tikzcd}$$

In particular $\mathrm{res}(\Phi_{L_2}) \subseteq \Phi_{L_1}$ *and* $\mathrm{Ver}(\Phi_{L_1}) \subseteq \Phi_{L_2}$.

(Note that multiplication by $\deg_i(\phi)^{-1}$ on $\mathbb{T}_\ell$ makes sense since the degree of inseparability is either 1 or a power of the characteristic of k, which is invertible in $\mathbb{Z}_\ell$.)

Proof. Let $f \in \operatorname{Hom}(\operatorname{Div}^0(C_2), \mathbb{T}_\ell)$. Denote by f also a map $C_2 \to \mathbb{T}_\ell$ with

$$f\Big(\sum_P n_P P\Big) = \sum_P n_P f(P),$$

and by ϕ^* the inclusion $L_1 \hookrightarrow L_2$. For $x \in L_1^\times$ we have

$$\begin{aligned}
\big\langle \operatorname{res}(\alpha_2(f)), x\big\rangle &= \big\langle \alpha_2(f), \phi^*(x)\big\rangle \\
&= \sum_{P \in C_2} \operatorname{ord}_P(\phi^*(x)) f(P) \\
&= \sum_{P \in C_2} e(P|\phi(P)) \operatorname{ord}_{\phi(P)}(x) f(P) \\
&= \sum_{Q \in C_1} \sum_{P \in \phi^{-1}(Q)} e(P|Q) \operatorname{ord}_Q(x) f(P) \\
&= \sum_{Q \in C_1} \operatorname{ord}_Q(x) f(\phi^*(Q)) \\
&= \big\langle \alpha_1(f \circ \phi^*), x\big\rangle.
\end{aligned}$$

For the second square, assume first that ϕ is separable. Let us add two terms in the middle, so we get the following diagram:

$$\begin{tikzcd}
\operatorname{Hom}(\operatorname{Div}^0(C_2), \mathbb{T}_\ell) \arrow[r, "-\circ \operatorname{div}"] & \operatorname{Hom}(L_2^\times, \mathbb{T}_\ell) \arrow[r] & U_{L_2}^{\mathrm{ab},\ell} \\
\operatorname{Hom}(\operatorname{Div}^0(C_1), \mathbb{T}_\ell) \arrow[r, "-\circ \operatorname{div}"] \arrow[u, "-\circ\phi_*"] & \operatorname{Hom}(L_1^\times, \mathbb{T}_\ell) \arrow[r] \arrow[u, "-\circ \operatorname{Nm}"] & U_{L_1}^{\mathrm{ab},\ell} \arrow[u, "\operatorname{Ver}"]
\end{tikzcd}$$

Here, $\operatorname{Nm} : L_2^\times \to L_1^\times$ denotes the norm homomorphism. The square on the left commutes because the norm and the pushforward satisfy the formula $\operatorname{div}(\operatorname{Nm} x) = \phi_*(\operatorname{div}(x))$ for $x \in L_2^\times$ ([Liu02], Ex. 7.2.6(c)). So it just remains to prove the commutativity of the right square which amounts to the formula

$$\langle \operatorname{Ver} \sigma, x\rangle_n = \langle \sigma, \operatorname{Nm} x\rangle_n \tag{6.2}$$

for $\sigma \in U_{L_1}^{\mathrm{ab},\ell}$, $x \in L_2^\times$ and $n \in \mathbb{N}$. For this, we use the fact that the corestriction homomorphism from group cohomology commutes with the connecting homomorphisms of the long exact cohomology sequence ([NSW08], Prop. 1.5.2) and is given by the norm in degree zero. Let us apply this to the exact sequence of U_{L_1}-modules

$$1 \longrightarrow \mu_{\ell^n} \longrightarrow (L_1^{\mathrm{sep}})^\times \xrightarrow{(-)^{\ell^n}} (L_1^{\mathrm{sep}})^\times \longrightarrow 1$$

with respect to the open subgroup $U_{L_2} \subseteq U_{L_1}$. This yields a commutative square

$$\begin{tikzcd}
L_2^\times \arrow[r, "\delta"] \arrow[d, "\mathrm{cor}"] & \mathrm{Hom}(U_{L_2}^{\mathrm{ab},\ell}, \mu_{\ell^n}) \arrow[d, "\mathrm{cor}"] \\
L_1^\times \arrow[r, "\delta"] & \mathrm{Hom}(U_{L_1}^{\mathrm{ab},\ell}, \mu_{\ell^n})
\end{tikzcd}$$

where the connecting homomorphisms are given by $\delta(x)(\sigma) = \langle \sigma, x \rangle_n$. Choosing a primitive ℓ^n-th root of unity defines an injective homomorphism of trivial U_{L_1}-modules $\mu_{\ell^n} \cong \frac{1}{\ell^n}\mathbb{Z}/\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}$ and gives a commutative diagram

$$\begin{tikzcd}
L_2^\times \arrow[r, "\delta"] \arrow[d, "\mathrm{Nm}"] & \mathrm{Hom}(U_{L_2}^{\mathrm{ab},\ell}, \mu_{\ell^n}) \arrow[r, hook] \arrow[d, "\mathrm{cor}"] & \mathrm{Hom}(U_{L_2}^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z}) \arrow[d, "\mathrm{cor}"] \\
L_1^\times \arrow[r, "\delta"] & \mathrm{Hom}(U_{L_2}^{\mathrm{ab},\ell}, \mu_{\ell^n}) \arrow[r, hook] & \mathrm{Hom}(U_{L_1}^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z})
\end{tikzcd}$$

The vertical map on the right is (by definition, if you want) the Pontryagin dual of the transfer homomorphism, i. e. it is given by $f \mapsto f \circ \mathrm{Ver}$. Thus, the middle vertical map is also given by $f \mapsto f \circ \mathrm{Ver}$. Writing out the commutativity of the left square and using $\delta(x)(\sigma) = \langle \sigma, x \rangle_n$, we get the desired formula (6.2).

Now assume that ϕ is purely inseparable of degree p^n, i. e. $L_2 = L_1^{p^{-n}}$. Then over each point of C_1 lies exactly one point of C_2, the ramification index being p^n. Therefore, $\phi_* \circ \phi^*$ is just multiplication by p^n on $\mathrm{Div}^0(C_1)$. Moreover, we have $U_{L_1} = U_{L_2}$ and the restriction and transfer map are the identity. In the diagram

$$\begin{tikzcd}
\mathrm{Hom}(\mathrm{Div}^0(C_2), \mathbb{T}_\ell) \arrow[r, "\alpha_2"] \arrow[d, swap, "p^{-n}\cdot(-\circ\phi_*)"] & U_{L_2}^{\mathrm{ab},\ell} \arrow[d, "\mathrm{Ver}=\mathrm{id}"] \\
\mathrm{Hom}(\mathrm{Div}^0(C_1), \mathbb{T}_\ell) \arrow[r, "\alpha_1"] \arrow[d, swap, "-\circ\phi^*"] & U_{L_1}^{\mathrm{ab},\ell} \arrow[d, "\mathrm{res}=\mathrm{id}"] \\
\mathrm{Hom}(\mathrm{Div}^0(C_2), \mathbb{T}_\ell) \arrow[r, "\alpha_2"] & U_{L_2}^{\mathrm{ab},\ell}
\end{tikzcd}$$

the lower square and the outer rectangle commute, hence so does the upper square.

Since a general morphism can be factored into a separable and a purely inseparable morphism and everything behaves functorially with respect to composition, we are done. □

Corollary 6.10. *Let U be a compact open subgroup of G. Then the notion of a decomposition subgroup in $U^{\mathrm{ab},\ell}$ is independent of the choice of L with $U = U_L$.*

Proof. This follows from the second square applied to a purely inseparable extension. □

The following corollary shows that, given an inclusion $L_1 \subseteq L_2$ of function fields in F, the corresponding map $\phi : C_2 \to C_1$ between their complete nonsingular models can be seen group-theoretically on the level of decomposition subgroups. We can also recover some information about the ramification indices, namely their ℓ-part for $\ell \neq \mathrm{char}(k)$.

Corollary 6.11. *In the situation of proposition 6.9, let $P \in C_2$ and $Q \in C_1$ such that $\phi(P) = Q$. Then $\underline{Q}$ is the unique decomposition subgroup of $U_{L_1}^{\mathrm{ab},\ell}$ containing $\mathrm{res}(\underline{P})$, the index is finite and equals the ℓ-part of the ramification index:*

$$(\underline{Q} : \mathrm{res}(\underline{P})) = \ell^{v_\ell(e(P|Q))}.$$

Proof. By proposition 6.4, every element σ in $\underline{P}$ comes from a delta function f at P, say $f(P') = \delta_{PP'}\omega$. By proposition 6.9, $\mathrm{res}(\sigma)$ is induced by the map

$$Q' \longmapsto \sum_{P' \in \phi^{-1}(Q')} e(P'|Q') f(P') = e(P|Q)\delta_{QQ'}\omega.$$

This shows that $\mathrm{res}(\underline{P}) = e(P|Q)\,\underline{Q} \subseteq \underline{Q}$. The quotient is isomorphic to

$$\underline{Q}/\,\mathrm{res}(\underline{P}) \cong \mathbb{T}_\ell / e(P|Q)\mathbb{T}_\ell \cong \mathbb{Z}_\ell / e(P|Q)\mathbb{Z}_\ell,$$

whose order is the ℓ-part of $e(P|Q)$ since the prime-to-ℓ part is invertible in $\mathbb{Z}_\ell$ and $\mathbb{Z}_\ell/\ell^v\mathbb{Z}_\ell \cong \mathbb{Z}/\ell^v\mathbb{Z}$. For $Q' \neq Q$, the decomposition subgroup $\underline{Q'}$ cannot contain $\mathrm{res}(\underline{P})$ since $\underline{Q} \cap \underline{Q'} = 1$ but $\mathrm{res}(\underline{P})$ contains nontrivial elements. □

7 Detecting Decomposition Subgroups: Rational Curves

Let $F|k$, G and ℓ be as before. As a further step towards the main result, we aim to describe the decomposition subgroups in $U_L^{\mathrm{ab},\ell}$ for $L = k(x)$ a rational function field in a group-theoretic way, so as to prove the following proposition.

Proposition 7.1. *Let (k', F', G') and $\lambda : G \xrightarrow{\sim} G'$ be as in theorem B and let $L|k$ and $L'|k'$ be rational function fields in F and F' such that $\lambda^{-1}(U_{L'}) = U_L$. Then the isomorphism $\lambda^{\mathrm{ab},\ell} : U_L^{\mathrm{ab},\ell} \xrightarrow{\sim} U_{L'}^{\mathrm{ab},\ell}$ induces a bijection*

$$\{\, \textit{decomposition subgroups of } U_{L'}^{\mathrm{ab},\ell} \,\} \xrightarrow{\ \sim\ } \{\, \textit{decomposition subgroups of } U_L^{\mathrm{ab},\ell} \,\},$$

given by $D' \mapsto (\lambda^{\mathrm{ab},\ell})^{-1}(D')$.

