# Tame Class Field Theory for Global Function Fields

Florian Hess, Maike Massierer

# Tame Class Field Theory for Global Function Fields

Florian Hess[1] and Maike Massierer*[2]

[1]Institut für Mathematik, Carl von Ossietzky Universität Oldenburg, 26111 Oldenburg, Germany,
florian.hess@uni-oldenburg.de, phone +49 441 798 2906
[2]Mathematisches Institut, Universität Basel, Rheinsprung 21, 4051 Basel, Switzerland,
maike.massierer@inria.fr, phone +33 3 54 95 86 13

**Abstract**

We give a function field specific, algebraic proof of the main results of class field theory for abelian extensions of degree coprime to the characteristic. By adapting some methods known for number fields and combining them in a new way, we obtain a different and much simplified proof, which builds directly on a standard basic knowledge of the theory of function fields. Our methods are explicit and constructive and thus relevant for algorithmic applications. We use generalized forms of the Tate–Lichtenbaum and Ate pairings, which are well-known in cryptography, as an important tool.

**Mathematics Subject Classification (2010)** primary: 11R37, secondary: 11R58, 11T71
**Keywords** Class field theory, global function fields, Tate–Lichtenbaum pairing

## 1 Introduction

The aim of class field theory for global and local fields is to classify all abelian extensions of a given base field $F$ in terms of data associated to $F$ alone. If $F$ is a global function field, class field theory establishes a one-to-one correspondence between the finite abelian extensions of $F$ and the subgroups of finite index of ray divisor class groups $\mathcal{C}\ell_{\mathfrak{m}}(F)$. Every such subgroup $H$ of $\mathcal{C}\ell_{\mathfrak{m}}(F)$ is associated with its class field $E$, an abelian extension of $F$ uniquely determined by $H$, which is unramified outside of the support of an effective divisor $\mathfrak{m}$. The class field $E$ is characterized by the property $\mathrm{Gal}(E|F) \cong \mathcal{C}\ell_{\mathfrak{m}}(F)/H$ under the Artin map.

The study of class field theory, which originated during the second half of the 19th century with the focus on number fields, has a long tradition in number theory, and several different proofs of the main results exist. While some apply only to number fields or local fields of characteristic zero as base fields and use specific methods exploiting their properties, others provide general frameworks that cover several types of base fields and apply to even more general geometric forms of class field theory. These more general proofs use involved and abstract machinery such as in particular group cohomology. Algebraic proofs for class field theory of global function fields in the literature are presented in such general contexts. Since number fields were historically considered first, these proofs for function fields are usually a minimum adaption of those for number fields.

The goal of this work is to attempt a best possible adaption and give a tailored algebraic proof of class field theory for global function fields in a classical style. Our approach is short,

*The author was supported by the Swiss National Science Foundation under grant no. 123393 and 151884.

direct and self-contained and requires a much smaller apparatus of definitions and concepts than the known proofs. In fact, it builds directly on the content of introductory books to the theory of function fields, such as [Ros02, Sti93], without requiring any further theory. Moreover, our approach is rather explicit and therefore interesting from an algorithmic point of view, e.g. for the computation of class fields or in cryptography.

**Literature.** Some standard works of class field theory are [AT67, CF67, Lan70, Jan73, Wei73, Ser79, Ser88, Neu99, NSW08] and [Mil08]. Gras [Gra03] is a more unconventional book that omits the proofs of the central results, but concentrates more on comprehension and applications. An elaborate account of the historical development of class field theory for global function fields, including many references, is given by Roquette [Roq02]. Two particularly prominent original publications, which essentially concluded the work on class field theory for global function fields, are due to Schmid [Sch37] and Witt [Wit35].

Most of the standard works cited above treat only number fields. Artin and Tate [AT67] and Weil [Wei73] axiomatize their theory so that it also applies to global function fields. So does Tate [CF67], but his proofs are restricted to abelian extensions of degree coprime to the characteristic. These proofs in [AT67, Wei73, CF67] are based on local class field theory and Galois cohomology or Brauer groups. Lang [Lan70] presents a more classical proof using global considerations. He covers only number fields but states that the proof carries over to (abelian extensions of degree coprime to the characteristic of) function fields with only minor modifications. The original development and proof of class field theory for global function fields, and in particular the approach of [Wit35], are similar to the exposition of [CF67, Lan70] in many aspects. Serre [Ser88] provides a geometric approach, based on algebraic groups and more precisely on generalized Jacobians, which applies to function fields only. Villa Salvador [Vil06] presents a summary of global and local class field theory for function fields with main reference to [CF67] and provides a detailed exposition for the analytic, "complex multiplication" approach of Carlitz, Drinfeld and Hayes. Greenberg [Gre74] gives an elementary proof of the Kronecker–Weber Theorem.

**Our Contribution.** We provide a function field specific, algebraic proof of class field theory for abelian extensions of degree coprime to the characteristic that is short, direct and requires a minimum of prerequisities. It does not make reference to local class field theory, Galois cohomology, Brauer groups, involved index computations, $L$-series or Drinfeld modules. Methodically our approach is purely global and thus somewhat similar to the classical global approaches for number fields, as presented e.g. in [Lan70]. It is also related to the general duality framework presented in [Mil06], which is based on a cup pairing on cohomology groups, as one of the main tools in our proof is also a pairing. Our improvements are essentially due to three ingredients: Firstly, we exploit specific properties of function fields, such as the evaluation of functions and in particular Weil reciprocity, that are not available for number fields. Secondly, we reduce to maximal abelian extensions of fixed exponents and unramified outside finite sets instead of cyclic extensions for simplification. Thirdly, we rearrange the flow of arguments that usually builds class field theory.

The proofs in the literature that deal with function fields treat number fields at the same time. Since number fields have less specific properties and are more difficult to handle, the resulting proofs are more complicated for function fields than would be necessary. Also, these aforementioned proofs apply to abelian extensions of degree coprime to the characteristic only. The case of abelian extensions where the degree is a power of the characteristic does not occur for number fields and needs to be treated separately for function fields. In this paper we focus on the simplifications in the treatment of the first case that can be specifically achieved for function fields and leave the second case aside, since it requires rather different considerations.

An outline of our proof is as follows. First we give a short and self-contained proof of the surjectivity of the Artin map in Section 3 as stated in Theorem 3.3. This is based on the surjectivity of the Artin map in constant field extensions, which is rather trivially established, and a Galois twisting argument that is also used in the proof of the Chebotarev density theorem in [FJ86, Ch. 6] and in the proof of the reciprocity law of Artin in [Lan70, Ch. X.2]. This immediately gives us the first inequality for general abelian extensions, namely that the norm index is greater than or equal to the extension degree. In the standard proofs of [CF67, Lan70] the first inequality is obtained from local norm index computations and cohomological machinery, for cyclic extensions only. The surjectivity of the Artin map is then derived from the first inequality for cyclic extensions using the openness of local norm groups and implies the first inequality for general abelian extensions.

In Section 4, we prove the reciprocity law of Artin. Lemma 4.3 gives a concrete algebraic description of the Artin map by means of function evaluation for cyclic extensions of degree dividing $n$, for some $n$ coprime to the characteristic of $F$. This is a generalization of a result for the case when the $n$-th roots of unity are contained in the base field, shown by Hasse in [Has35]. Using Weil reciprocity and a straightforward calculation, Lemma 4.3 implies the reciprocity law of Artin, which is Theorem 4.5. The standard proofs of [CF67, Lan70] proceed differently. Both prove the second inequality, namely that the norm index is less than or equal to the extension degree for general abelian extensions, prior to the reciprocity law. In [Lan70] this is done analytically using $L$-series. The reciprocity law is then reduced via the aforementioned Galois twisting argument to the reciprocity law in cyclic cyclotomic extensions, where it is proved by direct computation, and to the already established norm index equality in such extensions. In [CF67], the second inequality is proved together with other cohomological statements and statements about Brauer groups, using the algebraic approach of Chevalley. The latter are then used to reduce the reciprocity law to the reciprocity law in cyclic cyclotomic extensions, which are essentially dealt with as in [Lan70].

At this stage the second inequality and the existence theorem are yet to be proven in our approach. To this end we prove in Theorem 6.3 of Section 6 that the kernel of the Artin map for the maximal abelian extension of exponent $n$ of a base field containing the $n$-th roots of unity, which is unramified outside an arbitrary finite set $\mathcal{S}$, consists precisely of $n$-th multiples. Analogous statements are proved in [CF67, Lan70] for the existence theorem, with the main difference being that they crucially use the second inequality that we have not yet established. We offer a proof that does not require the second inequality. Instead we rely on a generalization of the Tate–Lichtenbaum pairing and a proof of its non-degeneracy obtained from various symmetries in the evaluation of functions at divisors that are exhibited in Section 5 with its main Theorem 5.2. An interesting feature of the proofs is that while [CF67, Lan70] need to enlarge $\mathcal{S}$ to complete their arguments, we actually reduce $\mathcal{S}$ to the empty set. In Section 7 we generalize the final existence proofs in [CF67, Lan70] to the situation of not using the second inequality by means of a suitable induction and obtain our final Theorem 7.8.

Summarizing, we see Lemma 4.3, Theorems 5.1 and 5.2, the induction argument in Theorem 7.8 and their composition to a full proof of class field theory coprime to the characteristic as essential new contributions of our work.

Our approach has been inspired by constructive methods used in cryptography. In particular, our main pairing $t_{n,\mathfrak{m}}$ is a generalization of the Tate–Lichtenbaum pairing [1, 6, 7]. Moreover, the function $h$ of Lemma 4.3 is closely related to the Ate pairings [2, 3, 8]. These pairings play an important role in cryptography. Our proof of Lemma 4.3 features similarities with the proof of the bilinearity and non-degeneracy of the Ate pairings. In cryptography, pairings are usually considered for elliptic or hyperelliptic curves and prime exponents $n$. Since our setting here is much more general, Lemma 4.3 can be used to derive new Ate pairings for general curves and composite exponents $n$. We give a brief further discussion of pairings in geometry and cryptography and their relation to our paper and class field theory in Appendix B.

# 2 Preliminaries

We collect some basic facts that will be used frequently in this paper. Unless defined here we will use standard notation as in [Sti93]. By global function field, we mean the function field of an irreducible smooth projective curve over a finite field.

### Ray Class Groups and Artin Map

We fix a global function field $F$ with exact constant field $\mathbb{F}_q$ and an algebraic closure $\bar{F}$. All extension fields of $F$ in this paper are finite and separable over $F$ and contained in $\bar{F}$. The multiplicative group of $n$-th roots of unity in $\bar{F}$ is denoted by $\mu_n$.

**Definition 2.1.** Let $\mathfrak{m}$ be an effective divisor of $F$ and $L$ an extension field of $F$. We denote the group of divisors of $L$ with support disjoint from the support of the conorm $\mathrm{Con}_{L|F}(\mathfrak{m})$ of $\mathfrak{m}$ by $\mathcal{D}_\mathfrak{m}(L)$. This group has a subgroup $\mathcal{P}_\mathfrak{m}(L)$, called the **ray** of $L$ modulo $\mathfrak{m}$, consisting of principal divisors $\mathrm{div}_L(f)$ with $f \in L^\times$ satisfying the congruence $f \equiv 1 \bmod \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\mathrm{Con}_{L|F}(\mathfrak{m}))}$ in the valuation ring $\mathcal{O}_\mathfrak{p}$ for all places $\mathfrak{p}$ of $L$. The **ray class group** of $L$ modulo $\mathfrak{m}$ is then

$$\mathcal{C}\ell_\mathfrak{m}(L) = \mathcal{D}_\mathfrak{m}(L)/\mathcal{P}_\mathfrak{m}(L).$$

Further details about these groups can be found in [Sti93] for $\mathfrak{m} = 0$ and in [HPP03] for general $\mathfrak{m}$. We abbreviate $\mathcal{D}(L) = \mathcal{D}_0(L)$ and $\mathcal{P}(L) = \mathcal{P}_0(L)$, which are the usual group of divisors and its subgroup of principal divisors.

**Remark 2.2.** Notice that $\mathcal{D}_\mathfrak{m}(L)$ depends only on the support of $\mathfrak{m}$ while $\mathcal{P}_\mathfrak{m}(L)$ and $\mathcal{C}\ell_\mathfrak{m}(L)$ depend on $\mathfrak{m}$ itself. Later we will also use, and prove, that $\mathcal{C}\ell_\mathfrak{m}(L)/n\mathcal{C}\ell_\mathfrak{m}(L)$ depends again only on the support of $\mathfrak{m}$ when $n$ is coprime to $q$.

**Remark 2.3.** The most frequently used case of the above definition in this paper is for $L = F$. Then $\mathcal{D}(F)$ and $\mathcal{P}(F)$ are the groups of divisors and principal divisors of $F$, respectively, and we have

$$\begin{aligned}
\mathcal{D}_\mathfrak{m}(F) &= \{\mathfrak{d} \in \mathcal{D}(F) \mid \mathrm{supp}(\mathfrak{d}) \cap \mathrm{supp}(\mathfrak{m}) = \emptyset\} && (1)\\
\mathcal{P}_\mathfrak{m}(F) &= \{\mathrm{div}_F(f) \in \mathcal{P}(F) \mid f \in F^\times, f \equiv 1 \bmod \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}\mathfrak{m}} \text{ in } \mathcal{O}_\mathfrak{p} \text{ for all places } \mathfrak{p} \text{ of } F\} && (2)\\
\mathcal{C}\ell_\mathfrak{m}(F) &= \mathcal{D}_\mathfrak{m}(F)/\mathcal{P}_\mathfrak{m}(F). && (3)
\end{aligned}$$

**Definition 2.4.** Let $F'$ be an extension field of $F$ and $E'$ an extension field of $F'$. We say that $E'|F'$ is **unramified outside** $\mathfrak{m}$ if $E'|F'$ is unramified at all places of $F'$ outside the support of $\mathrm{Con}_{F'|F}(\mathfrak{m})$.

We have conorm and norm maps $\mathrm{Con}_{E'|F'} : \mathcal{D}_\mathfrak{m}(F') \to \mathcal{D}_\mathfrak{m}(E')$ and $\mathrm{N}_{E'|F'} : \mathcal{D}_\mathfrak{m}(E') \to \mathcal{D}_\mathfrak{m}(F')$ with $\mathrm{Con}_{E'|F'}(\mathcal{P}_\mathfrak{m}(F')) \subseteq \mathcal{P}_\mathfrak{m}(E')$ and $\mathrm{N}_{E'|F'}(\mathcal{P}_\mathfrak{m}(E')) \subseteq \mathcal{P}_\mathfrak{m}(F')$.

**Definition 2.5.** Assume now $E'|F'$ abelian and let $\mathfrak{p}$ be a place of $F'$ unramified in $E'$. Define $\mathrm{N}(\mathfrak{p}) = \#\mathcal{O}_\mathfrak{p}/\mathfrak{p} = q^{\deg(\mathfrak{p})}$. There is a uniquely determined automorphism $\sigma_\mathfrak{p} \in \mathrm{Gal}(E'|F')$ such that

$$\sigma_\mathfrak{p}(x) \equiv x^{\mathrm{N}(\mathfrak{p})} \bmod \mathfrak{q}$$

for all $x \in \mathcal{O}_\mathfrak{q}$ and all places $\mathfrak{q}$ of $E'$ lying above $\mathfrak{p}$. Let $\mathfrak{m}$ denote an effective divisor of $F$ such that $E'|F'$ is unramified outside $\mathfrak{m}$. The **Artin map** is defined as

$$\mathrm{A}_{E'|F'} : \mathcal{D}_\mathfrak{m}(F') \to \mathrm{Gal}(E'|F'), \quad \mathfrak{d} \mapsto \prod_\mathfrak{p} \sigma_\mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\mathfrak{d})}, \tag{4}$$

where the product runs over all places $\mathfrak{p}$ of $F'$. If $\mathcal{P}_\mathfrak{m}(F') \subseteq \ker \mathrm{A}_{E'|F'}$ then $\mathfrak{m}$ is called a **modulus** of $E'|F'$.

