Computation of Maximal Orders of Cyclic Extensions of Function Fields

vorgelegt von
Diplom-Mathematiker
Robert Fraatz
Berlin

von der Fakultät II - Mathematik und Naturwissenschaften
der Technischen Universität Berlin
zur Erlangung des akademischen Grades
Doktor der Naturwissenschaften

genehmigte Dissertation

Promotionsausschuss:

Vorsitzender: Prof. Dr. Rainer Wüst
Berichter: Prof. Dr. M. E. Pohst
Berichter: Prof. Dr. F. Heß

Tag der wissenschaftlichen Aussprache: 16.02.2005

Berlin 2005

D83

Contents

Introduction

The set of all rational functions over a field k, i. e. functions of the form $\frac{p(x)}{q(x)}$, where $p(x)$ and $q(x)$ are polynomials over k, form a field $k(x)$ under the usual arithmetic operations. As in the case of number fields, if we adjoin a root of an irreducible polynomial $f(x,t)$ to $k(x)$ we again obtain a field, say F, that contains $k(x)$ as a subfield. The field F is called an algebraic function field. If k is a finite field, then F is said to be global.

Since the 1930s it is well known that the global function fields together with the number fields form a class of fields, called global fields. These admit a class field theory, that is, they allow a description of all Abelian extensions. (An Abelian extension is a Galois extension whose automorphism group is Abelian.) Global function fields have been investigated by pure mathematicians ever since. However, while it is relatively easy to compute examples of number fields by hand this is hard in the case of function fields, because of the complexity of even basic operations like addition of elements.

While computations in number fields have been the focus of research in computer algebra since the 1970s, function fields have been neglected until recently. They were deemed to be too complicated. However, the development of highly efficient methods in the number field case together with the availability of relatively cheap fast computers brought the function fields into interest of computational researchers.

Work by the Russian mathematician Goppa (see for instance [Gop81], [Gop88]) added a new dimension to the interest in function fields. He demonstrated that they can be used to define good error-correcting codes, i. e. codes that allow the correction of many data transmission or storage errors in comparison to their size. These codes are dramatically better than any previously constructed codes. By "better" we mean that the Goppa codes allow the correction of more transmission errors in comparison to the block length (number of symbols transmitted) of the code.

Let $F = k(x)[t]/f(x,t)$ be a function field. A place of F is called rational if it has degree 1. The rational places correspond to the roots of f in k. If one considers f as defining a curve, then the set of rational places corresponds to the set of points on the curve over k. However, as our approach is based entirely on function field methods, we will use function field terminology.

In order to obtain good codes using Goppa's construction, it is necessary to find function fields having as many rational places as possible. A field E

with a large number of rational places may be constructed by taking a small field F where the number of places is known and constructing extensions E of F such that the splitting behaviour of the places is known in advance from theory. Class field theory is the most powerful technique currently available for building such extensions. In particular, using class field towers, it is possible to prove the existence of large good codes.

To be able to work efficiently with the resulting Abelian extensions of large degree it is important to develop explicit techniques for the fast computation of integral closures of Kummer extensions, Artin-Schreier-Witt extensions and their composita. In particular Artin-Schreier-Witt extensions have never been the focus of algorithmic investigation.

Integral bases of Kummer extensions of number fields were already treated by Daberkow ([Dab95]). He only obtains integral bases of Kummer extensions of prime degree directly. Integral bases of general cyclic Kummer extensions have to be computed in steps of prime degree, which involves computations in relative extensions of the ground field.

A (general) Kummer extension is an Abelian extension of exponent n of a field F which contains the set of all n-th roots of unity, where the characteristic of F is zero or coprime to n. Abelian extensions of a field F of exponent p^r, where $p > 0$ is the characteristic of F, are called Artin-Schreier-Witt extensions.

The existing general methods to determine integral closures are based on the Round 2 algorithm (see for instance [PZ89], [Fri97] and [Fri00]). This approach is of limited use in fields of large degree. In this thesis we develop a special method to compute an as small as possible set of "small" generators of the integral closures of Kummer and Artin-Schreier-Witt extensions.

A brief summary of this thesis follows.

Besides two short introductory sections about localization and Witt vectors, the main part of the first chapter introduces all the needed definitions, notations and facts about algebraic function fields. Moreover, we have developed an algorithmic version of the strong approximation theorem, a tool which is frequently used in this thesis.

In the second chapter we give a detailed exposition of General Kummer Theory, which describes an abstract method for the characterization of all Abelian extension of a given field.

In the third chapter we use the results of chapter two to describe Kummer

and Artin-Schreier-Witt extensions and list some important properties.

The fourth chapter contains the main results of this thesis, namely the computation of integral closures of Kummer and Artin-Schreier-Witt extensions. Let F be a function field, $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$ a set of places of F and E a Kummer or an Artin-Schreier-Witt extension of F. We present algorithms for computing the set of $\mathcal{O}_\mathcal{S}(E)$-integral elements of E. This is done by calculating for each $P \in \mathcal{S}$ a local integral basis for E/F. The set Ω which consists of all these elements is then a set of generators of $\mathcal{O}_\mathcal{S}(E)$ over $\mathcal{O}_\mathcal{S}$ (this is assured by Theorem 4.1.1).

Our algorithms were implemented using the algorithmic number theory tool MAGMA [C$^+$04]. In the fifth chapter we give examples which demonstrate the efficiency of our method for computing integral closures by comparing it with the general method.

Acknowledgements

I would like to thank

- Prof. Dr. M. E. Pohst for his support during the last years,
- Dr. S. Pauli and Prof. Dr. F. Heß, who spent hours and hours listening and discussing problems with me and accompanied me through the ups and downs of my research work,
- Dr. C. Fieker, who helped me a lot with the implementation of my algorithms in MAGMA,
- A. Schöpp and S. Freundt, who carefully read a preliminary version of this thesis.

Chapter 1

Foundations

1.1 Localization of Rings and Modules

In this section we introduce very shortly some basic facts about localization. We mainly only use the definitions and results of this section in Proposition 1.2.8 and Theorem 4.1.1. We refer the reader for instance to Chapter 5 and 9 of [AB74] (this is the source where we are citing from).

Let A be a **multiplicative subset** of an integral domain R, i. e. a subset of R with $1 \in A$ and $0 \notin A$ which is closed under multiplication. The subring R_A of the quotient field $Q(R)$ of R consisting of all quotients $\frac{r}{s}$ with $r \in R$ and $s \in A$ is called the **localization of R with respect to A**. We denote the canonical injection $R \hookrightarrow R_A$ by ι.

For each R-module M consider the equivalence relation $\sim$ on $M \times A$ given by

$$(m_1, s_1) \sim (m_2, s_2) \quad :\Longleftrightarrow \quad \exists s \in A \text{ with } s(m_1 s_2 - m_2 s_1) = 0.$$

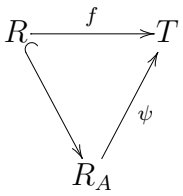
We denote the equivalence class of an element (m, s) by $\frac{m}{s}$. Now the set of equivalence classes $(M \times A)/A$ becomes an R_A-module in an obvious way. We call this module the **localization of M with respect to A** and denote it by M_A. We can use the canonical morphism $R \hookrightarrow R_A$ to consider M as an R-module. The canonical injection $M \hookrightarrow M_A$ is then easily seen to be an R-module homomorphism.

From now on all rings are supposed to be integral domains.

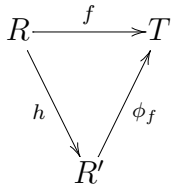
1.1.1 Proposition ([AB74, 1.5, p. 314]). *Let A be a multiplicative subset*

of a ring R.

(i) *If $f : R \longrightarrow T$ is a ring morphism with the property that $f(s)$ is a unit for all $s \in A$, then there is a unique ring morphism $\psi : R_A \longrightarrow T$ such that the following diagram commutes:*



(ii) *Let $h : R \longrightarrow R'$ be a ring morphism with the property that $h(s)$ is a unit in R' for all $s \in A$. Suppose that for each ring morphism $f : R \longrightarrow T$ with $f(s)$ is a unit in T for all $s \in A$ there is a unique ring morphism $\phi_f : R' \longrightarrow T$ such that the following diagram commutes:*

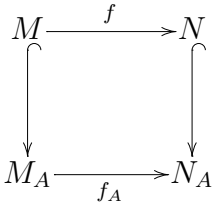


If now T equals R_A and f is the canonical injection $\iota : R \hookrightarrow R_A$, then ϕ_ι is a ring isomorphism.

1.1.2 Proposition ([AB74, 2.2, p. 317]). *Let A be a multiplicative subset of a ring R.*

(i) *Let M be an R-module. If M is generated by a subset X of M as an R-module, then the image of X in M_A under the canonical morphism generates M_A as an R_A-module.*

(ii) *If $f : M \longrightarrow N$ is an R-module homomorphism, then there exists a unique morphism $f_A : M_A \longrightarrow N_A$ such that the following diagram commutes:*



The only example of localization we will consider is the following: For any prime ideal $\mathfrak{p}$ of a ring R, the set $A := R \setminus \mathfrak{p}$ is a multiplicative subset of R. In this case the localization of R (respectively of an R-module M) with respect to A is called the **localization of R (respectively M) at $\mathfrak{p}$** and is denoted by $R_{\mathfrak{p}}$ (respectively $M_{\mathfrak{p}}$). If $f : M \longrightarrow N$ is an R-module homomorphism, then the unique homomorphism $M_{\mathfrak{p}} \longrightarrow N_{\mathfrak{p}}$ of the last proposition is denoted by $f_{\mathfrak{p}}$.

We now finish this first section with the following

1.1.3 Proposition ([AB74, 3.10, p. 323]). *Let $f : M \longrightarrow N$ be an R-module homomorphism. Then f is a monomorphism (epimorphism, isomorphism) iff $f_{\mathfrak{p}}$ is a monomorphism (epimorphism, isomorphism) for all maximal ideals $\mathfrak{p}$ in R.*

1.2 Algebraic Function Fields

In this section we give all the necessary basic definitions, notations and facts about algebraic function fields which are used in this thesis. Unless otherwise stated, we will very closely follow the book of Stichtenoth [Sti93], Chapters I and III.

Throughout this section, let k be an arbitrary perfect field. An **(algebraic) function field F/k (of one variable) over** k is a finite algebraic extension of the **rational function field** $k(x)$ for some $x \in F$ which is transcendental over k. k is the **constant field** and the algebraic closure $\tilde{k}$ of k in F the **full constant field** of F. If k is finite then F/k is a **global** function field. The rational function field is no invariant of F/k, since it depends on the choice of x. There always exist x and ρ in F such that

- $f(x, \rho) = 0$ for some irreducible polynomial $f \in k[x, t]$ which is monic and separable with respect to t and $\deg_t f = n$.
- $F = k(x, \rho)$ and $[F : k(x)] = n$.

Such x is called a **separating element** for F/k.

1.2.1 Definition and Proposition. *A ring $k \subsetneq \mathcal{O} \subsetneq F$ with $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$ for all $0 \neq z \in F$ is called a* **valuation ring** *of F/k. Such a ring has the following properties:*

(i) *$\mathcal{O}$ is a local ring with (unique) maximal ideal $P = \mathcal{O} \setminus \mathcal{O}^*$ where $\mathcal{O}^*$ is the set of units of $\mathcal{O}$.*

(ii) *For $0 \neq a \in F$: $a \in P \iff a^{-1} \notin \mathcal{O}$.*

(iii) *P is principal, i. e. $P = \mathcal{O} \cdot t$ for some $t \in \mathcal{O}$. t is called a* **prime element** *for P.*

(iv) *Each element $0 \neq a \in F$ has a unique representation of the form $a = ut^n$ for some $u \in \mathcal{O}^*$ and some integer n.*

A **place** of F is the unique maximal ideal of some valuation ring $\mathcal{O}$ of F. Since $\mathcal{O}$ is uniquely determined by P (1.2.1(ii)), we write $\mathcal{O}_P := \mathcal{O}$ and call $\mathcal{O}_P$ the **valuation ring** of P. We denote by $\mathbb{P}_F$ the set of places of F.

1.2.2 Definition. A **discrete valuation** of F/k is a function $v : F \to \mathbb{Z} \cup \{\infty\}$ with the following properties:

(i) $v(a) = \infty \iff a = 0$.

(ii) $v(ab) = v(a) + v(b)$ for all $a, b \in F$.

(iii) $v(a + b) \geq \min\{v(a), v(b)\}$ for all $a, b \in F$.

(iv) $v(z) = 1$ for some $z \in F$.

(v) $v(a) = 0$ for any $0 \neq a \in k$.

A stronger version of (iii) is given by

1.2.3 Lemma (Strict Triangularity). *If $v(a) \neq v(b)$, then*

$$v(a + b) = \min\{v(a), v(b)\}.$$

We now use the representation of an element $0 \neq a \in F$ given in 1.2.1(vi) to define a discrete valuation v_P for any place P of F by

$$v_P(0) := \infty \quad \text{and} \quad v_P(a) = v_P(ut^n) := n$$

(note that this definition does not depend on the choice of the prime element t). Then

$$\mathcal{O}_P = \{a \in F \mid v_P(a) \geq 0\},$$

$$\mathcal{O}_P^* = \{a \in F \mid v_P(a) = 0\}$$

and

$$P := \{a \in F \mid v_P(a) > 0\}.$$

If on the other hand v is a discrete valuation of F/k, then the set

$$\{a \in F \mid v(a) > 0\}$$

is a place of F and

$$\{a \in F \mid v_P(a) \geq 0\}$$

is the corresponding valuation ring. To summarize the above, one has bijections between the sets of places, valuations and valuation rings of F given by

$$P \longleftrightarrow v_P \longleftrightarrow \mathcal{O}_P.$$

The field $\overline{\mathcal{O}_P} := \mathcal{O}_P/P$ is called the **residue class field** of P and the integer $[\overline{\mathcal{O}_P} : k]$ the **degree** of P.

1.2.4 Definition. Let F/k be a function field with full constant field k. A function field E/K (where K is the full constant field of E) is called an **algebraic extension** of F/k, if E/F is an algebraic field extension and $k \subseteq K$. The extension is a **constant field extension** if $E = FK$. A place $P' \in \mathbb{P}_E$ is said to **lie over** $P \in \mathbb{P}_F$ if $P \subseteq P'$. We also say P' is **above** P, P' is an **extension** of P or P **lies under** P' and write $P'|P$.

1.2.5 Remark. In the situation of 1.2.4 the following three assertions are equivalent:

(1) $P'|P$.

(2) $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.

(3) There exists an integer $e := e(P'|P) \geq 1$ with $v_{P'}(x) = ev_P(x)$ for all $x \in F$.

If $P'|P$ then $P = P' \cap F$ and $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$. For each $P' \in \mathbb{P}_E$ there is exactly one place $P \in \mathbb{P}_F$ lying under P', namely $P' \cap F$. On the other hand, any place $P \in \mathbb{P}_F$ has at least one, but only finitely many extensions $P' \in \mathbb{P}_E$. Moreover, we have a canonical embedding $\overline{\mathcal{O}_P} \hookrightarrow \overline{\mathcal{O}_{P'}}$.

$f(P'|P) := [\overline{\mathcal{O}_{P'}} : \overline{\mathcal{O}_P}]$ is called the **relative degree** of P' over P. It is finite iff E/F is a finite extension. $e(P'|P)$ is called the **ramification index** of P'

over P. If the function field L is an algebraic extension of E and $P'' \in \mathbb{P}_L$ a place above P', then

$$e(P''|P) = e(P''|P')e(P'|P) \text{ and } f(P''|P) = f(P''|P')f(P'|P).$$

The extension $P'|P$ is **ramified** if $e(P'|P) > 1$, otherwise it is **unramified**. P is called **totally ramified** in E if there is exactly one extension P' of P in E and $e(P'|P) = [E : F]$. P is **completely inert** in E if there is exactly one extension P' of P in E and $f(P'|P) = [E : F]$. And P is **completely decomposed** in E if there are exactly $n := [E : F]$ extensions $P_1, \ldots, P_n$ of P. To finish this remark suppose $P_1, \ldots, P_r$ are all the places of E above P. Then

$$\sum_{i=1}^{r} e(P_i|P)f(P_i|P) = [E : F]. \tag{1.2.a}$$

The following remark describes the relatively easy ramification behaviour of places in a finite Galois extension. Recall that a finite algebraic field extension E/F is **Galois** if the automorphism group

$$\begin{aligned}\text{Aut}\,(E/F) := \{\sigma : E \to E \mid \sigma \text{ is an automorphism} \\ \text{and } \sigma(a) = a \text{ for each } a \text{ in } F\}\end{aligned}$$

has order $[E : F]$. In such a case, $\text{Aut}\,(E/F)$ is called the **Galois group** of E/F and is denoted by $\text{Gal}(E/F)$.

1.2.6 Remark. (**Hilbert's ramification theory**) Let E/F be a finite Galois extension of function fields with Galois group $G := \text{Gal}(E/F)$ and $P_1, \ldots, P_r$ be all the extensions of a place P of F to E. Then all the ramification indices and relative degrees of $P_i|P$ are equal, i. e.

$$e(P_i|P) = e(P_j|P) =: e(P) \text{ and } f(P_i|P) = f(P_j|P) =: f(P) \text{ for all } i, j$$

and therefore (see (1.2.a)) $e(P)f(P)r = [E : F]$. For each $1 \leq i \leq r$ we call

$$G_Z(P_i|P) := \{\sigma \in G \mid \sigma(P_i) = P_i\}$$

the **decomposition group** and

$$G_T(P_i|P) := \{\sigma \in G \mid v_{P_i}(\sigma z - z) > 0 \text{ for all } z \in \mathcal{O}_{P_i}\}$$

the **inertia group** of P_i over P. Obviously we have

$$G_T(P_i|P) \subseteq G_Z(P_i|P) \subseteq G.$$

The field $Z_i := Z(P_i|P) := \mathrm{Fix}_{E/F}\big(G_Z(P_i|P)\big)$ is called the **decomposition field** and the field $T_i := T(P_i|P) := \mathrm{Fix}_{E/F}\big(G_T(P_i|P)\big)$ is called the **inertia field** of P_i over P. If we denote by P_{Z_i} the restriction of P_i to Z_i and by P_{T_i} the restriction of P_i to T_i, then we have the following diagram:

$$\begin{array}{cc} E & P_i \\ | & | \\ & \quad e(P_i|P_{T_i}) = e(P_i|P) = [E : T_i] \\ & \quad \text{and } f(P_i|P_{T_i}) = 1 \\ T_i & P_{T_i} \\ | & | \\ & \quad f(P_{T_i}|P_{Z_i}) = f(P_i|P) = [T_i : Z_i] \\ & \quad \text{and } e(P_{T_i}|P_{Z_i}) = 1 \\ Z_i & P_{Z_i} \\ | & | \\ & \quad e(P_{Z_i}|P) = f(P_{Z_i}|P) = 1 \\ & \quad \text{and } [Z_i : F] = r \\ F & P \end{array}$$

In particular, if E/F is cyclic of degree p^n for a prime p, then we have exactly $n-1$ intermediate fields of E/F, say

$$F := E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{n-1} \subseteq E_n =: E,$$

and $[E_r : E_{r-1}] = p$ for all $1 \leq r \leq n$. From the above it then follows that there exist $1 \leq d \leq t \leq n$ such that $Z_i = Z_j =: Z = E_d$ and $T_i = T_j =: T = E_t$ for all $1 \leq i, j \leq n$. This means that P is completely decomposed in Z/F, each P_{Z_i} is completely inert in T/Z and each P_{T_i} is totally ramified in E/T.

1.2.7 Definition. A ring $k \subset R \subset F$ which is not a field is called a **subring** of F/k. An element a of F is called **integral over** R or R-**integral** if $f(a) = 0$ for some monic polynomial $f(X) \in R[X]$. The ring

$$\mathcal{C}l(R, F) := \{a \in F \mid a \text{ is integral over } R\}$$

is called **the integral closure** of R in F. Let Q be the quotient field of R in F. R is called **integrally closed** if $\mathcal{C}l(R, Q) = R$.

A ring $R \subset F$ which is of the form

$$R = \mathcal{O}_{\mathcal{S}} := \{a \in F \mid v_P(a) \geq 0 \text{ for all } P \in \mathcal{S}\} = \bigcap_{P \in \mathcal{S}} \mathcal{O}_P$$

for $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$ is called a **holomorphy ring** of F/k. A holomorphy ring is also a subring of F/k.