Lemma 7.2. *For the function field $k(x)$ of a rational curve, we have*

$$\Phi_{k(x)} = U_{k(x)}^{\mathrm{ab},\ell}.$$

Proof. Let C be a complete nonsingular model of $k(x)$. We have to show that

$$- \circ \mathrm{div} : \mathrm{Hom}(\mathrm{Div}^0(C), \mathbb{T}_\ell) \to \mathrm{Hom}(k(x)^\times, \mathbb{T}_\ell)$$

is surjective. Since C is a rational curve, every degree zero divisor is the divisor of a rational function, i. e. we have an exact sequence

$$1 \longrightarrow k^\times \longrightarrow k(x)^\times \xrightarrow{\text{div}} \operatorname{Div}^0(C) \longrightarrow 1.$$

Applying the functor $\operatorname{Hom}(-, \mathbb{T}_\ell)$, we get another exact sequence

$$1 \longrightarrow \operatorname{Hom}(\operatorname{Div}^0(C), \mathbb{T}_\ell) \xrightarrow{-\circ\text{div}} \operatorname{Hom}(k(x)^\times, \mathbb{T}_\ell) \longrightarrow \operatorname{Hom}(k^\times, \mathbb{T}_\ell).$$

Since $k^\times$ is ℓ-divisible, the right group is trivial and therefore $- \circ \operatorname{div}$ is surjective. □

Lemma 7.3. *Let $L|k$ be a rational function field in F with complete nonsingular model C and define $H = \{\sigma \in G : \sigma L = L\}$. For $\sigma \in H$, let $\phi_\sigma \in \operatorname{Aut}(C)$ be the corresponding automorphism of C, and let $\operatorname{ad}(\sigma) \in \operatorname{Aut}(U_L^{\text{ab},\ell})$ be induced by conjugation with σ. Then an element of $U_L^{\text{ab},\ell}$ belongs to the decomposition subgroup of a point $P \in C$ if and only if it is fixed under $\operatorname{ad}(\sigma)$ for all σ in the stabiliser $\operatorname{Stab}_H(P) = \{\sigma \in H : \phi_\sigma(P) = P\}$.*

Proof. By lemma 6.8, we have for all $\sigma \in H$ a commutative square

$$\begin{tikzcd}
\operatorname{Map}(C, \mathbb{T}_\ell) \arrow[r, two heads] \arrow[d, "-\circ\phi_\sigma"] & U_L^{\text{ab},\ell} \arrow[d, "\operatorname{ad}(\sigma)"] \\
\operatorname{Map}(C, \mathbb{T}_\ell) \arrow[r, two heads] & U_L^{\text{ab},\ell}
\end{tikzcd}$$

with surjective horizontal arrows by lemma 7.2. Thus, we have to prove that $f : C \to \mathbb{T}_\ell$ is a delta function at P if and only if $f \circ \phi_\sigma = f$ for all $\sigma \in \operatorname{Stab}_H(P)$. Since C is a rational curve, the action of $\operatorname{Aut}(C)$ on C is 3-transitive, so there exists for all $Q, Q' \in C \setminus \{P\}$ an element $\sigma \in N$ satisfying $\phi_\sigma(Q) = Q'$ and $\phi_\sigma(P) = P$. Thus, if $f \circ \phi_\sigma = f$ for all $\phi_\sigma \in \operatorname{Stab}_H(P)$, then f is constant on $C \setminus \{P\}$ and is therefore a delta function at P. The converse is clear. □

In order to detect the decomposition subgroups of $U_{k(x)}^{\text{ab}}$ group-theoretically, we are lead by the previous proposition to the question how we can group-theoretically characterise the stabiliser subgroups of $\operatorname{Aut}(\mathbb{P}^1)$.

Lemma 7.4. *A subgroup of $\operatorname{Aut}(\mathbb{P}^1)$ is the stabiliser subgroup of a point $P \in \mathbb{P}^1$ if and only if it is maximal among the subgroups H with the property that H is infinite, solvable and contains no abelian subgroup of finite index.*

Proof. We first show that every stabiliser subgroup of $\operatorname{Aut}(\mathbb{P}^1)$ has the claimed properties. Since the action is transitive, all stabilisers are conjugate to each other, so it suffices to consider $\operatorname{Stab}(\infty)$. Let us write simply $\frac{az+b}{cz+d}$ for the automorphism of $\mathbb{P}^1$ that sends $z \in \mathbb{P}^1$ to $\frac{az+b}{cz+d}$. The stabiliser subgroup of $\infty \in \mathbb{P}^1$ consists then of the automorphisms $az + b$ with $a \in k^\times$ and $b \in k$. The translations $z + b$ form a normal subgroup and $\operatorname{Stab}(\infty)$ is solvable via the resolution

$$1 \lhd (\text{translations}) \lhd \operatorname{Stab}(\infty)$$

with abelian quotients k and $k^\times$ respectively. Furthermore, $\mathrm{Stab}(\infty)$ is infinite since k is. Assume $K \leq \mathrm{Stab}(\infty)$ is a subgroup of finite index. As in the proof of lemma 4.7, K must contain a non-trivial translation $z+b$ and homothety az, which do not commute, so that K is not abelian. Therefore, $\mathrm{Stab}(\infty)$ has the claimed properties.

Now let $H \leq \mathrm{Aut}(\mathbb{P}^1)$ be any infinite solvable subgroup with no abelian subgroup of finite index. We have to prove that H is contained in the stabiliser subgroup of a point $P \in \mathbb{P}^1$. Let

$$1 \lhd H_1 \lhd H_2 \lhd \ldots \lhd H_r = H$$

be a resolution of H with non-trivial abelian quotients H_{i+1}/H_i. Let $\varphi \in H_1$, $\varphi \neq 1$, and consider the fixed points of φ. Since a linear automorphism of $k \times k$ which is not a scalar multiple of the identity has one or two 1-dimensional eigenspaces, φ has one or two fixed points in $\mathbb{P}^1$. Assume first that φ has only one fixed point $P \in \mathbb{P}^1$. In the subsequent arguments we make repeated use of the following simple fact:

> If P is a fixed point of φ and $\psi \in \mathrm{Aut}(\mathbb{P}^1)$ is arbitrary, then $\psi(P)$ is a fixed point of $\psi\varphi\psi^{-1}$.

Here, we have $\psi\varphi\psi^{-1} = \varphi$ for all $\psi \in H_1$ since H_1 is abelian, thus $\psi(P)$ is again a fixed point of φ. But we assumed that P is the only fixed point of φ, hence $\psi(P) = P$ for all $\psi \in H_1$. We prove inductively that P is a global fixed point of H. Assume we already know that P is a global fixed point of H_{i-1} where $2 \leq i \leq r$. Then for all $\psi \in H_i$, the point $\psi(P)$ is a global fixed point of $\psi H_{i-1}\psi^{-1}$, which equals H_{i-1} by normality. In particular, $\psi(P)$ is fixed by φ, thus $\psi(P) = P$. This proves the induction and shows that H is contained in the stabiliser subgroup of P.

Now consider the case where $\varphi \in H_1$ has two distinct fixed points. After replacing H with a suitable conjugate, we may assume that the set of fixed points of φ is $\{0, \infty\}$. Since $\psi\varphi\psi^{-1} = \varphi$ for all $\psi \in H_1$, every element of H_1 either fixes or interchanges 0 and ∞. If the same is true for all elements of H, then H contains only elements of the form az or a/z with $a \in k^\times$. In this case, the elements of the type az form an abelian subgroup of index ≤ 2, which contradicts our assumption. Thus, H contains an element that neither fixes nor interchanges $0, \infty$. Let $\psi \in H_i$ be such an element with $i \in \{2, \ldots, r\}$ minimal, so that all elements of H_{i-1} permute $\{0, \infty\}$. Then $\psi\varphi\psi^{-1} \in H_{i-1}$ permutes $\{0, \infty\}$, but its set of fixed points is $\{\psi(0), \psi(\infty)\} \neq \{0, \infty\}$, so it must interchange $0, \infty$. This means that $\psi\varphi\psi^{-1}$ is of the form a/z for some $a \in k^\times$. Since we may replace H with a suitable conjugate $\rho H \rho^{-1}$ where $\rho \in \mathrm{Aut}(\mathbb{P}^1)$ fixes 0 and ∞, we can assume $a = 1$. We see that φ has order 2, hence $\varphi(z) = -z$. The same argument with other elements of H_{i-1} taking the role of φ shows that $\pm z$ are the only elements of H_{i-1} that fix $0, \infty$. If $c/z \in H_{i-1}$ is an element interchanging $0, \infty$, then $(c/z) \circ (1/z) = cz$ is contained in H_{i-1} and fixes $0, \infty$, thus $c = \pm 1$. Altogether, this proves that H_{i-1} is a finite group consisting of the four elements

$$H_{i-1} = \left\{ z, -z, \frac{1}{z}, -\frac{1}{z} \right\}.$$

We prove inductively that H is also finite. Assume we have already established the finiteness of H_{j-1} where $i \leq j \leq r$. Let S be the set of all points in $\mathbb{P}^1$ that are fixed by some non-identity element in H_{j-1}. This is then a finite set containing at least the six elements $\{0, \infty, 1, -1, i, -i\}$ which are fixed points of elements in H_{i-1}. For $\psi \in H_j$ and $P \in S$, the point $\psi(P)$ is fixed by a non-identity element in $\psi H_{j-1}\psi^{-1} = H_{j-1}$, thus $\psi(P) \in S$. Hence H_j acts by permutations on S. Since a Möbius transformation is determined by the image of any three distinct points, the action is faithful and H_j embeds into the symmetric group over S. This shows inductively that H is finite, again contradicting our assumption. □

Now we can prove the main result of this section.

Proof of proposition 7.1. Let $H := \{\sigma \in G : \sigma L = L\}$ and define H' similarly. Then H consists precisely of those elements of G that normalise U_L and are infinitely ℓ-divisible in $N_G(U_L)/U_L$ (using 4.2, 4.5 and 4.6), hence $\lambda(H) = H'$. Let C and C' be complete nonsingular models of L and L'. In lemma 7.4 we described group-theoretically the stabiliser subgroups for the right-actions of H on C and of H' on C', therefore the isomorphism $\lambda : H \xrightarrow{\sim} H'$ induces a bijection between those sets of stabiliser subgroups. Let P be a point on C and let $P' \in C'$ such that $\mathrm{Stab}_H(P)$ is mapped isomorphically to $\mathrm{Stab}_{H'}(P')$. For $\sigma \in H$ and $\sigma' = \lambda(\sigma) \in H'$, the square

$$\begin{tikzcd}
U_L^{\mathrm{ab},\ell} \arrow[r, "\lambda^{\mathrm{ab},\ell}", "\sim"'] \arrow[d, "\mathrm{ad}(\sigma)"] & U_{L'}^{\mathrm{ab},\ell} \arrow[d, "\mathrm{ad}(\sigma')"] \\
U_L^{\mathrm{ab},\ell} \arrow[r, "\lambda^{\mathrm{ab},\ell}", "\sim"'] & U_{L'}^{\mathrm{ab},\ell}
\end{tikzcd}$$

commutes, so that the fixed points of $\mathrm{ad}(\sigma)$ are mapped by $\lambda^{\mathrm{ab},\ell}$ to fixed points of $\mathrm{ad}(\sigma')$. By our description of decomposition subgroups in lemma 7.3, $\lambda^{\mathrm{ab},\ell}$ maps $\underline{P}$ isomorphically to $\underline{P'}$. □

8 Detecting Decomposition Subgroups: General Curves

In this section we will prove for general curves the result that we proved for rational curves in the previous section. As before, we fix an algebraically closed ground field k, an algebraically closed extension $F|k$ of transcendence degree one with automorphism group $G = \mathrm{Aut}(F|k)$, and a prime number $\ell \neq \mathrm{char}(k)$.

Proposition 8.1. *Let (k', F', G') and $\lambda : G \xrightarrow{\sim} G'$ be as in theorem B and let $L|k$ and $L'|k'$ be function fields in F and F' such that $\lambda^{-1}(U_{L'}) = U_L$. Then $\lambda^{\mathrm{ab},\ell} : U_L^{\mathrm{ab},\ell} \xrightarrow{\sim} U_{L'}^{\mathrm{ab},\ell}$ induces a bijection*

$$\{\, \textit{decomposition subgroups of } U_{L'}^{\mathrm{ab},\ell} \,\} \xrightarrow{\sim} \{\, \textit{decomposition subgroups of } U_L^{\mathrm{ab},\ell} \,\},$$

given by $D' \mapsto (\lambda^{\mathrm{ab},\ell})^{-1}(D')$.

We will first show that the isomorphism $\lambda^{\mathrm{ab},\ell} : U_L^{\mathrm{ab},\ell} \xrightarrow{\sim} U_{L'}^{\mathrm{ab},\ell}$ restricts to an isomorphism $\Phi_L \xrightarrow{\sim} \Phi_{L'}$.