These definitions apply in particular to the case where $F' = F$. The following general properties of the Artin map are used frequently in this paper.

**Theorem 2.6.** *We use the same notation as in Definition 2.5.*

*(i) Let $E$ be an intermediate field of $E'|F$. Then*

$$\mathrm{A}_{E|F}(\mathrm{N}_{F'|F}(\mathfrak{d})) = \mathrm{A}_{E'|F'}(\mathfrak{d})|_E$$

*for all $\mathfrak{d} \in \mathcal{D}_\mathfrak{m}(F')$.*

*(ii) Let $\sigma \in \mathrm{Hom}(E', \bar{F})$. Then*

$$\mathrm{A}_{\sigma(E')|\sigma(F')}(\sigma(\mathfrak{d})) = \sigma \circ \mathrm{A}_{E'|F'}(\mathfrak{d}) \circ \sigma^{-1}$$

*for all $\mathfrak{d} \in \mathcal{D}_\mathfrak{m}(F')$.*

*Proof.* See [Ros02, Prop. 9.10, Prop. 9.11] or [AT67]. □

**Corollary 2.7.** *If $E'|F$ is abelian with modulus $\mathfrak{m}$ then any $\mathfrak{n} \geq \mathfrak{m}$ is also a modulus of $E'|F$. Every intermediate field $E$ of $E'|F$ also has modulus $\mathfrak{m}$. If $E_1|F$ and $E_2|F$ are abelian with modulus $\mathfrak{m}$ then $E_1E_2|F$ is abelian with modulus $\mathfrak{m}$.*

*Proof.* The first statement follows from $\mathcal{P}_\mathfrak{n}(F) \subseteq \mathcal{P}_\mathfrak{m}(F)$. The second statement is an easy consequence of Theorem 2.6, $(i)$ with $F' = F$. The third statement is an easy consequence of Theorem 2.6, $(i)$ with $F' = F$, $E' = E_1E_2$, $E = E_1$ or $E = E_2$, some Galois theory and the Lemma of Abhyankar [Sti93, Prop. III.8.9]. □

### Pairings

Let $A$ and $B$ be abelian groups with dual groups $A^\vee = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ and $B^\vee = \mathrm{Hom}(B, \mathbb{Q}/\mathbb{Z})$.

**Definition 2.8.** A **pairing** is a bilinear map $\tau : A \times B \to \mathbb{Q}/\mathbb{Z}$. It defines two homomorphisms $\tau_{\mathrm{left}} : A \to B^\vee$ and $\tau_{\mathrm{right}} : B \to A^\vee$. The left and right kernels of $\tau$ are $\ker(\tau_{\mathrm{left}})$ and $\ker(\tau_{\mathrm{right}})$ respectively. If $\tau_{\mathrm{left}}$ is injective then $\tau$ is called non-degenerate on the left. If $\tau_{\mathrm{right}}$ is injective then $\tau$ is called non-degenerate on the right. Finally, $\tau$ is called **non-degenerate** if it is non-degenerate on the left and right.

If $A$ and $B$ have exponent $n$ we will replace the codomain of $\tau$ by some other cyclic group of order $n$, such as $\mu_n \subseteq \bar{F}$ if $n$ and $q$ are coprime.

The following two criteria for non-degeneracy of a pairing will be useful.

**Lemma 2.9.** *Let $A$ and $B$ be finite abelian groups and $\tau : A \times B \to \mathbb{Q}/\mathbb{Z}$ a pairing. Then $\tau$ is non-degenerate if and only if $\tau$ is non-degenerate on the left (or right) and $\#A = \#B$.*

*Proof.* If $\tau$ is non-degenerate then it is non-degenerate on the left and right by definition. Conversely, suppose $\tau$ is non-degenerate on the left, so $\tau_{\text{left}}$ is injective. We have $B \cong \prod_{i=1}^n B_i$ for suitable finite cyclic groups $B_i$. Then $B_i^\vee \cong B_i$ and $B^\vee \cong \prod_{i=1}^n B_i^\vee \cong \prod_{i=1}^n B_i \cong B$, thus $\#B^\vee = \#B$. Since $\#B = \#A$ by assumption, $\tau_{\text{left}}$ is also surjective by the finite and equal cardinalities of $A$ and $B$. $\square$

Let $\phi_i : A_i \to A_{i+1}$ and $\psi_i : B_{i+1} \to B_i$ for $1 \leq i \leq 4$ denote two exact sequences of finite abelian groups. Let $\tau_i : A_i \times B_i \to \mathbb{Q}/\mathbb{Z}$ be pairings such that the maps $\phi_i$ and $\psi_i$ are adjoint with respect to $\tau_i$ and $\tau_{i+1}$, that is $\tau_i(x, \psi_i(y)) = \tau_{i+1}(\phi_i(x), y)$ for all $x \in A_i$, $y \in B_{i+1}$ and $1 \leq i \leq 4$.

**Lemma 2.10.** *If $\tau_1$, $\tau_2$, $\tau_4$ and $\tau_5$ are non-degenerate, then $\tau_3$ is non-degenerate.*

*Proof.* Dualization gives an exact sequence $\psi_i^\vee : B_i^\vee \to B_{i+1}^\vee$, and the adjoint condition reads $\psi_i^\vee \circ (\tau_i)_{\text{left}} = (\tau_{i+1})_{\text{left}} \circ \phi_i$ for all $1 \leq i \leq 4$. As in Lemma 2.9 the non-degeneracy of $\tau_i$ and finiteness of the groups imply that $(\tau_1)_{\text{left}}$, $(\tau_2)_{\text{left}}$, $(\tau_4)_{\text{left}}$ and $(\tau_5)_{\text{left}}$ are isomorphisms. Then $(\tau_3)_{\text{left}}$ is an isomorphism by the five lemma and $\tau_3$ is non-degenerate by Lemma 2.9. $\square$

# 3 Surjectivity of the Artin Map

In this section we give a self-contained proof of the surjectivity of the Artin map, as stated in Theorem 3.3, that reduces via a Galois twisting argument to the surjectivity of the Artin map for constant field extensions as in Lemma 3.2. The proofs can be seen as a much simplified version of the proof of the full Cebotarev density theorem from [FJ86, Ch. 6].

**Definition 3.1.** The **Frobenius automorphism** $\varphi$ of a constant field extension $F'$ of $F$ is defined as follows. Let $\mathbb{F}_{q^n}$ denote the exact constant field of $F'$. Then $F$ and $\mathbb{F}_{q^n}$ are linearly disjoint over $\mathbb{F}_q$, and thus $\mathrm{Gal}(F'|F) \cong \mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ by restriction of automorphisms. Then $\varphi$ is defined as the unique extension of the $q$-power Frobenius automorphism of $\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ to $\mathrm{Gal}(F'|F)$.

The definition is compatible with restriction, so we use the same symbol $\varphi$ for different constant field extensions without further mentioning.

**Lemma 3.2.** *Let $F'|F$ be a constant field extension. Then $\mathrm{Gal}(F'|F)$ is generated by the Frobenius automorphism $\varphi$ and*

$$\mathrm{A}_{F'|F} : \mathcal{D}(F) \to \mathrm{Gal}(F'|F)$$

*is given by*

$$\mathrm{A}_{F'|F}(\mathfrak{d}) = \varphi^{\deg(\mathfrak{d})}.$$

*The zero divisor of $F$ is a modulus of $F'|F$.*

*Proof.* The first statement is clear from $\mathrm{Gal}(F'|F) \cong \mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$. For the second statement let $\mathfrak{p}$ be a place of $F$ and $\mathfrak{q}$ a place of $F'$ above $\mathfrak{p}$. Then $\mathrm{A}_{F'|F}(\mathfrak{p})(x) \equiv x^{\mathrm{N}(\mathfrak{p})} \bmod \mathfrak{q}$ for all $x \in \mathcal{O}_{\mathfrak{q}}$ by the definition of $\mathrm{A}_{F'|F}(\mathfrak{p})$. Let $z$ be a primitive element of $\mathbb{F}_{q^n}|\mathbb{F}_q$. Then $z$ is also a primitive element of $F'|F$, and $z \in \mathcal{O}_{\mathfrak{q}}$ since it is a constant. Now $\mathrm{A}_{F'|F}(\mathfrak{p})(z)$ and $z^{\mathrm{N}(\mathfrak{p})}$ are also constants, so $\mathrm{A}_{F'|F}(\mathfrak{p})(z) - z^{\mathrm{N}(\mathfrak{p})} \in \mathfrak{q}$ is a constant with zeros and hence must be identically zero. Thus $\mathrm{A}_{F'|F}(\mathfrak{p})(z) = z^{\mathrm{N}(\mathfrak{p})} = \varphi^{\deg(\mathfrak{p})}(z)$. Since $\mathrm{A}_{F'|F}(\mathfrak{p})$ and $\varphi^{\deg(\mathfrak{p})}$ are $F$-linear and agree on the primitive element $z$ of $F'|F$ we get $\mathrm{A}_{F'|F}(\mathfrak{p}) = \varphi^{\deg(\mathfrak{p})}$ on all of $F'$. Finally, by linearity, $\mathrm{A}_{F'|F}(\mathfrak{d}) = \varphi^{\deg(\mathfrak{d})}$ for all divisors $\mathfrak{d} \in \mathcal{D}(F)$.

If $\mathfrak{d} \in \mathcal{P}(F)$ then $\deg(\mathfrak{d}) = 0$ and $\mathrm{A}_{F'|F}(\mathfrak{d}) = \varphi^{\deg(\mathfrak{d})} = \mathrm{id}$, so $\mathcal{P}(F) \subseteq \ker \mathrm{A}_{F'|F}$ and 0 is a modulus of $F'|F$. $\square$

**Theorem 3.3.** *Let $E|F$ be an abelian extension. The Artin map defines an epimorphism*

$$\mathrm{A}_{E|F} : \mathcal{D}_{\mathfrak{m}}(F) \to \mathrm{Gal}(E|F)$$

*for any effective divisor $\mathfrak{m}$ containing the ramified places of $F$.*

*Proof.* The proof is by generalizations from special to more general cases.

($i$): Let $E|F$ be a constant field extension. By [Sti93, p. 191] there is a divisor $\mathfrak{d}$ of $F$ of degree one. The approximation theorem [Sti93, p. 12, p. 33] shows that $\mathfrak{d}$ can be chosen coprime to $\mathfrak{m}$. Then $\mathrm{A}_{E|F}(\mathfrak{d})$ is a generator of $\mathrm{Gal}(E|F)$ by Lemma 3.2, and $\mathrm{A}_{E|F}$ is thus surjective.

($ii$): Let $E|F$ be regular and cyclic of degree $n$. Denote the exact constant field of $F$ and $E$ by $\mathbb{F}_q$. Define $L = E\mathbb{F}_{q^n} = E(F\mathbb{F}_{q^n})$. Then $L|F$ is abelian and ramified only inside $\mathfrak{m}$. More precisely, since $E$ and $F\mathbb{F}_{q^n}$ are linearly disjoint over $F$, we have $\mathrm{Gal}(L|F) \cong \mathrm{Gal}(E|F) \times \mathrm{Gal}(F\mathbb{F}_{q^n}|F)$ by restriction. Thus there is $\tau \in \mathrm{Gal}(L|F)$ such that $\tau|_E$ is a generator $\sigma$ of $\mathrm{Gal}(E|F)$ and $\tau|_{F\mathbb{F}_{q^n}} = \varphi$ is a generator of $\mathrm{Gal}(F\mathbb{F}_{q^n}|F)$. Let $E_\tau$ be the fixed field of $\tau$ in $L$. Then $L|E_\tau$ is cyclic of degree $n$ generated by $\tau$, and the exact constant field of $E_\tau$ is $\mathbb{F}_q$. Thus $L = E_\tau\mathbb{F}_{q^n}$, and $L|E_\tau$ is a constant field extension of degree $n$. By ($i$) there is $\mathfrak{d} \in \mathcal{D}_{\mathfrak{m}}(E_\tau)$ such that $\mathrm{A}_{L|E_\tau}(\mathfrak{d}) = \tau$. Define $\mathfrak{e} = \mathrm{N}_{E_\tau|F}(\mathfrak{d}) \in \mathcal{D}_{\mathfrak{m}}(F)$. Then $\tau = \mathrm{A}_{L|E_\tau}(\mathfrak{d}) = \mathrm{A}_{L|F}(\mathfrak{e})$ and $\sigma = \tau|_E = \mathrm{A}_{E|F}(\mathfrak{e})$. Thus $\mathrm{A}_{E|F}$ is surjective.

($iii$): Let $E|F$ be arbitrary cyclic and let $\mathbb{F}_{q^n}$ be the exact constant field of $E$. Let $L = F\mathbb{F}_{q^n}$. Then $L|F$ is a constant field extension and $E|L$ is regular and cyclic. By ($i$) and ($ii$), $\mathrm{A}_{L|F} : \mathcal{D}_{\mathfrak{m}}(F) \to \mathrm{Gal}(L|F)$ and $\mathrm{A}_{E|L} : \mathcal{D}_{\mathfrak{m}}(L) \to \mathrm{Gal}(E|L)$ are surjective. To prove that $\mathrm{A}_{E|F}$ is surjective let $\sigma \in \mathrm{Gal}(E|F)$. Then there is $\mathfrak{d} \in \mathcal{D}_{\mathfrak{m}}(F)$ such that $\mathrm{A}_{L|F}(\mathfrak{d}) = \sigma|_L$. Let $\tau = \sigma \circ \mathrm{A}_{E|F}(\mathfrak{d})^{-1}$. Then $\tau \in \mathrm{Gal}(E|L)$ and there is $\mathfrak{a} \in \mathcal{D}_{\mathfrak{m}}(L)$ such that $\mathrm{A}_{E|L}(\mathfrak{a}) = \tau$. Let $\mathfrak{b} = \mathrm{N}_{L|F}(\mathfrak{a}) \in \mathcal{D}_{\mathfrak{m}}(F)$. Then $\mathrm{A}_{E|F}(\mathfrak{b}) = \tau$ and $\sigma = \tau \circ \mathrm{A}_{E|F}(\mathfrak{d}) = \mathrm{A}_{E|F}(\mathfrak{b}) \circ \mathrm{A}_{E|F}(\mathfrak{d}) = \mathrm{A}_{E|F}(\mathfrak{b} + \mathfrak{d})$. Thus $\mathrm{A}_{E|F}$ is surjective.

($iv$): Finally, let $E|F$ be abelian and let $\sigma \in \mathrm{Gal}(E|F)$. Let $L$ denote the fixed field of $\sigma$ in $E$. Then $E|L$ is cyclic with generator $\sigma$. By ($iii$) we have $\sigma = \mathrm{A}_{E|L}(\mathfrak{d})$ for some $\mathfrak{d} \in \mathcal{D}_{\mathfrak{m}}(L)$. Let $\mathfrak{e} = \mathrm{N}_{L|F}(\mathfrak{d}) \in \mathcal{D}_{\mathfrak{m}}(F)$. Then $\sigma = \mathrm{A}_{E|L}(\mathfrak{d}) = \mathrm{A}_{E|F}(\mathfrak{e})$. Thus $\mathrm{A}_{E|F}$ is surjective. ☐

# 4 Reciprocity Law

Let $E|F$ be abelian of order coprime to $q$ and unramified outside $\mathfrak{m}$. The goal of this section is to give a new, function field specific proof that $\mathfrak{m}$ is a modulus of $E|F$. This is also known as the reciprocity law. Our main tools will be Weil reciprocity and a generalization of a result by Hasse [Has35] on the algebraic representation of $\mathrm{A}_{E|F}$ by means of function evaluation, when $E|F$ is cyclic and $F$ contains enough roots of unity, to the case of arbitrary $F$, as given in Lemma 4.3.

We fix some notation.