The following proposition lists some properties of holomorphy rings:

1.2.8 Proposition. (i) *For $P \in \mathbb{P}_F$ we have $\mathcal{O}_\mathcal{S} \subseteq \mathcal{O}_P \iff P \in \mathcal{S}$.*

(ii) *The quotient field of $\mathcal{O}_\mathcal{S}$ is F and $\mathcal{O}_\mathcal{S}$ is integrally closed.*

(iii) *$\mathcal{O}_\mathcal{S}$ is a Dedekind domain.*

(iv) *There is a 1-1-correspondence between $\mathcal{S}$ and the set of maximal ideals of $\mathcal{O}_\mathcal{S}$, given by*

$$P \longleftrightarrow P \cap \mathcal{O}_\mathcal{S}.$$

(v) *For each $P \in \mathcal{S}$, the localization $(\mathcal{O}_\mathcal{S})_{P\cap\mathcal{O}_\mathcal{S}}$ of $\mathcal{O}_\mathcal{S}$ at P equals $\mathcal{O}_P$ (this follows from 1.1.1(ii)).*

(vi) *If $\mathcal{S}$ is non empty and finite, then $\mathcal{O}_\mathcal{S}$ is a principal ideal domain.*

For a subring R of F we define the set $\Gamma(R,F) := \{P \in \mathbb{P}_F \mid R \subseteq \mathcal{O}_P\}$. Then $\emptyset \neq \Gamma(R,F) \subsetneqq \mathbb{P}_F$ and we have

$$\mathcal{C}l(R,F) = \mathcal{O}_{\Gamma(R,F)}.$$

This implies that if E is a finite separable extension of F,

$$\mathcal{C}l(R,E) = \mathcal{C}l\big(\mathcal{C}l(R,F),E\big).$$

For $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$ we then get

$$\begin{aligned} \mathcal{C}l(\mathcal{O}_\mathcal{S},E) &= \mathcal{O}_{\Gamma(\mathcal{O}_\mathcal{S},E)} \\ &= \{a \in E \mid v_{P'}(a) \geq 0 \ \forall P'|P, \ \ P \in \mathcal{S}\} \\ &= \bigcap_{\substack{P'|P \\ P\in\mathcal{S}}} \mathcal{O}_{P'}. \end{aligned} \tag{1.2.b}$$

1.2.9 Remark. If E is a finite separable extension of F and $P \in \mathbb{P}_F$ or $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$, then we sometimes write $\mathcal{O}_P(E)$ for $\mathcal{C}l(\mathcal{O}_P,E)$ and $\mathcal{O}_\mathcal{S}(E)$ for $\mathcal{C}l(\mathcal{O}_\mathcal{S},E)$, respectively.

For a place P of F (a set $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$) we call the elements of $\mathcal{O}_P$ and $\mathcal{O}_P(E)$ ($\mathcal{O}_\mathcal{S}$ and $\mathcal{O}_\mathcal{S}(E)$, respectively) **integral over** P or simply P**-integral** (**integral over** $\mathcal{S}$ or $\mathcal{S}$**-integral**, respectively).

We now describe some special cases of holomorphy rings of a function field F/k. The set of places of the rational function field $k(x)/k$ is given by

$$\mathbb{P}_{k(x)} = \{P_\infty\} \cup \{P_\pi \mid \pi \in k[x] \text{ irreducible}\},$$

where

$$P_\infty := \{g/h \mid g,h \in k[x], \deg g < \deg h\}$$

and

$$P_\pi := \{g/h \mid g, h \in k[x], h \neq 0, \pi \mid g, \pi \nmid h\}.$$

The corresponding valuation rings are

$$\mathcal{O}_\infty := \{g/h \mid g, h \in k[x], \deg g \leq \deg h\}$$

and

$$\mathcal{O}_\pi := k[x]_\pi := \{g/h \mid g, h \in k[x], h \neq 0, \pi \nmid h\}$$

respectively, and we have

$$k[x] = \bigcap_{\substack{\pi \in k[x] \\ \text{irreducible}}} \mathcal{O}_\pi.$$

We define by

$$\mathbb{P}_F^\infty := \{P \in \mathbb{P}_F \mid P | P_\infty\},$$

the set of **infinite places** and by

$$\mathbb{P}_F^0 := \mathbb{P}_F \setminus \mathbb{P}_F^\infty = \{P \in \mathbb{P}_F \mid \exists \pi \in k[x],\ \pi \text{ irreducible and } P \mid P_\pi\},$$

the set of **finite places** of F. We call

$$\mathcal{O}_F^\infty := \mathcal{O}_{\mathbb{P}_F^\infty} = \mathcal{C}l(\mathcal{O}_\infty, F).$$

the **infinite maximal order** and

$$\mathcal{O}_F := \mathcal{O}_F^0 := \mathcal{O}_{\mathbb{P}_F^0} = \mathcal{C}l(k[x], F)$$

the **finite maximal order** of F/k.

1.2.10 Theorem. *Let R be an integrally closed subring of F/k with quotient field F and let E be a finite separable extension of F of degree n. Then there exists a basis of E/F which is contained in $\mathcal{C}l(R, E)$. If R is a principal ideal domain, then there exists a basis $\{\alpha_1, \ldots, \alpha_n\}$ of E/F with*

$$\mathcal{C}l(R, E) = \sum_{i=1}^{n} R\alpha_i.$$

From (1.2.b) and 1.2.10 it follows that for a place P in F the integral closure of its valuation ring $\mathcal{O}_P$ in E is

$$\mathcal{O}_P(E) := \mathcal{C}l(\mathcal{O}_P, E) = \bigcap_{P'|P} \mathcal{O}_{P'} = \{a \in E \mid v_{P'}(a) \geq 0\ \forall P'|P\} \qquad (1.2.c)$$

and that there exists a basis $\{\alpha_1, \ldots, \alpha_n\}$ of E/F with

$$\mathcal{C}l(\mathcal{O}_P, E) = \sum_{i=1}^{n} \mathcal{O}_P \cdot \alpha_i \ ,$$

called an **integral basis** of $\mathcal{C}l(\mathcal{O}_P, E)$ over $\mathcal{O}_P$ or a **local integral basis** of E/F for P.

1.2.11 Remark. Throughout this thesis we use the following notation: if E/F is a field extension and y an element of E, then we write

$$\chi_{(y,\, E/F)}(T) \in F[T]$$

for the the minimal polynomial of y over F.

We finish this section with some statements concerning the ramification behaviour of places and special integral bases. For a place P of a function field F and a polynomial $\phi(T) = \sum c_i T^i \in \mathcal{O}_P[T]$ we set

$$\overline{\phi}(T) := \sum \overline{c_i} T^i \in \overline{\mathcal{O}_P}[T],$$

where $\overline{c_i} \in \overline{\mathcal{O}_P} = \mathcal{O}_P/P$ is the residue class of $c_i \in \mathcal{O}_P$.

1.2.12 Theorem. *Let $E = F(y)$ be an extension of a function field F of degree n, P a place of F and y integral over P. Set $\chi(T) := \chi_{(y,\, E/F)}(T)$. Let*

$$\overline{\chi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\epsilon_i}$$

be the decomposition of $\overline{\chi}(T)$ into irreducible factors over $\overline{\mathcal{O}_P}$, i. e. the polynomials $\gamma_i(T)$ are monic, irreducible, pairwise distinct and $\epsilon_i \geq 1$. For each $\gamma_i(T)$ we choose a monic polynomial $\phi_i(T) \in \mathcal{O}_P[T]$ with $\overline{\phi_i}(T) = \gamma_i(T)$ and $\deg \phi_i(T) = \deg \gamma_i(T)$. Then there are for each $1 \leq i \leq r$ places P_i of E over P with

$$\phi_i(y) \in P_i \quad \textit{and} \quad f(P_i|P) \geq \deg \gamma_i(T).$$

If moreover $\{1, y, \ldots, y^{n-1}\}$ is an integral basis for P, then there exists for each $1 \leq i \leq r$ exactly one place P_i of E over P with

$$\phi_i(y) \in P_i, \quad f(P_i|P) = \deg \gamma_i(T), \quad e(P_i|P) = \epsilon_i,$$

and $P_1, \ldots, P_r$ are the only places of E over F.

Proof. See for instance [Sti93, III.3.7]. □

1.2.13 Proposition. *Let E be a finite separable extension of a function field F of degree n.*

(i) *Suppose $E = F(y)$ and $\chi(T) = \chi_{(y,\,E/F)}(T)$ is the minimal polynomial of y. If for some $P \in \mathbb{P}_F$ we have*

$$\chi(T) \in \mathcal{O}_P[T] \quad \text{and} \quad v_{P'}(\chi'(y)) = 0$$

for all $P' \in \mathbb{P}_E$ with $P'|P$ then P is unramified in E and $\{1, y, \ldots, y^{n-1}\}$ is a local integral basis for P in E/F.

(ii) *If a place $Q'|Q$ (where $Q \in \mathbb{P}_F$ and $Q' \in \mathbb{P}_E$) is totally ramified in E/F and π a prime element for Q', then $\{1, \pi, \ldots, \pi^{n-1}\}$ is a local integral basis for Q in E/F.*

Proof. [Sti93, III.5.11 and III.5.12]. □

1.3 Strong Approximation

A main tool for all results presented in this thesis is the strong approximation theorem. Since it is also of independent interest, we give an algorithmic solution in this section.

1.3.1 Theorem (Strong Approximation). *Let $F/\mathbb{F}_q$ be a function field, $\emptyset \neq \mathcal{S} \subsetneq \mathbb{P}_F$ and $P_1, \ldots, P_r \in \mathcal{S}$. Suppose there are given $a_1, \ldots, a_r \in F$ and $n_1, \ldots, n_r \in \mathbb{Z}$. Then there exists an element $z \in F$ such that*

$$\begin{aligned} v_{P_i}(z - a_i) &= n_i \qquad 1 \leq i \leq r, \text{ and} \\ v_P(z) &\geq 0 \qquad \text{for all } P \in \mathcal{S} \setminus \{P_1, \ldots, P_r\}. \end{aligned} \tag{1.3.a}$$

Our proof follows Stichtenoth [Sti93], but is constructive.

1.3.2 Lemma. *Suppose we are in the situation of the theorem. Then there exists an element $y \in F$ such that*

$$\begin{aligned} v_{P_i}(y - a_i) &> n_i \qquad 1 \leq i \leq r, \text{ and} \\ v_P(y) &\geq 0 \qquad \text{for all } P \in \mathcal{S} \setminus \{P_1, \ldots, P_r\}. \end{aligned} \tag{1.3.b}$$

Proof. For $1 \leq i \leq r$ we set $\tilde{n}_i := n_i + 1$. We take a divisor A of positive degree whose support is disjoint to S. Then there exists $l \in \mathbb{N}$ such that the divisor $D := lA - \sum_{j=1}^{r} \tilde{n}_j P_j$ is non-special.

We now describe how to find for each $1 \leq i \leq r$ an element $y_i \in F$ with

$$\begin{aligned} v_{P_i}(y_i - a_i) &\geq \tilde{n}_i \qquad 1 \leq i \leq r, \\ v_{P_j}(y_i) &\geq \tilde{n}_j \qquad 1 \leq i \leq r, \;\; j \neq i \text{ and} \\ v_P(y_i) &\geq 0 \qquad \text{for all } P \in \mathcal{S} \setminus \{P_1, \ldots, P_r\}. \end{aligned} \tag{1.3.c}$$

The element $y = \sum_{i=1}^{r} y_i$ then satisfies (1.3.b).

If $v_{P_i}(a_i) \geq \tilde{n}_i$ we can set $y_i := 0$ and are done.

Suppose now $v_{P_i}(a_i) < \tilde{n}_i$. The non-speciality of D implies $\mathcal{A}_F = \mathcal{A}_F(D) + F$. Therefore there exists $\beta \in F$ such that $(\beta - \alpha_i) \in \mathcal{A}_F(D)$, where $\alpha_i \in \mathcal{A}_F$ is the adele whose P_i-component equals a_i and which is zero at all other components. This implies $v_{P_i}(\beta - a_i) \geq \tilde{n}_i > v_{P_i}(a_i)$. Strict triangularity then yields $v_{P_i}(\beta) = v_{P_i}(a_i)$, therefore

$$\beta \in \mathcal{L} := \mathcal{L}\Big(lA - \sum_{j=1}^{r} \tilde{n}_j P_j + \tilde{n}_i P_i - v_{P_i}(a_i) P_i\Big)$$

and $y_i := \beta$ satisfies (1.3.c). We finish the proof by showing how to actually compute β:

[i] Let $\mathcal{B} := b_1, \ldots, b_s$ be a basis of $\mathcal{L}$ (for the computation of the Riemann-Roch spaces we refer to [Hes02]).

[ii] For each element $\gamma \in \{a_i\} \cup \mathcal{B}$ we compute a (finite) series expansion in the following sense: Let π be a prime element of P_i and $\omega_1, \ldots, \omega_l$ a set of representatives of an $\mathbb{F}_q$-basis of the residue class field of P_i. We set $\tilde{\gamma} := \gamma \pi^{-v_{P_i}(a_i)}$ and then, iteratively for $v_{P_i}(a_i) \leq w \leq \tilde{n}_i$, we lift $\tilde{\gamma}(P_i)$ to $\gamma_w = \sum_{\mu=1}^{l} \gamma_{w,\mu} \omega_\mu$ and do $\tilde{\gamma} \leftarrow \frac{\tilde{\gamma} - \gamma_w}{\pi}$. This yields the expansion $\sum_{w=v_{P_i}(a_i)}^{\tilde{n}_i} \gamma_w \pi^w$ of γ. (Here, $\tilde{\gamma}(P_i)$ denotes the residue class of $\tilde{\gamma}$ modulo P_i.)

[iii] We construct a matrix M over $\mathbb{F}_q$ whose columns correspond to the elements of $\mathcal{B}$. Let $c = (c_1, \ldots, c_s)$ be such that $Mc = a_i$ (from what was said above it is clear that c exists.)

[iv] Set $\beta := \sum_{v=1}^{s} c_v b_v$.

□

We summarize the proof of the lemma in the following algorithm:

1.3.3 Algorithm.

Input: $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$, $P_1, \ldots, P_r \in \mathcal{S}$ $a_1, \ldots, a_r \in F$, $n_1, \ldots, n_r \in \mathbb{Z}$.

Output: $y \in F$ such that $v_{P_i}(y - a_i) > n_i$ for all $1 \leq i \leq r$ and $v_P(y) \geq 0$ for all $P \in \mathcal{S} \setminus \{P_1, \ldots, P_r\}$.

1. **for** $1 \leq i \leq r$ **do**
2. $\quad \tilde{n}_i := n_i + 1$.
3. **end for**
4. Choose a divisor A with $\deg A > 0$ whose support is disjoint to S.
5. Compute $l \in \mathbb{N}$ such that $D := lA - \sum_{j=1}^{r} \tilde{n}_j P_j$ is non-special.
6. **for** $1 \leq i \leq r$ **do**
7. $\quad$ **if** $v_{P_i}(a_i) \geq \tilde{n}_i$ **then**
8. $\quad\quad y_i := 0$
9. $\quad$ **else**
10. $\quad\quad$ Compute β as described in [i]-[iv] in the above proof.
11. $\quad\quad y_i := \beta$.
12. $\quad$ **end if**
13. **end for**
14. $y = \sum_{i=1}^{r} y_i$.

Proof of Theorem 1.3.1. We use algorithm 1.3.3 to compute $y \in F$ with

$$\begin{aligned} v_{P_i}(y - a_i) &> n_i \qquad 1 \le i \le r, \text{ and} \\ v_P(y) &\ge 0 \qquad \text{for all } P \in \mathcal{S} \setminus \{P_1, \dots, P_r\} \end{aligned}$$

and $\tilde{y} \in F$ with

$$\begin{aligned} v_{P_i}(\tilde{y} - \pi_i^{n_i}) &> n_i \qquad 1 \le i \le r, \text{ and} \\ v_P(\tilde{y}) &\ge 0 \qquad \text{for all } P \in \mathcal{S} \setminus \{P_1, \dots, P_r\}. \end{aligned}$$

The strict triangle equation then shows that the element $z := y + \tilde{y}$ satisfies (1.3.a). □

1.4 The Ring of Witt vectors

In this section we introduce the definition as well as important properties of Witt vectors, which yield a basic tool for describing all Abelian extensions of degree p^n of a field of characteristic $p > 0$ (see Section 3.2). Witt vectors were constructed by Witt in his famous work "Zyklische Körper und Algebren der Charakteristik p vom Grad p^n" ([Wit36]). Other references we use are [Sch36a], [Sch36b], [Lor90] and [Has80, p. 156-161].

Let p be a natural prime number and

$$\mathbb{Z}[X_1, Y_1, X_2, Y_2, \dots, X_n, Y_n, \dots]$$

the polynomial ring in countably many variables over the the ring $\mathbb{Z}$. We consider vectors $Z = (Z_1, Z_2, \dots)$ with $Z_i \in \mathbb{Z}[X_1, Y_1, X_2, Y_2, \dots]$ and define for $n = 1, 2, \dots$

$$Z^{(n)} := \sum_{i=1}^{n} p^{i-1} Z_i^{p^{n-i}} = Z_1^{p^{n-1}} + pZ_2^{p^{n-2}} + \cdots + p^{n-1} Z_n.$$

These so called "Ghost components" $Z^{(1)}, Z^{(2)}, \dots$ of Z uniquely determine the vector Z: Using the **Frobenius map**

$$\mathcal{F}(Z) := (Z_1^p, Z_2^p, \dots) \tag{1.4.a}$$

the above definitions become

$$\begin{aligned} Z^{(1)} &= Z_1, \\ Z^{(n)} &= (\mathcal{F}(Z))^{(n-1)} + p^{n-1} Z_n, \quad n > 1. \end{aligned} \tag{1.4.b}$$

From these formulas we can derive the components Z_i of Z as well defined polynomial expressions in $Z^{(1)}, Z^{(2)}, \dots$ with coefficients in $\mathbb{Z}[\frac{1}{p}]$, e.g.,

$$\begin{aligned} Z_1 &= Z^{(1)}, \\ Z_2 &= -\frac{1}{p}(\mathcal{F}(Z))^{(1)} + \frac{1}{p}(Z^{(2)}). \end{aligned}$$

Let $*$ be one of the operations $+$ or $\cdot$. For vectors $A := (A_1, A_2, \dots)$ and $B := (B_1, B_2, \dots)$ with components in $\mathbb{Z}[X_1, Y_1, X_2, Y_2, \dots]$ we define $A * B$ by

$$(A * B)^{(n)} := A^{(n)} * B^{(n)}, \tag{1.4.c}$$

e.g.,

$$\begin{aligned} (A * B)_1 &= A_1 * B_1, \\ (A \pm B)_2 &= (A_2 \pm B_2) - \frac{(A_1 \pm B_1)^p - (A_1^p \pm B_1^p)}{p} \\ &= (A_2 \pm B_2) - \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} A_1^{p-i} (\pm B_1)^i - \frac{(\pm 1)^p - (\pm 1)}{p} B_1^p, \\ (A \cdot B)_2 &= (A_1^p B_2 + A_2 B_1^p) + p A_2 B_2. \end{aligned}$$

In these examples all the polynomials on the right side have integral coefficients. It is a very important fact, that this holds generally.

1.4.1 Proposition. *The polynomials $S_n^*(A, B) := (A*B)_n$ only have integral coefficients, i. e.*

$$S_n^*(A, B) \in \mathbb{Z}[X_1, Y_1, X_2, Y_2, \dots, X_n, Y_n].$$

Proof. See for instance [Lor90, p. 139] or [Has80, pp. 157-159]. □

1.4.2 Proposition.

$$\begin{aligned} S_i^{\pm}(A, B) &= (A \pm B)_i \\ &= A_i \pm B_i + \frac{A_{i-1}^p \pm B_{i-1}^p - (A \pm B)_{i-1}^p}{p} \\ &\qquad + \frac{A_{i-2}^{p^2} \pm B_{i-2}^{p^2} - (A \pm B)_{i-2}^{p^2}}{p^2} + \cdots \\ &\qquad\qquad \cdots + \frac{A_1^{p^{i-1}} \pm B_1^{p^{i-1}} - (A \pm B)_1^{p^{i-1}}}{p^{i-1}} \end{aligned} \tag{1.4.d}$$

Proof. For all vectors Z we have

$$\begin{aligned}\big(\mathcal{F}(Z)\big)^{(i-1)} &= \big(\mathcal{F}^2(Z)\big)^{(i-2)} + p^{i-2}\big(\mathcal{F}(Z)\big)_{i-1}\\ &= \big(\mathcal{F}^3(Z)\big)^{(i-3)} + p^{i-3}\big(\mathcal{F}^2(Z)\big)_{i-2} + p^{i-2}\big(\mathcal{F}(Z)\big)_{i-1}\\ &\dots\\ &= \big(\mathcal{F}^{i-1}(Z)\big)^{(1)} + p\big(\mathcal{F}^{i-2}(Z)\big)_2 + p^2\big(\mathcal{F}^{i-3}(Z)\big)_3 + \cdots\\ &\qquad\qquad \cdots + p^{i-3}\big(\mathcal{F}^2(Z)\big)_{i-2} + p^{i-2}\big(\mathcal{F}(Z)\big)_{i-1}\\ &= Z_1^{p^{i-1}} + pZ_2^{p^{i-2}} + p^2Z_3^{p^{i-3}} + \cdots + p^{i-3}Z_{i-2}^{p^2} + p^{i-2}Z_{i-1}^{p}\end{aligned} \tag{1.4.e}$$

From (1.4.b) we get

$$(A \pm B)^{(i)} = \big(\mathcal{F}(A \pm B)\big)^{(i-1)} + p^{i-1}(A \pm B)_i$$

and from (1.4.c)

$$\begin{aligned}(A \pm B)^{(i)} &= A^{(i)} \pm B^{(i)}\\ &= \big(\mathcal{F}(A)\big)^{(i-1)} + p^{i-1}(A)_i \pm \big(\mathcal{F}(B)\big)^{(i-1)} \pm p^{i-1}(B)_i,\end{aligned}$$

hence

$$(A \pm B)_i = A_i \pm B_i + \frac{\big(\mathcal{F}(A)\big)^{(i-1)} \pm \big(\mathcal{F}(B)\big)^{(i-1)} - \big(\mathcal{F}(A \pm B)\big)^{(i-1)}}{p^{i-1}}.$$

The result then follows from (1.4.e). □

Now we have seen that (1.4.c) defines a ring structure on the set of vectors $Z = (Z_1, Z_2, \dots)$ with $Z_i \in \mathbb{Z}[X_1, Y_1, X_2, Y_2, \dots]$. The zero element is the vector $(0, 0, \dots)$ (since all its ghost components are 0) and the one element is the vector $(1, 0, 0, \dots)$ (since all its ghost components are 1). One easily verifies

$$Z = (Z_1, \dots, Z_n, 0, \dots) + (0, \dots, 0, Z_{n+1}, Z_{n+2}, \dots) \tag{1.4.f}$$

for each vector $Z = (Z_1, Z_2, \dots)$.