Lemma 8.2 (Adjusting Degrees of Inseparability)**.** *Assume* $\operatorname{char}(k) = p > 0$*. If* L_1 *and* L_2 *are function fields in* F *such that* $L_1^i \subseteq L_2^i$*, then for every* $n \in \mathbb{N}_0$ *there exists a unique function field* $\tilde{L}_2$ *purely inseparably equivalent to* L_2 *such that* $L_1 \subseteq \tilde{L}_2$ *and* $[\tilde{L}_2 : L_1]_i = p^n$*. Similarly, there exists a unique function field* $\tilde{L}_1$ *purely inseparably equivalent to* L_1 *such that* $\tilde{L}_1 \subseteq L_2$ *and* $[L_2 : \tilde{L}_1]_i = p^n$*.*

Proof. Since $L_1 \subseteq L_2^i$ and $L_1|k$ is finitely generated, there exists $m \in \mathbb{N}_0$ such that $L_1^{p^m} \subseteq L_2$, or equivalently $L_1 \subseteq L_2^{p^{-m}}$. Replacing L_2 with $L_2^{p^{-m}}$, we may assume $L_1 \subseteq L_2$. Then replacing L_2 with the separable closure of L_1 in L_2, we may moreover assume that $L_2|L_1$ is separable. Then $\tilde{L}_2 := L_2^{p^{-n}}$ has the claimed properties and the uniqueness is clear.

The second claim follows from the first: If $\tilde{L}_2$ is given, $\tilde{L}_2 = L_2^{p^m}$ with $m \in \mathbb{Z}$, then we take $\tilde{L}_1 := L_1^{p^{-m}}$. □

Lemma 8.3. *Let* $L|k$ *be a function field in* F*. Then* Φ_L *is topologically spanned by the images of the pro-*ℓ *transfer maps* $\operatorname{Ver} : V^{\mathrm{ab},\ell} \to U_L^{\mathrm{ab},\ell}$ *where* V *runs through the compact open subgroups* $V \subseteq G$ *containing* U_L *such that* $V = U_{k(x)}$ *for some* $x \in F \setminus k$*.*

Proof. Let $V \subseteq G$ be a compact open subgroup as above. By the previous lemma, we can choose $x \in F \setminus k$ with $V = U_{k(x)}$ such that $k(x) \subseteq L$ and this extension is separable. By proposition 6.9, we have $\operatorname{Ver}(\Phi_{k(x)}) \subseteq \Phi_L$, and by lemma 7.2 we have $\Phi_{k(x)} = U_{k(x)}^{\mathrm{ab},\ell}$, so the image of $\operatorname{Ver} : V^{\mathrm{ab},\ell} \to U_L^{\mathrm{ab},\ell}$ is contained in Φ_L. Denoting by C a complete nonsingular model of $L|k$ and by $\phi : C \to \mathbb{P}^1$ the separable morphism corresponding to the inclusion $k(x) \subseteq L$, proposition 6.9 shows that we have a commutative square

$$\begin{tikzcd}
\operatorname{Map}(C, \mathbb{T}_\ell) \arrow[r] & U_L^{\mathrm{ab},\ell} \\
\operatorname{Map}(\mathbb{P}^1, \mathbb{T}_\ell) \arrow[r] \arrow[u, "- \circ \phi"] & U_{k(x)}^{\mathrm{ab},\ell}. \arrow[u, "\operatorname{Ver}"']
\end{tikzcd}$$

Since Φ_L is topologically spanned by the decomposition subgroups (proposition 6.7) it suffices to show that every normalised delta function is in the image of the left vertical map for some separable morphism $\phi : C \to \mathbb{P}^1$. So let $P \in C$ be a point and let $f(Q) = \delta_{P,Q}\,\omega$ be a normalised delta function at P. If g is the genus of C, then for $n \geq 2g+1$, the global sections $\Gamma(C, \mathcal{O}_C(nP))$ have dimension ≥ 2 over k by the Riemann-Roch theorem, so there exists $x \in L \setminus k$ with $nP + \operatorname{div}(x) \geq 0$. Then x has a pole of order $\leq n$ at P and has no other poles. If $\operatorname{char}(k) = p > 0$, we can replace x with $x^{p^{-m}}$ for suitable $m \in \mathbb{N}_0$ and assume that $L|k(x)$ is separable. Let $\phi : C \to \mathbb{P}^1$ be the corresponding separable morphism and let $h : \mathbb{P}^1 \to \mathbb{T}_\ell$ be the delta function at $\infty \in \mathbb{P}^1$ with value $\omega = f(P)$. Then we have

$$(h \circ \phi)(Q) = \delta_{\infty,\phi(Q)}\,\omega = \delta_{P,Q}\,\omega = f(Q),$$

so f is in the image of $\operatorname{Map}(\mathbb{P}^1, \mathbb{T}_\ell) \xrightarrow{-\circ\phi} \operatorname{Map}(C, \mathbb{T}_\ell)$. □

Lemma 8.4. *In the situation of proposition 8.1, $\lambda^{\mathrm{ab},\ell} : U_L^{\mathrm{ab},\ell} \xrightarrow{\sim} U_{L'}^{\mathrm{ab},\ell}$ restricts to an isomorphism $\Phi_L \xrightarrow{\sim} \Phi_{L'}$.*

Proof. If V runs through the compact open subgroups of G containing U_L such that $V = U_{k(x)}$ for some $x \in F \setminus k$, then $V' := \lambda(V)$ runs through the analogous set of compact open subgroups of G' containing $U_{L'}$ since V belongs to a rational function field iff V' does (proposition 4.1). Moreover, $\lambda^{\mathrm{ab},\ell}$ commutes with the transfer maps as in the diagram

$$\begin{tikzcd}
V^{\mathrm{ab},\ell} \arrow[r, "\lambda^{\mathrm{ab},\ell}"] \arrow[d, "\mathrm{Ver}"] & V'^{\mathrm{ab},\ell} \arrow[d, "\mathrm{Ver}"] \\
U_L^{\mathrm{ab},\ell} \arrow[r, "\lambda^{\mathrm{ab},\ell}"] & U_{L'}^{\mathrm{ab},\ell}
\end{tikzcd}$$

so the closed subgroup in $U_L^{\mathrm{ab},\ell}$ which is topologically generated by the images of all the transfers $V^{\mathrm{ab},\ell} \to U_L^{\mathrm{ab},\ell}$ is mapped by $\lambda^{\mathrm{ab},\ell}$ to the analogous subgroup of $U_{L'}^{\mathrm{ab},\ell}$. By lemma 8.3, this means $\lambda^{\mathrm{ab},\ell}(\Phi_L) = \Phi_{L'}$. □

We now characterise the decomposition subgroups of $U_L^{\mathrm{ab},\ell}$ as the maximal subgroups D with the property that D is contained in Φ_L and whenever $V \subseteq G$ is a compact open subgroup containing U_L such that $V = U_{k(x)}$ for some $x \in F \setminus k$, then the image of D under $\mathrm{res} : U_L^{\mathrm{ab},\ell} \to V^{\mathrm{ab},\ell}$ is a finite-index subgroup of a decomposition subgroup of $V^{\mathrm{ab},\ell}$. First, we need some lemmas.

Lemma 8.5 (Lemma 3.4′ in [Bog91]). *Let X be a set, $n \in \mathbb{N}_0$ and $f : \mathbb{P}_k^n \to X$ a function such that the restriction of f to any projective line is a delta function, i. e. constant outside a point. Then there exists a filtration of $\mathbb{P}^n$ by projective subspaces*

$$P_0 \subset P_1 \subset \ldots \subset P_r = \mathbb{P}^n$$

such that f is constant on P_0 and on $P_j \setminus P_{j-1}$ for $j = 1, \ldots, r$.

Proof. We proceed by induction on n, where the cases $n = 0, 1$ are trivial, so we may assume $n \geq 2$. For every hyperplane $H \subset \mathbb{P}^n$, the restriction of f to H satisfies again the hypotheses of the lemma, so by induction there exists a lower-dimensional subspace $E \subset H$ such that f is constant on $H \setminus E$. Thus, we may speak of the *generic value* of f on H and call E an *exceptional subspace* of H. Denote by $(\mathbb{P}^n)^\vee$ the set of hyperplanes in $\mathbb{P}^n$ and consider the function

$$\begin{aligned} f^\vee : (\mathbb{P}^n)^\vee &\longrightarrow X, \\ H &\longmapsto \text{generic value of } f \text{ on } H. \end{aligned}$$

We prove that $f^\vee$ is also a delta function, i. e. f takes the same generic value on all hyperplanes with at most a single exception. We can check this property on finite sets, so let $H_1, \ldots, H_s$ be hyperplanes with exceptional subspaces $E_1, \ldots, E_s$. We claim that there exists a projective line in $\mathbb{P}^n$ which simultaneously avoids $E_1, \ldots, E_s$. A line in $\mathbb{P}^n$ is given by a linear system $Ax = 0$ of $n-1$ equations such that the matrix A has full rank. We view A as a point in affine space $\mathbb{A}^{(n-1)(n+1)}$. Since the full rank condition is equivalent to the non-vanishing of all $(n-1) \times (n-1)$ minors, the set of all projective lines in $\mathbb{P}^n$ is parametrised by a non-empty Zariski-open subset of $\mathbb{A}^{(n-1)(n+1)}$. Let L be a line in $\mathbb{P}^n$, defined by $Ax = 0$, and let $B_i x = 0$ be a set of linear equations for the exceptional subspace $E_i \subset H_i$. Then L does not meet E_i if and only if the matrix $\begin{pmatrix} A \\ B_i \end{pmatrix}$ has rank $n+1$, which again is expressed via the non-vanishing of the $(n+1) \times (n+1)$ minors. Thus the set of all lines $L \subset \mathbb{P}^n$ avoiding E_i is parametrised by a Zariski-open subset U_i in $\mathbb{A}^{(n-1)(n+1)}$, which moreover is non-empty since $\operatorname{rank} B_i = n - \dim E_i \geq 2$. Since $\mathbb{A}^{(n-1)(n+1)}$ is irreducible, $U_1 \cap \ldots \cap U_s$ is again non-empty and open. Therefore, there exists a line $L \subset \mathbb{P}^n$ simultaneously avoiding all the subspaces $E_1, \ldots, E_s$. This line intersects the hyperplanes $H_1, \ldots, H_s$ in non-exceptional points $P_1, \ldots, P_s$, so we have $f^\vee(H_i) = f(P_i)$. Since f is a delta function on L, this shows that $f^\vee$ is a delta function on $\{H_1, \ldots, H_s\}$ and hence on $(\mathbb{P}^n)^\vee$.

Let $x_0 \in X$ be the generic value of $f^\vee$ and consider the set of exceptional points

$$S := \{P \in \mathbb{P}^n : f(P) \neq x_0\}.$$

Assume for contradiction that S is not contained in any hyperplane. Then there exists a subset $\{P_0, \ldots, P_n\} \subseteq S$ of $n+1$ points which is not contained in any hyperplane. Let H be a non-exceptional hyperplane (i. e. $f^\vee(H) = x_0$) containing n of the points, say $P_1, \ldots, P_n \in H$. But then at least one P_i lies outside the exceptional subspace of H, and we would have $f(P_i) = x_0$, contradicting $P_i \in S$. Therefore the set S of exceptional points is contained in a proper subspace of $\mathbb{P}^n$, and we are done by induction. □

Lemma 8.6. *Let k be an algebraically closed field and C a complete nonsingular curve of genus g over k. For two sheaves of $\mathcal{O}_C$-modules $\mathcal{F}, \mathcal{G}$, define*

$$S(\mathcal{F}, \mathcal{G}) := \operatorname{coker}\left[\Gamma(C, \mathcal{F}) \otimes_k \Gamma(C, \mathcal{G}) \longrightarrow \Gamma(C, \mathcal{F} \otimes_{\mathcal{O}_C} \mathcal{G})\right].$$

Then the following is true:

(a) If $\mathcal{F}$ has finite support and $\mathcal{L}$ is an invertible sheaf without base points, then $S(\mathcal{F}, \mathcal{L}) = 0$.

(b) If $\mathcal{L}, \mathcal{L}'$ are invertible sheaves, $\mathcal{L}'$ has no base points and $H^1(C, \mathcal{L} \otimes \mathcal{L}'^\vee) = 0$, then $S(\mathcal{L}, \mathcal{L}') = 0$.