**Definition 4.1.** Let $L$ be a finite extension of $F$ with exact constant field $\mathbb{F}_{q^r}$. Let $\mathfrak{p}$ be a place of $L$ and $f \in \mathcal{O}_\mathfrak{p}$. The residue class field $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$ of $\mathfrak{p}$ is denoted by $L_\mathfrak{p}$, and the image of $f$ in $L_\mathfrak{p}$ is denoted by $f_\mathfrak{p}$. If $\mathfrak{d} \in \mathcal{D}(L)$ is coprime to $f$ we define the **evaluation** $f(\mathfrak{d})$ of $f$ at $\mathfrak{d}$ as

$$f(\mathfrak{d}) = \prod_{\mathfrak{p} \in \mathrm{supp}(\mathfrak{d})} \mathrm{N}_{L_\mathfrak{p}|\mathbb{F}_{q^r}}(f_\mathfrak{p})^{\mathrm{ord}_\mathfrak{p}(\mathfrak{d})}. \tag{5}$$

Let $n$ be a positive integer, $\mathcal{S}$ an arbitrary set of places of $F$ and $\mathcal{T}$ the set of places of $L$ lying above the places of $\mathcal{S}$. We define the **generalized Selmer group**

$$L_{n,\mathcal{S}} = \{\, f \in L^\times \mid \mathrm{ord}_\mathfrak{p}(f) \equiv 0 \bmod n \text{ for all } \mathfrak{p} \notin \mathcal{T} \,\}.$$

If $\mathfrak{m}$ is an effective divisor of $F$ then we also write

$$L_{n,\mathfrak{m}} = L_{n,\mathrm{supp}(\mathfrak{m})}.$$

The group $L_{n,\emptyset}$ is the ordinary Selmer group as defined in [Coh00, p. 231].

**Remark 4.2.** This notation is most frequently used in this paper for $L = F$ and $\mathcal{S} = \mathrm{supp}(\mathfrak{m})$. Then we have

$$F_{n,\mathcal{S}} = \{f \in F^{\times} \mid \mathrm{ord}_{\mathfrak{p}}(f) \equiv 0 \bmod n \text{ for all } \mathfrak{p} \notin \mathcal{S}\} \quad (6)$$
$$F_{n,\mathfrak{m}} = \{f \in F^{\times} \mid \mathrm{ord}_{\mathfrak{p}}(f) \equiv 0 \bmod n \text{ for all } \mathfrak{p} \notin \mathrm{supp}(\mathfrak{m})\}. \quad (7)$$

For the rest of this section we let $E'|F$ be an abelian extension containing an intermediate field $F'$ such that $F'|F$ is a constant field extension and $\mu_n \subseteq F'$. Also, let $\mathfrak{m}$ be an effective divisor such that $E'|F$ is unramified outside $\mathfrak{m}$. We consider $\mathrm{A}_{E'|F} : \mathcal{D}_{\mathfrak{m}}(F) \to \mathrm{Gal}(E'|F)$.

**Lemma 4.3.** *Let $n$ be coprime to $q$, and suppose that $E'|F'$ is cyclic of degree dividing $n$. Let $\mathfrak{d} \in \mathcal{D}_{\mathfrak{m}}(F)$. Then $\mathrm{A}_{E'|F}(\mathfrak{d})$ is described by the following expression.*

*There is an extension $\sigma$ of $\varphi$ to $E'$ and $y \in E'$ such that $y^n \in F'_{n,\mathfrak{m}}$ and $y^n$ is coprime to $\mathrm{Con}_{F'|F}(\mathfrak{d})$. Let $h = \sigma^{-1}(y)^q y^{-1}$. Then $h \in F'^{\times}$ is coprime to $\mathrm{Con}_{F'|F}(\mathfrak{d})$ and*

$$\mathrm{A}_{E'|F}(\mathfrak{d}) = \tau_{\mathfrak{d}} \circ \sigma^{\deg \mathfrak{d}}.$$

*Here $\tau_{\mathfrak{d}} \in \mathrm{Gal}(E'|F')$ is defined by*

$$\tau_{\mathfrak{d}}(y)y^{-1} = h(\mathrm{Con}_{F'|F}(\mathfrak{d})) \in \mu_n,$$

*where $h(\mathrm{Con}_{F'|F}(\mathfrak{d}))$ stands for the evaluation of the function $h$ at the divisor $\mathrm{Con}_{F'|F}(\mathfrak{d})$, see (5) with $L = F'$.*

*Proof.* Since $E'|F$ is normal, there exists an extension $\sigma \in \mathrm{Gal}(E'|F)$ of $\varphi$.

By Kummer theory there is $y_0 \in E'$ such that $E' = F'(y_0)$ and $y_0^n \in F'^{\times}$. Define $f_0 = y_0^n$. Then $f_0 \in F'_{n,\mathfrak{m}}$ since $E'|F'$ is unramified outside $\mathfrak{m}$, by [Sti93, p. 111]. Abbreviate $\mathcal{S} = \mathrm{supp}(\mathrm{Con}_{F'|F}(\mathfrak{d}))$. Since $f_0 \in F'_{n,\mathfrak{m}}$, we can find $g \in F'^{\times}$ such that $\mathrm{supp}(f_0 g^n)$ is disjoint from $\mathcal{S}$ by the approximation theorem. Define $f = f_0 g^n$ and $y = y_0 g$. Then clearly $E' = F'(y)$ and $y^n = f \in F'_{n,\mathfrak{m}}$ is coprime to $\mathrm{Con}_{F'|F}(\mathfrak{d})$.

Let $\tau \in \mathrm{Gal}(E'|F')$. Then $\tau(y) = \zeta y$ for some $\zeta \in \mu_n$. Since $E'|F$ is abelian we get

$$\begin{aligned}\tau(h) &= (\tau \circ \sigma^{-1})(y)^q \tau(y)^{-1} = (\sigma^{-1} \circ \tau)(y)^q \tau(y)^{-1} \\ &= \sigma^{-1}(\zeta y)^q (\zeta y)^{-1} = h.\end{aligned}$$

Since $\tau$ is arbitary it follows that $h \in F'^{\times}$. Also, we have $h^n = \sigma^{-1}(y^n)^q (y^n)^{-1} = \varphi^{-1}(f)^q f^{-1}$ and

$$\mathrm{supp}(h) = \mathrm{supp}(h^n) = \mathrm{supp}(\varphi^{-1}(f)^q f^{-1}).$$

Now $\mathrm{supp}(f) \cap \mathcal{S} = \emptyset$ and $\varphi(\mathcal{S}) = \mathcal{S}$, so we obtain $\mathrm{supp}(h) \cap \mathcal{S} = \emptyset$, and $h$ is coprime to $\mathrm{Con}_{F'|F}(\mathfrak{d})$.

Let $\mathfrak{p}$ be a place in the support of $\mathfrak{d}$. Then

$$\mathrm{A}_{E'|F}(\mathfrak{p}) = \tau \circ \sigma^{\deg(\mathfrak{p})}$$

for some $\tau \in \mathrm{Gal}(E'|F')$. Indeed, we have

$$\mathrm{A}_{E'|F}(\mathfrak{p})|_{F'} = \mathrm{A}_{F'|F}(\mathfrak{p}) = \varphi^{\deg \mathfrak{p}},$$

where the last equality holds because $F'|F$ is a constant field extension, by Lemma 3.2. Then $\tau = \mathrm{A}_{E'|F}(\mathfrak{p}) \circ \sigma^{-\deg(\mathfrak{p})}$ is the required automorphism.

Now $\tau(y) = \zeta y$ for some $\zeta \in \mu_n$. We show below that

$$\zeta = h(\mathrm{Con}_{F'|F}(\mathfrak{p})).$$

Then $\tau = \tau_{\mathfrak{p}}$ and

$$\mathrm{A}_{E'|F}(\mathfrak{p}) = \tau_{\mathfrak{p}} \circ \sigma^{\deg \mathfrak{p}}.$$

From this the assertion follows for $\mathfrak{d}$ by the linearity of the maps $\mathfrak{d} \mapsto \sigma^{\deg(\mathfrak{d})}$, $\mathfrak{d} \mapsto \mathrm{A}_{E'|F}(\mathfrak{d}) \circ \sigma^{-\deg(\mathfrak{d})}$ as $\mathrm{Gal}(E'|F)$ is abelian, $\tau \mapsto \zeta$, and $\mathfrak{d} \mapsto h(\mathrm{Con}_{F'|F}(\mathfrak{d}))$.

We are left to show $\zeta = h(\mathrm{Con}_{F'|F}(\mathfrak{p}))$. Let $g = \varphi(h)^{-1}$ and $d = \deg(\mathfrak{p})$. Then $g \in F'^{\times}$, $\mathrm{supp}(g) \cap \mathcal{S} = \emptyset$ and $\sigma(y) = y^q g$ observing $\sigma(g) = \phi(g)$ since $g \in F'^{\times}$. Iterated application of $\sigma$ to $y$ gives

$$\sigma^d(y) = y^{q^d} \prod_{j=0}^{d-1} \varphi^j(g)^{q^{d-1-j}}.$$

Using this we have

$$\begin{aligned}
\mathrm{A}_{E'|F}(\mathfrak{p})(y) = (\tau \circ \sigma^d)(y) &= \tau\left( y^{q^d} \prod_{j=0}^{d-1} \varphi^j(g)^{q^{d-1-j}} \right) \\
&= \zeta^{q^d} y^{q^d} \prod_{j=0}^{d-1} \varphi^j(g)^{q^{d-1-j}} \qquad (8)
\end{aligned}$$

by direct computation. On the other hand, we have

$$\mathrm{A}_{E'|F}(\mathfrak{p})(y) \equiv y^{q^d} \bmod \mathfrak{q} \qquad (9)$$

for all places $\mathfrak{q}$ of $E'$ above $\mathfrak{p}$ by the definition of $\mathrm{A}_{E'|F}(\mathfrak{p})$. Notice that we have chosen $y$ such that this is well-defined and non-zero, i.e. $y \in \mathcal{O}_{\mathfrak{q}}^{\times}$ for all $\mathfrak{q}$. By equating (8) and (9) and canceling $y^{q^d}$, we get

$$\zeta^{q^d} \cdot \prod_{j=0}^{d-1} \varphi^j(g)^{q^{d-1-j}} \equiv 1 \bmod \mathfrak{q}. \qquad (10)$$

Both sides and all factors of the left side are already in $F'$, so the congruence holds in fact modulo all places $\mathfrak{q}$ of $F'$ above $\mathfrak{p}$, and then also modulo all places $\mathfrak{q}$ of arbitrary constant field extensions $L$ of $F'$ above $\mathfrak{p}$.

We now consider a constant field extension $L$ of $F'$ such that $\mathfrak{p}$ splits completely in $L$, i.e. $\mathrm{Con}_{L|F}(\mathfrak{p}) = \sum_{j=0}^{d-1} \mathfrak{q}_j$ with $\deg \mathfrak{q}_j = 1$ for all $j$. The $\mathfrak{q}_j$ are all conjugates, say $\mathfrak{q}_j = \varphi^{-j}(\mathfrak{q})$ for $\mathfrak{q} = \mathfrak{q}_0$. Finally, the support of $g$ is disjoint from the support of $\mathrm{Con}_{L|F}(\mathfrak{p})$. We compute

$$\begin{aligned}
g(\mathrm{Con}_{L|F}(\mathfrak{p}))^{q^{d-1}} &= \prod_{j=0}^{d-1} g(\varphi^{-j}(\mathfrak{q}))^{q^{d-1}} = \prod_{j=0}^{d-1} \varphi^{-j}(\varphi^j(g)(\mathfrak{q}))^{q^{d-1}} \\
&= \prod_{j=0}^{d-1} \varphi^j(g)(\mathfrak{q})^{q^{d-1-j}} \equiv \prod_{j=0}^{d-1} \varphi^j(g)^{q^{d-1-j}} \equiv \zeta^{-q^d} \bmod \mathfrak{q}.
\end{aligned}$$

Here the first equation holds by definition of function evaluation, the second equation holds since function evaluation commutes with automorphisms, the third equation holds since $\varphi^{-j}$ is raising to the power $q^{-j}$ on the constant field of $L$, the first congruence holds since $\deg(\mathfrak{q}) = 1$, and the second congruence holds by (10) and the remark thereafter.

As $g(\mathrm{Con}_{L|F}(\mathfrak{p}))^{q^{d-1}}$ and $\zeta^{-q^d}$ are elements of the constant field of $L$, and $L$ has trivial intersection with $\mathfrak{q}$, we get

$$g(\mathrm{Con}_{L|F}(\mathfrak{p}))^{q^{d-1}} = \zeta^{-q^d} \quad \text{and thus} \quad g(\mathrm{Con}_{L|F}(\mathfrak{p}))^{-q^{-1}} = \zeta.$$

Finally,

$$\begin{aligned} h(\mathrm{Con}_{F'|F}(\mathfrak{p})) &= (\varphi^{-1}(g)^{-1})(\mathrm{Con}_{F'|F}(\mathfrak{p})) = g(\mathrm{Con}_{F'|F}(\mathfrak{p}))^{-q^{-1}} \\ &= g(\mathrm{Con}_{L|F}(\mathfrak{p}))^{-q^{-1}} = \zeta = \tau(y)/y \in \mu_n. \end{aligned}$$

Here the first equation holds by definition of $g$, the second equation holds since function evaluation commutes with automorphisms and $\varphi^{-1}(\mathrm{Con}_{F'|F}(\mathfrak{p})) = \mathrm{Con}_{F'|F}(\mathfrak{p})$, the third equation holds by the invariance of function evaluation under constant field extension, and $\zeta = \tau(y)/y \in \mu_n$ by definition. □

The following theorem is well-known. It is obvious for rational function fields and follows for arbitrary algebraic function fields by a reduction to the rational case.

**Theorem 4.4** (Weil reciprocity)**.** *Let $f, g \in F^\times$ such that $\mathrm{div}_F(f)$ and $\mathrm{div}_F(g)$ have disjoint support. Then*

$$f(\mathrm{div}_F(g)) = g(\mathrm{div}_F(f)).$$

*Proof.* See [Lan73, p. 243]. □

Combining Lemma 4.3 and Theorem 4.4 we obtain the main result of this section.

**Theorem 4.5.** *Let $n$ be coprime to $q$, and suppose that $E'|F'$ is abelian of degree dividing $n$. Then $\mathfrak{m}$ is a modulus of $E'|F$, i.e.*

$$\mathcal{P}_{\mathfrak{m}}(F) \subseteq \ker \mathrm{A}_{E'|F}.$$

*Proof.* Since $E'|F'$ is abelian there are intermediate fields $E'_i$ such that $E'_i|F'$ is cyclic and $E'$ is the compositum of the $E'_i$ over $F'$ and over $F$. Then $\mathrm{A}_{E'|F}(\mathfrak{d}) = \mathrm{id}$ if and only if $\mathrm{A}_{E'|F}(\mathfrak{d})|_{E'_i} = \mathrm{A}_{E'_i|F}(\mathfrak{d}) = \mathrm{id}$ for all $i$. It is thus sufficient to show $\mathcal{P}_{\mathfrak{m}}(F) \subseteq \ker \mathrm{A}_{E'|F}$ under the assumption that $E'|F'$ is cyclic. Hence we can apply Lemma 4.3.

Let $\mathfrak{d} \in \mathcal{P}_{\mathfrak{m}}(F)$. Choose $\sigma$, $y$ and $h$ as in Lemma 4.3. Then

$$\mathrm{A}_{E'|F}(\mathfrak{d}) = \tau_{\mathfrak{d}} \circ \sigma^{\deg(\mathfrak{d})}$$

with $\tau_{\mathfrak{d}}(y) = h(\mathrm{Con}_{F'|F}(\mathfrak{d})) \cdot y$. We wish to show that $\mathrm{A}_{E'|F}(\mathfrak{d}) = \mathrm{id}$. As $\deg(\mathfrak{d}) = 0$ and hence $\sigma^{\deg(\mathfrak{d})} = \mathrm{id}$ it remains to be shown that $\tau_{\mathfrak{d}} = \mathrm{id}$ or equivalently $h(\mathrm{Con}_{F'|F}(\mathfrak{d})) = 1$.