Let now A be an arbitrary commutative ring with 1. We denote by $W(A)$ the set of all vectors $x = (x_0, x_1, \dots)$ with $x_i \in A$. Although in this case the ghost components

$$x^{(n)} := \sum_{i=1}^{n} p^{i-1} x_i^{p^{n-i}} \tag{1.4.g}$$

of x in general do not uniquely determine x (e.g., if A is of characteristic p), one can show that by the above definitions

$$(x * y)_n = S_n^*(x, y) = S_n^*(x_1, y_1, x_2, y_2, \dots, x_n, y_n) \tag{1.4.h}$$

the set $W(A)$ becomes a commutative ring with zero element $(0, 0, \dots)$ and one element $(1, 0, 0, \dots)$. $W(A)$ is called the **Ring of Witt vectors over** A.

1.4.3 Remark. In order to write down some important properties of Witt vectors we first need to generalize slightly some of our earlier notations. A **discrete valuation** of a field E is a surjective mapping $v : E \to \mathbb{Z} \cup \{\infty\}$ with the following properties:

(i) $v(a) = \infty \iff a = 0$.

(ii) $v(ab) = v(a) + v(b)$ for all a, $b \in E$.

(iii) $v(a + b) \geq \min\{v(a), v(b)\}$ for all a, $b \in E$.

Like in Section 1.2 one has the **Strict Triangle Inequality**

$$v(a + b) = \min\{v(a), v(b)\} \quad \text{if } a, b \in E \text{ and } v(a) \neq v(b).$$

The pair (E, v) has the following properties:

(i) The set
$$R := \{a \in E \mid v(a) \geq 0\}$$
is a subring of E, the **valuation ring** of E with respect to v.

(ii) E is the quotient field of R.

(iii) $\mathfrak{p} := \{a \in E \mid v(a) > 0\}$ is an ideal of R, the **valuation ideal** with respect to v.

(iv) $R^* = R \setminus \mathfrak{p}$, i. e. $\mathfrak{p}$ is a maximal ideal of R and each ideal $\mathfrak{a} \subsetneq R$ of R is contained in $\mathfrak{p}$. Therefore R is a local ring with maximal ideal $\mathfrak{p}$.

(v) The field $R/\mathfrak{p}$ is called the **residue class field** of E with respect to v.

Let now E be a perfect field of characteristic p. The p-fold sum of a vector $x \in W(E)$ is given by

$$px = x + \dots + x = (0, x_1^p, x_2^p, \dots). \tag{1.4.i}$$

Therefore and since E is perfect, i. e. $E = E^p$, the ideal $p^n W(E)$ of $W(E)$ equals the set of vectors whose first n component are zero. Then we can define a map $v : W(E) \to \mathbb{Z} \cup \{\infty\}$ by

$$v(x) := \min\{i \mid x_{i+1} \neq 0\}.$$

1.4.4 Proposition. (i) *$W(E)$ has no zero divisors. Its quotient field is denoted by $Q(E)$.*

(ii) *The canonical extension of the map v to $Q(E)$ is a discrete valuation with valuation ring $W(E)$ and valuation ideal $pW(E)$. Therefore the units of $W(E)$ are exactly the vectors whose first component is not zero.*

(iii) *$Q(E)$ has characteristic 0.*

(iv) *$W(\mathbb{F}_p) = \mathbb{Z}_p$.*

For any natural $n > 0$ let us now consider the **Ring $W_n(E)$ of Witt vectors of length n** (consisting of the "truncated" vectors $x = (x_1, \ldots, x_n)$). Here addition and multiplication is defined in the same way as above for the first n coordinates. For this case we only note the following

1.4.5 Proposition. (i) *The units of $W_n(E)$ are exactly the vectors whose first component is not zero.*

(ii) *$W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$.*

Chapter 2

General Kummer Theory

General Kummer theory provides us with an abstract tool to describe all Abelian extensions of a given field F. The most important result for this thesis is corollary 2.3.2 to the main Theorem 2.1.11. This corollary characterizes all cyclic extensions of F of a given degree.

Since the way in which the representation of general Kummer theory is given in this chapter (and later used in this thesis) follows in most parts the lecture script "Algebra 2" held by Florian Heß at TU Berlin in the winter semester of 2003, we have decided to include all proofs. For other sources we refer the reader for instance to [Neu92, Chapter IV] or [Coh99, 10.2].

2.1 Preliminaries

We begin by stating the main theorem of infinite Galois theory. For details we refer the reader to [Neu92, Chapter IV.1]. We recall that a (finite or infinite) algebraic field extension L/F is **Galois** if L/F is normal and separable and that for each sub-extension E/F of L/F the extension L/E is Galois.

> *For the entire chapter we choose a field F and an arbitrary (finite or infinite) Galois extension L of F with Galois group $G := \mathrm{Gal}(L/F)$.*

We equip G with the following topology: for each $\sigma \in \mathrm{Gal}(L/E)$ we take the cosets σG as a neighborhood basis of σ, where E/F runs through all finite sub-extensions of L/F. The so defined topology is called **Krull topology**.

2.1.1 Theorem (Main Theorem of Infinite Galois Theory). *Let $\mathcal{G}$ be the set of closed (under the Krull topology) subgroups of G and $\mathcal{L}$ the set of intermediate fields of L/F. The maps*

$$\mathrm{Fix}_{L/F} : \mathcal{G} \longrightarrow \mathcal{L}, \quad H \mapsto \mathrm{Fix}_{L/F}(H) := \{l \in L \mid \sigma(l) = l \text{ for all } \sigma \in H\}$$

and

$$\begin{aligned}\mathrm{Gal}_{L/F} : \mathcal{L} \longrightarrow \mathcal{G}, \quad E \mapsto \mathrm{Gal}_{L/F}(E) &:= \mathrm{Gal}(L/E) \\ &:= \{\sigma \in G \mid \sigma(e) = e \text{ for all } e \in E\}\end{aligned}$$

are mutually inverse. Under this bijection, the open subgroups of $\mathcal{G}$ correspond exactly to the finite sub-extensions E/F of L/F.

Consider a subset A of L^m for some $m \in \mathbb{Z}^{\geq 1}$ on which we define a coordinatewise operation of G, i. e.

$$\sigma(a) = \sigma\big((a_1, \ldots, a_m)\big) := \big(\sigma(a_1), \ldots, \sigma(a_m)\big).$$

A shall possess a group structure $*$ which is compatible with this operation, i. e.

$$\sigma(a * b) = \sigma(a) * \sigma(b)$$

for all $\sigma \in G$ and all $a, b \in A$. Then A is called a G-**module**.

For a subgroup H of G we define a subgroup A^H of A by

$$A^H := \{\alpha \in A \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\} \tag{2.1.a}$$

and for a subset B of A a subgroup G_B of G by

$$G_B := \{\sigma \in G \mid \sigma(\beta) = \beta \text{ for all } \beta \in B\}. \tag{2.1.b}$$

In this way we get mappings $A^{(\,)}\big(H \mapsto A^H\big)$ and $G_{(\,)}\big(B \mapsto G_B\big)$ between $\mathcal{G}$ and the set $\mathcal{A}$ of subsets of A.

We now use these four maps to define the maps

$$F(\,) : \mathcal{A} \longrightarrow \mathcal{L}, \quad B \mapsto F(B) := \mathrm{Fix}_{L/F}(G_B) \tag{2.1.c}$$

and

$$A_{(\,)} : \mathcal{L} \longrightarrow \mathcal{A}, \quad E \mapsto A_E := A^{\mathrm{Gal}_{L/F}(E)}. \tag{2.1.d}$$

One easily verifies

$$A_E = A \cap E^m. \tag{2.1.e}$$

Let B be a subset of $\mathcal{A}$ and $F\big(\{B\}\big)$ be the subfield of L which is obtained by adjoining all the coordinates of the elements of B to F. Since

$$\begin{aligned}\mathrm{Gal}_{L/F}\big(F\big(\{B\}\big)\big) &= \big\{\sigma \in G \mid \sigma(y) = y \text{ for all } y \in F\big(\{B\}\big)\big\}\\ &= \big\{\sigma \in G \mid \sigma(\beta) = \beta \text{ for all } \beta \in B\big)\big\}\\ &= G_B\end{aligned}$$

we get

$$F(\{B\}) = \mathrm{Fix}_{L/F}\big(\mathrm{Gal}_{L/F}\big(F\big(\{B\}\big)\big)\big) = \mathrm{Fix}_{L/F}\big(G_B\big) = F(B) \qquad (2.1.\mathrm{f})$$

and

$$G_B = \mathrm{Gal}_{L/F}\big(F\big(\{B\}\big)\big) = \mathrm{Gal}_{L/F}\big(F(B)\big). \qquad (2.1.\mathrm{g})$$

Since $\mathrm{Gal}_{L/F}\big(F(B)\big) = \mathrm{Gal}(L/F(B))$ is closed (under the Krull topology) in $\mathrm{Gal}(L/F)$, this last equation shows

2.1.2 Proposition. *For each subset B of A the group G_B is closed in* $\mathrm{Gal}(L/F)$.

We know that $F(B)/F$ is Galois iff $\mathrm{Gal}(L/F(B)) = G_B$ is normal in G. We obviously have

2.1.3 Proposition. *If $B \subseteq \mathcal{A}$ is fixed under G, then G_B is normal in G.*

Let $E_1 \subseteq E_2$ be intermediate fields of L/F and R be a complete irreducible set of representatives of $\mathrm{Gal}_{L/F}(E_2)$ in $\mathrm{Gal}_{L/F}(E_1)$. We now define the map

$$\mathrm{N}_{E_2/E_1} : A_{E_2} \longrightarrow A_{E_1}, \quad a \mapsto \prod_{\tau \in R} \tau(a)$$

if the group structure $*$ in A is written multiplicatively and

$$\mathrm{Tr}_{E_2/E_1} : A_{E_2} \longrightarrow A_{E_1}, \quad a \mapsto \sum_{\tau \in R} \tau(a)$$

if the group structure in A is written additively. (For the rest of this section we stay with the first case, but everything works the same way for the second.) Since for each $\sigma \in \mathrm{Gal}_{L/F}(E_1)$ also $R' := \{\sigma\tau \mid \tau \in R\}$ is a complete irreducible set of representatives of $\mathrm{Gal}_{L/F}(E_2)$ in $\mathrm{Gal}_{L/F}(E_1)$, we have

$$\sigma(\mathrm{N}_{E_2/E_1}(a)) = \mathrm{N}_{E_2/E_1}(a)$$

for each $\sigma \in \mathrm{Gal}_{L/F}(E_1)$, hence $\mathrm{N}_{E_2/E_1}(a) \in A_{E_1}$ and N_{E_2/E_1} is well defined.

2.1.4 Theorem. *We keep the above notations.*

(i) N_{E_2/E_1} *is well defined.*

(ii) N_{E_2/E_1} *is a homomorphism.*

(iii) *For each* $a \in A_{E_2}$ *and each* $\sigma \in G$ *we have*

$$\mathrm{N}_{\sigma(E_2)/\sigma(E_1)}(\sigma(a)) = \sigma\big(\mathrm{N}_{E_2/E_1}(a)\big).$$

(i), (ii) and (iii) analogously hold for Tr_{E_2/E_1}.

Proof. (i) was shown above, (ii) is obvious and (iii) follows from the definition and the fact that for each $\sigma \in \mathrm{Gal}_{L/F}(E_1)$ the set $R'' := \{\sigma\tau\sigma^{-1} \mid \tau \in R\}$ is a complete irreducible set of representatives of $\sigma\mathrm{Gal}_{L/F}(E_2)\sigma^{-1} = \mathrm{Gal}_{L/F}(\sigma(E_2))$ in $\sigma\mathrm{Gal}_{L/F}(E_1)\sigma^{-1} = \mathrm{Gal}_{L/F}(\sigma(E_1))$. □

For the rest of this chapter we now suppose that we have a surjective **G-homomorphism**

$$\wp : A \longrightarrow A$$

with finite cyclic kernel $\mu_\wp \subseteq A_F$. Here G-homomorphism means

$$\sigma(\wp(a)) = \wp(\sigma(a)) \text{ for all } \sigma \in G \text{ and } a \in A. \tag{2.1.h}$$

Moreover we make the following

2.1.5 Axiomatic Assumption. *Let* E/F *be a finite cyclic extension of* F *with* $E \subseteq L$ *and* σ *a generator of* $\mathrm{Gal}(E/F)$. *Let* $a \in A_E$. *Then*

$$\mathrm{N}_{E/F}(a) = 1 \iff \exists b \in A_E : \ a = \sigma(b) \cdot b^{-1}.$$

(In the additively written case this becomes

$$\mathrm{Tr}_{E/F}(a) = 0 \iff \exists b \in A_E : \ a = \sigma(b) - b.)$$

2.1.6 Remark. We note that from 2.1.4(iii) follows that "$\Longleftarrow$" in (2.1.5) always holds.

Let now U be a subset of A_F and Δ_U the subgroup of A_F which is generated by the set

$$\{u^i * \wp(A_F) \mid u \in U,\ i \in \mathbb{Z}\},$$

i. e. the set $\{\overline{u} \mid u \in U\}$ generates the group $\Delta_U/\wp(A_F)$ (in particular $\wp(A_F) \subseteq \Delta_U$). Moreover, let $Y \subseteq A$ with $\wp(Y) = U$ and Γ_Y be the subgroup of A which is generated by the set

$$\{y^i * A_F \mid y \in Y,\ i \in \mathbb{Z}\}.$$

(Note that for elements u and y in A_F with $\wp(y) = u$ we write $\Delta_u := \Delta_{\{u\}}$ and $\Gamma_u := \Gamma_{\{y\}}$, respectively.) We now show

$$\wp^{-1}(\Delta_U) = \Gamma_Y. \tag{2.1.i}$$

Obviously $\Gamma_Y \subseteq \wp^{-1}(\Delta_U)$. Take $a \in \wp^{-1}(\Delta_U)$. Then

$$\wp(a) = u_1^{\lambda_1} * \cdots * u_r^{\lambda_r} * \wp(\alpha)$$

for some $u_i \in U$, $\lambda_i \in \mathbb{Z}$ and $\alpha \in A_F$ and

$$\wp\big(y_1^{\lambda_1} * \cdots * y_r^{\lambda_r} * \alpha\big) = \wp(a)$$

for some $y_i \in Y$. Therefore

$$a^{-1} * \big(y_1^{\lambda_1} * \cdots * y_r^{\lambda_r} * \alpha\big) \in \mu_\wp \subseteq A_F,$$

i. e. $a \in \Gamma_Y$ and (2.1.i) is shown.

2.1.7 Proposition. *Let $U \subseteq A_F$. Then*

(i) $F\big(\{Y\}\big) = F\big(Y\big) = F\big(\Gamma_Y\big) = F\big(\wp^{-1}(\Delta_U)\big) = F\big(\wp^{-1}(U)\big)$.

(ii) $F\big(\wp^{-1}(U)\big)/F$ *is Galois.*

Proof. (i) follows directly from (2.1.f), (2.1.i) and the definitions. (ii) follows since $\wp$ is a G-homomorphism, $U \subseteq A_F$ is invariant under G and (2.1.3). □

2.1.8 Definition. Let L/F be a field extension. Then L/F is called

(i) **cyclic**, if L/F is Galois and its Galois group G is cyclic,

(ii) **Abelian**, if L/F is Galois and its Galois group G is Abelian and

(iii) **of exponent** m, if L/F is Galois and the exponent of its Galois group G divides m, i. e. if $\sigma^m = 1$ for all $\sigma \in G$. (Note that m is not unique, i. e. if L/F is of exponent m, then also of exponent l for each $m \mid l$.)

2.1.9 Lemma. *Let $u \in A_F$ and $y \in A$ with $\wp(y) = u$, i. e. $F(y) = F(\wp^{-1}(u)) = F(\wp^{-1}(\Delta_u))$. Then we have an injective group homomorphism*

$$\psi_u : \mathrm{Gal}(F(y)/F) \hookrightarrow \mu_\wp, \quad \sigma \mapsto \sigma(y) * y^{-1}.$$

In particular, $\mathrm{Gal}(F(y)/F)$ *is cyclic of exponent* $|\mu_\wp|$.

Proof. First we note that the definition of ψ_u does not depend on the choice of y, i. e. if $y_1 \in A$ is another element satisfying $\wp(y_1) = u$, then

$$\begin{aligned} \wp(y) = \wp(y_1) &\implies y * y_1^{-1} \in \mu_\wp \subseteq A_F \\ &\implies \sigma(y * y_1^{-1}) = y * y_1^{-1} \\ &\implies \sigma(y) * y^{-1} = \sigma(y_1) * y_1^{-1}. \end{aligned}$$

Moreover,

$$\begin{aligned} \wp(y) = u \in A_F &\implies \wp(\sigma(y)) = \sigma(\wp(y)) = \sigma(u) = u \\ &\implies \wp(\sigma(y)) = \wp(y) \\ &\implies \sigma(y) * y^{-1} \in \mu_\wp \end{aligned}$$

for all $\sigma \in \mathrm{Gal}(F(y)/F)$, hence we have shown that ψ_u is well defined.

ψ_u is injective since from $\sigma(y) * y^{-1} = \tau(y) * y^{-1}$ follows $\sigma(y) = \tau(y)$ and therefore $\sigma = \tau$. □

2.1.10 Lemma. *If E/F (with $E \subseteq L$) is cyclic of exponent $|\mu_\wp|$, then $E = F(y) = F(\wp^{-1}(u))$ with $y \in A_E$ and $\wp(y) = u \in A_F$.*

Proof. Let σ be a generator of $\mathrm{Gal}(E/F)$ and ξ_σ an element of $\mu_\wp$ with

$$|\xi_\sigma| = |\sigma| = [E : F].$$

Then $\mathrm{N}_{E/F}(\xi_\sigma) = \xi_\sigma^{[E:F]} = 1$ and 2.1.5 gives us an element $y \in A_E$ with

$$\xi_\sigma = \sigma(y)y^{-1}. \tag{2.1.j}$$

We claim

$$F(y) = E.$$

$y \in A_E$ implies $F(y) \subseteq E$. (2.1.j) gives $\sigma^i(y) = \xi_\sigma^i y$. Therefore and since ξ_σ has order $[E : F]$ we get

$$\sigma^i(y) = y \text{ iff } i \equiv 0 \mod [E : F],$$

hence $E \subseteq F(y)$. Now

$$\frac{\sigma(\wp(y))}{\wp(y)} = \frac{\wp(\sigma(y))}{\wp(y)} = \frac{\wp(\xi_\sigma y)}{\wp(y)} = \wp(\xi_\sigma) = 1,$$

i. e. $\sigma(\wp(y)) = \wp(y)$ and therefore

$$\wp(y) =: u \in A_F$$

and we are done. □

2.1.11 Theorem.

(i) *Let Δ be a subgroup of A_F with $\wp(A_F) \subseteq \Delta \subseteq A_F$ and $E := F(\wp^{-1}(\Delta)) \subseteq L$. Then E/F is Abelian of exponent $|\mu_\wp|$.*

(ii) *Conversely, if E/F is Abelian of exponent $|\mu_\wp|$, then $E = F(\wp^{-1}(\Delta))$ with $\Delta = \wp(A_E) \cap A_F$. In particular we have $\wp(A_F) \subseteq \Delta \subseteq A_F$.*

Proof. (i): Since

$$E = F(\wp^{-1}(\Delta)) = \coprod_{y \in \wp^{-1}(\Delta)} F(y) = \coprod_{u \in \Delta} F(\wp^{-1}(u))$$

we get from 2.1.9 a monomorphism

$$\mathrm{Gal}(E/F) \xrightarrow{\cong} \coprod_{u \in \Delta} \mathrm{Gal}\big(F(\wp^{-1}(u))/F\big) \xrightarrow{\prod_{u \in \Delta} \psi_u} \mu_\wp^\Delta.$$

Therefore $\mathrm{Gal}(E/F)$ is Abelian of exponent $|\mu_\wp|$.