(c) If $\mathcal{L}, \mathcal{L}'$ are invertible sheaves of degree $\geq 4g$, then $S(\mathcal{L}, \mathcal{L}') = 0$.

Lemma 8.6(c) is lemma 3.3 in [Rov03], but for the proof we prefer to (roughly) follow Mumford's proof of his "generalised lemma of Castelnuovo" ([Mum11], theorem 2). With a little more work, he proves that 8.6(c) holds with the weaker hypotheses $\deg(\mathcal{L}) \geq 2g+1$ and $\deg(\mathcal{L}') \geq 2g$ (loc. cit, theorem 6).

Proof. For the sake of brevity, let us write $\Gamma(\mathcal{F})$ and $H^1(\mathcal{F})$ instead of $\Gamma(C,\mathcal{F})$ and $H^1(C,\mathcal{F})$.

(a) For every $P \in \operatorname{Supp}\mathcal{F}$, the set $\{t \in \Gamma(\mathcal{L}) : t_P \in \mathfrak{m}_P\mathcal{L}_P\}$ is a hyperplane in $\Gamma(\mathcal{L})$ since $\mathcal{L}$ has no base points. Thus there exists $t \in \Gamma(\mathcal{L})$ such that $t_P \notin \mathfrak{m}_P\mathcal{L}_P$ for all $P \in \operatorname{Supp}\mathcal{F}$. For the stalks of $\mathcal{F} \otimes \mathcal{L}$ at $P \in \operatorname{Supp}\mathcal{F}$, we have

$$(\mathcal{F} \otimes \mathcal{L})_P = \mathcal{F}_P \otimes_{\mathcal{O}_P} \mathcal{L}_P = \mathcal{F}_P \otimes_{\mathcal{O}_P} \mathcal{O}_P t_P.$$

It follows that, given a global section $s \in \Gamma(\mathcal{F} \otimes \mathcal{L})$, we find $f_P \in \mathcal{F}_P$ such that $s_P = f_P \otimes t_P$. Put $f := \sum_P f_P \in \bigoplus_{P\in\operatorname{Supp}\mathcal{F}} \mathcal{F}_P = \Gamma(\mathcal{F})$. Then $f \otimes t$ maps to s on all stalks, hence also globally.

(b) $\mathcal{L}'$ basepoint-free implies $\Gamma(\mathcal{L}') \neq 0$, so pick any $s \in \Gamma(\mathcal{L}')$, $s \neq 0$. Since $\mathcal{L}'$ is isomorphic to a subsheaf of the constant sheaf $\mathcal{K}$ with value the function field of C, the restriction $s|_U$ of s to any open subset $U \subseteq C$ remains non-zero. Because $\mathcal{L}'$ is locally free of rank one, $s|_U$ is not a torsion element over $\mathcal{O}_C(U)$, and the morphism of $\mathcal{O}_C$-modules $\mathcal{O}_C \to \mathcal{L}'$, $1 \mapsto s$, is injective. By local freeness, it remains injective after tensoring with the invertible sheaf $\mathcal{L} \otimes \mathcal{L}'^\vee$. Define $\mathcal{F}$ via the exact sequence of $\mathcal{O}_C$-modules

$$0 \longrightarrow \mathcal{L} \otimes \mathcal{L}'^\vee \longrightarrow \mathcal{L} \longrightarrow \mathcal{F} \longrightarrow 0. \qquad (*)$$

The set $\{P \in C : s_P \notin \mathfrak{m}_P\mathcal{L}'_P\}$ is open and non-empty, so it contains all but finitely many points. For P in this set, the maps $\mathcal{O}_P \to \mathcal{L}_P$, $1 \mapsto s_P$, and $\mathcal{L}_P \otimes_{\mathcal{O}_P} \mathcal{L}'^\vee_P \to \mathcal{L}_P$ are isomorphisms. Thus $\mathcal{F}$ has finite support and we conclude $S(\mathcal{F},\mathcal{L}') = 0$ by (a). Now consider the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & \Gamma(\mathcal{L}\otimes\mathcal{L}'^\vee)\otimes\Gamma(\mathcal{L}') \arrow[r] \arrow[d] & \Gamma(\mathcal{L})\otimes\Gamma(\mathcal{L}') \arrow[r] \arrow[d] & \Gamma(\mathcal{F})\otimes\Gamma(\mathcal{L}') \arrow[r] \arrow[d] & H^1(\mathcal{L}\otimes\mathcal{L}'^\vee)\otimes\Gamma(\mathcal{L}') \\
0 \arrow[r] & \Gamma(\mathcal{L}) \arrow[r] \arrow[d] \arrow[ur, dashed, "\alpha"] & \Gamma(\mathcal{L}\otimes\mathcal{L}') \arrow[r] \arrow[d] & \Gamma(\mathcal{F}\otimes\mathcal{L}') \arrow[d] & \\
& S(\mathcal{L}\otimes\mathcal{L}'^\vee,\mathcal{L}') \arrow[r] & S(\mathcal{L},\mathcal{L}') \arrow[r] & S(\mathcal{F},\mathcal{L}') &
\end{tikzcd}$$

The first row is exact since it consists of the first terms of the cohomology sequence for $(*)$, tensored with $\Gamma(\mathcal{L}')$ over k. The second row comes from tensoring $(*)$ with $\mathcal{L}'$ and then taking global sections, so it is exact as well. Finally, the columns are exact by definition of $S(-,-)$. The rightmost term in the first row vanishes, since we assumed $H^1(\mathcal{L}\otimes\mathcal{L}'^\vee) = 0$. So the snake lemma applies and yields exactness of the third row. If we define the map $\alpha : \Gamma(\mathcal{L}) \to \Gamma(\mathcal{L}) \otimes \Gamma(\mathcal{L}')$ by $f \mapsto f \otimes s$, then the triangle under it commutes, which implies that $S(\mathcal{L}\otimes\mathcal{L}'^\vee,\mathcal{L}') \to S(\mathcal{L},\mathcal{L}')$ is the zero map. Together with the fact that $S(\mathcal{F},\mathcal{L}') = 0$ we conclude $S(\mathcal{L},\mathcal{L}') = 0$.

(c) The statement is symmetric in $\mathcal{L},\mathcal{L}'$, so we may assume $\deg\mathcal{L} \leq \deg\mathcal{L}'$. Let $D \geq 0$ be an arbitrary effective divisor on C of degree $\deg D = 2g-1$. Then D defines a subsheaf $\mathcal{O}_C(-D)$ of $\mathcal{O}_C$, and the injective morphism $\mathcal{O}_C(-D) \to \mathcal{O}_C$ is an isomorphism outside the finite support of D. Tensoring with $\mathcal{L}$ gives an injective morphism $\mathcal{L}(-D) \to \mathcal{L}$ where $\mathcal{L}(-D) := \mathcal{L} \otimes \mathcal{O}_C(-D)$. Let $\mathcal{F}$ be the cokernel, so that we have an exact sequence of $\mathcal{O}_C$-modules

$$0 \longrightarrow \mathcal{L}(-D) \longrightarrow \mathcal{L} \longrightarrow \mathcal{F} \longrightarrow 0.$$

We have $\deg \mathcal{L}(-D) = \deg \mathcal{L} - (2g-1) \geq 2g+1$, hence $\mathcal{L}(-D)$ has vanishing first cohomology: $H^1(\mathcal{L}(-D)) = 0$. With the same argument as in the proof of (b), we conclude that the natural sequence

$$S(\mathcal{L}(-D), \mathcal{L}') \longrightarrow S(\mathcal{L}, \mathcal{L}') \longrightarrow S(\mathcal{F}, \mathcal{L}')$$

is exact. Since $\deg(\mathcal{L}') \geq 4g \geq 2g$, the sheaf $\mathcal{L}'$ has no basepoints (proposition 3.2). Moreover, the support of $\mathcal{F}$ is finite because $\mathcal{L}(-D) \to \mathcal{L}$ is an isomorphism outside $\operatorname{Supp} D$. Thus the hypotheses of (a) are satisfied and we conclude $S(\mathcal{F}, \mathcal{L}') = 0$. Let us now apply (b) with $\mathcal{L}'$ and $\mathcal{L}(-D)$ taking the roles of $\mathcal{L}$ and $\mathcal{L}'$, respectively. This is possible since $\deg \mathcal{L}(-D) \geq 2g+1$ and

$$\deg(\mathcal{L}' \otimes \mathcal{L}(-D)^\vee) = \deg \mathcal{L}' - \deg \mathcal{L} + 2g - 1 \geq 2g-1,$$

so that $\mathcal{L}(-D)$ is basepoint-free and $H^1(\mathcal{L}' \otimes \mathcal{L}(-D)^\vee) = 0$. Thus (b) applies and yields $S(\mathcal{L}', \mathcal{L}(-D)) = 0$. Since the definition of $S(-,-)$ is symmetric in the two arguments, this implies $S(\mathcal{L}(-D), \mathcal{L}') = 0$. Finally we have $S(\mathcal{L}, \mathcal{L}') = 0$ by exactness of the sequence above. □

Lemma 8.7. *Let C be a complete nonsingular curve over k. For $d \in \mathbb{N}_0$, denote by $\operatorname{Pic}^{\geq d}(C)$ the set of isomorphism classes of invertible sheaves of degree $\geq d$ on C. Suppose we have a function $h : \operatorname{Pic}^{\geq d} \to \mathbb{T}_\ell$ such that*

$$h(\mathcal{L} \otimes \mathcal{L}') = h(\mathcal{L}) + h(\mathcal{L}')$$

for all $\mathcal{L}, \mathcal{L}' \in \operatorname{Pic}^{\geq d}$. Then $h(\mathcal{L})$ depends only on the degree of $\mathcal{L}$.

Proof. We first show that h extends to a group homomorphism $\operatorname{Pic}(C) \to \mathbb{T}_\ell$. Every invertible sheaf is isomorphic to $\mathcal{L} \otimes \mathcal{L}'^\vee$ with $\mathcal{L}, \mathcal{L}' \in \operatorname{Pic}^{\geq d}$, so we define

$$h(\mathcal{L} \otimes \mathcal{L}'^\vee) := h(\mathcal{L}) - h(\mathcal{L}').$$

To show that this is well-defined, assume $\mathcal{M}, \mathcal{M}' \in \operatorname{Pic}^{\geq d}$ satisfy $\mathcal{L} \otimes \mathcal{L}'^\vee \cong \mathcal{M} \otimes \mathcal{M}'^\vee$. Then we have $\mathcal{L} \otimes \mathcal{M}' \cong \mathcal{M} \otimes \mathcal{L}'$, thus $h(\mathcal{L}) + h(\mathcal{M}') = h(\mathcal{M}) + h(\mathcal{L}')$, and hence $h(\mathcal{L}) - h(\mathcal{L}') = h(\mathcal{M}) - h(\mathcal{M}')$. So h is indeed the restriction of a homomorphism $\operatorname{Pic}(C) \to \mathbb{T}_\ell$. Recall that we have an exact sequence

$$0 \longrightarrow \operatorname{Pic}^0(C) \longrightarrow \operatorname{Pic}(C) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0.$$

The subgroup $\operatorname{Pic}^0(C)$ is ℓ-divisible but $\mathbb{T}_\ell$ has no nontrivial infinitely ℓ-divisible elements, so the homomorphism is trivial on $\operatorname{Pic}^0(C)$ and hence factors over $\deg : \operatorname{Pic}(C) \to \mathbb{Z}$. □

Lemma 8.8. *Let $L|k$ be a function field in F. Then a subgroup $D \subseteq U_L^{\mathrm{ab},\ell}$ is a decomposition subgroup if and only if D is maximal with the property that D is contained in Φ_L and whenever $V \subseteq G$ is a compact open subgroup containing U_L such that $V = U_{k(x)}$ for some $x \in F \setminus k$, then the image of D under* $\mathrm{res} : U_L^{\mathrm{ab},\ell} \to V^{\mathrm{ab},\ell}$ *is a finite-index subgroup of a decomposition subgroup in $V^{\mathrm{ab},\ell}$.*

Proof. Let C be a complete nonsingular model of $L|k$ and let g be its genus. If $D \subseteq U_L^{\mathrm{ab},\ell}$ is the decomposition subgroup of a point $P \in C$, then its elements are induced by delta functions at P and are in particular contained in Φ_L. If $V \subseteq G$ is a compact open subgroup as above, then for a suitably chosen $x \in F \setminus k$ with $V = U_{k(x)}$ we have $k(x) \subseteq L$. Let $\phi : C \to \mathbb{P}^1$ be the morphism corresponding to $k(x) \subseteq L$. Then the image of D in $U_{k(x)}^{\mathrm{ab},\ell}$ is contained in the decomposition subgroup of $\phi(P)$, the index being the ℓ-part of the ramification index $e(P|\phi(P))$ by proposition 6.11.