Since $\mathfrak{d} \in \mathcal{P}_{\mathfrak{m}}(F)$ there is $g \in F^\times$ such that $\mathfrak{d} = \mathrm{div}_F(g)$ and $g \equiv 1 \bmod \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})}$ in $\mathcal{O}_{\mathfrak{p}}$ for all places $\mathfrak{p}$ of $F$. We have $\mathrm{Con}_{F'|F}(\mathrm{div}_F(g)) = \mathrm{div}_{F'}(g)$, therefore

$$h(\mathrm{Con}_{F'|F}(\mathfrak{d})) = h(\mathrm{div}_{F'}(g)) = g(\mathrm{div}_{F'}(h)) \tag{11}$$

by Weil reciprocity Theorem 4.4.

Let $\mathcal{S} = \operatorname{supp}(\operatorname{Con}_{F'|F}(\mathfrak{d}))$ and $\mathcal{T} = \operatorname{supp}(\operatorname{Con}_{F'|F}(\mathfrak{m}))$. Since $f = y^n \in F'_{n,\mathfrak{m}}$ there are $\mathfrak{b} \in \mathcal{D}_{\mathfrak{m}}(F')$ and $\mathfrak{a} \in \mathcal{D}(F')$ with $\operatorname{supp}(\mathfrak{a}) \subseteq \mathcal{T}$ such that

$$\operatorname{div}_{F'}(f) = \mathfrak{a} + n\mathfrak{b}. \tag{12}$$

Then $\mathcal{T} \cap \operatorname{supp}(\mathfrak{b}) = \emptyset$ and $\mathcal{S} \cap (\mathcal{T} \cup \operatorname{supp}(\mathfrak{b})) = \emptyset$, the latter by definition of $y$. We have

$$h^n = \sigma^{-1}(y^n)^q (y^n)^{-1} = \varphi^{-1}(f)^q f^{-1}. \tag{13}$$

Taking principal divisors in (13) and combining with (12) gives

$$\begin{aligned} n \operatorname{div}_{F'}(h) &= q\varphi^{-1}(\operatorname{div}_{F'}(f)) - \operatorname{div}_{F'}(f) \\ &= q\varphi^{-1}(\mathfrak{a}) - \mathfrak{a} + n\big(q\varphi^{-1}(\mathfrak{b}) - \mathfrak{b}\big) \end{aligned}$$

with $q\varphi^{-1}(\mathfrak{a}) - \mathfrak{a} \in n\mathcal{D}(F')$ because the other terms are in $n\mathcal{D}(F')$. Division by $n$ yields

$$\operatorname{div}_{F'}(h) = \mathfrak{c} + q\varphi^{-1}(\mathfrak{b}) - \mathfrak{b}$$

for $\mathfrak{c} = (q\varphi^{-1}(\mathfrak{a}) - \mathfrak{a})/n \in \mathcal{D}(F')$. Since $\varphi(\mathcal{T}) = \mathcal{T}$, $\operatorname{supp}(\mathfrak{a}) \subseteq \mathcal{T}$, and $\mathcal{T} \cap \operatorname{supp}(\mathfrak{b}) = \emptyset$ we have

$$\operatorname{supp}(\mathfrak{c}) \subseteq \mathcal{T}, \tag{14}$$

and $\mathfrak{c}$ and $q\varphi^{-1}(\mathfrak{b}) - \mathfrak{b}$ are coprime. Furthermore, $\varphi(\mathcal{S}) = \mathcal{S} = \operatorname{supp}(\operatorname{div}_{F'}(g))$ and $\mathcal{S} \cap (\mathcal{T} \cup \operatorname{supp}(\mathfrak{b})) = \emptyset$, so we also have that $\mathfrak{c}$ and $q\varphi^{-1}(\mathfrak{b}) - \mathfrak{b}$ are coprime with $g$. Then

$$g(\operatorname{div}_{F'}(h)) = g(\mathfrak{c}) \cdot g(q\varphi^{-1}(\mathfrak{b}) - \mathfrak{b}). \tag{15}$$

Since $g \in F^\times$ by construction, we have $\varphi(g) = g$. Together with

$$g(q\varphi^{-1}(\mathfrak{b})) = g(\varphi^{-1}(\mathfrak{b}))^q = (\varphi^{-1}(g)(\varphi^{-1}(\mathfrak{b})))^q = \varphi^{-1}(g(\mathfrak{b}))^q = g(\mathfrak{b})$$

we get

$$g(q\varphi^{-1}(\mathfrak{b}) - \mathfrak{b}) = 1. \tag{16}$$

By assumption, $g \equiv 1 \bmod \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\mathfrak{m})}$ in $\mathcal{O}_{\mathfrak{p}}$ for all places $\mathfrak{p}$ of $F$ and thus $g \equiv 1 \bmod \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\operatorname{Con}_{F'|F}(\mathfrak{m}))}$ in $\mathcal{O}_{\mathfrak{p}}$ for all places $\mathfrak{p}$ of $F'$. Hence $g(\mathfrak{p}) = 1$ for all $\mathfrak{p} \in \mathcal{T}$ and therefore, observing (14),

$$g(\mathfrak{c}) = 1. \tag{17}$$

Combining (11), (15), (16) and (17) we obtain

$$h(\operatorname{Con}_{F'|F}(\mathfrak{d})) = g(\operatorname{div}_{F'}(h)) = 1,$$

as was to be shown. ◻

In the rest of this paper the Artin map will only occur for extensions $E'|F$ as in Theorem 4.5, whence $\mathcal{P}_{\mathfrak{m}}(F) \subseteq \ker \mathrm{A}_{E'|F}$. We will thus regard $\mathrm{A}_{E'|F}$ as a well-defined epimorphism

$$\mathrm{A}_{E'|F} : \mathcal{C}\ell_{\mathfrak{m}}(F) \to \operatorname{Gal}(E'|F). \tag{18}$$

# 5 Evaluation of Functions and Pairings

We now consider pairings derived from the evaluation of functions at divisors and various symmetries between these pairings. This yields a key tool in proving Theorem 6.3 on the kernel of the Artin map in the next section.

Suppose that $\mu_n \subseteq F$ and so $q \equiv 1 \bmod n$. It will be sufficient to work modulo $n$-th powers or $n$-th multiples in every group that occurs. If $f \in F^\times$ and $\mathrm{ord}_\mathfrak{p}(f) \equiv 0 \bmod n$, we define the residue $f_{n,\mathfrak{p}}$ of $f$ at $\mathfrak{p}$ modulo $n$-th powers as follows: By the approximation theorem there is $g \in F^\times$ such that $\mathrm{ord}_\mathfrak{p}(g) = \mathrm{ord}_\mathfrak{p}(f)/n$. Then $fg^{-n} \in \mathcal{O}_\mathfrak{p}^\times$ and we set

$$f_{n,\mathfrak{p}} = (fg^{-n})_\mathfrak{p} \cdot (F_\mathfrak{p}^\times)^n \in F_\mathfrak{p}^\times/(F_\mathfrak{p}^\times)^n. \tag{19}$$

One can check directly that $f_{n,\mathfrak{p}}$ does not depend on the choice of $g$. If $\mathrm{ord}_\mathfrak{p}(f) \not\equiv 0 \bmod n$ we set $f_{n,\mathfrak{p}} = 1$ in $F_\mathfrak{p}^\times/(F_\mathfrak{p}^\times)^n$. Furthermore, for each $\mathfrak{p}$ we have an isomorphism

$$\phi_{n,\mathfrak{p}} : F_\mathfrak{p}^\times/(F_\mathfrak{p}^\times)^n \to \mu_n, \quad x \cdot (F_\mathfrak{p}^\times)^n \mapsto \mathrm{N}_{F_\mathfrak{p}|\mathbb{F}_q}(x)^{(q-1)/n}. \tag{20}$$

Let $\mathcal{S}$ be an arbitrary set of places of $F$. Combining all this we define

$$\mathrm{ev}_{n,\mathcal{S}} : F_{n,\mathcal{S}} \to \prod_{\mathfrak{p}\notin\mathcal{S}} \mu_n, \quad f \mapsto (\, \phi_{n,\mathfrak{p}}(f_{n,\mathfrak{p}})\,)_{\mathfrak{p}\notin\mathcal{S}}. \tag{21}$$

Next we define a divisor group

$$\mathcal{D}_{n,\mathcal{S}}(F) = \{\mathfrak{d} \in \mathcal{D}(F) \,|\, \mathrm{ord}_\mathfrak{p}(\mathfrak{d}) \equiv 0 \bmod n \text{ for all } \mathfrak{p} \in \mathcal{S}\}. \tag{22}$$

There is an epimorphism

$$\mathrm{ord}_{n,\mathcal{S}} : \mathcal{D}_{n,\mathcal{S}}(F) \to \coprod_{\mathfrak{p}\notin\mathcal{S}} \mathbb{Z}/n\mathbb{Z}, \quad \mathfrak{d} \mapsto (\, \mathrm{ord}_\mathfrak{p}(\mathfrak{d}) + n\mathbb{Z}\,)_{\mathfrak{p}\notin\mathcal{S}}. \tag{23}$$

Since $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$, the groups $\prod_{\mathfrak{p}\notin\mathcal{S}} \mu_n$ and $\coprod_{\mathfrak{p}\notin\mathcal{S}} \mathbb{Z}/n\mathbb{Z}$ are dual under the non-degenerate pairing

$$\tau : \prod_{\mathfrak{p}\notin\mathcal{S}} \mu_n \times \coprod_{\mathfrak{p}\notin\mathcal{S}} \mathbb{Z}/n\mathbb{Z} \to \mu_n, \quad ((x_\mathfrak{p})_{\mathfrak{p}\notin\mathcal{S}}, (y_\mathfrak{p} + n\mathbb{Z})_{\mathfrak{p}\notin\mathcal{S}}) \mapsto \prod_{\mathfrak{p}\notin\mathcal{S}} x_\mathfrak{p}^{y_\mathfrak{p}}. \tag{24}$$

Pulling back with $\mathrm{ev}_{n,\mathcal{S}}$ and $\mathrm{ord}_{n,\mathcal{S}}$ gives a pairing

$$\tau_{n,\mathcal{S}} : F_{n,\mathcal{S}} \times \mathcal{D}_{n,\mathcal{S}}(F) \to \mu_n, \quad (f, \mathfrak{d}) \mapsto \tau(\mathrm{ev}_{n,\mathcal{S}}(f), \mathrm{ord}_{n,\mathcal{S}}(\mathfrak{d})). \tag{25}$$

Note that

$$\tau_{n,\mathcal{S}}(f, \mathfrak{d}) = f(\mathfrak{d})^{(q-1)/n}$$

for all $f \in F_{n,\mathcal{S}}$ and $\mathfrak{d} \in \mathcal{D}_{n,\mathcal{S}}(F)$ with $f$ and $\mathfrak{d}$ coprime.

Let $\bar{\mathcal{S}}$ denote the complement of $\mathcal{S}$ in the set of all places of $F$. Let ${\tau_{n,\mathcal{S}}}^{\mathrm{opp}}$ denote $\tau_{n,\mathcal{S}}$ with the arguments swapped, that is

$${\tau_{n,\mathcal{S}}}^{\mathrm{opp}}(x, y) = \tau_{n,\mathcal{S}}(y, x). \tag{26}$$

**Theorem 5.1.** *Let $\mathcal{S}$ be an arbitrary set of places.*

(*i*) *In each square of the diagram*

$$\begin{tikzcd}
F_{n,\emptyset} \arrow[r, "\subseteq"] \arrow[d, dash, "\tau_{n,\emptyset}"] & F_{n,\mathcal{S}} \arrow[r, "\mathrm{div}_F"] \arrow[d, dash, "\tau_{n,\mathcal{S}}"] & \mathcal{D}_{n,\bar{\mathcal{S}}}(F) \arrow[r, "\subseteq"] \arrow[d, dash, "{\tau_{n,\bar{\mathcal{S}}}}^{\mathrm{opp}}"] & \mathcal{D}_{n,\emptyset}(F) \arrow[d, dash, "{\tau_{n,\emptyset}}^{\mathrm{opp}}"] \\
\mathcal{D}_{n,\emptyset}(F) & \mathcal{D}_{n,\mathcal{S}}(F) \arrow[l, "\supseteq"'] & F_{n,\bar{\mathcal{S}}} \arrow[l, "\mathrm{div}_F"'] & F_{n,\emptyset} \arrow[l, "\supseteq"']
\end{tikzcd}$$

*the horizontal maps are adjoint with respect to the pairings on the left and right vertical lines.*

(*ii*) *The left kernel of* $\tau_{n,\mathcal{S}}$ *contains* $F^1_{n,\mathcal{S}}(F^\times)^n$ *where*

$$F^1_{n,\mathcal{S}} = \{f \in F_{n,\mathcal{S}} \,|\, \mathrm{ord}_\mathfrak{p}(f) = 0 \textit{ and } f_\mathfrak{p} = 1 \textit{ for all } \mathfrak{p} \notin \mathcal{S}\}. \tag{27}$$

*The right kernel of* $\tau_{n,\mathcal{S}}$ *contains* $\mathcal{P}^1_{n,\bar{\mathcal{S}}}(F) + n\mathcal{D}(F)$ *where*

$$\begin{aligned}\mathcal{P}^1_{n,\bar{\mathcal{S}}}(F) &= \mathrm{div}_F(F^1_{n,\bar{\mathcal{S}}}) \qquad (28)\\ &= \{\mathrm{div}_F(f) \,|\, f \in F_{n,\bar{\mathcal{S}}}, \mathrm{ord}_\mathfrak{p}(f) = 0 \textit{ and } f_\mathfrak{p} = 1 \textit{ for all } \mathfrak{p} \in \mathcal{S}\}.\end{aligned}$$

*Proof.* (*i*): Consider the first row. It is easy to check that the domains and codomains indeed fit together to give a sequence of homomorphisms. If $\mathcal{S}$ is replaced by $\bar{\mathcal{S}}$ then this also holds for the second row by symmetry.

Suppose $f \in F_{n,\emptyset}$ and $\mathfrak{d} \in \mathcal{D}_{n,\mathcal{S}}(F)$. Then, observing the definitions and $\mathrm{ord}_\mathfrak{p}(\mathfrak{d}) \equiv 0 \bmod n$ for all $\mathfrak{p} \in \mathcal{S}$,

$$\begin{aligned}\tau_{n,\emptyset}(f, \mathfrak{d}) = \tau(\mathrm{ev}_{n,\emptyset}(f), \mathrm{ord}_{n,\emptyset}(\mathfrak{d})) &= \prod_{\mathfrak{p}\notin\emptyset} \phi_{n,\mathfrak{p}}(f_{n,\mathfrak{p}})^{\mathrm{ord}_\mathfrak{p}(\mathfrak{d})}\\ &= \prod_{\mathfrak{p}\notin\mathcal{S}} \phi_{n,\mathfrak{p}}(f_{n,\mathfrak{p}})^{\mathrm{ord}_\mathfrak{p}(\mathfrak{d})} = \tau(\mathrm{ev}_{n,\mathcal{S}}(f), \mathrm{ord}_{n,\mathcal{S}}(\mathfrak{d})) = \tau_{n,\mathcal{S}}(f, \mathfrak{d}),\end{aligned}$$

showing the adjointness in the first square.