(ii): We first show $F(\wp^{-1}(\Delta)) \subseteq E$ by showing $\wp^{-1}(\Delta) \subseteq A_E$. Let $b \in \wp^{-1}(\Delta)$, i. e.

$$\begin{aligned} \wp(b) \in \Delta = \wp(A_E) \cap A_F &\implies \exists a \in A_E \text{ with } \wp(b) = \wp(a) \in A_F \\ &\implies b = a\xi, \ \ \xi \in \mu_\wp \subseteq A_F \\ &\implies b \in A_E. \end{aligned}$$

We now want to show $E \subseteq F(\wp^{-1}(\Delta))$. Since E/F is Abelian of exponent $|\mu_\wp|$, we have an injection $\mathrm{Gal}(E/F) \overset{\iota}{\hookrightarrow} \prod_{i\in I} \mu_\wp$. For each i we consider the homomorphism

$$\iota_i : \mathrm{Gal}(E/F) \overset{\iota}{\hookrightarrow} \prod_i \mu_\wp \overset{\pi_i}{\twoheadrightarrow} \mu_\wp$$

(here π_i is the i-th projection), define $H_i := \ker(\iota_i)$ and set $E_i := \mathrm{Fix}_{L/F}(H_i)$. Since $\bigcap_i H_i = \{\mathrm{id}\}$ we know

$$\mathrm{Fix}_{L/F}\Big(\bigcap_i H_i\Big) = E.$$

Now, for each $\sigma \in G$

$$\sigma \in \mathrm{Gal}_{L/F}\Big(\coprod_i E_i\Big) \iff \sigma \in \mathrm{Gal}_{L/F}(E_i) \text{ for all } i$$

and therefore

$$\mathrm{Gal}_{L/F}\Big(\coprod_i E_i\Big) = \bigcap_i \mathrm{Gal}_{L/F}\big(\mathrm{Fix}_{L/F}(H_i)\big) = \bigcap_i H_i.$$

This yields

$$\coprod_i E_i = \mathrm{Fix}_{L/F}\Big(\mathrm{Gal}_{L/F}\Big(\coprod_i E_i\Big)\Big) = \mathrm{Fix}_{L/F}\Big(\bigcap_i H_i\Big) = E.$$

Each of the extensions E_i/F is Galois and, since

$$\mathrm{Gal}(E_i/F) \cong {\mathrm{Gal}(E/F)}\Big/{\mathrm{Gal}(E/E_i)} = {\mathrm{Gal}(E/F)}\Big/{H_i}$$

even cyclic of exponent $|\mu_\wp|$. From 2.1.10 we get

$$E_i = F(y_i) = F(\wp^{-1}(u_i))$$

for some $y_i \in A_{E_i}$ with

$$\wp(y_i) =: u_i \in \wp(A_{E_i}) \cap A_F \subseteq \wp(A_E) \cap A_F = \Delta,$$

i. e. $y_i \in \wp^{-1}(\Delta)$. Therefore

$$E = \coprod_i E_i = \coprod_i F(y_i) \subseteq F(\wp^{-1}(\Delta)).$$

The last statement $\wp(A_F) \subseteq \Delta \subseteq A_F$ of (ii) follows from the definition of Δ and the fact that $\sigma(\wp(x)) = \wp(\sigma(x)) = \wp(x)$ for all $x \in A_F$ and $\sigma \in G$. □

2.2 Pairings between Groups

2.2.1 Lemma. *Let H be a cyclic group of exponent n, i. e. $H \cong \mathbb{Z}/q\mathbb{Z}$ for some q with $q|n$. Then*

$$H \cong \mathrm{Hom}(H, \mathbb{Z}/n\mathbb{Z}).$$

Proof. Let a be a generator of H and $f \in \mathrm{Hom}(H, \mathbb{Z}/n\mathbb{Z})$. Then

$$\mathrm{ord}\, f(a) \big| \,\mathrm{ord}(a) = q$$

and we are done since the number of elements b of $\mathbb{Z}/n\mathbb{Z}$ with $qb = 0$ equals q. □

2.2.2 Lemma. *Let U be a finite Abelian group of exponent n. Then*

$$U \cong \mathrm{Hom}(U, \mathbb{Z}/n\mathbb{Z}).$$

Proof. Follows from

$$U \cong \bigoplus_{i=1}^{r} \mathbb{Z}/q_i\mathbb{Z} \text{ with } q_i|n,$$

$$\mathrm{Hom}\Big(\bigoplus_{i=1}^{r} \mathbb{Z}/q_i\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}\Big) \cong \prod_{i=1}^{r} \mathrm{Hom}\big(\mathbb{Z}/q_i\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}\big)$$

and 2.2.1. □

Let C, D be Abelian groups of exponent n. A **pairing** of C and D in the additive group $\mathbb{Z}/n\mathbb{Z}$ is a map

$$\Psi := \langle\ ,\ \rangle : C \times D \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

which is homomorphic in both arguments. Each one of given homomorphisms $C \longrightarrow \mathrm{Hom}(D, \mathbb{Z}/n\mathbb{Z})$ and $D \longrightarrow \mathrm{Hom}(C, \mathbb{Z}/n\mathbb{Z})$ defines a pairing. On the other hand each pairing defines the homomorphisms

$$\iota_{\Psi,1} : C \longrightarrow \mathrm{Hom}(D, \mathbb{Z}/n\mathbb{Z}), \quad c \mapsto \langle c,\ \rangle \tag{2.2.a}$$

and

$$\iota_{\Psi,2} : D \longrightarrow \mathrm{Hom}(C, \mathbb{Z}/n\mathbb{Z}), \quad c \mapsto \langle\ , d\rangle. \tag{2.2.b}$$

A pairing is called **non-degenerate**, if $\iota_{\Psi,1}$ and $\iota_{\Psi,2}$ are injective. We denote by $\mathcal{C}$ and $\mathcal{D}$ the set of subgroups of C and D, respectively, and define the following maps

$$\phi_{\Psi,1} : \mathcal{C} \longrightarrow \mathcal{D}, \quad U \longmapsto V := \big\{ d \in D \mid \langle U, d\rangle = \{0\} \big\} \tag{2.2.c}$$

and

$$\phi_{\Psi,2} : \mathcal{D} \longrightarrow \mathcal{C}, \quad V \longmapsto U := \big\{ c \in C \mid \langle c, V\rangle = \{0\} \big\}. \tag{2.2.d}$$

2.2.3 Remark. Let U be a subgroup of C. Then of course the homomorphism

$$\iota_{\Psi,1}\big|_U : U \longrightarrow \mathrm{Hom}(D, \mathbb{Z}/n\mathbb{Z})$$

is also injective. Let $h := \iota_{\Psi,1}\big|_U(u)$ for some $u \in U$ be in the image of $\iota_{\Psi,1}\big|_U$. From the definition of $\phi_{\Psi,1}$ it then follows

$$\phi_{\Psi,1}(U) \subseteq \ker h.$$

□

2.2.4 Lemma. *Let C, D be Abelian groups of exponent n and $\Psi := \langle\ ,\ \rangle$ be a non-degenerate pairing. Let U be a subgroup of C. Then*

(i) *U is infinite iff $D/\phi_{\Psi,1}(U)$ is infinite.*

(ii) *If U is finite, then $|U| = \big|D/\phi_{\Psi,1}(U)\big|$.*

(iii) *If U is finite, then*

$$U \cong \mathrm{Hom}(D/\phi_{\Psi,1}(U), \mathbb{Z}/n\mathbb{Z}) \cong D/\phi_{\Psi,1}(U)$$

and

$$D/\phi_{\Psi,1}(U) \cong \mathrm{Hom}(U, \mathbb{Z}/n\mathbb{Z}) \cong U.$$

(The same assertions of course hold for subgroups V of D and $C/\phi_{\Psi,2}(V)$.)

Proof. For each subgroup U of C the pairing Ψ induces a pairing

$$\Psi_U : U \times D/\phi_{\Psi,1}(U) \longrightarrow \mathbb{Z}/n\mathbb{Z}.$$

That Ψ_U is well defined follows from the above definitions and 2.2.3.

Ψ_U is non-degenerate: $\iota_{\Psi_U,1} : U \longrightarrow \mathrm{Hom}(D/\phi_{\Psi,1}(U), \mathbb{Z}/n\mathbb{Z})$ is injective because $\iota_{\Psi,1}$ is, and $\iota_{\Psi_U,2} : D/\phi_{\Psi,1}(U) \longrightarrow \mathrm{Hom}(U, \mathbb{Z}/n\mathbb{Z})$ is injective since the homomorphism

$$D \longrightarrow \mathrm{Hom}(U, \mathbb{Z}/n\mathbb{Z}), \quad d \mapsto \langle\ , d\rangle\big|_U$$

has kernel $\phi_{\Psi,1}(U)$. This shows (i). If U is finite, then we also get that

$$|U| \quad \text{divides} \quad \big|\mathrm{Hom}(D/\phi_{\Psi,1}(U), \mathbb{Z}/n\mathbb{Z})\big| \underset{2.2.2}{=} \big|D/\phi_{\Psi,1}(U)\big|$$

and

$$\big|D/\phi_{\Psi,1}(U)\big| \quad \text{divides} \quad \big|\mathrm{Hom}(U, \mathbb{Z}/n\mathbb{Z})\big| \underset{2.2.2}{=} \big|U\big|,$$

i. e.

$$|U| = \big|D/\phi_{\Psi,1}(U)\big|.$$

This means that for finite U the homomorphisms $\iota_{\Psi_U,1}$ and $\iota_{\Psi_U,2}$ are bijections and (ii) and (iii) are shown. (The second equality in each equation of (iii) follows from 2.2.2.) □

2.2.5 Lemma. *Suppose C, D are Abelian groups of exponent n and $\Psi := \langle\ ,\ \rangle$ is a non-degenerate pairing of C and D. For an element $d \in D$ we denote by $\langle d\rangle$ the subgroup of D generated by d. Assume that for each subgroup V of D and each $d \in D$ with $\phi_{\Psi,2}(V) = \phi_{\Psi,2}(V + \langle d\rangle)$ there exists a finite subgroup $V_0 \subseteq V$ with $\phi_{\Psi,2}(V_0) = \phi_{\Psi,2}(V_0 + \langle d\rangle)$. Then $\phi_{\Psi,1} \circ \phi_{\Psi,2}$ is the identity.*

Proof. From the definitions of the maps $\phi_{\Psi,1}$ and $\phi_{\Psi,2}$ we easily see $\phi_{\Psi,2} \circ \phi_{\Psi,1} \circ \phi_{\Psi,2} = \phi_{\Psi,2}$. If we can show that $\phi_{\Psi,2}$ is injective, then the result follows.

Let V and V' be subgroups of D with $\phi_{\Psi,2}(V) = \phi_{\Psi,2}(V')$. Then also $\phi_{\Psi,2}(V + V') = \phi_{\Psi,2}(V)$. We now want to show that this last equation implies

$$V + V' \subseteq V. \tag{2.2.e}$$

In the same way also $V + V' \subseteq V'$ holds, i. e. $V = V'$, and the injectivity of $\phi_{\Psi,2}$ follows. To verify (2.2.e) we take $d \in D$ with $\phi_{\Psi,2}(V) = \phi_{\Psi,2}(V + \langle d\rangle)$ and show $d \in V$. Our assumption gives us a finite subgroup V_0 of D with $\phi_{\Psi,2}(V_0) = \phi_{\Psi,2}(V_0 + \langle d\rangle)$. From 2.2.4(ii) applied to subgroups of D we get

$$|V_0| = \big|C/\phi_{\Psi,2}(V_0)\big| = \big|C/\phi_{\Psi,2}(V_0 + \langle d\rangle)\big| = \big|V_0 + \langle d\rangle\big|$$

(note that from 2.2.4(i) we know that $\big|C/\phi_{\Psi,2}(V_0 + \langle d\rangle)\big|$ is finite iff $\big|V_0 + \langle d\rangle\big|$ is finite), i. e. $d \in V_0 \subseteq V$. □

2.3 The Kummer Pairing

Now we are ready to prove the main theorem of this chapter. We keep the notations and definitions of Section 2.1. In particular, we have a G-module $A \subseteq L^m$ and a surjective G-homomorphism $\wp : A \to A$ with finite cyclic kernel $\mu_\wp$.

2.3.1 Theorem (Kummer Pairing). *Let $\mathfrak{D}$ the be the set of subgroups Δ of A with $\wp(A_F) \subseteq \Delta \subseteq A_F$ and $\mathfrak{E}$ be the set of Abelian extensions E of F of exponent $|\mu_\wp|$ (with $E \subseteq L$).*

(a) *The maps*

$$\Theta : \mathfrak{D} \longrightarrow \mathfrak{E}, \quad \Delta \longmapsto E := F(\wp^{-1}(\Delta))$$

and

$$\Xi : \mathfrak{E} \longrightarrow \mathfrak{D}, \quad E \longmapsto \Delta_E := \wp(A_E) \cap A_F$$

are mutually inverse and are preserving inclusions.

Take an arbitrary $\Delta \in \mathfrak{D}$ and set $E := F(\wp^{-1}(\Delta)) = \Theta(\Delta)$.

(b) (i) *There is a non-degenerate pairing*

$$\begin{aligned} \Psi_{\Delta,E} : \mathrm{Gal}(E/F) \times \Delta/\wp(A_F) &\longrightarrow \quad \mu_\wp \\ (\sigma, \delta * \wp(A_F)) &\longmapsto \sigma(y) * y^{-1}, \end{aligned}$$

where $y \in \wp^{-1}(\delta)$.

(ii) $\mathrm{Gal}(E/F)$ *is finite iff $\Delta/\wp(A_F)$ is finite.*

(iii) *If* $\mathrm{Gal}(E/F)$ *is finite this pairing induces isomorphisms*

$$\mathrm{Gal}(E/F) \cong \mathrm{Hom}(\Delta/\wp(A_F), \mu_\wp) \cong \Delta/\wp(A_F)$$

and

$$\Delta/\wp(A_F) \cong \mathrm{Hom}(\mathrm{Gal}(E/F), \mu_\wp) \cong \mathrm{Gal}(E/F).$$

In particular

$$[E : F] = \big|\Delta/\wp(A_F)\big|.$$

Proof. Note that for each $\Delta' \in \mathfrak{D}$ and each subgroup Γ of $\overline{\Delta'} := \Delta'/\wp(A_F)$ there is a unique $\Delta \in \mathfrak{D}$ with $\overline{\Delta} = \Gamma$.

We first show (b).

(i): We choose $\Delta \in \mathfrak{D}$ and set $E := F(\wp^{-1}(\Delta))$.

$\Psi_{\Delta,E}$ *is well defined:* Like in the proof of 2.1.9 we see that the definition of $\Psi_{\Delta,E}$ does not depend on the choice of y, i. e. if $y_1 \in A$ is another element satisfying $\wp(y_1) = \delta$, then

$$\sigma(y) * y^{-1} = \sigma(y_1) * y_1^{-1}$$

since $\mu_\wp \in A_F$. Take $\delta \in \Delta$ and $y \in \wp^{-1}(\delta)$. Then

$$\begin{aligned} \wp(y) = \delta \in A_F &\Longrightarrow \wp(\sigma(y)) = \sigma(\wp(y)) = \sigma(\delta) = \delta \\ &\Longrightarrow \wp(\sigma(y)) = \wp(y) \\ &\Longrightarrow \sigma(y) * y^{-1} \in \mu_\wp, \end{aligned}$$

i. e. the image of $\Psi_{\Delta,E}$ is contained in $\mu_\wp$. Suppose now $\delta \in \wp(A_F)$. Then for all $\sigma \in \mathrm{Gal}(E/F)$

$$\begin{aligned} \sigma(y) * y^{-1} = 1 &\implies \sigma(y) = y \\ &\implies y \in A_F \\ &\implies \wp(y) = \delta \in \wp(A_F), \end{aligned}$$

i. e. $\Psi_{\Delta,E}$ is well defined in the second argument. That it is homomorphic in both arguments follows from the definition of $\wp$. Hence we have shown that $\Psi_{\Delta,E}$ is a well defined pairing.

$\Psi_{\Delta,E}$ *is non degenerate:* Suppose for some $\sigma \in \mathrm{Gal}(E/F)$ we have $\iota_{\Psi_{\Delta,E},1}(\sigma) = 1$, i. e. $\sigma(y) * y^{-1} = 1$, hence $\sigma(y) = y$ for all $y \in \wp^{-1}(\Delta)$. Then $\sigma = \mathrm{id}_E$ and $\iota_{\Psi_{\Delta,E},1}$ is injective. For the second argument, suppose $\iota_{\Psi_{\Delta,E},2}(\overline{\delta}) = 1$ for some $\overline{\delta} \in \overline{\Delta}$, i. e. $\sigma(y) = y$ for some $y \in \wp^{-1}(\delta)$ and all $\sigma \in \mathrm{Gal}(E/F)$. Then $y \in A_F$ and $\delta \in \wp(A_F)$, hence $\iota_{\Psi_{\Delta,E},2}$ is injective.

(ii) and (iii) follow from (i) and 2.2.4, since

$$\begin{aligned} \phi_{\Psi_{\Delta,E},1}\big(\mathrm{Gal}(E/F)\big) &= \big\{\overline{\delta} \in \overline{\Delta} \;\big|\; \Psi_{\Delta,E}(\mathrm{Gal}(E/F), \overline{\delta}) = \{1\}\big\} \\ &= \big\{\overline{\delta} \in \overline{\Delta} \;\big|\; \sigma(y) = y \;\forall\, \sigma \in \mathrm{Gal}(E/F),\ y \in \wp^{-1}(\delta)\big\} \\ &= \overline{\wp(A^{\mathrm{Gal}(E/F)}) \cap \Delta} \\ &= \overline{\wp(A_F) \cap \Delta} \\ &= \overline{\wp(A_F)} = 0, \end{aligned}$$

i. e.

$$\overline{\Delta}\Big/\phi_{\Psi_{\Delta,E},1}\big(\mathrm{Gal}(E/F)\big) = \overline{\Delta}.$$

We now proceed to prove (a).

From 2.1.11 we know that Θ and Ξ are well defined. It remains to show that they are mutually inverse, i. e.

$$(\Xi \circ \Theta)(\Delta) = \Delta_{F(\wp^{-1}(\Delta))} = \Delta \tag{2.3.a}$$

and

$$(\Theta \circ \Xi)(E) = F(\wp^{-1}(\Delta_E)) = E. \tag{2.3.b}$$

Let $K := F(\wp^{-1}(A_F))$. The associated pairing $\Psi := \Psi_{A_F,K}$ then induces the homomorphisms

$$\begin{aligned}\phi_{\Psi,1}\Big(H \longmapsto \overline{\Delta} :&= \big\{\overline{\delta} \in \overline{A_F} \;\big|\; \Psi(H,\overline{\delta}) = \{1\}\big\} \\ &= \big\{\overline{\delta} \in \overline{A_F} \;\big|\; \sigma(y) = y \;\forall\, \sigma \in H,\ y \in \wp^{-1}(\delta)\big\} \\ &= \overline{\wp(A^H) \cap A_F}\ \Big)\end{aligned}$$

and

$$\begin{aligned}\phi_{\Psi,2}\Big(\overline{\Delta} \longmapsto H :&= \big\{\sigma \in \mathrm{Gal}(K/F) \;\big|\; \Psi(\sigma,\overline{\Delta}) = \{1\}\big\} \\ &= \big\{\sigma \in \mathrm{Gal}(K/F) \;\big|\; \sigma(y) = y \;\forall y \in \wp^{-1}(\Delta)\big\} \\ &= G_{\wp^{-1}(\Delta)}\ \Big)\end{aligned}$$

between subgroups of $\mathrm{Gal}(K/F)$ and subgroups of $\overline{A_F}$.