For the converse, assume that $D \subseteq \Phi_L$ is a subgroup such that for all $x \in L \setminus k$, its image in $U_{k(x)}^{\mathrm{ab},\ell}$ is a finite-index subgroup of a decomposition subgroup. We have to prove that D is itself contained in a decomposition subgroup. Let σ be an element in D, defined by a map $f : C \to \mathbb{T}_\ell$, which we consider by linear extension as an element of $\mathrm{Hom}(\mathrm{Div}(C), \mathbb{T}_\ell)$. Let $\mathcal{L}$ be an invertible sheaf on C. Then the associated complete linear system $|\mathcal{L}|$ is a subset of $\mathrm{Div}(C)$, so we have an induced map $f : |\mathcal{L}| \to \mathbb{T}_\ell$. Viewing $|\mathcal{L}|$ as a projective space over k via the bijection $\mathbb{P}\Gamma(C, \mathcal{L}) \cong |\mathcal{L}|$, we show that it satisfies the hypotheses of lemma 8.5, i. e. f restricts to a delta function on every projective line. A line u in $|\mathcal{L}|$ has a unique decomposition $u = B + m$ into a *fixed part* and a *moving part*, i. e. $B \geq 0$ is the divisor of base points of u and m is a basepoint-free line in $|\mathcal{L}(-B)|$. By lemma 3.3, m is the set of inverse image divisors of a morphism $\phi : C \to \mathbb{P}^1$, so that u is given by

$$u = \{B + \phi^*(Q) : Q \in \mathbb{P}^1\}.$$

Let $k(x) \hookrightarrow L$ be the subfield corresponding to ϕ, then proposition 6.9 implies that we have a commutative square

$$\begin{tikzcd}
\mathrm{Hom}(\mathrm{Div}(C), \mathbb{T}_\ell) \arrow[r] \arrow[d, "-\circ\phi^*"'] & U_L^{\mathrm{ab},\ell} \arrow[d, "\mathrm{res}"] \\
\mathrm{Map}(\mathbb{P}^1, \mathbb{T}_\ell) \arrow[r] & U_{k(x)}^{\mathrm{ab},\ell}.
\end{tikzcd}$$

By hypothesis, $\mathrm{res}(\sigma)$ is contained in a decomposition subgroup of a point $Q_0 \in \mathbb{P}^1$, hence $f \circ \phi^*$, as a map $\mathbb{P}^1 \to \mathbb{T}_\ell$, is a delta function at Q_0. Therefore, the restriction of f to u is a delta function at $B + \phi^*(Q_0)$.

So we can apply lemma 8.5 which shows that we have a well-defined function

$$\begin{aligned} f^\vee : |\mathcal{L}|^\vee &\longrightarrow \mathbb{T}_\ell, \\ H &\longmapsto \text{generic value of } f \text{ on } H, \end{aligned}$$

on the set of hyperplanes in $|\mathcal{L}|$, and moreover $f^\vee$ is a delta function, i. e. it takes the same value on all hyperplanes with at most one exception. If now $\mathcal{L}$ is very ample, then every point on C determines in an injective fashion a hyperplane in $|\mathcal{L}|$ via

$$\begin{aligned} i_{\mathcal{L}} : C &\hookrightarrow |\mathcal{L}|^\vee, \\ P &\longmapsto \{E \in |\mathcal{L}| : P \in \operatorname{Supp} E\} = P + |\mathcal{L}(-P)|. \end{aligned}$$

Composing with $f^\vee$, we get for every very ample invertible sheaf $\mathcal{L}$ on C a delta function

$$\begin{aligned} f_{\mathcal{L}} : C &\longrightarrow \mathbb{T}_\ell, \\ P &\longmapsto f^\vee(i_{\mathcal{L}}(P)) = f(P) + f(\text{general point on } |\mathcal{L}(-P)|). \end{aligned}$$

For an invertible sheaf $\mathcal{M}$, define $h(\mathcal{M}) := f(\text{general point on } |\mathcal{M}|)$, so that we have $f_{\mathcal{L}}(P) = f(P) + h(\mathcal{L}(-P))$ for all $P \in C$ and all very ample invertible sheaves $\mathcal{L}$. Given two very ample invertible sheaves $\mathcal{L}, \mathcal{L}'$ we have a commutative square

$$\begin{tikzcd} \mathbb{P}\Gamma(C,\mathcal{L}) \times \mathbb{P}\Gamma(C,\mathcal{L}') \arrow[r] \arrow[d, "\wr"'] & \mathbb{P}\Gamma(C,\mathcal{L}\otimes\mathcal{L}') \arrow[d, "\wr"'] \\ |\mathcal{L}| \times |\mathcal{L}'| \arrow[r] & |\mathcal{L}\otimes\mathcal{L}'| \end{tikzcd}$$

with the first row induced by the bilinear map $\Gamma(C,\mathcal{L}) \times \Gamma(C,\mathcal{L}') \to \Gamma(C,\mathcal{L}\otimes\mathcal{L}')$, and the second row given by addition of divisors, $(E,E') \mapsto E + E'$. If $\mathcal{L}$ and $\mathcal{L}'$ have degree $\geq 4g$, then the images of the horizontal maps are not contained in a proper subspace by lemma 8.6, so the sum of two general points in $|\mathcal{L}|$ and $|\mathcal{L}'|$ is a general point in $|\mathcal{L}\otimes\mathcal{L}'|$. Therefore we have $h(\mathcal{L}\otimes\mathcal{L}') = h(\mathcal{L}) + h(\mathcal{L}')$ for $\mathcal{L}, \mathcal{L}' \in \operatorname{Pic}^{\geq d}$, where $d = \max\{2g+1, 4g\}$. By lemma 8.7, $h(\mathcal{L})$ depends only on the degree of $\mathcal{L}$, thus we have

$$f(P) = f_{\mathcal{L}}(P) + h(\mathcal{L}(-P)) = f_{\mathcal{L}}(P) + \text{const}$$

for all $P \in C$ and $\mathcal{L} \in \operatorname{Pic}^{\geq d}$, with a constant that depends only on $\mathcal{L}$ but not on P. Choose for $\mathcal{L}$ an arbitrary invertible sheaf of degree $\geq d$, then $f_{\mathcal{L}}$ is a delta function, so f is a delta function and σ is contained in a decomposition subgroup. Since any two decomposition subgroups have trivial intersection, there exists a single decomposition subgroup containing all elements of D. □

We can now prove proposition 8.1.

Proof of proposition 8.1. The claim follows from the characterisation of decomposition subgroups in lemma 8.8, together with the following facts:

- $\lambda(\Phi_L) = \Phi_{L'}$ (lemma 8.4);
- If V runs through the compact open subgroups of G containing U_L such that $V = U_{k(x)}$ for some $x \in F \setminus k$, then $V' := \lambda(V)$ runs through the analogous set of subgroups of G' containing $U_{L'}$.

- λ is compatible with restriction homomorphisms. The following squares commute by the functoriality of $(-)^{\mathrm{ab},\ell}$:

$$\begin{tikzcd} U_L^{\mathrm{ab},\ell} \arrow[r, "\lambda^{\mathrm{ab},\ell}", "\sim"'] \arrow[d, "\mathrm{res}"] & U_{L'}^{\mathrm{ab},\ell} \arrow[d, "\mathrm{res}"] \\ V^{\mathrm{ab},\ell} \arrow[r, "\lambda^{\mathrm{ab},\ell}", "\sim"'] & V'^{\mathrm{ab},\ell} \end{tikzcd}$$

- λ induces a bijection between the decomposition subgroups of $V^{\mathrm{ab},\ell}$ and $V'^{\mathrm{ab},\ell}$ (proposition 7.1). □

9 Proof of Main Result

In this final section we complete the proof of theorem B. We consider two triples (k, F, G) and (k', F', G') as in the theorem and an isomorphism of topological groups $\lambda : G \xrightarrow{\sim} G'$. We also fix a prime number $\ell \neq \mathrm{char}(k) = \mathrm{char}(k')$. If $L|k$ and $L'|k'$ are function fields in F and F' with $\lambda^{-1}(U_{L'}) = U_L$, then λ induces by proposition 8.1 a bijection

$$\lambda^* : C' \xrightarrow{\sim} C$$

between their complete nonsingular models, given by $\lambda^*(P') = P$ whenever the decomposition subgroup $\underline{P}$ is mapped isomorphically to $\underline{P'}$ under $\lambda^{\mathrm{ab},\ell} : U_L^{\mathrm{ab},\ell} \xrightarrow{\sim} U_{L'}^{\mathrm{ab},\ell}$. We start by proving some properties of λ^*.

Lemma 9.1 (Compatibility of λ^* with morphisms)**.** *Let $L_1 \subseteq L_2$ be an inclusion of function fields in F with complete nonsingular models C_1 and C_2, respectively, and let $\phi : C_2 \to C_1$ be the corresponding morphism. Let $L_1' \subseteq L_2'$ be function fields in F' such that $\lambda^{-1}(U_{L_i'}) = U_{L_i}$ $(i = 1, 2)$. Define C_1', C_2' and $\phi' : C_2' \to C_1'$ correspondingly. Then the bijections $\lambda^* : C_i' \xrightarrow{\sim} C_i$ are compatible with the maps ϕ and ϕ', i. e. the following square commutes:*

$$\begin{tikzcd} C_2' \arrow[r, "\lambda^*", "\sim"'] \arrow[d, "\phi'"] & C_2 \arrow[d, "\phi"] \\ C_1' \arrow[r, "\lambda^*", "\sim"'] & C_1. \end{tikzcd}$$

Proof. By functoriality of $(-)^{\mathrm{ab},\ell}$, we have a commutative square

$$\begin{tikzcd} U_{L_2}^{\mathrm{ab},\ell} \arrow[r, "\lambda^{\mathrm{ab},\ell}", "\sim"'] \arrow[d, "\mathrm{res}"] & U_{L_2'}^{\mathrm{ab},\ell} \arrow[d, "\mathrm{res}"] \\ U_{L_1}^{\mathrm{ab},\ell} \arrow[r, "\lambda^{\mathrm{ab},\ell}", "\sim"'] & U_{L_1'}^{\mathrm{ab},\ell}. \end{tikzcd}$$

Let $P' \in C_2'$ be a point, $Q' = \phi'(P')$. By corollary 6.11, we have $\operatorname{res}(\underline{P'}) \subseteq \underline{Q'}$. The fact that $\lambda^{\mathrm{ab},\ell}$ restricts to isomorphisms $\underline{\lambda^*(P')} \xrightarrow{\sim} \underline{P'}$ and $\underline{\lambda^*(Q')} \xrightarrow{\sim} \underline{Q'}$ together with the commutativity of the square implies $\operatorname{res}(\underline{\lambda^*(P')}) \subseteq \underline{\lambda^*(Q')}$. Using corollary 6.11 again, $\phi(\lambda^*(P')) = \lambda^*(Q')$. □

Lemma 9.2. *Identify the ℓ-adic Tate modules of k and k' via an arbitrarily chosen isomorphism of $\mathbb{Z}_\ell$-modules; denote both by $\mathbb{T}_\ell$. Let $L|k$ and $L'|k'$ be function fields with $\lambda^{-1}(U_{L'}) = U_L$ and let C and C' be complete nonsingular models. Then there exists a unique ℓ-adic unit $\varepsilon_L \in \mathbb{Z}_\ell^\times$ (depending on L, L' and the chosen isomorphism of Tate modules) such that the following square commutes:*

$$\begin{tikzcd}
\operatorname{Map}(C, \mathbb{T}_\ell)/\mathbb{T}_\ell \arrow[r, hook] \arrow[d, "\varepsilon_L\cdot(-\circ\lambda^*)"', "\wr"] & U_L^{\mathrm{ab},\ell} \arrow[d, "\lambda^{\mathrm{ab},\ell}"', "\wr"] \\
\operatorname{Map}(C', \mathbb{T}_\ell)/\mathbb{T}_\ell \arrow[r, hook] & U_{L'}^{\mathrm{ab},\ell}.
\end{tikzcd}$$