Suppose $f \in F_{n,\mathcal{S}}$ and $g \in F_{n,\bar{\mathcal{S}}}$. From the definitions we have $\ker(\mathrm{ev}_{n,\mathcal{S}}) \supseteq (F^\times)^n$ and $\ker(\mathrm{ord}_{n,\mathcal{S}}) \supseteq n\mathcal{D}(F)$, so the left and right kernel of $\tau_{n,\mathcal{S}}$ contain $(F^\times)^n$ and $n\mathcal{D}(F)$ respectively. There are $f' \in F_{n,\mathcal{S}}$ and $g' \in F_{n,\bar{\mathcal{S}}}$ with $f'f^{-1}, g'g^{-1} \in (F^\times)^n$ such that $f'$ and $g'$ are coprime. Indeed, let $\mathfrak{p} \in \mathrm{supp}(f) \cap \mathrm{supp}(g)$. Then $\mathrm{ord}_\mathfrak{p}(f) \equiv 0 \bmod n$ or $\mathrm{ord}_\mathfrak{p}(g) \equiv 0 \bmod n$. Assume $\mathrm{ord}_\mathfrak{p}(f) \equiv 0 \bmod n$. By the approximation theorem there is $h \in F^\times$ such that $\mathrm{ord}_\mathfrak{p}(h) = 1$ and $\mathrm{ord}_\mathfrak{q}(h) = 0$ for all other $\mathfrak{q} \in \mathrm{supp}(f) \cup \mathrm{supp}(g)$. Then $f(h^{-\mathrm{ord}_\mathfrak{p}(f)/n})^n$ differs from $f$ by an $n$-th power, is coprime to $g$ in $\mathfrak{p}$ and the valuations at all other places $\mathfrak{q}$ are unaffected. Continuing this for all $\mathfrak{p} \in \mathrm{supp}(f) \cap \mathrm{supp}(g)$ leads to $f'$ and $g'$ as desired. Then

$$\begin{aligned}\tau_{n,\mathcal{S}}(f, \mathrm{div}_F(g)) &= \tau_{n,\mathcal{S}}(f', \mathrm{div}_F(g')) =\\ &= \prod_{\mathfrak{p}\notin\mathcal{S}} \phi_{n,\mathfrak{p}}(f'_{n,\mathfrak{p}})^{\mathrm{ord}_\mathfrak{p}(g')} = \prod_{\mathfrak{p}\notin\emptyset} \phi_{n,\mathfrak{p}}(f'_{n,\mathfrak{p}})^{\mathrm{ord}_\mathfrak{p}(g')} = f'(\mathrm{div}_F(g'))\\ &\overset{(*)}{=} g'(\mathrm{div}_F(f')) = \prod_{\mathfrak{p}\notin\emptyset} \phi_{n,\mathfrak{p}}(g'_{n,\mathfrak{p}})^{\mathrm{ord}_\mathfrak{p}(f')} = \prod_{\mathfrak{p}\notin\bar{\mathcal{S}}} \phi_{n,\mathfrak{p}}(g'_{n,\mathfrak{p}})^{\mathrm{ord}_\mathfrak{p}(f')}\\ &= \tau_{n,\bar{\mathcal{S}}}(g', \mathrm{div}_F(f')) = \tau_{n,\bar{\mathcal{S}}}(g, \mathrm{div}_F(f)).\end{aligned}$$

Here equation $(*)$ holds by Weil reciprocity Theorem 4.4. This shows the adjointness in the second square.

The adjointness in the third square follows from the adjointness in the first square by symmetry, if $\mathcal{S}$ is replaced by $\bar{\mathcal{S}}$.

$(ii)$: We have already observed that the left kernel of $\tau_{n,\mathcal{S}}$ contains $(F^\times)^n$. It is directly clear from the definitions that $F^1_{n,\mathcal{S}}$ is contained in $\ker(\mathrm{ev}_{n,\mathcal{S}})$, whence also in the left kernel of $\tau_{n,\mathcal{S}}$. Since $\tau_{n,\mathcal{S}}$ is homomorphic in the first argument this proves the first assertion.

We have already observed that the right kernel of $\tau_{n,\mathcal{S}}$ contains $n\mathcal{D}(F)$. By the adjointness of $\mathrm{div}_F$ the image $\mathcal{P}^1_{n,\bar{\mathcal{S}}}(F)$ of $F^1_{n,\bar{\mathcal{S}}}$ is also contained the the right kernel of $\tau_{n,\mathcal{S}}$. Since $\tau_{n,\mathcal{S}}$ is homomorphic in the second argument this proves the second assertion. □

Abbreviate

$$\overline{F}_{n,\mathcal{S}} = \frac{F_{n,\mathcal{S}}}{F^1_{n,\mathcal{S}}(F^\times)^n} \tag{29}$$

$$\overline{\mathcal{D}}_{n,\mathcal{S}}(F) = \frac{\mathcal{D}_{n,\mathcal{S}}(F)}{\mathcal{P}^1_{n,\bar{\mathcal{S}}}(F) + n\mathcal{D}(F)}. \tag{30}$$

Since $F^1_{n,\mathcal{S}}(F^\times)^n$ and $\mathcal{P}^1_{n,\bar{\mathcal{S}}}(F) + n\mathcal{D}(F)$ are contained in the left and right kernel of $\tau_{n,\mathcal{S}}$ respectively, $\tau_{n,\mathcal{S}}$ induces a pairing

$$\overline{\tau}_{n,\mathcal{S}} : \overline{F}_{n,\mathcal{S}} \times \overline{\mathcal{D}}_{n,\mathcal{S}}(F) \to \mu_n. \tag{31}$$

In Section 6 it will be the central step to prove that $\overline{\tau}_{n,\mathcal{S}}$ is non-degenerate for any finite $\mathcal{S}$ subject to the assumption $\mu_n \subseteq F$. The following nicely symmetric theorem shows that we can reduce the general case of finite $\mathcal{S}$ to $\mathcal{S} = \emptyset$. We write again

$$\overline{\tau}_{n,\mathcal{S}}{}^{\mathrm{opp}}(x,y) = \overline{\tau}_{n,\mathcal{S}}(y,x). \tag{32}$$

**Theorem 5.2.** *Let $\mathcal{S}$ be an arbitrary set of places.*

$(i)$ *The diagram from Theorem 5.1 induces the diagram*

$$\begin{tikzcd}
\overline{F}_{n,\emptyset} \arrow[r] \arrow[d, dash, "\overline{\tau}_{n,\emptyset}"] & \overline{F}_{n,\mathcal{S}} \arrow[r] \arrow[d, dash, "\overline{\tau}_{n,\mathcal{S}}"] & \overline{\mathcal{D}}_{n,\bar{\mathcal{S}}}(F) \arrow[r] \arrow[d, dash, "\overline{\tau}_{n,\bar{\mathcal{S}}}{}^{\mathrm{opp}}"] & \overline{\mathcal{D}}_{n,\emptyset}(F) \arrow[d, dash, "\overline{\tau}_{n,\emptyset}{}^{\mathrm{opp}}"] \\
\overline{\mathcal{D}}_{n,\emptyset}(F) & \overline{\mathcal{D}}_{n,\mathcal{S}}(F) \arrow[l] & \overline{F}_{n,\bar{\mathcal{S}}} \arrow[l] & \overline{F}_{n,\emptyset} \arrow[l]
\end{tikzcd}$$

*which has exact rows, and in each square of the diagram the horizontal maps are adjoint with respect to the pairings on the left and right vertical lines.*

*Suppose $\mathcal{S}$ is finite.*

$(ii)$ *The groups $\overline{\mathcal{D}}_{n,\bar{\mathcal{S}}}(F)$ and $\overline{F}_{n,\bar{\mathcal{S}}}$ are finite and $\overline{\tau}_{n,\bar{\mathcal{S}}}{}^{\mathrm{opp}}$ is non-degenerate.*

$(iii)$ *If $\overline{F}_{n,\emptyset}$ and $\overline{\mathcal{D}}_{n,\emptyset}(F)$ are finite and $\overline{\tau}_{n,\emptyset}$ is non-degenerate then $\overline{\tau}_{n,\mathcal{S}}$ is non-degenerate.*

*Proof.* $(i)$: We have $F^1_{n,\emptyset}(F^\times)^n \subseteq F^1_{n,\mathcal{S}}(F^\times)^n$, $\mathrm{div}_F(F^1_{n,\mathcal{S}}(F^\times)^n) \subseteq \mathcal{P}^1_{n,\mathcal{S}}(F) + n\mathcal{D}(F)$ and $\mathcal{P}^1_{n,\mathcal{S}}(F) + n\mathcal{D}(F) \subseteq \mathcal{P}^1_{n,\bar{\emptyset}}(F) + n\mathcal{D}(F)$, so the first row in the diagram of Theorem 5.1 indeed induces a sequence of homomorphisms

$$\overline{F}_{n,\emptyset} \to \overline{F}_{n,\mathcal{S}} \to \overline{\mathcal{D}}_{n,\bar{\mathcal{S}}}(F) \to \overline{\mathcal{D}}_{n,\emptyset}(F).$$

To prove exactness at $\overline{F}_{n,\mathcal{S}}$ let $f \in F_{n,\emptyset}$. Then $f \in F_{n,\mathcal{S}}$ and $\operatorname{div}_F(f) \in n\mathcal{D}(F) \subseteq \mathcal{P}^1_{n,\mathcal{S}}(F) + n\mathcal{D}(F)$. Conversely, let $f \in F_{n,\mathcal{S}}$ with $\operatorname{div}_F(f) \in \mathcal{P}^1_{n,\mathcal{S}}(F) + n\mathcal{D}(F)$. Then there is $h \in F^1_{n,\mathcal{S}}$ such that $\operatorname{div}_F(fh^{-1}) \in n\mathcal{D}(F)$ and thus $fh^{-1} \in F_{n,\emptyset}$. So $f \in F_{n,\emptyset}F^1_{n,\mathcal{S}}$ and the exactness at $\overline{F}_{n,\mathcal{S}}$ is shown.

To prove exactness at $\overline{\mathcal{D}}_{n,\bar{\mathcal{S}}}(F)$ let $f \in F_{n,\mathcal{S}}$. Then $\operatorname{div}_F(f) \in \mathcal{P}^1_{n,\bar{\emptyset}}(F) \subseteq \mathcal{P}^1_{n,\bar{\emptyset}}(F) + n\mathcal{D}(F)$. Conversely, let $\mathfrak{d} \in \mathcal{D}_{n,\bar{\mathcal{S}}}(F)$ with $\mathfrak{d} \in \mathcal{P}^1_{n,\bar{\emptyset}}(F) + n\mathcal{D}(F)$. There is thus $f \in F^\times$ such that $\operatorname{div}_F(f) \in \mathfrak{d} + n\mathcal{D}(F) \subseteq \mathcal{D}_{n,\bar{\mathcal{S}}}(F) + n\mathcal{D}(F)$. This implies $f \in F_{n,\mathcal{S}}$ and $\mathfrak{d} \in \operatorname{div}_F(F_{n,\mathcal{S}}) + n\mathcal{D}(F)$, so the exactness at $\overline{\mathcal{D}}_{n,\bar{\mathcal{S}}}(F)$ is shown.

By symmetry, the second row is also well-defined and exact. Since we have factored by subgroups of the kernels of the pairings, the horizontal homomorphisms in each square are still adjoint as in the diagram of Theorem 5.1.

*(ii)*: Consider $\operatorname{ev}_{n,\bar{\mathcal{S}}} : F_{n,\bar{\mathcal{S}}} \to \prod_{\mathfrak{p}\in\mathcal{S}} \mu_n$. Since $\mathcal{S}$ is finite and $\mu_n \subseteq F$, the approximation theorem shows that $\operatorname{ev}_{n,\bar{\mathcal{S}}}$ is surjective and that $\ker(\operatorname{ev}_{n,\bar{\mathcal{S}}}) = F^1_{n,\bar{\mathcal{S}}}(F^\times)^n$, so $\overline{F}_{n,\bar{\mathcal{S}}} \cong \prod_{\mathfrak{p}\in\mathcal{S}} \mu_n$ under $\operatorname{ev}_{n,\bar{\mathcal{S}}}$. Now consider $\operatorname{ord}_{n,\bar{\mathcal{S}}} : \mathcal{D}_{n,\bar{\mathcal{S}}}(F) \to \coprod_{\mathfrak{p}\in\mathcal{S}} \mathbb{Z}/n\mathbb{Z}$. This is surjective and $\ker(\operatorname{ord}_{n,\bar{\mathcal{S}}}) = n\mathcal{D}(F) = \mathcal{P}^1_{n,\mathcal{S}}(F) + n\mathcal{D}(F)$ since $\mathcal{P}^1_{n,\mathcal{S}}(F) = 0$ by the finiteness of $\mathcal{S}$. So $\overline{\mathcal{D}}_{n,\bar{\mathcal{S}}}(F) \cong \coprod_{\mathfrak{p}\in\mathcal{S}} \mathbb{Z}/n\mathbb{Z}$ under $\operatorname{ord}_{n,\bar{\mathcal{S}}}$. Thus the non-degeneracy of $\tau$ implies that of $\overline{\tau}_{n,\bar{\mathcal{S}}}{}^{\mathrm{opp}}$.

*(iii)*: The map $\overline{F}_{n,\emptyset} \to \overline{F}_{n,\mathcal{S}}$ is injective since $F^1_{n,\mathcal{S}}(F^\times)^n \cap F_{n,\emptyset} = F^1_{n,\emptyset}(F^\times)^n$ from $F^1_{n,\mathcal{S}} = F^1_{n,\emptyset} = 1$ as $\mathcal{S}$ is finite and $(F^\times)^n \subseteq F_{n,\emptyset}$. The map $\overline{\mathcal{D}}_{n,\mathcal{S}}(F) \to \overline{\mathcal{D}}_{n,\emptyset}(F)$ is surjective: The set $\mathcal{P}^1_{n,\bar{\emptyset}}(F)$ is just the set of all principal divisors of $F$, so by the approximation theorem and the finiteness of $\mathcal{S}$ every class in $\overline{\mathcal{D}}_{n,\emptyset}(F)$ has a representing divisor lying in $\mathcal{D}_{n,\mathcal{S}}(F)$. This means that we can supplement the diagram in $(i)$ on the left by zero groups and the non-degenerate zero pairing on the vertical line and still have exact rows and adjoint horizontal maps for all pairings on the vertical lines. Then $\overline{\tau}_{n,\mathcal{S}}$ has two non-degenerate pairings on its left and on its right side. By the exactness of the rows in $(i)$, by $(ii)$ and by our finiteness assumptions we obtain that $\overline{F}_{n,\mathcal{S}}$ and $\overline{\mathcal{D}}_{n,\bar{\mathcal{S}}}(F)$ are also finite. Lemma 2.10 can be applied and yields the non-degeneracy of $\overline{\tau}_{n,\mathcal{S}}$. ☐

# 6 Artin Kernel

Let $n$ be coprime to $q$ and assume that $\mu_n \subseteq F$. Let $\mathfrak{m}$ be an effective divisor and $E|F$ an abelian extension of $F$ unramified outside $\mathfrak{m}$ and of exponent $n$. We have the epimorphism

$$\mathrm{A}_{E|F} : \mathcal{C}\!\ell_{\mathfrak{m}}(F) \to \operatorname{Gal}(E|F) \quad \text{with} \quad \ker \mathrm{A}_{E|F} \subseteq n\mathcal{C}\!\ell_{\mathfrak{m}}(F),$$

observing our convention (18).

Suppose now $E|F$ is the maximal extension of $F$ satisfying the above assumptions. The main result of this section is that $E|F$ is finite and that

$$\ker \mathrm{A}_{E|F} = n\mathcal{C}\!\ell_{\mathfrak{m}}(F).$$

We prove this by establishing the non-degeneracy of various pairings defined below.