Now we show that the assumptions of 2.2.5 are fulfilled in our situation. Let $\overline{\Delta}$ be a subgroup of A_F and $a \in A_F$ with $\phi_{\Psi,2}(\overline{\Delta}) = \phi_{\Psi,2}(\overline{\Delta} + \overline{\Delta_a})$, hence

$$G_{\wp^{-1}(\Delta)} = \phi_{\Psi,2}(\overline{\Delta}) = \phi_{\Psi,2}(\overline{\Delta} + \overline{\Delta_a}) = G_{\wp^{-1}(\Delta+\Delta_a)}$$

and

$$\begin{aligned}F\big(\wp^{-1}(\Delta)\big) = \mathrm{Fix}_{L/F}\big(G_{\wp^{-1}(\Delta)}\big) &= \mathrm{Fix}_{L/F}\big(G_{\wp^{-1}(\Delta+\Delta_a)}\big) \\ &= F\big(\wp^{-1}(\Delta + \Delta_a)\big) \\ &= F\big(\wp^{-1}(\Delta) + \wp^{-1}(\Delta_a)\big) \\ &= F\big(\wp^{-1}(\Delta), \wp^{-1}(\Delta_a)\big) \\ &= F\big(\wp^{-1}(\Delta), y\big)\end{aligned}$$

for some $y \in \wp^{-1}(a)$. Then $y \in F\big(\wp^{-1}(\Delta)\big)$. Therefore there exist $y_1, \ldots, y_r \in \wp^{-1}(\Delta)$ with $y \in F(y_1, \ldots, y_r)$ and for $B := \{\wp(y_1), \ldots, \wp(y_r)\}$ we have

$\Delta_B \subseteq \Delta$, $\overline{\Delta_B}$ is finite and $y \in F\big(\wp^{-1}(\Delta_B)\big)$. Hence

$$\begin{aligned}\mathrm{Fix}_{L/F}\big(G_{\wp^{-1}(\Delta_B)}\big) = F\big(\wp^{-1}(\Delta_B)\big) &= F\big(\wp^{-1}(\Delta_B), y\big)\\ &= F\big(\wp^{-1}(\Delta_B), \wp^{-1}(\Delta_a)\big)\\ &= \mathrm{Fix}_{L/F}\big(G_{\wp^{-1}(\Delta_B+\Delta_a)}\big)\end{aligned}$$

and therefore

$$\phi_{\Psi,2}(\overline{\Delta_B}) = G_{\wp^{-1}(\Delta_B)} = G_{\wp^{-1}(\Delta_B+\Delta_a)} = \phi_{\Psi,2}(\overline{\Delta_B} + \overline{\Delta_a}).$$

Hence we can use 2.2.5 and see that $\phi_{\Psi,1} \circ \phi_{\Psi,2}$ is the identity.

Now for each $\Delta \in \mathfrak{D}$ we have

$$\begin{aligned}\overline{\Delta} = \phi_{\Psi,1} \circ \phi_{\Psi,2}(\overline{\Delta}) &= \phi_{\Psi,1}(G_{\wp^{-1}(\Delta)})\\ &= \overline{\wp\big(A^{G_{\wp^{-1}(\Delta)}}\big) \cap A_F}\\ &= \overline{\wp\big(A^{\mathrm{Gal}(L/F(\wp^{-1}(\Delta)))}\big) \cap A_F}\\ &= \overline{\wp\big(A_{F(\wp^{-1}(\Delta))}\big) \cap A_F}\\ &= \overline{\Delta_{F(\wp^{-1}(\Delta))}}\end{aligned}$$

hence

$$\Delta = \Delta_{F(\wp^{-1}(\Delta))},$$

which shows (2.3.a).

For each $\Delta \in \mathfrak{D}$ its image

$$\phi_{\Psi,2}(\overline{\Delta}) = G_{\wp^{-1}(\Delta)}$$

is closed (under the Krull topology) in $\mathrm{Gal}(K/F)$ (see 2.1.2) and therefore also

$$\phi_{\Psi,1} \circ \mathrm{Gal}_{L/F} \circ \mathrm{Fix}_{L/F} \circ \phi_{\Psi,2} = \mathrm{id},$$

i. e. $\phi_{\Psi,1} \circ \mathrm{Gal}_{L/F}$ is surjective and $\mathrm{Fix}_{L/F} \circ \phi_{\Psi,2}$ is injective. From 2.1.11(ii) follows that $\mathrm{Fix}_{L/F} \circ \phi_{\Psi,2}$ is surjective, hence $\phi_{\Psi,1} \circ \mathrm{Gal}_{L/F}$ is an isomorphism and so

$$\mathrm{Fix}_{L/F} \circ \phi_{\Psi,2} \circ \phi_{\Psi,1} \circ \mathrm{Gal}_{L/F} = \mathrm{id}\,.$$

Now for each $E \in \mathfrak{E}$

$$\begin{aligned}\mathrm{Fix}_{L/F} \circ \phi_{\Psi,2} \circ \phi_{\Psi,1} \circ \mathrm{Gal}_{L/F}(E) &= \mathrm{Fix}_{L/F} \circ \phi_{\Psi,2} \circ \phi_{\Psi,1}(\mathrm{Gal}(L/E))\\ &= \mathrm{Fix}_{L/F} \circ \phi_{\Psi,2}(\overline{\Delta_E})\\ &= \mathrm{Fix}_{L/F}(G_{\wp^{-1}(\Delta_E)})\\ &= F(\wp^{-1}(\Delta_E))\end{aligned}$$

which shows (2.3.b) and finishes the proof of the theorem. □

The following important result is a direct consequence of 2.1.9, 2.1.10 and 2.3.1(b)(iii).

2.3.2 Corollary.

(i) *Set* $n := |\mu_\wp|$ *and let* $u \in A_F$ *and* $y \in A$ *with* $\wp(y) = u$ *and* $u^d \notin \wp(A_F)$ *for all* $d \mid n$, $d < n$, *i. e.* $\overline{\Delta_u}$ *is cyclic of degree* n. *If* $E := F(y) = F(\wp^{-1}(u)) = F(\wp^{-1}(\Delta_u))$, *then* E/F *is cyclic of order* n. *In particular, the map*

$$\psi_u : \mathrm{Gal}(F(y)/F) \hookrightarrow \mu_\wp, \quad \sigma \mapsto \sigma(y) * y^{-1}$$

is an isomorphism.

(ii) *Conversely, if* E/F *is cyclic of degree* $n = |\mu_\wp|$, *then* $E = F(\wp^{-1}(\Delta_u)) = F(\wp^{-1}(u)) = F(y)$ *with* $\wp(y) = u \in A_F$ *and* $u^d \notin \wp(A_F)$ *for all* $d \mid n$, $d < n$.

Chapter 3

Abelian Extensions

We now apply the results of the last chapter to some important cases of Abelian and especially cyclic extensions.

> *For the whole chapter let F be a field of characteristic p and $\bar{F}$ the separable closure of F in some algebraic closure of F. Then $\bar{F}$ is the maximal Galois extension of F. We set $G := \mathrm{Gal}\big(\bar{F}/F\big)$.*

Section 3.1 characterizes all Abelian extensions of F of exponent n, assuming that F contains a primitive n-th root of unity and, if $p \neq 0$, that n is coprime to p. In Section 3.2 we describe all Abelian extensions of exponent p^r of F for the case $p \neq 0$.

3.1 Kummer Extensions

We begin this section by stating an important field theoretic result (see for instance [Jan73, p. 213]).

3.1.1 Proposition. *Let E/F be a finite cyclic Galois extension of order n. Then there exists a normal basis for E/F, i. e. an element c of E such that $\{\sigma(c) \mid \sigma \in \mathrm{Gal}(E/F)\}$ is a basis of E/F. c is called a* **normal basis element** *for E/F. In particular, if E/F is cyclic and σ a generator of $\mathrm{Gal}(E/F)$, then $c, \ldots, \sigma^{n-1}c$ is a basis of E over F.*

Suppose F contains the set μ_n of all $n-$th roots of unity, where the characteristic of F is zero or coprime to n. Then the map (where $A := \bar{F}^*$)

$$\wp : A \longrightarrow A, \quad a \longmapsto a^n$$

is a surjective G-homomorphism with cyclic kernel $\mu_\wp = \mu_n \subseteq A_F = F^*$ of order n.

Before we can apply the results of general Kummer theory to the G-module A and the G-homomorphism $\wp$ we first need to show that 2.1.5 holds in this case.

3.1.2 Theorem (Hilbert 90). *Let E/F be a finite cyclic extension with $E \subseteq \bar{F}$ and σ a generator of* $\mathrm{Gal}(E/F)$. *Let $a \in A_E = E^*$. Then*

$$\mathrm{N}_{E/F}(a) = 1 \iff \exists b \in A_E = E^* : \ a = \sigma(b) \cdot b^{-1}.$$

Proof. Because of 2.1.6 we only need to show "$\Longrightarrow$". Let $\gamma \in E$ be a normal basis element for E/F and set

$$b := \gamma + a\sigma(\gamma) + \big(a\sigma(a)\big)\sigma^2(\gamma) + \cdots + \big(a\sigma(a)\cdots\sigma^{n-2}(a)\big)\sigma^{n-1}(\gamma) \neq 0.$$

Applying σ and multiplying with a gives

$$a\sigma(b) = a\sigma(\gamma) + \big(a\sigma(a)\big)\sigma^2(\gamma) + \big(a\sigma(a)\sigma^2(a)\big)\sigma^3(\gamma) + \cdots + \underbrace{\big(a\sigma(a)\cdots\sigma^{n-1}(a)\big)}_{=1}\underbrace{\sigma^n(\gamma)}_{=\gamma} = b.$$

□

Now we can use 2.3.1 and see that there is a one-one correspondence between the so called **Kummer extensions** of F, i. e. the Abelian extensions $E \subseteq \bar{F}^*$ of F of exponent $n = |\mu_\wp|$, and the subgroups Δ of $\bar{F}^*$ with $\wp(F^*) \subseteq \Delta \subseteq F^*$. These extensions are of the form $E = F(\wp^{-1}(\Delta))$, i. e. are obtained by adjoining all n-th roots of elements of Δ to F. We finish this section with two statements about the cyclic case.

3.1.3 Proposition. *Let F be a field which contains the set μ_n of all $n-$th roots of unity, where the characteristic of F is zero or coprime to n. Then the following statements are equivalent:*

(i) *E/F is a cyclic Kummer extension of degree n.*

(ii) *$E = F(y)$, where $y^n = u \in F^*$ and $u^l \neq x^n$ for all $x \in F$, $l \mid n$ and $l < n$.*

(iii) $E = F(y)$ *where* $y^n = u \in F^*$ *and* $u \neq w^d$ *for all* $w \in F$, $d \mid n$ *and* $d > 1$.

Proof. 2.3.2. □

Each element $y \in E$ satisfying one of the equivalent conditions 3.1.3(ii) or (iii) is called a **Kummer generator** of E/F.

The following proposition helps us to determine the ramification behaviour of places in Kummer extensions of function fields.

3.1.4 Proposition. *Let F/k be a function field and E/F be a cyclic Kummer extension of degree n with generator $y \in E$ and $y^n =: u \in F^*$. If P is a place of F and P' an extension of P in E, then*

$$e(P'|P) = \frac{n}{r_{P,E}},$$

where

$$r_{P,E} := \gcd\big(n, v_P(u)\big) > 0.$$

Proof. [Has34]. □

3.2 Artin-Schreier-Witt Extensions

We now study Abelian extensions of degree p^n for a prime p, where p is the characteristic of the ground field.

Artin-Schreier Extensions

We begin with the special case of cyclic p extensions. These extensions have been completely investigated by Artin and Schreier in [AS27]. We first state their characterization here without providing proofs, since we deal with the more general situation in the next subsection.

Let $\wp : \bar{F} \longrightarrow \bar{F}$ be defined by $\wp(x) := x^p - x$. Then the following assertions for a field extension E/F with $E \subseteq \bar{F}$ are equivalent:

(1) E/F is cyclic of degree p.

(2) $E = F(y)$, $\wp(y) = y^p - y = u \in F$ and $u \neq \alpha^p - \alpha$ for all $\alpha \in F$.

An extension, for which (1) or (2) holds, is called an **Artin-Schreier extension**. The elements of $\mathrm{Gal}(E/F)$ are given by $\sigma(y) = y + \nu$, $\nu \in \mathbb{F}_p$. Each $y' \in E$ with $E = F(y')$ and $\wp(y') = y'^p - y' \in F$ is called an **Artin-Schreier generator** of E/F. An element $y' \in E$ is an Artin-Schreier generator iff there exist $\mu \in \mathbb{F}_p \subset F$ and $\zeta \in F$ such that $y' = \mu y + \zeta$ and $y'^p - y' = u' = \mu u + (\zeta^p - \zeta)$, i. e. iff $y' \in \wp^{-1}(u')$ with $u' \in F$ and $u' - \mu u \in \wp(F)$ for some $\mu \in \mathbb{F}_p$. The minimal polynomial of y' over F is $T^p - T - u' \in F[T]$.

3.2.1 Proposition. *Let F/k be a function field of characteristic $p > 0$, k perfect and $P \in \mathbb{P}_F$ a place of F.*

(i) *For each $u \in F$ we can define a unique*

$$\lambda_P(u) := \begin{cases} \lambda & \text{if there exists an element } \zeta := \zeta(P,u) \in F \text{ with} \\ & v_P\big(u + (\zeta^p - \zeta)\big) = -\lambda < 0,\ \lambda \not\equiv 0 \bmod p \\ 0 & \text{if there exists an element } \zeta := \zeta(P,u) \in F \text{ with} \\ & v_P\big(u + (\zeta^p - \zeta)\big) \geq 0. \end{cases}$$

(Note that if there are ζ_1 and ζ_2 in F with $\lambda_1 := v_P\big(u + (\zeta_1^p - \zeta_1)\big)$ and $\lambda_2 := v_P\big(u + (\zeta_2^p - \zeta_2)\big)$ are negative and $\not\equiv 0 \bmod p$, then $\lambda_1 = \lambda_2$.)

(ii) *If E/F is an Artin-Schreier extension and $y \in E$ an Artin-Schreier generator of E/F with $\wp(y) = u \in F$, then*

- *P is unramified in E iff $\lambda_P(u) = 0$ and*
- *P is totally ramified in E iff $\lambda_P(u) > 0$.*

Moreover, from (i) *follows that, if y' is another Artin-Schreier generator of E/F with $\wp(y') = u' \in F$, then*

$$\lambda_P(u) = \lambda_P(u').$$

Proof. [Sti93, III.7.7 and III.7.8]. □

For later applications it will be important to actually compute $\lambda_P(u)$ from 3.2.1(i). We describe the procedure for doing this in the following algorithm. We keep the notations of Proposition 3.2.1.

3.2.2 Algorithm. *Reduction*

Input: $P \in \mathbb{P}_F$, $u \in F$, $\operatorname{char} F = p > 0$.

Output: $\zeta := \zeta(P,u) \in F$ and $\lambda = \lambda_P(u) \in \mathbb{Z}$ (see 3.2.1(i)) with either
$v_P(u + (\zeta^p - \zeta)) \geq 0$ (in this case $\lambda := 0$)
or
$v_P(u + (\zeta^p - \zeta)) = -\lambda < 0,\ \lambda \not\equiv 0 \bmod p$.

1. $\zeta \leftarrow 0$, $\lambda \leftarrow v_P(u)$, $x \leftarrow u$
2. **while** $\lambda < 0$ **and** $\lambda \equiv 0 \bmod p$ **do**
3. $\quad l \leftarrow \lambda/p$
4. $\quad$ Choose $t \in F$ with $v_P(t) = l$.
5. $\quad$ Choose $\alpha \in \mathcal{O}_P^*$ with
$$\frac{x}{t^p} + P = \big(\alpha + P\big)^p = \alpha^p + P \tag{3.2.a}$$
$\quad$ (In the comments below we show how to find α.)
6. $\quad \zeta \leftarrow \zeta - \alpha t$
7. $\quad x \leftarrow u + (\zeta^p - \zeta)$
8. $\quad \lambda \leftarrow v_P(x)$
9. **end while**
10. **if** $\lambda < 0$ **then**
11. $\quad \lambda := -\lambda$
12. **else**
13. $\quad \lambda := 0$
14. **end if**
15. **return** ζ, λ

We finish this subsection by showing the correctness of this algorithm: First we note that $x = u + (\zeta^p - \zeta)$ and t^p are non zero. Since

$$v_P(t^p) = pv_P(t) = pl = \lambda = v_P(x),$$

we have $v_P\big(\frac{x}{t^p}\big) = 0$, hence $0 \neq \frac{x}{t^p} + P \in \mathcal{O}_P/P$. Then there exists an $\alpha \in \mathcal{O}_P$ satisfying (3.2.a), since $\mathcal{O}_P/P$ is perfect. Moreover, $\alpha \in \mathcal{O}_P^*$ since $v_P(\alpha^p) = v_P\big(\frac{x}{t^p}\big) = 0$.

Now (3.2.a) implies $\big(\frac{x}{t^p} - \alpha^p\big) \in P$, i. e. $v_P\big(\frac{x}{t^p} - \alpha^p\big) > 0$. This implies

$$v_P\big(x - (\alpha t)^p\big) > v_P(t^p) = \lambda. \tag{3.2.b}$$

It now remains to show

$$v_P\big(u + \big((\zeta - \alpha t)^p - (\zeta - \alpha t)\big)\big) > v_P(u + (\zeta^p - \zeta)) = v_P(x) = \lambda, \tag{3.2.c}$$

since we then know that λ strictly increases in every step of the while loop, so the algorithm terminates and does what we want. But since

$$\begin{aligned} v_P\big(u + \big((\zeta - \alpha t)^p - (\zeta - \alpha t)\big)\big) &= v_P\big(u + (\zeta^p - \zeta) - ((\alpha t)^p - \alpha t)\big) \\ &= v_P\big(x - ((\alpha t)^p - \alpha t)\big), \end{aligned}$$

(3.2.c) follows from $v_P(\alpha t) = v_P(t) = l > lp = \lambda$ and (3.2.b) (note that during the while loop λ and therefore l are negative).

Artin-Schreier-Witt Extensions

Let now n be a fixed natural number and A be the additive group in the ring of Witt vectors $W_n(\bar{F})$ of length n. A becomes an (additive) G-module by coordinatewise operation, i. e. $\mathrm{id}(a) = a$, $\sigma(a+b) = \sigma(a)+\sigma(b)$ and $\sigma(\tau(a)) = (\sigma\tau)(a)$ $(a, b \in A, \sigma, \tau \in G)$. For each intermediate field $F \subseteq E \subseteq \bar{F}$ we get from (2.1.e)

$$A_E = A \cap E^m = W_n(E).$$

3.2.3 Proposition. *The homomorphism*

$$\wp : W_n(\bar{F}) \longrightarrow W_n(\bar{F}), \quad (x_1, \ldots, x_n) \longmapsto (x_1^p, \ldots, x_n^p) - (x_1, \ldots, x_n)$$

has the following properties:

(i) *$\wp$ is G-linear.*

(ii) *$\wp$ is surjective.*

(iii) *The kernel $\mu_\wp$ of $\wp$ is finite and cyclic of order p^n, more precisely we have*

$$\mu_\wp = W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Proof. (i) is clear.

(ii). Given $(b_1, \dots, b_n) \in W_n(\bar{F})$, we need to show the existence of some $(a_1, \dots, a_n) \in W_n(\bar{F})$ with

$$\wp\big((a_1, \dots, a_n)\big) = (b_1, \dots, b_n). \tag{3.2.d}$$

Since the polynomial $T^p - T - b_1 \in \bar{F}[T]$ is separable, there exists $a_1 \in \bar{F}$ with $a_1^p - a_1 = b_1$.

Suppose we find $d_2, \dots, d_n$ with

$$\begin{aligned} \wp\big((0, d_2, \dots, d_n)\big) &= (b_1, b_2, \dots, b_n) - \wp\big((a_1, 0, \dots, 0)\big) \\ &=: (0, b_2', \dots, b_n'). \end{aligned} \tag{3.2.e}$$

Then

$$\begin{aligned} \wp\big((a_1, d_2, \dots, d_n)\big) &= \wp\big((0, d_2, \dots, d_n)\big) + \wp\big((a_1, 0, \dots, 0)\big) \\ &= (b_1, b_2, \dots, b_n) \end{aligned}$$

and we are done. But

$$\wp\big((0, d_2, \dots, d_n)\big) = (0, b_2', \dots, b_n') \text{ in } W_n(\bar{F})$$

iff

$$\wp\big((d_2, \dots, d_n)\big) = (b_2', \dots, b_n') \text{ in } W_{n-1}(\bar{F}).$$

This shows that we can find the vector $(a_1, \dots, a_n) \in W_n(\bar{F})$ satisfying (3.2.d) inductively.

(iii). The first equality follows from

$$\begin{aligned} \mu_\wp &= \big\{x \in W_n(\bar{F}) \;\big|\; \wp(x) = 0\big\} \\ &= \big\{x \in W_n(\bar{F}) \;\big|\; \mathcal{F}(x) - x\big\} \\ &= \big\{x = (x_1, \dots, x_n) \in W_n(\bar{F}) \;\big|\; (x_1^p, \dots, x_n^p) = (x_1, \dots, x_n)\big\} \\ &= \big\{x = (x_1, \dots, x_n) \in W_n(\bar{F}) \;\big|\; x_i \in \mathbb{F}_p\big\}. \end{aligned}$$

The second is just 1.4.5(ii). □

Now we want to apply the results of general Kummer theory to the G-module A and the surjective G-homomorphism $\wp$. Again we first need to show that 2.1.5 holds in this case.