Proof. The horizontal maps are isomorphisms onto their images Φ_L and $\Phi_{L'}$ (proposition 6.2). By lemma 8.4, $\lambda^{\mathrm{ab},\ell}$ restricts to an isomorphism $\Phi_L \xrightarrow{\sim} \Phi_{L'}$, so there exists some isomorphism of topological groups $\varphi : \operatorname{Map}(C, \mathbb{T}_\ell)/\mathbb{T}_\ell \xrightarrow{\sim} \operatorname{Map}(C', \mathbb{T}_\ell)/\mathbb{T}_\ell$ making the square commutative. For points $P \in C$ and $P' \in C'$ with $\lambda^*(P') = P$, the decomposition subgroup $\underline{P}$ is mapped isomorphically to the decomposition subgroup $\underline{P'}$ under $\lambda^{\mathrm{ab},\ell}$, thus φ maps the subgroup of delta functions at P isomorphically to the subgroup of delta functions at P'. These groups are both isomorphic to $\mathbb{T}_\ell$, which is a free $\mathbb{Z}_\ell$-module of rank 1. Since $\lambda^{\mathrm{ab},\ell}$ is $\mathbb{Z}_\ell$-linear, φ is also $\mathbb{Z}_\ell$-linear, so there exists a unique ℓ-adic unit $\varepsilon_{P'} \in \mathbb{Z}_\ell^\times$ such that

$$\varphi(\delta_P\,\omega) = \varepsilon_{P'}\;\delta_{P'}\,\omega \text{ for all } \omega \in \mathbb{T}_\ell,$$

where $\delta_P\,\omega(Q) = \delta_{PQ}\,\omega$ is the (normalised) delta function at P with value ω. We show that $\varepsilon_{P'}$ is independent of the point P'. Let $\varepsilon \in \operatorname{Map}(C', \mathbb{Z}_\ell^\times)$ be the function $P' \mapsto \varepsilon_{P'}$. Consider the diagram

$$\begin{tikzcd}
\operatorname{Map}(C, \mathbb{T}_\ell) \arrow[r, dashed, "\psi", "\sim"'] \arrow[d, two heads, "\pi"] & \operatorname{Map}(C', \mathbb{T}_\ell) \arrow[d, two heads, "\pi'"] \\
\operatorname{Map}(C, \mathbb{T}_\ell)/\mathbb{T}_\ell \arrow[r, "\varphi", "\sim"'] & \operatorname{Map}(C', \mathbb{T}_\ell)/\mathbb{T}_\ell
\end{tikzcd}$$

where ψ is defined by $f \mapsto \varepsilon \cdot (f \circ \lambda^*)$. Then $\pi' \circ \psi$ and $\varphi \circ \pi$ are both continuous homomorphisms and they agree on all normalised delta functions. Those span $\operatorname{Map}(C, \mathbb{T}_\ell)$ topologically, hence $\pi' \circ \psi = \varphi \circ \pi$. Now ψ maps constant functions to constant functions, so for arbitrary $\omega \in \mathbb{T}_\ell$ the map $P' \mapsto \varepsilon_{P'}\omega$ is constant, which implies that the $\varepsilon_{P'}$ are equal for all points. The common value of the $\varepsilon_{P'}$ is our $\varepsilon_L \in \mathbb{Z}_\ell^\times$. □

Lemma 9.3 (Compatibility of λ^* with pullbacks)**.** *In the situation of lemma 9.1, assume in addition that $L_2'|L_1'$ has the same degree of inseparability as $L_2|L_1$. Define*

$\lambda^* : \mathrm{Div}(C'_i) \xrightarrow{\sim} \mathrm{Div}(C_i)$ *by linear extension* ($i = 1, 2$)*. Then* λ^* *is compatible with pullbacks of divisors in the sense that the following square commutes:*

$$\begin{tikzcd}
\mathrm{Div}(C'_1) \arrow[r, "\lambda^*", "\sim"'] \arrow[d, "\phi'^*"] & \mathrm{Div}(C_1) \arrow[d, "\phi^*"] \\
\mathrm{Div}(C'_2) \arrow[r, "\lambda^*", "\sim"'] & \mathrm{Div}(C_2).
\end{tikzcd}$$

Recall that the degree of *separability* of $L_2|L_1$ equals the index $(U_{L_1} : U_{L_2})$, so that in the situation of lemma 9.1, we have a priori $[L_2 : L_1]_s = [L'_2 : L'_1]_s$. The assertion that $L_2|L_1$ and $L'_2|L'_1$ have the same degree of inseparability is therefore equivalent to $[L_2 : L_1] = [L'_2 : L'_1]$.

Proof. As in the previous lemma, identify the ℓ-adic Tate modules of k and k' via an arbitrarily chosen isomorphism of $\mathbb{Z}_\ell$-modules. Let $\varepsilon_1, \varepsilon_2 \in \mathbb{Z}_\ell^\times$ be the ℓ-adic units from lemma 9.2 for (L_1, L'_1) and (L_2, L'_2). Consider the following diagram:

$$\begin{tikzcd}
 & \mathrm{Hom}(\mathrm{Div}^0(C_2), \mathbb{T}_\ell) \arrow[rr, hook] \arrow[dl, "-\circ\phi^*"'] \arrow[dd, "\varepsilon_2\cdot(-\circ\lambda^*)"' near start] & & U^{\mathrm{ab},\ell}_{L_2} \arrow[dl, "\mathrm{res}"] \arrow[dd, "\lambda^{\mathrm{ab},\ell}"] \\
\mathrm{Hom}(\mathrm{Div}^0(C_1), \mathbb{T}_\ell) \arrow[rr, hook] \arrow[dd, "\varepsilon_1\cdot(-\circ\lambda^*)"'] & & U^{\mathrm{ab},\ell}_{L_1} \arrow[dd, "\lambda^{\mathrm{ab},\ell}" near start] & \\
 & \mathrm{Hom}(\mathrm{Div}^0(C'_2), \mathbb{T}_\ell) \arrow[rr, hook] \arrow[dl, "-\circ\phi'^*"'] & & U^{\mathrm{ab},\ell}_{L'_2} \arrow[dl, "\mathrm{res}"] \\
\mathrm{Hom}(\mathrm{Div}^0(C'_1), \mathbb{T}_\ell) \arrow[rr, hook] & & U^{\mathrm{ab},\ell}_{L'_1} &
\end{tikzcd}$$

All faces except possibly the left one commute: the right one by the functoriality of $(-)^{\mathrm{ab},\ell}$, front and back by definition of ε_1 and ε_2 (making use of the isomorphism $\mathrm{Map}(C_i, \mathbb{T}_\ell)/\mathbb{T}_\ell \cong \mathrm{Hom}(\mathrm{Div}^0(C_i), \mathbb{T}_\ell)$ from proposition 6.2), and top and bottom by proposition 6.9. Together with the injectivity of the front lower horizontal map, this implies that the left face commutes as well.

Assume for the moment that ϕ and ϕ' are separable. Then the two morphisms are only ramified at a finite number of points, so we find $P \in C_2$ and $P' \in C'_2$ with $\lambda^*(P') = P$ such ϕ and ϕ' are unramified at P and P', respectively. Consider a normalised delta function $\delta_P\,\omega$ at P for some $\omega \in \mathbb{T}_\ell$. The commutativity of the left face for this function reads

$$\varepsilon_1 \cdot (\delta_P\,\omega \circ \phi^* \circ \lambda^*) = \varepsilon_2 \cdot (\delta_P\,\omega \circ \lambda^* \circ \phi'^*).$$

The left-hand side equals

$$\begin{aligned}
\varepsilon_1 \cdot (\delta_P\,\omega \circ \phi^* \circ \lambda^*) &= \varepsilon_1 \cdot (e(P|\phi(P))\,\delta_{\phi(P)}\,\omega \circ \lambda^*) \\
&= \varepsilon_1 \cdot (\delta_{\phi(P)}\,\omega \circ \lambda^*) && (\phi \text{ unramified at } P) \\
&= \varepsilon_1 \cdot \delta_{\phi'(P')}\,\omega && (\text{lemma 9.1})
\end{aligned}$$

and for the right hand side we obtain

$$\begin{aligned}\varepsilon_2 \cdot (\delta_P\, \omega \circ \lambda^* \circ \phi'^*) &= \varepsilon_2 \cdot (\delta_{P'}\, \omega \circ \phi'^*) \\ &= \varepsilon_2 \cdot e(P'|\phi'(P'))\, \delta_{\phi'(P')}\, \omega \\ &= \varepsilon_2 \cdot \delta_{\phi'(P')}\, \omega. && (\phi' \text{ unramified at } P')\end{aligned}$$

Comparing the two functions, we get $\varepsilon_1\omega = \varepsilon_2\omega$. Since $\omega \in \mathbb{T}_\ell$ was arbitrary, $\varepsilon_1 = \varepsilon_2$.

If ϕ and ϕ' are not necessarily separable, but have the same degree of inseparability p^n where $p = \mathrm{char}(k) = \mathrm{char}(k') > 0$, then the ramification indices of ϕ and ϕ' are p^n at all but a finite number of points, and the same argument as above applies.

In any case, we have $\varepsilon_1 = \varepsilon_2$, so we can "cancel" the two factors from our left face of the cube and obtain a commutative square

$$\begin{tikzcd}
\mathrm{Hom}(\mathrm{Div}^0(C_2), \mathbb{T}_\ell) \arrow[r, "-\circ\phi^*"] \arrow[d, "-\circ\lambda^*"] & \mathrm{Hom}(\mathrm{Div}^0(C_1), \mathbb{T}_\ell) \arrow[d, "-\circ\lambda^*"] \\
\mathrm{Hom}(\mathrm{Div}^0(C_2'), \mathbb{T}_\ell) \arrow[r, "-\circ\phi'^*"] & \mathrm{Hom}(\mathrm{Div}^0(C_1'), \mathbb{T}_\ell)
\end{tikzcd}$$

The homomorphism

$$\phi^* \circ \lambda^* - \lambda^* \circ \phi'^* : \mathrm{Div}^0(C_1') \to \mathrm{Div}^0(C_2)$$

becomes zero under $\mathrm{Hom}(-, \mathbb{T}_\ell)$. We can conclude $\phi^* \circ \lambda^* = \lambda^* \circ \phi'^*$ if for every divisor $D \in \mathrm{Div}^0(C_2)$, $D \neq 0$, there exists a homomorphism $f : \mathrm{Div}^0(C_2) \to \mathbb{T}_\ell$ such that $f(D) \neq 0$. Indeed, this follows from the fact that $\mathrm{Div}^0(C_2)$ is free as an abelian group (for any $P_0 \in C_2$, a $\mathbb{Z}$-basis is given by $\{P - P_0 : P \neq P_0\}$). So the following commutes:

$$\begin{tikzcd}
\mathrm{Div}^0(C_1') \arrow[r, "\phi'^*"] \arrow[d, "\lambda^*"] & \mathrm{Div}^0(C_2') \arrow[d, "\lambda^*"] \\
\mathrm{Div}^0(C_1) \arrow[r, "\phi^*"] & \mathrm{Div}^0(C_2)
\end{tikzcd}$$

It only remains to see that the commutativity carries over to divisors which are not necessarily of degree zero. Consider $Q' \in C_1'$. Let $S' \in C_1' \setminus \{Q'\}$ be arbitrary and put $Q = \lambda^*(Q')$, $S = \lambda^*(S')$. We have

$$\begin{aligned}(\phi^* \circ \lambda^*)(Q' - S') &= \phi^*(Q) - \phi^*(S), \\ (\lambda^* \circ \phi'^*)(Q' - S') &= (\lambda^* \circ \phi'^*)(Q') - (\lambda^* \circ \phi'^*)(S')\end{aligned}$$

and the equality $(\phi^* \circ \lambda^*)(Q') = (\lambda^* \circ \phi'^*)(Q')$ follows by comparing the positive parts. □

Remark. In characteristic zero, the same result can be proved with less difficulty by working with the full abelianisations U_L^{ab} instead of the maximal pro-ℓ abelian quotients $U_L^{\mathrm{ab},\ell}$ and noting that in corollary 6.11 the index $(\underline{Q} : \mathrm{res}(\underline{P}))$ equals the full ramification index $e(P|Q)$ rather than just the ℓ-part.