Without a finiteness assumption on $E|F$ we have the following general theorem on the Kummer pairing:

**Theorem 6.1.** *We have $E = F((F_{n,\mathfrak{m}})^{1/n})$ and there is a non-degenerate pairing*

$$\kappa_{n,\mathfrak{m}} : F_{n,\mathfrak{m}}/(F^\times)^n \times \operatorname{Gal}(E|F) \to \mu_n, \quad (f \cdot (F^\times)^n, \tau) \mapsto \tau(y)y^{-1} \tag{33}$$

*where $y \in E$ with $y^n = f$.*

*Proof.* The statements on $E$ and $\kappa_{n,\mathfrak{m}}$ are well-known facts that follow from general Kummer theory [Neu99, p. 279] and the ramification behavior of Kummer extensions [Sti93, p. 111]. $\square$

**Lemma 6.2.** *(i) The group $F_{n,\mathfrak{m}}/(F^\times)^n$ is finite and $E = F((F_{n,\mathfrak{m}})^{1/n})$ is finite over $F$.*

*(ii) The pairing*

$$t_{n,\mathfrak{m}} : F_{n,\mathfrak{m}}/(F^\times)^n \times \mathcal{C}\ell_{\mathfrak{m}}(F)/n\mathcal{C}\ell_{\mathfrak{m}}(F) \to \mu_n, \qquad (x, y + n\mathcal{C}\ell_{\mathfrak{m}}(F)) \mapsto \kappa_{n,\mathfrak{m}}(x, \mathrm{A}_{E|F}(y)) \tag{34}$$

*is a non-degenerate pairing of finite groups.*

*(iii) We have*

$$\#F_{n,\mathfrak{m}}/(F^\times)^n = \#\mathcal{C}\ell_{\mathfrak{m}}(F)/n\mathcal{C}\ell_{\mathfrak{m}}(F). \tag{35}$$

*Proof.* $(i)$: First we link to our notation from the previous section. Let $\mathcal{S} = \mathrm{supp}(\mathfrak{m})$. The finiteness of $\mathcal{S}$ implies

$$F_{n,\mathfrak{m}}/(F^\times)^n = F_{n,\mathcal{S}}/(F^\times)^n = \overline{F}_{n,\mathcal{S}} \quad \text{and} \quad \mathcal{C}\ell_{\mathfrak{m}}(F)/n\mathcal{C}\ell_{\mathfrak{m}}(F) \cong \overline{\mathcal{D}}_{n,\mathcal{S}}(F). \tag{36}$$

The two equalities in (36) follow directly from the definitions and $F^1_{n,\mathcal{S}} = 1$. To prove the isomorphism in (36) observe that we have epimorphisms

$$\mathcal{D}_{\mathfrak{m}}(F) \to \mathcal{D}_{n,\mathcal{S}}(F)/n\mathcal{D}(F) \to \overline{\mathcal{D}}_{n,\mathcal{S}}(F),$$

where the first epimorphism is given by the inclusion $\mathcal{D}_{\mathfrak{m}}(F) \subseteq \mathcal{D}_{n,\mathcal{S}}(F)$ and the second epimorphism is just the quotient map upon factoring out $\mathcal{P}^1_{n,\bar{\mathcal{S}}}(F) + n\mathcal{D}(F)$. The kernel of the composition epimorphism is thus

$$\big(\mathcal{P}^1_{n,\bar{\mathcal{S}}}(F) + n\mathcal{D}(F)\big) \cap \mathcal{D}_{\mathfrak{m}}(F) = \mathcal{P}^1_{n,\bar{\mathcal{S}}}(F) + n\mathcal{D}_{\mathfrak{m}}(F),$$

as $\mathcal{P}^1_{n,\bar{\mathcal{S}}}(F) \subseteq \mathcal{D}_{\mathfrak{m}}(F)$. It remains to show

$$\mathcal{P}^1_{n,\bar{\mathcal{S}}}(F) + n\mathcal{D}_{\mathfrak{m}}(F) = \mathcal{P}_{\mathfrak{m}}(F) + n\mathcal{D}_{\mathfrak{m}}(F). \tag{37}$$

The inclusion $\supseteq$ is obvious by $\mathcal{P}^1_{n,\bar{\mathcal{S}}}(F) \supseteq \mathcal{P}_{\mathfrak{m}}(F)$ from the definitions. For $\subseteq$ there is $e \in \mathbb{Z}^{\geq 1}$ such that $\sum_{\mathfrak{p} \in S} q^e \mathfrak{p} \geq \mathfrak{m}$. Since $f \equiv 1 \bmod \mathfrak{p}$ implies $f^{q^e} \equiv 1 \bmod \mathfrak{p}^{q^e}$ in $\mathcal{O}_{\mathfrak{p}}$ we obtain

$$q^e \mathcal{P}^1_{n,\bar{\mathcal{S}}}(F) \subseteq \mathcal{P}_{\mathfrak{m}}(F).$$

This together with $\gcd(q^e, n) = 1$ proves $\subseteq$, hence (37), and establishes the isomorphism in (36).

Write $\mathcal{C}\ell(F) = \mathcal{C}\ell_0(F)$ and denote by $\mathcal{C}\ell^0(F)$ the subgroup of $\mathcal{C}\ell(F)$ of divisor classes of degree zero. There are well-known exact sequences

$$0 \to \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^n \to F_{n,0}/(F^\times)^n \to \mathcal{C}\ell^0(F)[n] \to 0 \tag{38}$$

and

$$0 \to \mathcal{C}\ell^0(F)/n\mathcal{C}\ell^0(F) \to \mathcal{C}\ell(F)/n\mathcal{C}\ell(F) \to \mathbb{Z}/n\mathbb{Z} \to 0, \tag{39}$$

where the second homomorphisms in (38) and (39) are given by inclusion, the third homomorphism in (38) is given by $f \cdot (F^\times)^n \mapsto \mathrm{div}_F(f)/n + \mathcal{P}(F)$, and the third homomorphism in (39) is given by the degree function. The exactness of (38), (39), the equalities $n = \#\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^n = \#\mathbb{Z}/n\mathbb{Z}$ and the isomorphism $G[n] \cong G/nG$ for every finite abelian group $G$ yield

$$\begin{aligned}\#F_{n,0}/(F^\times)^n &= \#\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^n \cdot \#\mathcal{C}\ell^0(F)[n] \\ &= \#\mathbb{Z}/n\mathbb{Z} \cdot \#\mathcal{C}\ell^0(F)/n\mathcal{C}\ell^0(F) \\ &= \#\mathcal{C}\ell(F)/n\mathcal{C}\ell(F).\end{aligned} \tag{40}$$

We obtain the finiteness of $\overline{F}_{n,\emptyset} = F_{n,0}/(F^\times)^n$. The exactness of the rows in Theorem 5.2, $(i)$ together with $(ii)$ yields the finiteness of $\overline{F}_{n,\mathcal{S}} = F_{n,\mathfrak{m}}/(F^\times)^n$.

$(ii)$: We now wish to show by an application of Lemma 4.3 that $t_{n,\mathfrak{m}} = \overline{\tau}_{n,\mathcal{S}}$ under (36). Since here $F' = F$ we take $\sigma = \mathrm{id}$ in Lemma 4.3. Given arguments to $t_{n,\mathfrak{m}}$ we can choose coprime representatives $f \in F_{n,\mathfrak{m}}$ and $\mathfrak{d} \in \mathcal{D}_\mathfrak{m}(F)$ and $y \in E$ such that $y^n = f$ and $h = y^{q-1} = f^{(q-1)/n}$. Then $\mathrm{A}_{E|F}(\mathfrak{d} + \mathcal{P}_\mathfrak{m}(F))|_{F(y)} = \mathrm{A}_{F(y)|F}(\mathfrak{d} + \mathcal{P}_\mathfrak{m}(F)) = \tau_\mathfrak{d}$ and

$$\begin{aligned}t_{n,\mathfrak{m}}(f \cdot (F^\times)^n, (\mathfrak{d} + \mathcal{P}_\mathfrak{m}(F)) + n\mathcal{C}\ell_\mathfrak{m}(F)) &= \kappa_{n,\mathfrak{m}}(f \cdot (F^\times)^n, \mathrm{A}_{E|F}(\mathfrak{d} + \mathcal{P}_\mathfrak{m}(F))) \\ &= \tau_\mathfrak{d}(y)y^{-1} = h(\mathfrak{d}) = f(\mathfrak{d})^{(q-1)/n} \\ &= \tau_{n,\mathcal{S}}(f, \mathfrak{d}) = \overline{\tau}_{n,\mathcal{S}}(f \cdot (F^\times)^n, \mathfrak{d} + \mathcal{P}^1_{n,\bar{\mathcal{S}}}(F) + n\mathcal{D}(F)))\end{aligned} \tag{41}$$

by tracing through the definitions of $\tau_{n,\mathcal{S}}$ and $\overline{\tau}_{n,\mathcal{S}}$. This shows that indeed $t_{n,\mathfrak{m}} = \overline{\tau}_{n,\mathcal{S}}$ under (36).

By the surjectivity of $\mathrm{A}_{E|F}$ and the non-degeneracy of $\kappa_{n,\mathcal{S}}$ we have that $t_{n,\mathfrak{m}}$ is non-degenerate on the left for any $\mathfrak{m}$. Then $t_{n,0} = \overline{\tau}_{n,\emptyset}$ is non-degenerate by Lemma 2.9 and (36). Finally $t_{n,\mathfrak{m}} = \overline{\tau}_{n,\mathcal{S}}$ is non-degenerate for any $\mathfrak{m}$ by Theorem 5.2, $(iii)$.

$(iii)$: This is a direct consequence of $(ii)$ and Lemma 2.9. □

**Theorem 6.3.** *The maximal abelian extension $E|F$ of $F$ unramified outside $\mathfrak{m}$ of exponent $n$ satisfies*

$$\ker \mathrm{A}_{E|F} = n\mathcal{C}\ell_\mathfrak{m}(F) \quad \textit{and} \quad [E : F] = \#\mathcal{C}\ell_\mathfrak{m}(F)/n\mathcal{C}\ell_\mathfrak{m}(F).$$

*Proof.* Lemma 6.2, $(ii)$ and $(iii)$ imply $\ker \mathrm{A}_{E|F} = n\mathcal{C}\ell_\mathfrak{m}(F)$. The surjectivity of the Artin map (or a direct application of Kummer theory) and Lemma 6.2, $(i)$ yield $[E : F] = \#\mathcal{C}\ell_\mathfrak{m}(F)/n\mathcal{C}\ell_\mathfrak{m}(F)$, as desired. □

# 7 Class Fields

We finally prove our main Theorem 7.8 on class field theory for abelian extensions of degree coprime to $q$. Our reasoning consists of a number of reductions using mostly standard techniques. A novel feature is that we do not assume the second inequality. The induction proof of Theorem 7.8 implicitly takes care of this, so that the second inequality is proven together with the existence theorem in Theorem 7.8.

All fields will be contained in some fixed algebraic closure $\bar{F}$ of the global function field $F$ and be finite and separable over $F$.

**Definition 7.1.** Let $\mathfrak{m}$ be an effective divisor of $F$, $H$ a subgroup of $\mathcal{C}\ell_\mathfrak{m}(F)$ of finite index and $E|F$ an abelian extension. We say that $E$ is the **class field** over $F$ defined by $H$ modulo $\mathfrak{m}$ if $\mathfrak{m}$ is a modulus of $E|F$ and if

$$H = \ker \mathrm{A}_{E|F} = \mathrm{im}\, \mathrm{N}_{E|F}$$

for the maps $\mathrm{A}_{E|F} : \mathcal{C}\ell_\mathfrak{m}(F) \to \mathrm{Gal}(E|F)$ and $\mathrm{N}_{E|F} : \mathcal{C}\ell_\mathfrak{m}(E) \to \mathcal{C}\ell_\mathfrak{m}(F)$.

As the definition suggests, given $H$ there is at most one class field over $F$ defined by $H$ modulo $\mathfrak{m}$. This is shown by the following lemma.

**Lemma 7.2.** *Let $E_1|F$ and $E_2|F$ be abelian with modulus $\mathfrak{m}$. Then $E_1 = E_2$ if and only if* $\ker \mathrm{A}_{E_1|F} = \ker \mathrm{A}_{E_2|F}$.

*Proof.* It is clear that $E_1 = E_2$ implies $\ker \mathrm{A}_{E_1|F} = \ker \mathrm{A}_{E_2|F}$. For the other implication we observe that $E_1 E_2|F$ is abelian with modulus $\mathfrak{m}$ by Corollary 2.7 and

$$\ker \mathrm{A}_{E_1 E_2|F} = \ker \mathrm{A}_{E_1|F} \cap \ker \mathrm{A}_{E_2|F} = \ker \mathrm{A}_{E_1|F} = \ker \mathrm{A}_{E_2|F} .$$

The surjectivity of $\mathrm{A}_{E_1 E_2|F}$ shows $E_1 E_2 = E_1 = E_2$. ◻

The following further notions will be convenient.

**Definition 7.3.** Let $\mathcal{E}$ be a set of abelian extensions of $F$ and $\mathcal{H}$ a set of pairs $(\mathfrak{m}, H)$ of effective divisors $\mathfrak{m}$ of $F$ and subgroups $H$ of $\mathcal{C}\ell_{\mathfrak{m}}(F)$ of finite index. By Lemma 7.2 we have a partial map $C : \mathcal{H} \to \mathcal{E}$ associating to every $(\mathfrak{m}, H) \in \mathcal{H}$ its class field $E \in \mathcal{E}$ defined by $H$ modulo $\mathfrak{m}$, and $C$ is injective on subsets of pairs sharing the same modulus. We say that the **class field correspondence** holds for $\mathcal{E}$ and $\mathcal{H}$ if $C : \mathcal{H} \to \mathcal{E}$ is defined on all of $\mathcal{H}$ and is surjective.

Furthermore, we say that $F$ is a **base field for class field theory** (coprime to $q$, of exponent $n$) if the class field correspondence holds between the set of all abelian extensions of $F$ (of degree coprime to $q$, of exponent $n$) and the set of all pairs $(\mathfrak{m}, H)$ where $\mathfrak{m}$ is an effective divisor of $F$ and $H$ is a subgroup of $\mathcal{C}\ell_{\mathfrak{m}}(F)$ of finite index (with $(\mathcal{C}\ell_{\mathfrak{m}}(F) : H)$ coprime to $q$, with $H \supseteq n\mathcal{C}\ell_{\mathfrak{m}}(F)$).

**Lemma 7.4.** *Let $E|F$ be abelian with modulus $\mathfrak{m}$. Then*

$$\ker \mathrm{A}_{E|F} \supseteq \operatorname{im} \mathrm{N}_{E|F} \supseteq [E : F] \cdot \mathcal{C}\ell_{\mathfrak{m}}(F).$$

*Proof.* The first $\supseteq$ follows from Theorem 2.6, $(i)$. The second $\supseteq$ follows since $\mathrm{N}_{E|F} \circ \mathrm{Con}_{E|F}$ is equal to multiplication by $[E : F]$ on $\mathcal{C}\ell_{\mathfrak{m}}(F)$. ◻

We will use the following reductions.

**Lemma 7.5.** *Suppose $E$ is the class field over $F$ defined by $H$ modulo $\mathfrak{m}$. Then the class field correspondence holds for the set of all intermediate fields of $E|F$ and the set of all pairs $(\mathfrak{m}, U)$ where $U$ is a subgroup of $\mathcal{C}\ell_{\mathfrak{m}}(F)$ containing $H$.*

*Proof.* From the surjectivity of $\mathrm{A}_{E|F}$ it is clear that there is a bijection between overgroups $U$ of $H$ and intermediate fields of $E|F$ given by $U \mapsto \mathrm{Fix}(\mathrm{A}_{E|F}(U))$. It remains to be shown that $\mathrm{Fix}(\mathrm{A}_{E|F}(U))$ is the class field of $U$ modulo $\mathfrak{m}$.

Clearly $\ker \mathrm{A}_{\mathrm{Fix}(\mathrm{A}_{E|F}(U))|F} = U$ by Galois theory, so the kernels of the Artin maps are as desired. We are left to prove equality with the images of the norm maps. Because of Lemma 7.4, because of the finiteness of $\mathrm{Gal}(E|F)$ and of $\mathcal{C}\ell_{\mathfrak{m}}(F)/H$ respectively, and because of $\operatorname{im} \mathrm{N}_{E|F} = \ker \mathrm{A}_{E|F}$ by assumption, it is sufficient by a pigeonhole principle to show the following statement: If $E_1, E_2$ are intermediate fields of $E|F$ with $E_1 \supseteq E_2$ and $\operatorname{im} \mathrm{N}_{E_1|F} = \operatorname{im} \mathrm{N}_{E_2|F}$, then $E_1 = E_2$. So let $x \in \mathcal{C}\ell_{\mathfrak{m}}(E_2)$. Then there is $y \in \mathcal{C}\ell_{\mathfrak{m}}(E_1)$ with $\mathrm{N}_{E_1|F}(y) = \mathrm{N}_{E_2|F}(x)$. Let $z = \mathrm{N}_{E_1|E_2}(y)$ and $u = x - z$. Then $\mathrm{N}_{E_2|F}(u) = 0$. We obtain

$$\begin{aligned} \mathrm{A}_{E_1|E_2}(x) &= \mathrm{A}_{E_1|E_2}(u + z) = \mathrm{A}_{E_1|E_2}(u) \circ \mathrm{A}_{E_1|E_2}(z) \\ &= \mathrm{A}_{E_1|F}(\mathrm{N}_{E_2|F}(u)) \circ \mathrm{A}_{E_1|E_2}(\mathrm{N}_{E_1|E_2}(y)) = \mathrm{id} . \end{aligned}$$

Thus $\ker \mathrm{A}_{E_1|E_2} = \mathcal{C}\ell_{\mathfrak{m}}(E_2)$ and Lemma 7.2 implies $E_1 = E_2$ ◻

Looking at abelian extensions of exponent $n$ and with modulus $\mathfrak{m}$, Lemma 7.5 suggests to concentrate on the maximal case $H = n\mathcal{C}\ell_{\mathfrak{m}}(F)$. Using this we obtain further reduction possibilities.