3.2.4 Theorem. *Let E/F be a finite cyclic extension with $E \subseteq \bar{F}$ and σ a generator of* $\mathrm{Gal}(E/F)$. *Let $a \in A_E = W_n(E)$. Then*

$$\mathrm{Tr}_{E/F}(a) = 0 \iff \exists b \in W_n(E): \quad a = \sigma(b) - b.$$

Proof. Like above, because of 2.1.6 we only need to show "$\Longrightarrow$". Choose an element $c_1 \in E$ with $\mathrm{Tr}_{E/F}(c_1) = t \neq 0$. For $c := (c_1, 0, \ldots, 0) \in W_n(E)$ we then have

$$\mathrm{Tr}_{E/F}(c) = (t, *, \ldots, *) \in (W_n(F))^*$$

(see 1.4.5(i)). Now we set

$$b := \frac{1}{\mathrm{Tr}_{E/F}(c)}\Big[-a\sigma(c) - \Big(a + \sigma(a)\Big)\sigma^2(c) - \cdots - \Big(a + \sigma(a) + \cdots + \sigma^{n-2}(a)\Big)\sigma^{n-1}(c)\Big].$$

Considering that

$$\sigma(b) := \frac{1}{\mathrm{Tr}_{E/F}(c)}\Big[-\sigma(a)\sigma^2(c) - \Big(\sigma(a) + \sigma^2(a)\Big)\sigma^3(c) - \cdots - \underbrace{\Big(\sigma(a) + \sigma^2(a) + \cdots + \sigma^{n-1}(a)\Big)}_{=-a}\underbrace{\sigma^n(c)}_{=c}\Big]$$

we get

$$\sigma(b) - b = \frac{ac + a\sigma(c) + a\sigma^2(c) + \cdots + a\sigma^{n-1}(c)}{\mathrm{Tr}_{E/F}(c)} = a.$$

□

As in Section 3.1, we can apply 2.3.1 now and see that there is a one-one correspondence between the so called **Artin-Schreier-Witt extensions** of F, i. e. the Abelian extensions $E \subseteq \bar{F}$ of F of exponent $p^n = |\mu_\wp|$, and the subgroups Δ of $W_n(\bar{F})$ with $\wp(W_n(F)) \subseteq \Delta \subseteq W_n(F)$.

And again, as we are especially interested in the cyclic case, the rest of this section is devoted to it. We begin with the following

3.2.5 Lemma. *Let Δ be an additive subgroup of $A_F = W_n(F)$ with $\wp(A_F) = \wp(W_n(F)) \subseteq \Delta$. Then the following assertions are equivalent:*

(i) $\Delta/\wp\big(W_n(F)\big) \cong \mathbb{Z}/p^n\mathbb{Z}$

(ii) $\Delta = \Delta_u$ *for some* $u = (u_1, \dots, u_n) \in W_n(F)$ *with* $u_1 \neq \alpha^p - \alpha$ *for all* $\alpha \in F$.

Proof. Of course, if $\Delta/\wp\big(W_n(F)\big) \cong \mathbb{Z}/p^n\mathbb{Z}$, then $\Delta = \Delta_u$ for some $u = (u_1, \dots, u_n) \in W_n(F)$ and $p^i u \notin \wp\big(W_n(F)\big)$ for all $1 \leq i < n$. But, if $u_1 = \alpha^p - \alpha$ for some $\alpha \in F$, then

$$\begin{aligned} p^{n-1}(u_1, \dots, u_n) &\underset{(1.4.\mathrm{i})}{=} (0, \dots, 0, u_1^{p^{n-1}}) \in \wp\big(W_n(F)\big) \\ &= \wp\big((0, \dots, 0, \alpha^{p^{n-1}})\big) \in \wp\big(W_n(F)\big) \end{aligned}$$

since

$$u_1^{p^{n-1}} = (\alpha^p - \alpha)^{p^{n-1}} = \big(\alpha^{p^{n-1}}\big)^p - \alpha^{p^{n-1}}.$$

On the other hand, if $u_1 \neq \alpha^p - \alpha$ for all $\alpha \in F$, then, since F is perfect, also $(u_1)^{p^i} \neq \beta^p - \beta$ for all $\beta \in F$ and all natural numbers i and therefore $p^m u \notin \wp\big(W_n(F)\big)$ for all $0 \leq m < n$. □

3.2.6 Theorem. *The following statements are equivalent:*

(i) E/F *is a cyclic Artin-Schreier-Witt extension of degree* p^n.

(ii) $E = F(y) = F(\wp^{-1}(u)) = F(\wp^{-1}(\Delta_u))$, *where* $\wp(y) = u \in W_n(F)$, $p^i u \notin \wp\big(W_n(F)\big)$ *for all* $1 \leq i < n$, *i. e.* $\overline{\Delta} = \Delta_u/\wp\big(W_n(F)\big)$ *is cyclic of order* p^n.

(iii) $E = F(y) = F(\wp^{-1}(u)) = F(\wp^{-1}(\Delta_u))$, *where* $u = (u_1, \dots, u_n) \in W_n(F)$ *with* $\wp(y) = u$ *and* $u_1 \neq \alpha^p - \alpha$ *for all* $\alpha \in F$.

Proof. 2.3.2 and 3.2.5. □

Let now E/F be a cyclic Artin-Schreier-Witt extension of degree p^n, i. e. we have $u \in W_n(F)$, $u_1 \neq \alpha^p - \alpha$ for all $\alpha \in F$, $y = (y_1, \dots, y_n) \in \wp^{-1}(u)$ and $E = F(y_1, \dots, y_n)$. We set $E_0 := F$, $E_n := E$ and $E_i := F(y_1, \dots, y_i)$ for each $1 \leq i \leq n$. Note that, since E_i/F is cyclic, $F, E_1, \dots, E_{i-1}$ are the only intermediate fields of E_i/F, and therefore

$$E_i = F(y_1, \dots, y_i) = F(y_i).$$

3.2.7 Remark. From 1.4.2 we get the recursions

$$\begin{aligned} u_1 &= y_1^p - y_1, \\ u_2 &= y_2^p - y_2 - z_1, \\ &\vdots \\ u_n &= y_n^p - y_n - z_{n-1}, \end{aligned} \tag{3.2.f}$$

where $z_i \in E_i$ are polynomial expressions with coefficients in the prime field of F given by $z_0 = 0$ and

$$\begin{aligned} z_i &= -\frac{y_i^{p^2} - y_i^p - u_i^p}{p} - \frac{y_{i-1}^{p^3} - y_{i-1}^{p^2} - u_{i-1}^{p^2}}{p^2} - \dots - \frac{y_1^{p^{i+1}} - y_1^{p^i} - u_1^{p^i}}{p^i} \\ &= -\frac{(y_i + u_i + z_{i-1})^p - y_i^p - u_i^p}{p} \\ &\qquad - \frac{(y_{i-1} + u_{i-1} + z_{i-2})^{p^2} - y_{i-1}^{p^2} - u_{i-1}^{p^2}}{p^2} - \dots \\ &\qquad\qquad \dots - \frac{(y_1 + u_1)^{p^i} - y_1^{p^i} - u_1^{p^i}}{p^i}. \end{aligned} \tag{3.2.g}$$

Obviously, each extension E_i/E_{i-1} is an Artin-Schreier extension with generator y_i. □

Choose a generator σ of $\mathrm{Gal}(E/F)$. Since the map

$$\psi_u : \mathrm{Gal}(E/F) \hookrightarrow \mu_\wp, \quad \sigma \mapsto \sigma(y) - y$$

is an isomorphism (see 2.3.2(i)), we have $\sigma(y) = y + \alpha$ for some generator α of $\mu_\wp = W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$ and therefore $\sigma^l(y) = y + l\alpha$ for each $l \in \mathbb{N}$. In other words, the elements of $\mathrm{Gal}(E/F)$ are given by

$$\sigma^l(y_i) = (y + l\alpha)_i, \quad 1 \le i \le n, \;\; 1 \le l \le p^n.$$

Note that

$$\sigma(y) = y + \alpha = (y_1 + c_0, \dots, y_n + c_{n-1})$$

with $c_i \in E_i$, i. e.

$$\sigma_i(y_j) = y_j + c_{j-1} \;\; (1 \le j \le i \le n), \tag{3.2.h}$$

where $\sigma_i := \sigma|_{E_i}$ is a generator of the Galois group of E_i/F and, if $j < i$, then $\sigma_i\big|_{E_j} = \sigma_j$. Now (3.2.f) and (3.2.h) give

$$\sigma_{i-1}((z_{i-1} + u_i)) - (z_{i-1} + u_i) = c_{i-1}^p - c_{i-1}.$$

From

$$\begin{aligned}\sigma_{i+1}^{p^i}(y_{i+1}) &= y_{i+1} + c_i + \sigma_{i+1}(c_i) + \cdots + \sigma_{i+1}^{p^i-1}(c_i)\\ &= y_{i+1} + c_i + \sigma_i(c_i) + \cdots + \sigma_i^{p^i-1}(c_i)\\ &= y_{i+1} + \mathrm{Tr}_{E_i/F}(c_i)\end{aligned}$$

it follows that $\mathrm{Tr}_{E_i/F}(c_i) \neq 0$, since otherwise $\sigma_{i+1}^{p^i} = 1$, contradicting $\operatorname{ord}\sigma_{i+1} = p^{i+1}$.

Each $y' = (y'_1, \ldots, y'_n) \in \wp^{-1}\big(W_n(F)\big)$ with $E := E_n = F(y'_1, \ldots, y'_n)$ is called an **Artin-Schreier-Witt generator** of E/F. If y' is an Artin-Schreier-Witt generator of E/F, then, for each $1 \leq i \leq n$, $(y'_1, \ldots, y'_i)$ is an Artin-Schreier-Witt generator of E_i/F.

3.2.8 Proposition. *Let E/F be a cyclic Artin-Schreier-Witt extension of degree p^n, i. e. we have $u \in W_n(F)$, $u_1 \neq \alpha^p - \alpha\ \forall \alpha \in F$, $y = (y_1, \ldots, y_n) \in \wp^{-1}(u)$ and $E = F(y) = F(y_1, \ldots, y_n)$. Then, for $y' \in W_n(\bar{F})$, the following assertions are equivalent:*

(i) *y' is an Artin-Schreier-Witt generator of E/F.*

(ii) *$y' \in \wp^{-1}(u')$ for some $u' \in W_n(F)$ and $u' - \lambda u \in \wp\big(W_n(F)\big)$ for some $\lambda \in \big(\mathbb{Z}/p^n\mathbb{Z}\big)^*$.*

(iii) *$y' = \lambda y + \zeta$ for some $\lambda \in \big(\mathbb{Z}/p^n\mathbb{Z}\big)^*$ and $\zeta \in W_n(F)$.*

Proof. (i)$\Leftrightarrow$(ii):

$$\begin{aligned}F(y) = F(y') &\underset{2.1.7}{\iff} F\big(\wp^{-1}(\Delta_u)\big) = F\big(\wp^{-1}(\Delta_{u'})\big)\\ &\underset{2.3.1}{\iff} \Delta_u = \Delta_{u'}\\ &\iff \overline{\Delta_u} = \overline{\Delta_{u'}}\\ &\iff \exists\, \lambda \in \big(\mathbb{Z}/p^n\mathbb{Z}\big)^* \text{ with } u' - \lambda u \in \wp\big(W_n(F)\big).\end{aligned}$$

(ii)$\Rightarrow$(iii): Let

$$u' \equiv \lambda u \mod \wp\big(W_n(F)\big)$$

for some $\lambda \in \big(\mathbb{Z}/p^n\mathbb{Z}\big)^*$, i. e. $u' = \lambda u + \wp(\theta)$ for some $\theta \in W_n(F)$. $y' \in \wp^{-1}(u')$ implies $y' = \lambda y + \theta + \theta'$ with $\theta' \in \ker\wp \subseteq W_n(F)$.

(iii)$\Rightarrow$(ii): If $y' = \lambda y + \zeta$ for some $\lambda \in \big(\mathbb{Z}/p^n\mathbb{Z}\big)^*$ and $\zeta \in W_n(F)$, then $\wp(y') = \lambda u + \wp(\zeta) =: u' \in W_n(F)$ and $u - \lambda^{-1}u' = \wp(\zeta) \in \wp\big(W_n(F)\big)$. □

Chapter 4

Computing the Generators

In this chapter we present the main results of this thesis. We give the procedures and algorithms to compute a finite set Ω of $\mathcal{O}_\mathcal{S}$-generators of $\mathcal{O}_\mathcal{S}(E)$, where F/k is a function field with finite (in particular perfect) constant field k, $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$ and E is a cyclic Kummer (4.2) or Artin-Schreier-Witt extension (4.3) of F. This is done by first splitting $\mathcal{S}$ in finitely many disjoint subsets and then computing for each P in each of these sets a set Ω_P of $\mathcal{S}$-integral generators of $\mathcal{O}_P(E)$ over $\mathcal{O}_P$. Section 4.1 provides some auxiliary tools for this, 4.1.2 and 4.1.3. Theorem 4.1.1 assures that the set, which consists of the union of all Ω_P, is the sought-after set Ω of $\mathcal{O}_\mathcal{S}$-generators of $\mathcal{O}_\mathcal{S}(E)$. Ω is finite since the sets Ω_P are equal for all but finitely many $P \in \mathcal{S}$.

4.1 Preliminaries

The following fundamental theorem gives us one of the basic tools for our purpose of computing the generators of all $\mathcal{S}$-integral elements of E.

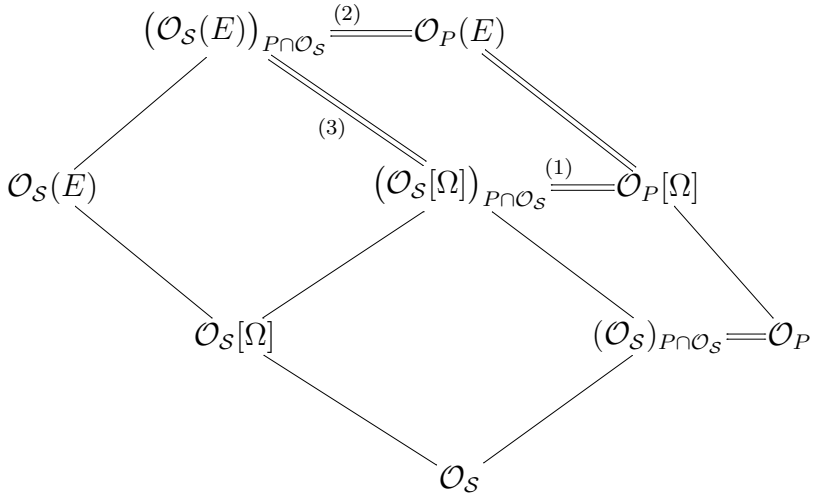
4.1.1 Theorem. *Let E be an extension of a function field F/k and $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$. Suppose there is a subset Ω of $\mathcal{O}_\mathcal{S}(E)$ which consists of $\mathcal{O}_P$-generators of $\mathcal{O}_P(E)$ for each $P \in \mathcal{S}$, i. e.*

$$\mathcal{O}_P(E) = \mathcal{O}_P[\Omega] \ \ \forall\, P \in \mathcal{S}.$$

Then Ω is a set of generators of $\mathcal{O}_\mathcal{S}(E)$ over $\mathcal{O}_\mathcal{S}$, i. e.

$$\mathcal{O}_\mathcal{S}(E) = \mathcal{O}_\mathcal{S}[\Omega].$$

Proof. For each $P \in \mathcal{S}$ we have the following picture:



Here, $(\mathcal{O}_\mathcal{S})_{P\cap\mathcal{O}_\mathcal{S}}$ is the localization of the ring $\mathcal{O}_\mathcal{S}$ at its prime ideal $P \cap \mathcal{O}_\mathcal{S}$ and $\big(\mathcal{O}_\mathcal{S}[\Omega]\big)_{P\cap\mathcal{O}_\mathcal{S}}$ and $\big(\mathcal{O}_\mathcal{S}(E)\big)_{P\cap\mathcal{O}_\mathcal{S}}$ are the localizations of the $\mathcal{O}_\mathcal{S}$-modules $\mathcal{O}_\mathcal{S}[\Omega]$ and $\mathcal{O}_\mathcal{S}(E)$, respectively. Since $(\mathcal{O}_\mathcal{S})_{P\cap\mathcal{O}_\mathcal{S}} = \mathcal{O}_P$ (see 1.2.8(v)), these are modules over $\mathcal{O}_P$ (see Section 1.1). Equality (1) and (2) follow from 1.1.2(i) (for (2), take any set of generators $\tilde{\Omega} \supseteq \Omega$ of $\mathcal{O}_\mathcal{S}(E)$ over $\mathcal{O}_\mathcal{S}$). (3) follows from (1) and (2).

This means that

$$\big(\mathcal{O}_\mathcal{S}(E)\big)_\mathfrak{p} = \big(\mathcal{O}_\mathcal{S}[\Omega]\big)_\mathfrak{p}$$

for all maximal ideals $\mathfrak{p}$ of $\mathcal{O}_\mathcal{S}$, and therefore

$$\mathcal{O}_\mathcal{S}(E) = \mathcal{O}_\mathcal{S}[\Omega]$$

(see Proposition 1.1.3). □

The next two results will help us to compute for a place P of a function field F a local integral basis for some field extension of F.

4.1.2 Proposition. *Suppose $F \subseteq D \subseteq E$ is a tower of extensions of a function field F, $P \in \mathbb{P}_F$ a place and $P_1, \ldots, P_r$ are all the places of D above P. Let $\Omega \subset \mathcal{O}_P(D)$ with*

$$\mathcal{O}_P(D) = \mathcal{O}_P[\Omega]$$

and $\Omega_1, \ldots, \Omega_r$ be subsets of $\mathcal{O}_P(E)$ with

$$\mathcal{O}_{P_i}(E) = \mathcal{O}_{P_i}[\Omega_i]$$

for all $1 \leq i \leq r$. *Then*

$$\mathcal{O}_P(E) = \mathcal{O}_P[\Omega, \Omega_1, \ldots, \Omega_r].$$

Proof. With $\mathcal{S} := \{P_1, \ldots, P_r\}$ we get from 4.1.1

$$\mathcal{O}_{\mathcal{S}}(E) = \mathcal{O}_{\mathcal{S}}[\Omega_1, \ldots, \Omega_r].$$

Since $\mathcal{O}_{\mathcal{S}} = \bigcap \mathcal{O}_{P_i} = \mathcal{O}_P(D) = \mathcal{O}_P[\Omega]$, the result follows. □

4.1.3 Corollary. *Let* $E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n$ *be a tower of field extensions of a function field* E_0 *and* P_0 *be a place of* E_0. *Suppose for each* $1 \leq i \leq n$ *there is a set* $\Delta_i \subseteq \mathcal{O}_P(E_i)$ *such that*

$$\mathcal{O}_{P_{i-1}}(E_i) = \mathcal{O}_{P_{i-1}}[\Delta_i]$$

for each place P_{i-1} *of* E_{i-1} *over* P_0. *Then*

$$\mathcal{O}_{P_0}(E_n) = \mathcal{O}_{P_0}[\Delta_1, \ldots, \Delta_n].$$

Proof. Repeated application of 4.1.2, with $F = E_0$, $D = E_1$, $E = E_2$ in the first step, $F = E_0$, $D = E_2$, $E = E_3$ in the second and so on. □

4.1.4 Remark. Let F be a function field over the rational function field $k(x)$ and $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$. Define $s := \{p \in \mathbb{P}_{k(x)} \mid \exists P \in \mathcal{S} \text{ with } P|p\}$ and $\mathcal{S}' := \{P \in \mathbb{P}_F \mid P|p \text{ for some } p \in s\}$. Then for each $a \in F$ there exists a representation $a = \frac{\text{num}(a)}{\text{den}(a)}$ satisfying

(1) $\text{num}(a) = a_1\omega_1 + \cdots + a_m\omega_m \in \mathcal{O}_{\mathcal{S}'}$ (here $\omega_1, \ldots, \omega_m$ is a basis of $\mathcal{O}_{\mathcal{S}'}$ over $\mathcal{O}_s$),

(2) $\text{den}(a) \in \mathcal{O}_s$ and

(3) $\gcd(\text{den}(a), a_1, \ldots, a_m) = 1$ (note that $\mathcal{O}_s$ is a unique factorization domain).

The following proposition provides us with a tool for finding for a given element of a function field another element such that their product is integral for a given set of places.