Given two vector spaces V and V' over (arbitrary) fields k and k', respectively, a **collineation** between the projective spaces $\mathbb{P}_{k'}V' = (V'\backslash\{0\})/k'^{\times}$ and $\mathbb{P}_k V$ is a bijection $\varphi : \mathbb{P}_{k'}V' \xrightarrow{\sim} \mathbb{P}_k V$ which maps projective lines to projective lines. We show now that in the situation of lemma 9.3, λ induces a collineation $\lambda^* : L'^{\times}/k'^{\times} \xrightarrow{\sim} L^{\times}/k^{\times}$. This will enable us to apply the fundamental theorem of projective geometry and conclude that λ^* is in fact induced by an isomorphism of field extensions $L'|k' \xrightarrow{\sim} L|k$.

Lemma 9.4. *For $L|k$ and $L'|k'$ as in the previous lemma, the following holds:*

(a) The image of a base-point-free line under $\lambda^* : \mathrm{Div}(C') \xrightarrow{\sim} \mathrm{Div}(C)$ is a base-point-free line.

(b) λ^* restricts to an isomorphism $\mathrm{PDiv}(C') \xrightarrow{\sim} \mathrm{PDiv}(C)$ between the subgroups of principal divisors.

(c) The induced isomorphism $\lambda^* : L'^{\times}/k'^{\times} \xrightarrow{\sim} L^{\times}/k^{\times}$ is a collineation of projective spaces.

Proof.

(a) Let $m' \subseteq \mathrm{Div}(C')$ be a base point free line. By lemma 3.3, there exists a morphism $\phi' : C' \to \mathbb{P}^1_{k'}$ such that m' is the set of inverse image divisors

$$m' = \{\phi'^*(Q') : Q' \in \mathbb{P}^1_{k'}\}.$$

Let $k'(x') \subseteq L$ be the corresponding subfield. There exists a rational function field $k(x)$ in F such that $\lambda^{-1}(U_{k'(x')}) = U_{k(x)}$. Using $\mathrm{char}(k) = \mathrm{char}(k')$ and lemma 8.2, we can choose x in such a way that $k(x) \subseteq L$ and such that $L|k(x)$ has the same degree of inseparability as $L'|k'(x')$. If $\phi : C \to \mathbb{P}^1_k$ is the corresponding morphism, then

$$\begin{tikzcd}
\mathrm{Div}(\mathbb{P}^1_{k'}) \arrow[r, "\lambda^*", "\sim"'] \arrow[d, "\phi'^*"] & \mathrm{Div}(\mathbb{P}^1_k) \arrow[d, "\phi^*"] \\
\mathrm{Div}(C') \arrow[r, "\lambda^*", "\sim"'] & \mathrm{Div}(C)
\end{tikzcd}$$

commutes by lemma 9.3, so that m' is mapped under λ^* to

$$\lambda^*(m') = \{\phi^*(Q) : Q \in \mathbb{P}^1_k\},$$

a base-point-free line in $\mathrm{Div}(C)$.

(b) Let $D' \in \mathrm{Div}(C')$ be a divisor. Write $D' = D'_+ - D'_-$ with $D'_+, D'_- \geq 0$ effective divisors with disjoint support. Then D' is principal if and only if there exists a dominant morphism $C' \to \mathbb{P}^1_{k'}$ having D'_+ and D'_- as its divisors of zeroes and poles, respectively, which is the case if and only if there exists a base-point-free line in $\mathrm{Div}(C')$ passing through D'_+ and D'_-. The claim now follows from (a).

(c) By lemma 3.4, a subset $m' \subseteq \mathrm{PDiv}(C')$ is a line if and only if there exists a divisor $D' \in \mathrm{Div}(C')$ such that $m' + D'$ is a base-point-free line in $|D'|$. Hence $\lambda^* : \mathrm{PDiv}(C') \xrightarrow{\sim} \mathrm{PDiv}(C)$ maps lines to lines and is therefore a collineation. □

We can now use the fundamental theorem of projective geometry ([Art57], Thm. 2.26).

Theorem 9.5 (Fundamental Theorem of Projective Geometry)**.** *Let k and k' be arbitrary fields, let V and V' be vector spaces of dimension ≥ 3 over k and k', respectively, and let*

$$\varphi : \mathbb{P}_{k'}V' \xrightarrow{\sim} \mathbb{P}_k V$$

be a collineation. Then there exists a pair (σ, τ) of a field isomorphism $\tau : k' \xrightarrow{\sim} k$ and a τ-semilinear isomorphism of abelian groups $\sigma : V' \xrightarrow{\sim} V$ which induces φ, i. e.

$$\varphi(v' \bmod k'^{\times}) = \sigma(v') \bmod k^{\times} \quad \textit{for } v' \in V' \setminus \{0\}.$$

If $(\tilde{\sigma}, \tilde{\tau})$ is another such pair, then $\tilde{\tau} = \tau$ and $\tilde{\sigma} = \sigma \circ m_\alpha$ for a unique $\alpha \in k'^{\times}$, where $m_\alpha \in \mathrm{Aut}_{k'}(V')$ is multiplication by α. □

Lemma 9.6. *Let k and k' be arbitrary fields, $L|k$ and $L'|k'$ two field extensions of degree ≥ 3 and*

$$\varphi : L'^{\times}/k'^{\times} \xrightarrow{\sim} L^{\times}/k^{\times}$$

a bijection that is simultaneously a collineation between projective spaces and an isomorphism of abelian groups. Then there exists a unique isomorphism of field extensions $\sigma : L'|k' \xrightarrow{\sim} L|k$ such that φ is induced by σ.

Proof. Let (σ, τ) be the pair from the fundamental theorem of projective geometry. We may replace σ with $\sigma \circ m_\alpha$ for a suitable $\alpha \in k'^{\times}$ and assume $\sigma(1) = 1$. It only remains to show that σ respects multiplication. Fix $x' \in L'^{\times}$ and let $m_{x'} : L' \to L'$ and $m_{\sigma(x')} : L \to L$ be multiplication by x' and $\sigma(x')$, respectively. Define

$$\begin{aligned} \phi &: L' \to L, \quad \phi = \sigma \circ m_{x'}, \\ \psi &: L' \to L, \quad \psi = m_{\sigma(x')} \circ \sigma. \end{aligned}$$

The multiplicativity of σ follows if we prove $\phi = \psi$. Both ϕ and ψ are τ-semilinear isomorphisms of abelian groups and they induce the same map $L'^{\times}/k'^{\times} \to L^{\times}/k^{\times}$:

$$\begin{aligned} \phi(a') &= \sigma(a'x') \\ &\equiv \sigma(a')\sigma(x') \bmod k^{\times} && \text{(multiplicativity of } \varphi) \\ &= \psi(a'), \end{aligned}$$

and this map is a collineation because $m_{\sigma(x')}$ and $m_{x'}$ are. By the uniqueness statement in the fundamental theorem of projective geometry, there exists a unique $\alpha \in k'^{\times}$ such that $\phi = \psi \circ m_\alpha$. Evaluate both sides at $1 \in L'$:

$$\begin{aligned} \phi(1) &= \sigma(x' \cdot 1) = \sigma(x'), \\ (\psi \circ m_\alpha)(1) &= \psi(\alpha \cdot 1) = \sigma(x') \cdot \sigma(\alpha \cdot 1) = \tau(\alpha)\sigma(x') && \text{(using } \sigma(1) = 1). \end{aligned}$$

We conclude $\tau(\alpha) = 1$, hence $\alpha = 1$ and $\phi = \psi$.

For the uniqueness statement, assume that $\tilde{\sigma} : L'|k' \xrightarrow{\sim} L|k$ is another isomorphism of field extensions inducing φ. Then $\tilde{\sigma}$ differs from σ only by precomposition with m_α for some $\alpha \in k'^\times$, but $\tilde{\sigma}(1) = 1$ forces $\alpha = 1$. □

We apply this lemma to the situation where $L|k$ is a function field in F and $L'|k'$ is a function field in F' such that $\lambda^{-1}(U_{L'}) = U_L$. By lemma 9.4 (c), $\lambda^* : L'^\times/k'^\times \xrightarrow{\sim} L^\times/k^\times$ is a collineation, so it comes from a unique isomorphism of field extensions

$$\sigma_L : L'|k' \xrightarrow{\sim} L|k.$$

Lemma 9.7. *Let $L_1 \subseteq L_2$ be an inclusion of function fields in F and let $L'_1 \subseteq L'_2$ be function fields in F' with $\lambda^{-1}(U_{L'_i}) = U_{L_i}$ for $i = 1, 2$, such that $L'_2|L'_1$ has the same degree of inseparability as $L_2|L_1$. Then the restriction of σ_{L_2} to L'_1 equals σ_{L_1}.*

Proof. Let C_1, C_2, C'_1, C'_2 be complete nonsingular models and let $\phi : C_2 \to C_1$ and $\phi' : C'_2 \to C'_1$ be the morphisms corresponding to $L_1 \subseteq L_2$ and $L'_1 \subseteq L'_2$. Denote the inclusions $L_1 \hookrightarrow L_2$ and $L'_1 \hookrightarrow L'_2$ by ϕ^* and ϕ'^*. Now consider the following diagram:

$$\begin{tikzcd}
L_1'^\times/k'^\times \arrow[rr, "\lambda^*", "\sim"'] \arrow[dr, "\phi'^*"] \arrow[dd, hook, "\text{div}"'] & & L_1^\times/k^\times \arrow[dr, "\phi^*"] \arrow[dd, hook, "\text{div}"] & \\
& L_2'^\times/k'^\times \arrow[rr, "\lambda^*", "\sim"'] \arrow[dd, hook, "\text{div}"] & & L_2^\times/k^\times \arrow[dd, hook, "\text{div}"] \\
\text{Div}(C'_1) \arrow[rr, "\lambda^*", "\sim"'] \arrow[dr, "\phi'^*"] & & \text{Div}(C_1) \arrow[dr, "\phi^*"] & \\
& \text{Div}(C'_2) \arrow[rr, "\lambda^*", "\sim"'] & & \text{Div}(C_2)
\end{tikzcd}$$

Front and back commute by definition of $\lambda^* : L_i'^\times/k'^\times \xrightarrow{\sim} L_i^\times/k^\times$, the left and right face commute by formula 3.4 and the bottom by lemma 9.3. Therefore, the top face commutes as well. This implies that σ_{L_2} restricts to an isomorphism $L'_1|k' \xrightarrow{\sim} L_1|k$, which by the uniqueness statement in lemma 9.6 coincides with σ_{L_1}. □

Lemma 9.8. *There exists a map $L \mapsto L'$ from the set of function fields in F to the set of function fields in F' such that the following holds:*

(1) $\lambda^{-1}(U_{L'}) = U_L$ for all L;

(2) whenever $L_1 \subseteq L_2$, then $L'_1 \subseteq L'_2$ and $L'_2|L'_1$ has the same degree of inseparability as $L_2|L_1$.