**Lemma 7.6.** *The field $F$ is a base field for class field theory of exponent $n$ coprime to $q$ if and only if for every effective divisor $\mathfrak{m}$ there is an abelian extension $E|F$ with modulus $\mathfrak{m}$ and*

$$\ker \mathrm{A}_{E|F} = n\mathcal{C}\ell_{\mathfrak{m}}(F).$$

*Proof.* If $F$ is such a base field then the assertion follows directly from the definitions. Conversely, let $\mathfrak{m}$ be an effective divisor. By assumption there is an abelian extension $E|F$ of exponent $n$ with modulus $\mathfrak{m}$ and $\ker \mathrm{A}_{E|F} = n\mathcal{C}\ell_{\mathfrak{m}}(F)$. Then

$$\ker \mathrm{A}_{E|F} \supseteq \operatorname{im} \mathrm{N}_{E|F} \supseteq n\mathcal{C}\ell_{\mathfrak{m}}(F) = \ker \mathrm{A}_{E|F}$$

by Lemma 7.4, thus $\ker \mathrm{A}_{E|F} = \operatorname{im} \mathrm{N}_{E|F}$ and $E$ is the class field over $F$ defined by $n\mathcal{C}\ell_{\mathfrak{m}}(F)$ modulo $\mathfrak{m}$. By Lemma 7.5 the class field of $H$ modulo $\mathfrak{m}$ exists for all overgroups $H \supseteq n\mathcal{C}\ell_{\mathfrak{m}}(F)$.

Let now $L|F$ be abelian of exponent $n$ coprime to $q$. Then $L|F$ has a modulus $\mathfrak{m}$ by Theorem 4.5 and $\ker \mathrm{A}_{L|F} \supseteq n\mathcal{C}\ell_{\mathfrak{m}}(F)$. We have already shown that the class field $E$ over $F$ corresponding to $n\mathcal{C}\ell_{\mathfrak{m}}(F)$ modulo $\mathfrak{m}$ exists, so $E$ is the maximal abelian extension of $F$ with modulus $\mathfrak{m}$ of exponent $n$. We obtain $L \subseteq E$, and $L$ is the class field for some $H$ modulo $\mathfrak{m}$ with $H \supseteq n\mathcal{C}\ell_{\mathfrak{m}}(F)$ by Lemma 7.5. ☐

**Lemma 7.7.** *Suppose $F'|F$ is a constant field extension and $F'$ is a base field for class field theory of exponent $n$ coprime to $q$. If $F'$ is a class field over $F$ or if $[F' : F]$ is coprime to $n$, then $F$ is a base field for class field theory of exponent $n$.*

*Proof.* Let $\mathfrak{m}$ be an arbitrary effective divisor of $F$, and let $E'$ be the class field of $F'$ defined by $n\mathcal{C}\ell_{\mathfrak{m}}(F') + \ker \mathrm{N}_{F'|F}$ modulo $\mathrm{Con}_{F'|F}(\mathfrak{m})$, where $\mathrm{N}_{F'|F} : \mathcal{C}\ell_{\mathfrak{m}}(F') \to \mathcal{C}\ell_{\mathfrak{m}}(F)$.

We first show that $E'|F$ is abelian with modulus $\mathfrak{m}$. We apply Theorem 2.6, $(ii)$. So let $\sigma$ be an $F$-monomorphism $\sigma : E' \to \bar{F}$. Then $\sigma(F') = F'$ since $F'|F$ is a constant field extension by assumption, and $\sigma$ extends an element of $\mathrm{Gal}(F'|F)$. Since $\operatorname{im} \mathrm{N}_{E'|F'} = n\mathcal{C}\ell_{\mathfrak{m}}(F') + \ker \mathrm{N}_{F'|F}$ and

$$\begin{aligned}\sigma(\operatorname{im} \mathrm{N}_{E'|F'}) &= n\sigma(\mathcal{C}\ell_{\mathfrak{m}}(F')) + \sigma(\ker \mathrm{N}_{F'|F}) \\ &= n\mathcal{C}\ell_{\mathfrak{m}}(F') + \ker \mathrm{N}_{F'|F} = \operatorname{im} \mathrm{N}_{E'|F'},\end{aligned}$$

$\sigma(E')$ is the class field over $F'$ defined by $\operatorname{im} \mathrm{N}_{\sigma(E')|F'} = \sigma(\operatorname{im} \mathrm{N}_{E'|F'}) = \operatorname{im} \mathrm{N}_{E'|F'}$. It follows that $\sigma(E') = E'$ and $E'|F$ is Galois. Now let $\sigma \in \mathrm{Gal}(E'|F)$ be an extension of a generator of the cyclic group $\mathrm{Gal}(F'|F)$. The elements of $\mathrm{Gal}(E'|F)$ are of the form $\tau \circ \sigma^i$ for $\tau \in \mathrm{Gal}(E'|F')$ and $i \in \mathbb{Z}$. Since $\sigma^i$ and $\sigma^j$ commute, it remains to be shown that $\sigma$ commutes with any $\tau$. Because $\mathrm{A}_{E'|F'}$ is surjective, there is an $x \in \mathcal{C}\ell_{\mathfrak{m}}(F')$ such that $\tau = \mathrm{A}_{E'|F'}(x)$. We then have $\sigma(x) - x \in \ker \mathrm{N}_{F'|F} \subseteq \operatorname{im} \mathrm{N}_{E'|F'}$ and

$$\sigma \circ \tau \circ \sigma^{-1} = \mathrm{A}_{E'|F'}(\sigma(x)) = \mathrm{A}_{E'|F'}(x)\, \mathrm{A}_{E'|F'}(\sigma(x) - x) = \mathrm{A}_{E'|F'}(x) = \tau.$$

We have thus proven that $E'|F$ is abelian. Furthermore, it is clear that $E'|F$ is only ramified in $\mathfrak{m}$ since this is the case for $E'|F'$ and $F'|F$ is unramified. By Theorem 4.5 we have that $\mathfrak{m}$ is a modulus of $E'|F$.

We now regard $\mathrm{A}_{E'|F}$ as a map defined on $\mathcal{C}\ell_{\mathfrak{m}}(F)$. We show that $\ker \mathrm{A}_{E'|F} \subseteq n\mathcal{C}\ell_{\mathfrak{m}}(F)$. Then $E'' = \mathrm{Fix}(\mathrm{A}_{E'|F}(n\mathcal{C}\ell_{\mathfrak{m}}(F)))$ satisfies $\ker \mathrm{A}_{E''|F} = n\mathcal{C}\ell_{\mathfrak{m}}(F)$. Lemma 7.6 then implies that $F$ is a base field of class field theory of exponent $n$.

Assume $F'$ is a class field of $F$. Let $x \in \ker \mathrm{A}_{E'|F}$. Then $x \in \ker \mathrm{A}_{F'|F}$, and by assumption there is $y \in \mathcal{C}\ell_{\mathfrak{m}}(F')$ with $x = \mathrm{N}_{F'|F}(y)$. Now $\mathrm{A}_{E'|F'}(y) = \mathrm{A}_{E'|F}(x) = 0$, so there is $z \in \mathcal{C}\ell_{\mathfrak{m}}(E')$ with $y = \mathrm{N}_{E'|F'}(z) \in n\mathcal{C}\ell_{\mathfrak{m}}(F') + \ker \mathrm{N}_{F'|F}$. We obtain $x = \mathrm{N}_{E'|F}(z)$ and $x = \mathrm{N}_{F'|F}(y) \in n\mathcal{C}\ell_{\mathfrak{m}}(F)$. Thus indeed $\ker \mathrm{A}_{E'|F} \subseteq n\mathcal{C}\ell_{\mathfrak{m}}(F)$.

Finally, let $d = [F' : F]$ and assume that $d$ and $n$ are coprime. Let $x \in \ker \mathrm{A}_{E'|F}$ and $y = \mathrm{Con}_{F'|F}(x)$. Then $\mathrm{A}_{E'|F'}(y) = \mathrm{A}_{E'|F}(\mathrm{N}_{F'|F}(y)) = \mathrm{A}_{E'|F}(dx) = 0$. So there are $z \in \mathcal{C}\ell_{\mathfrak{m}}(F')$ and $t \in \ker \mathrm{N}_{F'|F}$ such that $y = nz + t$. Then

$$dx = \mathrm{N}_{F'|F}(y) = n\,\mathrm{N}_{F'|F}(z) + \mathrm{N}_{F'|F}(t) = n\,\mathrm{N}_{F'|F}(z).$$

Write $ed = 1 + \lambda n$, which is possible since $d$ and $n$ are coprime by assumption. Then $edx = x + n(\lambda x) \in n\mathcal{C}\ell_{\mathfrak{m}}(F)$ and thus $x \in n\mathcal{C}\ell_{\mathfrak{m}}(F)$. Hence also in this case $\ker \mathrm{A}_{E'|F} \subseteq n\mathcal{C}\ell_{\mathfrak{m}}(F)$. $\square$

**Theorem 7.8.** *Every $F$ is a base field for class field theory coprime to $q$.*

*Proof.* It is enough to show that $F$ is a base field for class field theory of exponent $n$ for every $n$ coprime to $q$. The proof is by induction on $n$. The case $n = 1$ is trivially clear. Now let $n \geq 2$.

Define $F' = F(\mu_n)$. Then $F'|F$ is a constant field extension of degree less than $n$, and $F'$ is a base field for class field theory of exponent $n$ by Theorem 6.3 and Lemma 7.6. Furthermore there is an intermediate field $F \subseteq L \subseteq F'$ such that $[L : F]$ is coprime to $q$ and $[F' : L]$ is a power of the characteristic. Two applications of Lemma 7.7 show that $F$ is a base field for class field theory of exponent $n$: First, since $[F' : L]$ is coprime to $n$, $L$ is a base field for class field theory of exponent $n$ by Lemma 7.7. Second, by the induction hypothesis, $L$ is a class field over $F$, so $F$ is a base field for class field theory of exponent $n$ by Lemma 7.7. $\square$

# List of Notation

| | | |
|---|---|---|
| $\mathrm{A}_{E\|F}$ | Artin map of $E\|F$ defined on $\mathcal{D}_{\mathfrak{m}}(F)$, see eq. (4) | 5 |
| $\mathrm{A}_{E\|F}$ | Artin map of $E\|F$ defined on $\mathcal{C}\ell_{\mathfrak{m}}(F)$, see eq. (18) | 11 |
| $\mathcal{C}\ell_{\mathfrak{m}}(F)$ | class group of $F$ modulo $\mathfrak{m}$, see eq. (3) | 4 |
| $\mathrm{Con}_{L\|F}$ | conorm w.r.t. the field extension $L\|F$, see [Sti93, Def.ĨII.1.8] | 4 |
| $\mathfrak{d}$ | divisor, see [Sti93, Def. I.4.1] | 4 |
| $\deg \mathfrak{d}$ | degree of the divisor $\mathfrak{d}$, see [Sti93, Def. I.4.1] | 6 |
| $\mathrm{div}_F(f)$ | principal divisor of the function $f \in F^\times$, see [Sti93, Def. I.4.2] | 4 |
| $\mathcal{D}(F)$ | group of divisors of $F$, see [Sti93, Def. I.4.1] | 4 |
| $\mathcal{D}_{\mathfrak{m}}(F)$ | divisors of $F$ with support disjoint from the support of $\mathfrak{m}$, see eq. (1) | 4 |
| $\mathcal{D}_{n,\mathcal{S}}(F)$ | see eq. (22) | 12 |
| $\overline{\mathcal{D}}_{n,\mathcal{S}}(F)$ | see eq. (30) | 14 |
| $E$ | abelian extension field of $F$ | 7 |
| $E'$ | abelian extension field of $F'$ | 4 |
| $\mathrm{ev}_{n,\mathcal{S}}$ | see eq. (21) | 12 |
| $f(\mathfrak{d})$ | evaluation of $f \in F$ at $\mathfrak{d} \in \mathcal{D}(F)$, see eq. (5) with $L = F$ | 7 |
| $F$ | global function field, here always base field for class field theory | 4 |
| $F^\times$ | multiplicative group of the field $F$ | 4 |
| $F'$ | constant field extension of $F$ | 6 |
| $\bar{F}$ | algebraic closure of the field $F$ | 4 |
| $F_{n,\mathfrak{m}}$ | Selmer group of $F$ w.r.t. $\mathfrak{m}$, see eq. (7) | 8 |
| $F_{n,\mathcal{S}}$ | Selmer group of $F$ w.r.t. $\mathcal{S}$, see eq. (6) | 8 |

| | | |
|---|---|---|
| $F^1_{n,\mathcal{S}}$ | see eq. (27) | 13 |
| $\overline{F}_{n,\mathcal{S}}$ | see eq. (29) | 14 |
| $F_\mathfrak{p}$ | residue class field $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$ of the place $\mathfrak{p}$ of $F$, see [Sti93, Def. I.1.13] | 7 |
| $f_{n,\mathfrak{p}}$ | see eq. (19) | 12 |
| $f_\mathfrak{p}$ | image of $f \in F$ in the residue class field $F_\mathfrak{p}$, see [Sti93, Def. I.1.13] | 7 |
| $\mathbb{F}_q$ | finite field with $q$ elements, here always constant field of $F$ | 4 |
| Fix | fixed field of an automorphism group | |
| Gal | Galois group | |
| $H$ | subgroup of $\mathcal{C}\ell_\mathfrak{m}(F)$ defining a class field, see Def. 7.1 | 18 |
| Hom | homomorphism group | |
| $\kappa_{n,\mathfrak{m}}$ | Kummer pairing, see eq. (33) | 15 |
| ker | kernel of a map | |
| $L$ | extension field of $F$ | 4 |
| $\mathfrak{m}$ | an effective divisor, often a modulus of a field extension, see Def. 2.5 | 5 |
| $\mu_n$ | mutliplicative group of $n$-th roots of unity in $\bar{F}$ | 4 |
| $n$ | number coprime with $q$, here always degree of the class field extension | 4 |
| $\mathrm{N}_{L\mid F}$ | divisor norm w.r.t. the field extension $L\mid F$, see [Vil06, Def. 5.3.5] | 4 |
| $\mathrm{N}(\mathfrak{p})$ | norm of a place $\mathfrak{p}$, see Def. 2.5 | 4 |
| $\mathcal{O}_\mathfrak{p}$ | valuation ring of the place $\mathfrak{p}$, see [Sti93, Def. I.1.8] | 4 |
| $\mathrm{ord}_{n,\mathcal{S}}$ | see eq. (23) | 12 |
| $\mathrm{ord}_\mathfrak{p}(\mathfrak{d})$ | coefficient of the place $\mathfrak{p}$ in the divisor $\mathfrak{d}$ | 7 |
| $\mathfrak{p}$ | a place, see [Sti93, Def. I.1.8] | 4 |
| $\mathcal{P}(F)$ | group of principal divisors of $F$, see [Sti93, Def. I.4.3] | 4 |
| $\mathcal{P}_\mathfrak{m}(F)$ | ray of $F$ modulo $\mathfrak{m}$, see eq. (2) | 4 |
| $\mathcal{P}^1_{n,\bar{\mathcal{S}}}(F)$ | see eq. (28) | 13 |
| $\varphi$ | $q$-power Frobenius automorphism, see Def. 3.1 | 6 |
| $\phi_{n,\mathfrak{p}}$ | see eq. (20) | 12 |
| $q$ | cardinality of the constant field of $F$ | 4 |
| $\mathcal{S}$ | set of places of $F$ | 7 |
| $\bar{\mathcal{S}}$ | complement of $\mathcal{S}$ in the set of all places of $F$ | 12 |
| $\mathrm{supp}(\mathfrak{d})$ | support of the divisor $\mathfrak{d}$, see [Sti93, Def. I.4.1] | 4 |
| $\mathrm{supp}(f)$ | support of $\mathrm{div}_F(f)$ for $f \in F^\times$ | |
| $\mathcal{T}$ | set of places of $L$ | 7 |
| $t_{n,\mathfrak{m}}$ | see eq. (34) | 16 |
| $\tau$ | see eq. (24) | 12 |
| $\tau_{\mathrm{left}}$ | left homomorphism induced by the pairing $\tau$, see Def. 2.8 | 5 |
| $\tau_{\mathrm{right}}$ | right homomorphism induced by the pairing $\tau$, see Def. 2.8 | 5 |
| $\tau_{n,\mathcal{S}}$ | see eq. (25) | 12 |
| ${\tau_{n,\mathcal{S}}}^{\mathrm{opp}}$ | the pairing $\tau_{n,\mathcal{S}}$ with arguments swapped, see eq. (26) | 12 |
| $\overline{\tau}_{n,\mathcal{S}}$ | see eq. (31) | 14 |
| ${\overline{\tau}_{n,\mathcal{S}}}^{\mathrm{opp}}$ | the pairing $\overline{\tau}_{n,\mathcal{S}}$ with arguments swapped, see eq. (32) | 14 |

## References


[AT67] E. Artin and J. Tate. *Class Field Theory*. Benjamin, New York–Amsterdam, 1967.