4.1.5 Proposition. *Let E/F be a function field extension, $0 \neq \beta \in E$ and*

$$\chi_{(\beta,\, E/F)}(T) = \sum_{i=0}^{m} \alpha_i T^i$$

the minimal polynomial of β over F. Let $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$. If we define

$$\delta_\beta := \operatorname{lcm}\left\{ \operatorname{den}\left(\frac{\alpha_i}{\alpha_j}\right) \;\middle|\; 0 \leq i < j \leq m,\;\; \alpha_i, \alpha_j \neq 0 \right\},$$

then

$$\beta\delta_\beta \in \mathcal{O}_{\mathcal{S}}(E). \tag{4.1.a}$$

Suppose β is integral for some $P \in \mathcal{S}$. Using Strong Approximation we choose $\gamma \in F$ with

$$\begin{aligned} &v_P(\gamma) = -v_P(\delta_\beta) \text{ and} \\ &v_Q(\gamma) \geq 0 \text{ for all } Q \in \mathcal{S} \setminus \{P\}. \end{aligned}$$

Then also

$$\beta\delta_\beta\gamma \in \mathcal{O}_{\mathcal{S}}(E). \tag{4.1.b}$$

Proof. From the Newton polygon of $\chi_{(\beta,\, E/F)}$ we know that there exist $0 \leq r < s \leq m$ such that $0 \neq \alpha_r, \alpha_s$ and

$$v_{P'}(\beta) = e(P'|P)\, \frac{v_P(\alpha_r) - v_P(\alpha_s)}{s - r}$$

(see for instance [Cas86, Chapter 6.3]). Therefore

$$\begin{aligned} v_{P'}(\beta\delta_\beta) &= e(P'|P) \left(\frac{1}{s-r}\, v_P\left(\frac{\alpha_r}{\alpha_s}\right) + v_P(\delta_\beta) \right) \\ &= \frac{e(P'|P)}{s-r} \left(v_P\left(\frac{\alpha_r}{\alpha_s}\right) + (s-r) v_P(\delta_\beta) \right) \\ &= \frac{e(P'|P)}{s-r}\, v_P\left(\frac{\alpha_r}{\alpha_s}\, \delta_\beta^{s-r}\right) \geq 0 \end{aligned}$$

for each $P \in \mathcal{S}$ and $P' \in \mathbb{P}_E$ with $P'|P$. This proves (4.1.a). The proof of (4.1.b) is now trivial. ∎

4.2 Kummer Extensions

Let F/k be a function field which contains a primitive n-th root of unity, $n > 1$ and n relative prime to the characteristic p of F. Suppose E/F is a cyclic Kummer extension of F of degree n, i. e. $E = F(y)$ where

$$y^n = u \in F \text{ and } u \neq w^d \text{ for all } w \in F,\ d \mid n \text{ and } d > 1. \tag{4.2.a}$$

Let $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$. The task of this section is to find a set of $\mathcal{O}_\mathcal{S}(F)$-generators of $\mathcal{O}_\mathcal{S}(E)$. Let $P \in \mathcal{S}$ and $P' \in \mathbb{P}_E$ with $P'|P$. We recall from 3.1.4 that

$$e_E(P) := e(P'|P) = \frac{n}{r_{P,E}}, \tag{4.2.b}$$

where

$$r_{P,E} := \gcd\big(n, v_P(u)\big) > 0.$$

Let us first consider the unramified places. We notice

$$\begin{aligned} P \text{ unramified in } E/F &\iff e(P'|P) = 1 \ \ \forall P'|P \\ &\iff r_{P,E} = n \\ &\iff v_P(u) \equiv 0 \bmod n. \end{aligned}$$

We define

$$\begin{aligned} A :&= \{P \in \mathcal{S} \mid P \text{ unramified in } E/F\} \\ &= \{P \in \mathcal{S} \mid j_P n =: v_P(u) \equiv 0 \bmod n\} \end{aligned}$$

and

$$A_0 := \{P \in A \mid v_P(u) = 0 \text{ and } v_P(\delta_y) = 0\}$$

(δ_y was defined in 4.1.5). Then

$$A \setminus A_0 = \{P \in A \mid v_P(u) \neq 0 \text{ or } v_P(\delta_y) > 0\}. \tag{4.2.c}$$

4.2.1 Proposition ($\mathcal{S}$-integral $\mathcal{O}_P$-generators of $\mathcal{O}_P(E)$ for $P \in A$).

(i) $y\delta_y \in \mathcal{O}_\mathcal{S}(E)$.

(ii) *For all $P \in A_0$ we have*

$$\mathcal{O}_P(E) = \mathcal{O}_P[y\delta_y].$$

Using Strong Approximation we choose $\tau \in F$ with

$$v_P(\tau) = -(j_P + v_P(\delta_y)) \text{ for all } P \in A \setminus A_0 \text{ and}$$
$$v_Q(\tau) \geq 0 \text{ for all } Q \in \mathcal{S} \setminus \{A \setminus A_0\}.$$

Then

(iii) $y\delta_y\tau \in \mathcal{O}_{\mathcal{S}}(E)$

(iv) $\mathcal{O}_P(E) = \mathcal{O}_P[y\delta_y\tau]$ *for all* $P \in A \setminus A_0$.

Proof. (i) follows from 4.1.5.

We have

$$\chi_{(y,\,E/F)}(T) = T^n - u \in \mathcal{O}_P[T] \text{ for all } P \in A_0. \tag{4.2.d}$$

From $y^n = u$ and $v_P(u) = 0$ follows $v_{P'}(y) = 0$ and therefore

$$v_{P'}\big(\chi'_{(y,\,E/F)}(y)\big) = v_{P'}\big(n \cdot y^{n-1}\big) = (n-1)v_{P'}(y) = 0 \tag{4.2.e}$$

for all $P' \in \mathbb{P}_E$ above P. (4.2.d) and (4.2.e) together with 1.2.13(i) give

$$\mathcal{O}_P(E) = \mathcal{O}_P[y] \text{ for all } P \in A_0.$$

Since $v_P(\delta_y) = 0$ for all $P \in A_0$, this shows (ii).

Setting $\tilde{y} := y\delta_y\tau$ we get

$$\tilde{y}^n = u\delta_y^n\tau^n =: \tilde{u} \tag{4.2.f}$$

and

$$\tilde{u} \neq w^d \text{ for all } w \in F,\ d \mid n,\ d > 1. \tag{4.2.g}$$

(Suppose not, i. e. $\tilde{u} = w^d$. Then

$$u = \frac{w^d}{\delta_y^n\tau^n} = \left(\frac{w}{\delta_y^{\frac{n}{d}}\tau^{\frac{n}{d}}}\right)^d,$$

contradicting (4.2.a).) This means that $\tilde{y}$ is a Kummer generator of E/F with minimal polynomial

$$\chi_{(\tilde{y},\,E/F)}(T) = T^n - \tilde{u}.$$

4.1.5 and the definition of τ yields

$$v_{Q'}\big(\tilde{y}\big) \geq 0 \tag{4.2.h}$$

for all $Q'|Q$, $Q \in \mathcal{S} \setminus \{A \setminus A_0\}$. From

$$\begin{aligned} v_P\big(\tilde{u}\big) &= v_P\big((\tilde{y})^n\big) \\ &= v_P\big(y^n\big) + v_P\big(\delta_y^n\big) + v_P\big(\tau^n\big) \\ &= v_P(u) + nv_P(\delta_y) + nv_P(\tau) \\ &= j_P n + nv_P(\delta_y) - nj_P - nv_P(\delta_y) \\ &= 0 \end{aligned} \tag{4.2.i}$$

follows

$$v_{P'}\big(\tilde{y}\big) = 0 \tag{4.2.j}$$

for all $P' \in \mathbb{P}_E$ above P, $P \in A \setminus A_0$. (4.2.h) and (4.2.j) now give (iii).

For (iv) we note that from (4.2.i)) we get $\chi_{(\tilde{y},\, E/F)}(T) \in \mathcal{O}_P[T]$ and that (4.2.j) yields

$$v_{P'}\big(\chi'(\tilde{y})\big) = v_{P'}\big(n \cdot \tilde{y}^{n-1}\big) = (n-1)v_{P'}(\tilde{y}) = 0$$

for all $P' \in \mathbb{P}_E$ above P, $P \in A \setminus A_0$, and therefore (by 1.2.13(i))

$$\mathcal{O}_P(E) = \mathcal{O}_P[\tilde{y}]$$

for all $P \in A \setminus A_0$. □

Let us now consider the ramified places, i. e. the set

$$B := \mathcal{S} \setminus A = \{P \in \mathcal{S} \mid v_P(u) \not\equiv 0 \bmod n\}$$

We define

$$\begin{aligned} B_1 :&= \{P \in B \mid e_E(P) = n\} \\ &= \{P \in B \mid r_{P,E} = \gcd(n, v_P(u)) = 1\} \end{aligned} \tag{4.2.k}$$

and

$$B_2 := \{P \in B \mid 1 < e_E(P) < n\} = B \setminus B_1. \tag{4.2.l}$$

If $P \in B_1$, then P is totally ramified in E/F and there exist integers s_P and l_P with $l_P > 0$ such that

$$ns_P + l_P v_P(u) = 1. \tag{4.2.m}$$

Using Strong Approximation we choose $\gamma_P \in F$ satisfying

$$\begin{aligned} &v_P(\gamma_P) = s_P - l_P v_P(\delta_y) \text{ and} \\ &v_Q(\gamma_P) \geq 0 \text{ for all } Q \in \mathcal{S} \setminus \{P\}. \end{aligned} \tag{4.2.n}$$

Since $l_P > 0$ we get with 4.1.5

$$v_{Q'}\big(\gamma_P(y\delta_y)^{l_P}\big) \geq 0 \tag{4.2.o}$$

for all $Q'|Q$, $Q \in \mathcal{S} \setminus \{P\}$. Moreover, if P' is the place of E above P, then

$$\begin{aligned} v_{P'}\big(\gamma_P(y\delta_y)^{l_P}\big) &= e(P'|P)v_P(\gamma_P) + l_P v_{P'}(y) + e(P'|P)l_P v_P(\delta_y) \\ &= ns_P - nl_P v_P(\delta_y) + l_P v_P(u) + nl_P v_P(\delta_y) \\ &= ns_P + l_P v_P(u) \\ &= 1. \end{aligned} \tag{4.2.p}$$

(4.2.o), (4.2.p) and 1.2.13(ii) shows

4.2.2 Proposition ($\mathcal{S}$-integral $\mathcal{O}_P$-generators of $\mathcal{O}_P(E)$ for $P \in B_1$). *If $P \in B$ has ramification index $n = [E : F]$ (which is the case iff $r_{P,E} = \gcd(n, v_P(u)) = 1$) and γ_P is as in* (4.2.n)*, then*

(i) $\gamma_P(y\delta_y)^{l_P} \in \mathcal{O}_S(E)$ *and*

(ii) $\mathcal{O}_P(E) = \mathcal{O}_P[\gamma_P(y\delta_y)^{l_P}]$. □

Suppose now $P \in B_2$, i. e. P is ramified in E with ramification index $e := e_E(P)$, where $1 < e < n$. Hence

$$r := r_{P,E} = \frac{n}{e} = \gcd(n, v_P(u)). \tag{4.2.q}$$

Consider the intermediate field $E_r := F(y^e)$ of E/F and let $P_{r,1}, \ldots, P_{r,s}$ be all the places of E_r above P. Then E_r/F is a Kummer extension of degree r with Kummer generator y^e and defining polynomial $T^r - u$ and E/E_r is a Kummer extension of degree e with Kummer generator y and defining polynomial $T^e - y^e$. From (4.2.q) we get

$$r_{P,E_r} = \gcd(r, v_P(u)) = \gcd(n, v_P(u)) = r,$$

hence (see (4.2.b))

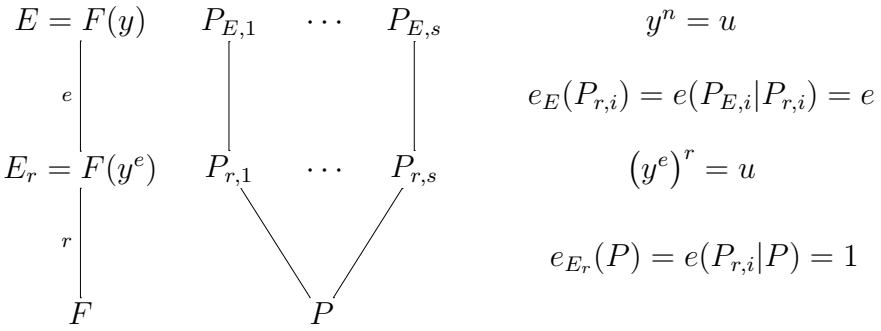
$$e_{E_r}(P) = \frac{r}{r_{P,E_r}} = 1. \tag{4.2.r}$$

This implies

$$e = e_E(P) = e_{E_r}(P) \cdot e_E(P_{r,i}) = e_E(P_{r,i}) \tag{4.2.s}$$

for each $1 \leq i \leq s$. This means that E_r is the inertia field of P in E, i. e. P is unramified in E_r/F and each $P_{r,i}$ is totally ramified in E/E_r. We summarize

the above in the following diagram:



(Here, $P_{E,1}, \ldots, P_{E,s}$ are all the places of E above P and $P_{E,i}|P_{r,i}$.) The unramified case (4.2.r) was dealt with in Proposition 4.2.1. Applied to our situation this means that we take $j_P \in \mathbb{Z}$ with

$$v_P(u) = j_P r,$$

use Strong Approximation to choose $\tau_P \in F$ with

$$\begin{aligned} &v_P(\tau_P) = -(j_P + v_P(\delta_{y^e})) \text{ and} \\ &v_Q(\tau_P) \geq 0 \text{ for all } Q \in \mathcal{S} \setminus \{P\} \end{aligned}$$

and set

$$\alpha_P := y^e \delta_{y^e} \tau_P. \tag{4.2.t}$$

4.2.1 then yields

$$\alpha_P \in \mathcal{O}_S(E_r) \quad \text{and} \quad \mathcal{O}_P(E_r) = \mathcal{O}_P[\alpha_P]. \tag{4.2.u}$$

On the other hand, the case (4.2.s) of total ramification was discussed in Proposition 4.2.2: For all $1 \leq i \leq s$ we have

$$\begin{aligned} v_{P_{E,i}}(y^n) = v_{P_{E,i}}(u) = e v_P(u) \\ \implies \quad & v_{P_{E,i}}(y^r) = v_P(u) \\ \implies \quad & v_{P_{E,i}}(y) = \frac{v_P(u)}{r} \\ \implies \quad & v_{P_{E,i}}(y^e) = e(P_{E,i}|P_{r,i}) v_{P_{r,i}}(y^e) = \frac{e v_P(u)}{r} \\ \implies \quad & v_{P_{r,i}}(y^e) = \frac{v_P(u)}{r}. \end{aligned}$$

Moreover we know

$$1 = r_{P_{r,i},E} = \gcd(e, v_{P_{r,i}}(y^e)).$$

Hence there exist integers s_P and l_P with $l_P > 0$ such that

$$es_P + l_P \frac{v_P(u)}{r} = 1.$$

We use Strong Approximation to find $\gamma_P \in F$ satisfying

$$\begin{aligned} &v_P(\gamma_P) = s_P - l_P v_P(\delta_y) \text{ and} \\ &v_Q(\gamma_P) \geq 0 \text{ for all } Q \in \mathcal{S} \setminus \{P\} \end{aligned}$$

and define

$$\beta_P := \gamma_P (y\delta_y)^{l_P}. \tag{4.2.v}$$

Now, since $l_P > 0$ we get with 4.1.5

$$v_{Q'}\big(\beta_P\big) \geq 0 \tag{4.2.w}$$

for all $Q'|Q$, $Q \in \mathcal{S} \setminus \{P\}$. Moreover, since P is unramified in E_r/F we get (similar to (4.2.p))

$$v_{P_{E,i}}\big(\beta_P\big) = 1 \tag{4.2.x}$$

for all $1 \leq i \leq s$. From (4.2.w), (4.2.x) and 1.2.13(ii) then follows

$$\beta_P \in \mathcal{O}_S(E) \quad \text{and} \quad \mathcal{O}_{P_{r,i}}(E) = \mathcal{O}_{P_{r,i}}[\beta_P] \tag{4.2.y}$$

for all $1 \leq i \leq s$. Putting together (4.2.u) and (4.2.y) and using 4.1.2 we get

4.2.3 Proposition ($\mathcal{S}$-integral $\mathcal{O}_P$-generators of $\mathcal{O}_P(E)$ for $P \in B_2$). *Let P be in B_2. With the notations just defined we get*

(i) $\alpha_P, \beta_P \in \mathcal{O}_S(E)$ *and*

(ii) $\mathcal{O}_P(E) = \mathcal{O}_P[\alpha_P, \beta_P]$. □

We are now able to give an algorithm which computes for each Kummer extension E of a function field F and each $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$ a set of $\mathcal{O}_\mathcal{S}$-generators of $\mathcal{O}_\mathcal{S}(E)$:

4.2.4 Algorithm.

Input: A Kummer extension $E = F(y)/F$ and $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$.
Output: A finite set Ω of $\mathcal{O}_\mathcal{S}$-generators of $\mathcal{O}_\mathcal{S}(E)$.

1. Compute the sets $A \setminus A_0$, B_1 and B_2 (see (4.2.c), (4.2.k) and (4.2.l)).
2. Compute $\Omega_{A_0} := \{y\delta_y\}$, where δ_y is as in 4.1.5.
3. Compute τ (see 4.2.1) and set $\Omega_{A\setminus A_0} := \{y\delta_y\tau\}$.
4. For each $P \in B_1$ compute s_P and l_P and γ_P satisfying (4.2.m) and (4.2.n), respectively and set
$$\Omega_{B_1} := \{\gamma_P(y\delta_y)^{l_P} \mid P \in B_1\}.$$
5. For each $P \in B_2$ compute α_P and β_P as in (4.2.t) and (4.2.v), respectively and set
$$\Omega_{B_2} := \{\alpha_P, \beta_P \mid P \in B_2\}$$
6. **return** $\Omega := \Omega_{A_0} \cup \Omega_{A\setminus A_0} \cup \Omega_{B_1} \cup \Omega_{B_2}$.

The correctness of this algorithm follows from $\mathcal{S} = A_0 \cup A \setminus A_0 \cup B_1 \cup B_2$ and Proposition 1.1.1. The set Ω is finite and contained in $\mathcal{O}_\mathcal{S}(E)$ since this is true for each of the sets Ω_{A_0}, $\Omega_{A\setminus A_0}$, Ω_{B_1} and Ω_{B_2} (note that $A \setminus A_0$, B_1 and B_2 are finite).

4.3 Artin-Schreier-Witt Extensions

For this entire section we consider the following situation:

> *Let E/F be a cyclic Artin-Schreier-Witt extension of degree p^n, i. e. we have $u \in W_n(F)$, $u_1 \neq \alpha^p - \alpha$ for all $\alpha \in F$, $y = (y_1, \ldots, y_n) \in \wp^{-1}(u)$ and $E = F(y_1, \ldots, y_n)$. We set $E_0 := F$, $E_n := E$ and $E_i := F(y_1, \ldots, y_i) = F(y_i)$ for each for each $1 \leq i \leq n$.*

Let $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$. Now we have all the necessary tools to compute a set of generators of $\mathcal{O}_\mathcal{S}(E)$ over $\mathcal{O}_\mathcal{S}$. We will give a brief survey of this section. Let $P \in \mathbb{P}_F$. We begin by defining a vector $\Lambda_P = (\Lambda_{P,1}, \ldots, \Lambda_{P,n}) \in \mathbb{Z}^n$ and a vector $\zeta_P = \zeta(P) \in W_n(F)$ which will give us important information about the ramification behaviour of P in E. We use these vectors to split $\mathcal{S}$ into finitely many disjoint subsets. Then we compute for each P in each of these sets a set of $\mathcal{S}$-integral generators of $\mathcal{O}_P(E)$ over $\mathcal{O}_P$. As mentioned above, Theorem 4.1.1 then guarantees that the set Ω, which consists of all these generators and will turn out to be finite, has the desired properties.