Proof. In characteristic zero, the first condition determines L' uniquely as the fixed field $L' = F'^{\lambda(U_L)}$ and second condition is trivially satisfied, so assume $\text{char}(k) = p > 0$. If

L_1 and L_2 are function fields in F with $L_1^i \subseteq L_2^i$ (but not necessarily $L_1 \subseteq L_2$), choose $n \in \mathbb{Z}$ with $L_1^{p^n} \subseteq L_2$ and define the **generalised degree of inseparability**

$$[L_2 : L_1]_i := p^{-n}[L_2 : L_1^{p^n}]_i \in p^{\mathbb{Z}}.$$

It is clear that this is independent of the choice of n, that $L_1 \subseteq L_2$ iff $[L_2 : L_1]_i \geq 1$, and that for $L_1^i \subseteq L_2^i \subseteq L_3^i$ the degree formula holds:

$$[L_3 : L_1]_i = [L_3 : L_2]_i \, [L_2 : L_1]_i.$$

Moreover, lemma 8.2 implies that given L_1 and L_2 with $L_1^i \subseteq L_2^i$ and given $n \in \mathbb{Z}$, there exist unique function fields $\tilde{L}_1$ and $\tilde{L}_2$ purely inseparably equivalent to L_1 and L_2, respectively, such that

$$[\tilde{L}_2 : L_1]_i = [L_2 : \tilde{L}_1]_i = p^n.$$

Now fix a function field L_0 in F, and arbitrarily choose L_0' with $\lambda^{-1}(U_{L_0'}) = U_{L_0}$. For every function field L containing L_0, define L' to be the unique function field in F' satisfying $\lambda^{-1}(U_{L'}) = U_L$ and $[L' : L_0']_i = [L : L_0]_i$. Then for an arbitrary function field L in F, the compositum LL_0 is a function field containing L_0, so we may define L' as the unique function field in F' satisfying $\lambda^{-1}(U_{L'}) = U_L$ and $[(LL_0)' : L']_i = [LL_0 : L]_i$.

To verify the second condition, consider $L_1 \subseteq L_2$ and look at the following diagram:

$$\begin{tikzcd}
 & & (L_0L_2)' \\
 & (L_0L_1)' \arrow[ur, dashed, no head] \arrow[dd, no head] & \\
L_0' \arrow[ur, no head] & & L_2' \arrow[uu, no head] \\
 & L_1' \arrow[ur, dashed, no head] &
\end{tikzcd}$$

A dashed line indicates that a priori the inclusion holds only after passing to the purely inseparable closure. Since the generalised degrees of inseparability $[(L_0L_2)' : L_0']_i$ and $[(L_0L_1)' : L_0']_i$ are the same as for the corresponding function field extensions in F, this is also true for $(L_0L_2)'|(L_0L_1)'$. A similar reasoning with the degrees in the parallelogram now implies $[L_2' : L_1']_i = [L_2 : L_1]_i$. This also shows that the dashed lines are in fact inclusions and in particular we have $L_1' \subseteq L_2'$. □

Lemma 9.9.

(a) *Let $\sigma \in \operatorname{Aut}(F)$ be a field automorphism such that $\sigma L = L$ for all function fields L in F. Then $\sigma = \mathrm{id}$.*

(b) *Assume $\operatorname{char}(k) = p > 0$ and let $\sigma \in \operatorname{Aut}(F)$ be a field automorphism such that $\sigma L^i = L^i$ for all function fields $L|k$ in F. Then σ is a power of the Frobenius automorphism.*

(c) *Let $\lambda \in \operatorname{Aut}(G)$ be a topological automorphism such that $\lambda(U) = U$ for all compact open subgroups U in G. Then $\lambda = \mathrm{id}$.*

Proof.

(a) Let $x \in F\backslash k$ be arbitrary and let $P(x) \in k[x]$ be a polynomial. For a prime number $\ell \neq \mathrm{char}(k)$ and all $n \in \mathbb{N}_0$, the fields $k(x)$ and $k(x, P(x)^{\ell^{-n}})$ are preserved by σ. From this it follows that $k(x, P(x)^{\ell^{-n}}) = k(x, \sigma P(x)^{\ell^{-n}})$. By Kummer theory, we have $\sigma P(x)/P(x) \in k(x)^{\times \ell^n}$. Since $n \in \mathbb{N}_0$ was arbitrary, $\sigma P(x)/P(x)$ is an infinitely ℓ-divisible element in $k(x)^\times$ and must therefore be a constant.

Now choosing $P(x) = x$ and $P(x) = x + 1$, we find $\lambda, \mu \in k^\times$ such that $\sigma(x) = \lambda x$ and $\sigma(x+1) = \mu(x+1)$. Comparing coefficients, we see $\mu = \lambda = 1$, hence $\sigma(x) = x$. Therefore, σ fixes all elements of $F \setminus k$. For $a \in k$, looking at $P(x) = x + a$ we find $\nu \in k^\times$ such that $\sigma(x + a) = \nu(x + a)$. Noting that $\sigma k = k$, we again compare coefficients and conclude that $\nu = 1$ and $\sigma(a) = a$.

(b) By our description of purely inseparable equivalence, there exists for each function field L a unique $n \in \mathbb{Z}$ such that $\sigma L = L^{p^n}$. We show that n is independent of L. Since any two function fields have a common finite extension (their compositum) it is enough to consider $L_1 \subseteq L_2$. If $\sigma L_i = L_i^{p^{n_i}}$ for $i = 1, 2$, then

$$\begin{aligned}
[\sigma L_2 : L_1^{p^{n_1}}] &= [\sigma L_2 : \sigma L_1] = [L_2 : L_1], \\
[\sigma L_2 : L_1^{p^{n_2}}] &= [L_2^{p^{n_2}} : L_1^{p^{n_2}}] = [L_2 : L_1],
\end{aligned}$$

so σL_2 has the same degree over its subfields $L_1^{p^{n_1}}$ and $L_1^{p^{n_2}}$. One is contained in the other, thus they are equal and $n_1 = n_2$.

This shows that there exists $n \in \mathbb{Z}$ such that $\sigma L = L^{p^n}$ for all function fields L in F. Now $(\sigma \circ \mathrm{Frob}^{-n})(L) = L$ for all function fields L, thus $\sigma = \mathrm{Frob}^n$ by (a).

(c) Let $\sigma \in G$. For all compact open subgroups U of G we have

$$\sigma U \sigma^{-1} = \lambda(\sigma U \sigma^{-1}) = \lambda(\sigma) U \lambda(\sigma)^{-1},$$

thus $\sigma^{-1}\lambda(\sigma)$ is contained in the normaliser of U. This implies $\sigma^{-1}\lambda(\sigma)(L^i) = L^i$ for all function fields $L|k$ in F, so $\sigma^{-1}\lambda(\sigma)$ is a power of the Frobenius by (b). But it also has to leave k pointwise fixed, hence $\sigma^{-1}\lambda(\sigma) = 1$. □

Now we can prove the main result.

Proof of theorem B. Choose a bijection $L \mapsto L'$ between function fields in F and function fields in F' as in lemma 9.8. Let us summarise what we haven shown so far: The isomorphisms

$$\lambda^{\mathrm{ab},\ell} : U_L^{\mathrm{ab},\ell} \xrightarrow{\sim} U_{L'}^{\mathrm{ab},\ell}$$

map decomposition groups to decomposition groups and therefore induce bijections $\lambda^* : C' \xrightarrow{\sim} C$ between complete nonsingular models. The induced isomorphisms $\lambda^* : \mathrm{Div}(C') \xrightarrow{\sim} \mathrm{Div}(C)$ restrict to isomorphisms between the subgroups of principal divisors, defining isomorphisms of abelian groups

$$\lambda^* : L'^\times / k'^\times \xrightarrow{\sim} L^\times / k^\times,$$

which are also collineations of projective spaces. The fundamental theorem of projective geometry implied that these come from isomorphisms of field extensions

$$\sigma_L : L'|k' \xrightarrow{\sim} L|k.$$

By lemma 9.7, the σ_L are compatible with restrictions, so they glue together to a global isomorphism

$$\sigma : F'|k' \xrightarrow{\sim} F|k,$$

such that $\sigma|_{L'} = \sigma_L$ for all L. With $\sigma^*(\tau) = \sigma^{-1}\tau\sigma$ for $\tau \in G$ we have

$$\sigma^*(U_L) = \sigma^{-1}U_L\sigma = U_{\sigma^{-1}L} = U_{L'} = \lambda(U_L)$$

for all L, hence $\lambda^{-1}\sigma^*$ is an automorphism of G preserving all open compact subgroups. By lemma 9.9 (c), $\lambda = \sigma^*$. This proves the surjectivity of

$$\mathrm{Isom}^i(F'|k', F|k) \longrightarrow \mathrm{Isom}(G, G').$$

Suppose $\tilde{\sigma}$ is another isomorphism with $\tilde{\sigma}^* = \sigma^*$. Then we have

$$U_L = (\tilde{\sigma}^*)^{-1}\sigma^*U_L = U_{\tilde{\sigma}\sigma^{-1}L},$$

hence $\tilde{\sigma}\sigma^{-1}L^i = L^i$ for all L. In characteristic zero, $L^i = L$ and we conclude $\tilde{\sigma} = \sigma$ by lemma 9.9 (a). In positive characteristic, $\tilde{\sigma}$ and σ differ by a power of the Frobenius by lemma 9.9 (b). □

References

[Art57] Emil Artin. *Geometric Algebra.* Interscience Publishers, New York, 1957.

[Bog91] Fedor A. Bogomolov. On two conjectures in birational algebraic geometry. In *ICM-90 Satellite Conference Proceedings*, pages 26–52. Springer, Japan, 1991.

[BT08] Fedor Bogomolov and Yuri Tschinkel. Reconstruction of function fields. *Geometric and Functional Analysis*, 18(2):400–462, 2008.

[Gro97] Alexander Grothendieck. Brief an G. Faltings. In *Geometric Galois actions, 1*, volume 242 of *London Math. Soc. Lecture Note Series*, pages 49–58. Cambridge University Press, Cambridge, 1997. With an English translation on pp. 285–293.

[GW10] U. Görtz and T. Wedhorn. *Algebraic Geometry: Part I: Schemes. With Examples and Exercises.* Vieweg+Teubner, Wiesbaden, 2010.

[Har77] Robin Hartshorne. *Algebraic geometry.* Springer, Berlin Heidelberg New York, 1977.

[Har95] David Harbater. Fundamental groups and embedding problems in characteristic p. In *Recent developments in the inverse Galois problem*, volume 186 of *Contemp. Math.*, pages 353–369. American Mathematical Society, Providence, RI, 1995.

[Lan02] Serge Lang. *Algebra.* Springer, 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.

[Mum74] David Mumford. *Abelian varieties.* Published for the Tata Institute of Fundamental Research, Bombay by Oxford University Press, 1974.

[Mum11] David Mumford. Varieties defined by quadratic equations. In E. Marchionna, editor, *Questions on Algebraic Varieties*, volume 51 of *C.I.M.E. Summer Schools*, pages 29–100. Springer, Berlin Heidelberg, 2011.

[Neu07] Jürgen Neukirch. *Algebraische Zahlentheorie.* Springer, Berlin Heidelberg New York, 2007.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields.* Grundlehren der mathematischen Wissenschaften. Springer, 2008.

[Pop95] Florian Pop. Étale Galois covers of affine smooth curves. The geometric case of a conjecture of Shafarevich. On Abhyankar's conjecture. *Inventiones Mathematicae*, 120(3):555–578, 1995.

[Pop00] Florian Pop. Alterations and birational anabelian geometry. In *Resolution of Singularities*, volume 181, pages 519–532. Birkhäuser, Basel, 2000.

[Pop12a] Florian Pop. On the birational anabelian program initiated by Bogomolov I. *Inventiones Mathematicae*, 187(3):511–533, 2012.

[Pop12b] Florian Pop. Recovering function fields from their decomposition graphs. In *Number theory, analysis and geometry*, pages 519–594. Springer, New York, 2012.

[PŠŠ66] I. I. Pjateckiĭ-Šapiro and I. R. Šafarevič. Galois theory of transcendental extensions and uniformization. *Izv. Akad. Nauk SSSR Ser. Mat.*, 30:671–704, 1966. In Russian. With an English Translation in Amer. Soc. Math. Translations, 69:111–145, 1968.

[Rov03] M. Rovinsky. On certain isomorphisms between absolute Galois groups. *Compositio Mathematica*, 136(1):61–67, 2003.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, Dordrecht Heidelberg London New York, 2009.

Declaration

I hereby declare that this thesis is my own work and effort and that it has not been submitted anywhere for any award. Where other sources of information have been used, they have been acknowledged.

Heidelberg, March 2015