[CF67] J. Cassels and A. Fröhlich. *Algebraic Number Theory*. Academic Press, New York–London, 1967.

[Coh00] H. Cohen. *Advanced Topics in Computational Number Theory*. Springer, Berlin–Heidelberg–New York, 2000.

[FJ86] M. D. Fried and M. Jarden. *Field Arithmetic*. Springer, Berlin–Heidelberg–New York, 1986.

[Gra03] G. Gras. *Class Field Theory. From Theory to Practice*. Springer, Berlin–Heidelberg–New York, 2003.

[Gre74] M. J. Greenberg. An elementary proof of the Kronecker-Weber Theorem. *Amer. Math. Monthly*, 81(6):601–607, 1974.

[Has35] H. Hasse. Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper. *J. reine angew. Math.*, 172:37–54, 1935.

[HPP03] F. Hess, S. Pauli, and M. Pohst. Computing the multiplicative group of residue class rings. *Math. Comp.*, 72(243):1531–1548, 2003.

[Jan73] G. J. Janusz. *Algebraic Number Fields*. Academic Press, New York–London, 1973.

[Lan70] S. Lang. *Algebraic Number Theory*. Addison–Wesley Publishing Company, Reading, Massachusetts, 1970.

[Lan73] S. Lang. *Elliptic Functions*. Addison–Wesley Publishing Company, Reading, Massachusetts, 1973.

[Mil06] J. S. Milne. *Arithmetic Duality Theorems*. BookSurge, LLC, second edition, 2006.

[Mil08] J. S. Milne. Class field theory (v4.02). Available at http://www.jmilne.org/math/CourseNotes/cft.html, 2008.

[Neu99] J. Neukirch. *Algebraic Number Theory*. Springer, Berlin–Heidelberg–New York, 1999.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*. Springer, Berlin–Heidelberg–New York, second edition, 2008.

[Roq02] P. Roquette. Class field theory in characteristic $p$, its origin and development. In *The Proceedings of the International Conference on Class Field Theory (Tokyo)*, 2002.

[Ros02] M. Rosen. *Number Theory in Function Fields*. Springer, Berlin–Heidelberg–New York, 2002.

[Sch37] H. L. Schmid. Zur Arithmetik der zyklischen $p$-Körper. *J. reine angew. Math.*, 176:161–167, 1937.

[Ser79] J.-P. Serre. *Local Fields*. Springer, Berlin–Heidelberg–New York, 1979.

[Ser88] J.-P. Serre. *Algebraic Groups and Class Fields*. Springer, Berlin–Heidelberg–New York, 1988.

[Sti93] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer, Berlin–Heidelberg–New York, 1993.

[Vil06] G. D. Villa Salvador. *Topics in the Theory of Algebraic Function Fields*. Birkhäuser Verlag, Boston–Basel–Berlin, 2006.

[Wei73] A. Weil. *Basic Number Theory*. Springer, Berlin–Heidelberg–New York, second edition, 1973.

[Wit35] E. Witt. Der Existenzsatz für abelsche Funktionenkörper. *J. reine angew. Math.*, 173:43–51, 1935.

# A Conductors

Let $\mathfrak{m}, \mathfrak{n}$ be two divisors of $F$. We write $\gcd(\mathfrak{m}, \mathfrak{n}) = \sum_{\mathfrak{p}} \min(v_{\mathfrak{p}}(\mathfrak{m}), v_{\mathfrak{p}}(\mathfrak{n}))\mathfrak{p}$ and $\mathfrak{m} \le \mathfrak{n}$ if and only if $v_{\mathfrak{p}}(\mathfrak{m}) \le v_{\mathfrak{p}}(\mathfrak{n})$ for all places $\mathfrak{p}$ of $F$. An application of the strong approximation theorem shows

$$\mathcal{P}_{\gcd(\mathfrak{m},\mathfrak{n})}(F) = \mathcal{P}_{\mathfrak{m}}(F)\mathcal{P}_{\mathfrak{n}}(F).$$

Thus if $E|F$ is an abelian extension, and $\mathfrak{m}$ as well as $\mathfrak{n}$ are moduli of $E|F$, then $\gcd(\mathfrak{m}, \mathfrak{n})$ is also a modulus for $E|F$. There is thus a smallest modulus of $E|F$ with respect to $\le$, the **conductor** $\mathfrak{f}(E|F)$ of $E|F$.

Let $E|F$ be an abelian extension of degree coprime to $q$. Theorem 4.5 shows that

$$\mathfrak{f}(E|F) = \sum_{\mathfrak{p} \text{ ramified in } E|F} \mathfrak{p}.$$

Conductors with higher multiplicites are possible, but of course only for abelian extensions whose degree is not coprime to $q$.

# B Relation to Pairings in Geometry and Cryptography

The Tate pairing was first considered in [7] for abelian varieties over local fields. Lichtenbaum [6] gave a specific description for Jacobians of curves over local fields in terms of a function evaluation on the associated curve. Frey and Rück [1] used reduction modulo $p$ to obtain a non-degenerate pairing for curves over finite fields. The resulting pairing is defined in terms of function fields as follows. Suppose $q \equiv 1 \bmod n$ and consider

$$t_n : \mathcal{C}\ell^0(F)[n] \times \mathcal{C}\ell^0(F)/n\mathcal{C}\ell^0(F) \to (\mathbb{F}_q^\times)/(\mathbb{F}_q^\times)^n. \tag{42}$$

Let $x \in \mathcal{C}\ell^0(F)[n]$ and $y \in \mathcal{C}\ell^0(F)/n\mathcal{C}\ell^0(F)$. There are $\mathfrak{d}, \mathfrak{e} \in \mathcal{D}(F)$ of degree zero such that $x = \mathfrak{e} + \mathcal{P}(F)$, $y = (\mathfrak{d} + \mathcal{P}(F)) + n\mathcal{C}\ell^0(F)$ and $\mathfrak{d}$, $\mathfrak{e}$ are coprime. Furthermore, there is $f \in F^\times$ with $\mathrm{div}_F(f) = n\mathfrak{e}$. Then

$$t_n(x, y) = f(\mathfrak{d}) \cdot (\mathbb{F}_q^\times)^n$$

and $t_n$ is a well-defined, non-degenerate pairing.

We can put $t_n$ in relation with $t_{n,\mathfrak{m}}$ and thus provide an interpretation of $t_n$ in terms of class field theory as follows. Let $\mathfrak{m} = 0$ and restrict $t_{n,0}$ to the non-degenerate pairing

$$\overline{t}_{n,0} : F_{n,0}/(\mathbb{F}_q^\times \cdot (F^\times)^n) \times \mathcal{C}\ell^0(F)/n\mathcal{C}\ell^0(F) \to \mu_n, \quad (f \cdot (\mathbb{F}_q^\times \cdot (F^\times)^n), y) \mapsto t_{n,0}(f \cdot (F^\times)^n, y).$$

Here $f \cdot (F^\times)^n$ is only defined up to multiples from $\mathbb{F}_q^\times$. But $t_{n,0}(f \cdot (F^\times)^n, y)$ is independent of this by (41) since $y$ has degree zero. Now define

$$\psi : \mathcal{C}\ell^0(F)[n] \to F_{n,0}/(\mathbb{F}_q^\times \cdot (F^\times)^n), \quad \mathfrak{d} + \mathcal{P}(F) \mapsto f \cdot (\mathbb{F}_q^\times \cdot (F^\times)^n) \text{ with } \mathrm{div}_F(f) = n\mathfrak{d},$$
$$\chi : \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^n \to \mu_n, \quad z \cdot (\mathbb{F}_q^\times)^n \mapsto z^{(q-1)/n}.$$

Taking (38) into consideration, these maps are easily seen to be well-defined isomorphisms. Putting things together readily yields

$$t_n(x, y) = \chi^{-1}(\,\overline{t}_{n,0}(\psi(x), y)\,).$$

We conclude that the Tate–Lichtenbaum pairing $t_n$ is essentially equal to our pairing $t_{n,\mathfrak{m}}$ for the special case $\mathfrak{m} = 0$, and this gives an alternative approach to proving that $t_n$ is a non-degenerate pairing. In terms of class field theory and somewhat vaguely speaking, the Tate–Lichtenbaum pairing thus provides information about the Artin map of the maximal unramified abelian extension $E|F$ of exponent $n$, under the condition that sufficiently many roots of unity are contained in the base field $F$. A parallel interpretation can be given for the Weil pairing, see [5].

Cryptography is built upon one-way functions $f : S \to T$. Suppose $S$ and $T$ are finite sets whose elements can be represented efficiently on a computer and $f(s)$ can be computed efficiently when given $s \in S$. The one-wayness of $f$ then means that the computation of preimages of $f(s)$ under $f$ for randomly chosen $s \in S$ is not feasible, up to current knowledge and technology. Additional assumptions may be imposed on $S$, $T$ and $f$. A case widely used since 1975 is of the form $S = \mathbb{Z}/n\mathbb{Z}$, $T = \mathbb{F}_q^\times$ and $f(x + n\mathbb{Z}) = \zeta^x$ for $n$ prime, $q$ a prime power and $\zeta$ a primitive $n$-th root of unity. It is believed that $f$ is a one-way isomorphism, if $n$ and $q$ are suitably chosen. It is also believed that the Tate–Lichtenbaum (42) and Weil pairings define one-way isomorphisms of each argument for a suitable choice of parameters. This richer structure includes other computationally hard problems and has led to striking new results in cryptography since 2000. Apart from security considerations, it is of interest to compute these pairings, or modifications thereof, most efficiently. This is where the Ate pairing [2, 4] and its variants [3, 8] come into play. The main point here is to reduce the degree of $f \in F^\times$, which is used to define the pairing value of the form $f(\mathfrak{d})^{(q-1)/n}$. This is achieved by restricting the domain of the Tate–Lichtenbaum pairing to certain eigenspaces of a Frobenius endomorphism, which allows for the definition of yet another pairing. We give a sketch of the relevant definitions and statements.

Let $F'|F$ denote a constant field extension such that $\mu_n \subseteq F'$. Now $q \equiv 1 \bmod n$ is usually not satisfied. Let $E|F$ be the maximal unramified extension of exponent $n$ and $E' = EF'$. Then $E$ is the class field over $F$ defined by $n\mathcal{C}\ell(F)$, and $E'|F$ is abelian. We define

$$\mathcal{C}\ell^0(F')[n, q - \phi] = \{x \in \mathcal{C}\ell^0(F')[n] \mid \phi(x) = qx\},$$
$$\Delta/(F'^\times)^n = \{x \in F'_{n,0}/(F'^\times)^n \mid \phi(x) = x^q\},$$

where $\Delta$ is supposed to be a subgroup of $F'_{n,0}$ containing $(F'^\times)^n$.

Using the $\phi$-equivariance of (34) it can be shown that $E' = F'(\Delta^{1/n})$. In a similar fashion as for the Tate-Lichtenbaum pairing above we finally define

$$a_n : \mathcal{C}\ell^0(F')[n, q - \phi] \times \mathcal{C}\ell^0(F)/n\mathcal{C}\ell^0(F) \to \mu_n$$

as follows. For $x \in \mathcal{C}\ell^0(F')[n, q - \phi]$ and $y \in \mathcal{C}\ell^0(F)/n\mathcal{C}\ell^0(F)$ there are $\mathfrak{d} \in \mathcal{D}(F)$ and $\mathfrak{e} \in \mathcal{D}(F')$ of degree zero such that $x = \mathfrak{e} + \mathcal{P}(F')$, $y = (\mathfrak{d} + \mathcal{P}(F)) + n\mathcal{C}\ell^0(F)$ and $\mathrm{Con}_{F'|F}(\mathfrak{d})$, $\mathfrak{e}$ are coprime. By Lemma 4.3 there is $h \in F'^\times$ with $\mathrm{div}_{F'}(h) = q\mathfrak{e} - \phi(\mathfrak{e})$ and coprime to $\mathrm{Con}_{F'|F}(\mathfrak{d})$. Then let

$$a_n(x, y) = h(\mathrm{Con}_{F'|F}(\mathfrak{d})).$$

Lemma 4.3 and Theorem 3.3 show that $a_n$ is a non-degenerate pairing. Note that $\phi$ acts by multiplication by $q$ on the left argument and as identity on the right argument of $a_n$.

In terms of class field theory and again somewhat vaguely speaking, this pairing provides information about the Artin map of $E'|F$ without the condition that sufficiently many roots of unity are contained in the base field $F$, whereas the Tate–Lichtenbaum pairing provides information about the Artin map of $E'|F'$.

The pairing $a_n$ occurs as Ate pairing on hyperelliptic curves [2]. For elliptic curves, one considers suitable products of $t_n$ and ${a_n}^{(q^k-1)/n}$ composed with powers of $\phi$, where $k = [F' : F]$.

One of the resulting pairings is called Ate pairing, systematic discussions can be found in [3, 8]. The description of $a_n$ given here provides the main ingredient for a further study of Ate pairings in the general curve and composite exponent $n$ case along the lines of [2, 3, 8].

# References for Appendix


[1] G. Frey and H.-G. Rück. A remark concerning $m$-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62(206):865–874, 1994.

[2] R. Granger, F. Hess, R. Oyono, N. Theriault, and F. Vercauteren. Ate pairing on hyperelliptic curves. In M. Naor, editor, *Advances in Cryptology – EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 430–447. Springer, 2007.

[3] F. Hess. Pairing lattices. In S. D. Galbraith and K. G. Paterson, editors, *Pairing-Based Cryptography – Pairing 2008*, volume 5209 of *LNCS*, pages 18–38. Springer, 2008.

[4] F. Hess, N. Smart, and F. Vercauteren. The Eta pairing revisited. *IEEE Trans. Inform. Theory*, 52(10):4595–4602, 2006.

[5] E. W. Howe. The Weil pairing and the Hilbert symbol. *Math. Ann.*, 305:337–392, 1996.

[6] S. Lichtenbaum. Duality theorems for curves over $p$-adic fields. *Invent. Math.*, 7:120–136, 1969.

[7] J. Tate. WC-groups over $p$-adic fields. *Séminaire N. Bourbaki*, 1956–1958, exposé no. 156:265–277, 1958.

[8] F. Vercauteren. Optimal pairings. *IEEE Trans. Inform. Theory*, 56(1):455–461, 2010.