We define the vector $\Lambda_P = (\Lambda_{P,1}, \ldots, \Lambda_{P,n}) \in \mathbb{Z}^n$ in the following way: Set $u^{[0]} := u$. Using algorithm 3.2.2 we choose an element $\zeta_1 := \zeta(P, u_1) \in F$ which determines $\lambda_P(u_1)$ (see 3.2.1(i)), that is,

$$\begin{aligned} \text{either} \qquad & v_P\big(u_1 + (\zeta_1^p - \zeta_1)\big) = -\lambda_P(u_1) \\ \text{or} \qquad & v_P\big(u_1 + (\zeta_1^p - \zeta_1)\big) \geq 0. \end{aligned}$$

We set $\Lambda_{P,1} := \lambda_P(u_1)$, $(\zeta_P)_1 := \zeta_1$ and

$$u^{[1]} := u^{[0]} + \wp\big((\zeta_1, 0, \ldots, 0)\big).$$

If $\Lambda_{P,1} > 0$, then $\Lambda_{P,j} := 0$, $(\zeta_P)_j := 0$ and $u^{[j]} := u^{[1]}$ for all $1 < j \leq n$. Else we choose an element $\zeta_2 := \zeta\left(P, (u^{[1]})_2\right) \in F$ which determines $\lambda_P\left((u^{[1]})_2\right)$ (see 3.2.1(i)), i. e.

$$\begin{aligned} \text{either} \qquad & v_P\big((u^{[1]})_2 + (\zeta_2^p - \zeta_2)\big) = -\lambda_P\left((u^{[1]})_2\right) \\ \text{or} \qquad & v_P\big((u^{[1]})_2 + (\zeta_2^p - \zeta_2)\big) \geq 0 \end{aligned}$$

and set $\Lambda_{P,2} := \lambda_P\left((u^{[1]})_2\right)$ and $(\zeta_P)_2 := \zeta_2$. Now we set recursively as long as $\Lambda_{P,i-1} = 0$

$$u^{[i]} := u^{[i-1]} + \wp(\zeta^{[i]}),$$

where $\zeta^{[i]} \in W_n(F)$ is given by

$$(\zeta^{[i]})_j = \begin{cases} \zeta_i & j = i \\ 0 & \text{else.} \end{cases}$$

Here $\zeta_i := \zeta\left(P, (u^{[i-1]})_i\right) \in F$ is an element which determines $\lambda_P\left((u^{[i-1]})_i\right)$, that is,

$$v_P\big((u^{[i-1]})_i + (\zeta_i^p - \zeta_i)\big) = v_P\big((u^{[i]})_i\big) \begin{cases} = -\lambda_P\left((u^{[i-1]})_i\right) & \text{or} \\ \geq 0 \end{cases}$$

and set

$$\Lambda_{P,i} := \lambda_P\left((u^{[i-1]})_i\right) \text{ and } (\zeta_P)_i := \zeta_i. \tag{4.3.a}$$

If we reach an $1 \leq r \leq n$ with $\Lambda_{P,r} > 0$, then we stop this procedure and set

$$\Lambda_{P,j} := 0,\ (\zeta_P)_j := 0 \text{ and } u^{[j]} := u^{[r]} \text{ for all } r < j \leq n. \tag{4.3.b}$$

Note that, if $1 < l < j \leq n$, then the first l coordinates of $u^{[l]}$ and $u^{[j]}$ are equal and

$$u^{[n]} = \left((u^{[0]})_1 + ((\zeta_P)_1^p - (\zeta_P)_1), \ldots, (u^{[n-1]})_n + ((\zeta_P)_n^p - (\zeta_P)_n)\right).$$

Moreover, since

$$(u^{[l]})_l = (u^{[l-1]})_l + (\zeta_l^p - \zeta_l)$$

we have

$$\lambda_P\left((u^{[l-1]})_l\right) = \lambda_P\left((u^{[l]})_l\right) = \cdots = \lambda_P\left((u^{[j]})_l\right).$$

The new Artin-Schreier-Witt generator of E/F which is obtained by the above procedure is

$$y_P := y + \zeta_P \tag{4.3.c}$$

with

$$u_P := \wp(y_P) = u^{[n]} = u + \wp\left(\zeta_P\right) \tag{4.3.d}$$

i. e. $E_j = E_{j-1}((y_P)_j)$ and

$$(y_P)_j^p - (y_P)_j = (u_P)_j + z_{P,j-1},$$

where $z_{P,j-1} \in E_{j-1}$ is as in (3.2.g).

4.3.1 Remark (Computing the inertia field of a place $P \in \mathbb{P}_F$). We denote by P_j an arbitrary extension of P to E_j. Since the E_j $(0 \leq j \leq n)$ are the only subfields of E_n, we know from 1.2.6 that the inertia field of P_n over P is E_t for some $0 \leq t \leq n$, i. e. P is unramified in E_t/F and P_j is totally ramified in E_l/E_j for each $t \leq j < l \leq n$. We claim that

$$t = \begin{cases} n & \text{if } \Lambda_{P,i} \text{ for all } 1 \leq i \leq n \\ \min\{1 \leq j-1 \leq n \mid \Lambda_{P,j-1} > 0\} & \text{else.} \end{cases} \tag{4.3.e}$$

From 3.2.1 we know that P_{j-1} is unramified in E_j/E_{j-1} iff $\lambda_{P_{j-1}}((u_P)_j + z_{P,j-1}) = 0$. Therefore we have established (4.3.e) if we show that

$$\Lambda_{P,j} = \lambda_{P_{j-1}}((u_P)_j + z_{P,j-1}) \quad \text{for} \quad 1 \le j \le t+1. \tag{4.3.f}$$

Since $\Lambda_{P,1} = \cdots = \Lambda_{P,t} = 0$ and $z_{P,j-1}$ is a polynomial expression in $(y_P)_l$, $(u_P)_l$ and $z_{P,l-1}$ $(1 \le l < j-1)$ with coefficients in the prime field of F (see remark 3.2.7), we have

$$v_{P_{j-1}}(z_{P,j-1}) \ge 0, \;\; 1 \le j \le t+1. \tag{4.3.g}$$

For $1 \le j \le t$ we have $\Lambda_{P,j} = 0$ and $v_P((u_P)_j) \ge 0$. Therefore

$$v_{P_{j-1}}((u_P)_j + z_{P,j-1}) \ge 0 \tag{4.3.h}$$

and thus $\lambda_{P_{j-1}}((u_P)_j + z_{P,j-1}) = 0$. It follows that P is unramified in E_t/E.

On the other hand, if $t < n$ and $j = t+1$, i. e. $v_P((u_P)_{t+1}) = -\Lambda_{P,t+1} < 0$, then strict triangularity and (4.3.g) yield

$$v_{P_t}((u_P)_{t+1} + z_{P,t}) = v_{P_t}((u_P)_{t+1}) = v_P((u_P)_{t+1}) \tag{4.3.i}$$

and we have proved (4.3.f) and hence (4.3.e). □

For later reference we note the following: since $P_{t+1}|P_t$ is totally ramified and $P_t|P$ is unramified we have

$$\begin{aligned} 0 > p \cdot v_{P_t}\big((u_P)_{t+1} + z_{P,t}\big) &= v_{P_{t+1}}\big((u_P)_{t+1} + z_{P,t}\big) \\ &\ge \min\big\{v_{P_{t+1}}\big((y_P)_{t+1}^p\big), v_{P_{t+1}}\big((y_P)_{t+1}\big)\big\} \\ &= p \cdot v_{P_{t+1}}\big((y_P)_{t+1}\big), \end{aligned}$$

i. e. (together with (4.3.i))

$$-\Lambda_{P,t+1} = v_P\big((u_P)_{t+1}\big) = v_{P_t}\big((u_P)_{t+1} + z_{P,t}\big) = v_{P_{t+1}}\big((y_P)_{t+1}\big). \tag{4.3.j}$$

Note that all the above equations do not depend on the choice of the place P_j over P for all $1 \le j \le t+1$.

4.3.2 Remark. We keep the notation of the above remark. In particular, E_t is the inertia field of P in E. For each $1 \le i \le t$ consider the minimal polynomial

$$\chi_{((y_P)_i,\, E_i/E_{i-1})}(T) = T^p - T - \big((u_P)_i + z_{P,i-1}\big)$$

of $(y_P)_i \in E_i$ over E_{i-1} (where $z_{P,i-1} \in E_{i-1}$ is as in (3.2.g), see remark 3.2.7). For each $P_{i-1} \in \mathbb{P}_{E_{i-1}}$ with $P_{i-1}|P$ we know from (4.3.h)

$$\chi_{((y_P)_i,\, E_i/E_{i-1})}(T) \in \mathcal{O}_{P_{i-1}}[T].$$

This implies that for each $1 \le i \le t$ the element $(y_P)_i$ is integral over P. $\square$

We now split $\mathcal{S}$ into subsets. We define

$$A := \{P \in \mathcal{S} \mid v_P(u_i) \ge 0 \text{ for all } 1 \le i \le n\},$$

$$B := B_{n+1} := \left\{P \in \mathcal{S} \setminus A \;\middle|\; \Lambda_{P,i} = 0 \text{ for all } 1 \le i \le n\right\} \tag{4.3.k}$$

and for $1 \le j \le n$

$$B_j := \{P \in \mathcal{S} \mid \Lambda_{P,i} = 0 \text{ for } 1 \le i < j \text{ and } \Lambda_{P,j} > 0\}. \tag{4.3.l}$$

Note that all the above sets are pairwise disjoint and that their union equals $\mathcal{S}$. From remark 4.3.1 we know that $A \cup B$ equals the set of places of $\mathcal{S}$ which are unramified in E/F and that, if $P \in B_j$, then E_{j-1} is the inertia field of P, that is, P is unramified in E_{j-1}/F and totally ramified in E_l/E_{j-1} for each $j \le l \le n$. We have

$$\overline{A} := \mathcal{S} \setminus A = \bigcup_{j=1}^{n+1} B_j.$$

We proceed by computing $B_1, \ldots, B_{n+1}$. For this purpose we define for $1 \le i \le n$

$$\begin{aligned}\overline{A}_i &:= \{P \in \mathcal{S} \mid v_P(u_i) < 0 \text{ and } v_P(u_j) \ge 0 \text{ for all } 1 \le j < i\} \\ &= \{P \in \mathcal{S} \mid v_P(u_i) < 0 \text{ and } P \notin \overline{A}_j \text{ for all } 1 \le j < i\}.\end{aligned}$$

These sets are also pairwise disjoint and their union equals $\overline{A}$. Moreover, they are given explicitly. Therefore our task of computing $B_1, \ldots, B_{n+1}$ can be solved by finding r with $P \in B_r$ for each $P \in \overline{A}_l$, $1 \le l \le n$. This can be done as follows using the definitions and procedures described in the first part of this section. If $P \in \overline{A}_l$, then obviously

$$\Lambda_{P,j} = 0 \;\text{ for all }\; 1 \le j < l.$$

All we have to do is to compute $\Lambda_{P,l}, \Lambda_{P,l+1}, \ldots$ until we find $r \ge l$ with $\Lambda_{P,r} > 0$ (because this means $P \in B_r$). We summarize this in the following

4.3.3 Algorithm.

Input: $P \in \overline{A}_l$ for some $1 \leq l \leq n$.

Output: ζ_P and Λ_P as defined in (4.3.a) and (4.3.b) and r with $P \in B_r$.

1. $m \leftarrow l-1,\ \lambda \leftarrow 0$
2. **for** i **in** $[1..n]$ **do**
3. $\quad (\zeta_P)_i \leftarrow 0, \quad \Lambda_{P,i} \leftarrow 0$
4. **end for**
5. **while** $\lambda = 0$ **and** $m < n$ **do**
6. $\quad m \leftarrow m + 1$
7. $\quad \zeta, \lambda \leftarrow \mathit{Reduction}\,(P, u_m)$ (see algorithm 3.2.2)
8. $\quad (\zeta_P)_m \leftarrow \zeta, \quad \Lambda_{P,i} \leftarrow \lambda$
9. $\quad u \leftarrow u + \wp(Z)$, where $Z \in W_n(F)$ is given by

$$Z_j = \begin{cases} \zeta & j = m \\ 0 & \text{else} \end{cases}$$

10. **end while**
11. **if** $m = n$ **and** $\lambda = 0$ **do**
12. $\quad r \leftarrow m+1$
13. **else do**
14. $\quad r \leftarrow m$
15. **end if**
16. **return** ζ_P, Λ_P, r.

For each P we now also can compute y_P and u_P as in (4.3.c) and (4.3.d). Of course, $y_P = y$ and $u_P = u$ for all $P \in A$.

Let $P \in \mathcal{S}$. In order to compute generators of $\mathcal{O}_P(E)$ we first choose $1 \leq t \leq n$ such that E_t is the inertia field of P, i. e.

$$t = \begin{cases} n & P \in A \cup B \\ r-1 & P \in B_r. \end{cases}$$

We recall from remark 4.3.2 that for each $1 \leq i \leq t$ and each $P_{i-1} \in \mathbb{P}_{E_{i-1}}$ with $P_{i-1}|P$ we have

$$\chi_{((y_P)_i,\, E_i/E_{i-1})}(T) = T^p - T - \big((u_P)_i + z_{P,i-1}\big) \in \mathcal{O}_{P_{i-1}}[T]. \tag{4.3.m}$$

Moreover,

$$v_{P_i}\big(\chi'_{((y_P)_i,\, E_i/E_{i-1})}\big((y_P)_i\big)\big) = 0 \tag{4.3.n}$$

for all $P_i \in \mathbb{P}_{E_i}$ with $P_i|P_{i-1}$. From (4.3.m), (4.3.n) and 1.2.13(i) follows

$$\mathcal{O}_{P_{i-1}}(E_i) = \mathcal{O}_{P_{i-1}}\big[(y_P)_i\big]. \tag{4.3.o}$$

With 4.1.3 then follows

$$\mathcal{O}_P(E_t) = \mathcal{O}_P\big[(y_P)_1, \ldots, (y_P)_t\big]. \tag{4.3.p}$$

We are done if $t = n$. Otherwise we still have to consider the ramified part. Let $P_{t,1}, \ldots, P_{t,r}$ be all the places of E_t and $P_{n,1}, \ldots, P_{n,r}$ be all the places of E_n above P with $P_{n,i}|P_{t,i}$. For each $1 \leq i \leq r$ we choose a prime element π_i for $P_{n,i}$. From (4.3.p), 1.2.13(ii) and 4.1.2 then follows

$$\mathcal{O}_P(E_n) = \mathcal{O}_P\big[(y_P)_1, \ldots, (y_P)_t, \pi_1, \ldots, \pi_r\big].$$

This set of $\mathcal{O}_P$-generators of $\mathcal{O}_P(E)$ is in general of course not a subset of $\mathcal{O}_\mathcal{S}$. In the following propositions we will show how to compute $\mathcal{S}$-integral generators of $\mathcal{O}_P(E)$ over $\mathcal{O}_P$ successively for the places P in the sets A, $B_1, \ldots, B_{n+1}$.

Using the definition in Proposition 4.1.5 we define the following subset of A:

$$A' := \{P \in A \mid v_P(\delta_{y_i}) > 0 \text{ for some } 1 \leq i \leq n\}. \tag{4.3.q}$$

4.3.4 Proposition ($\mathcal{S}$-integral $\mathcal{O}_P$-generators of $\mathcal{O}_P(E)$ for $P \in A$).

Set

$$\Omega_{A\setminus A'} := \{y_i\delta_{y_i} \mid 1 \leq i \leq n\}.$$

Then

(i) $y_i\delta_{y_i} \in \mathcal{O}_{\mathcal{S}}(E)$ *for each* $1 \leq i \leq n$.

(ii) *For all* $P \in A \setminus A'$ *we have*

$$\mathcal{O}_P(E) = \mathcal{O}_P\big[\Omega_{A\setminus A'}\big].$$

Let now $P \in A'$. *For each* $1 \leq i \leq n$ *we use Strong Approximation to find* $\gamma_{P,i} \in F$ *with*

$$\begin{aligned} &v_P(\gamma_{P,i}) = -v_P(\delta_{y_i}) \text{ and} \\ &v_Q(\gamma_{P,i}) \geq 0 \text{ for all } Q \in \mathcal{S} \setminus \{P\}. \end{aligned}$$

Define

$$\Omega_P := \{y_i\delta_{y_i}\gamma_{P,i} \mid 1 \leq i \leq n\}. \tag{4.3.r}$$

Then

(iii) $y_i\delta_{y_i}\gamma_{P,i} \in \mathcal{O}_{\mathcal{S}}(E)$ *for each* $1 \leq i \leq n$.

(iv) $\mathcal{O}_P(E) = \mathcal{O}_P\big[\Omega_P\big]$.

Proof. (i) and (iii) follow from 4.1.5.

Let $P \in A \setminus A'$. For all $1 \leq i \leq n$ we have $v_P(\delta_{y_i}) = 0$, hence δ_{y_i} is a unit in $\mathcal{O}_P$. Therefore (with (4.3.o))

$$\mathcal{O}_{P_{i-1}}(E_i) = \mathcal{O}_{P_{i-1}}\big[y_i\big] = \mathcal{O}_{P_{i-1}}\big[y_i\delta_{y_i}\big]$$

for each place P_{i-1} of E_{i-1} over P. (ii) then follows from 4.1.3.

If $P \in A'$, then $v_P(\delta_{y_i}\gamma_{P,i}) = 0$ for all $1 \leq i \leq n$, hence $\delta_{y_i}\gamma_{P,i}$ is a unit in $\mathcal{O}_P$.

Like above, with (4.3.o) follows

$$\mathcal{O}_{P_{i-1}}(E_i) = \mathcal{O}_{P_{i-1}}\big[y_i\big] = \mathcal{O}_{P_{i-1}}\big[y_i\delta_{y_i}\gamma_{P,i}\big]$$

for all $1 \le i \le n$ and each place P_{i-1} of E_{i-1} over P. Again, 4.1.3 gives (iv). □

4.3.5 Proposition ($\mathcal{S}$-integral $\mathcal{O}_P$-generators of $\mathcal{O}_P(E)$ for $P \in B$). *Let $P \in B$. For each $1 \le i \le n$ we use Strong Approximation to select $\gamma_{P,i} \in F$ with*

$$\begin{aligned} &v_P\big(\gamma_{P,i}\big) = -v_P\big(\delta_{(y_P)_i}\big) \text{ and} \\ &v_Q(\gamma_{P,i}) \ge 0 \text{ for all } Q \in \mathcal{S} \setminus \{P\}. \end{aligned}$$

Define

$$\Omega_P := \{(y_P)_i\, \delta_{(y_P)_i}\gamma_{P,i} \mid 1 \le i \le n\}. \tag{4.3.s}$$

Then

(i) $(y_P)_i\delta_{(y_P)_i}\gamma_{P,i} \in \mathcal{O}_{\mathcal{S}}(E)$ *for each* $1 \le i \le n$.

(ii) $\mathcal{O}_P(E_n) = \mathcal{O}_P\big[\Omega_P\big]$.

Proof. (i) follows from 4.1.5.

Since $v_{P_{i-1}}\big(\delta_{(y_P)_i}\gamma_{P,i}\big) = 0$ for each $1 \le i \le n$ and each place P_{i-1} of E_{i-1} over P, (ii) follows with the same argumentation as in the proof of 4.3.4 from 4.1.3. □

4.3.6 Proposition ($\mathcal{S}$-integral $\mathcal{O}_P$-generators of $\mathcal{O}_P(E)$ for $P \in B_n$). *Let $P \in B_n$ and $t := n-1$, i. e. E_t is the inertia field of P in E_n. For each $1 \le i \le t$ we use Strong Approximation to find $\gamma_{P,i} \in F$ with*

$$\begin{aligned} &v_P\big(\gamma_{P,i}\big) = -v_P\big(\delta_{(y_P)_i}\big) \text{ and} \\ &v_Q(\gamma_{P,i}) \ge 0 \text{ for all } Q \in \mathcal{S} \setminus \{P\}. \end{aligned}$$

Since for all $P_n \in \mathbb{P}_{E_n}$ with $P_n|P$ we have $v_{P_n}\big((y_P)_n\big) = -\Lambda_{P,n} \not\equiv 0 \mod p$ (this was shown in (4.3.j)), there exist l and $s \in \mathbb{Z}^{\ge 0}$ such that $s \cdot p - l \cdot \Lambda_{P,n} = 1$. We choose $\theta_{P,n} \in F$ with

$$\begin{aligned} &v_P\big(\theta_{P,n}\big) = s - l \cdot v_P\big(\delta_{(y_P)_n}\big) \text{ and} \\ &v_Q(\theta_{P,n}) \ge 0 \text{ for all } Q \in \mathcal{S} \setminus \{P\} \end{aligned}$$

and define

$$\Omega_P := \Big\{ (y_P)_i \delta_{(y_P)_i} \gamma_{P,i} \;\Big|\; 1 \le i \le t \Big\} \cup \Big\{ \theta_{P,n} \big((y_P)_n \delta_{(y_P)_n} \big)^l \Big\}. \tag{4.3.t}$$

Then

(i) $(y_P)_i \delta_{(y_P)_i} \gamma_{P,i} \in \mathcal{O}_{\mathcal{S}}(E)$ *for each* $1 \le i \le t$.

(ii) $\theta_{P,n} \big((y_P)_n \delta_{(y_P)_n} \big)^l \in \mathcal{O}_{\mathcal{S}}(E)$.

(iii) $\mathcal{O}_P(E_n) = \mathcal{O}_P\big[\Omega_P\big]$.

Proof. (i) follows from 4.1.5.

$v_P\big(\delta_{(y_P)_i} \gamma_{P,i}\big) = 0$ for each $1 \le i \le t$. Hence $\delta_{(y_P)_i} \gamma_{P,i}$ is a unit in $\mathcal{O}_P$. With (4.3.o) follows

$$\mathcal{O}_{P_{i-1}}(E_i) = \mathcal{O}_{P_{i-1}}\big[(y_P)_i\big] = \mathcal{O}_{P_{i-1}}\big[(y_P)_i \delta_{(y_P)_i} \gamma_{P,i}\big] \tag{4.3.u}$$

for all $1 \le i \le t$ and each place P_{i-1} of E_{i-1} over P.

Since $l \ge 0$,

$$v_{Q'}\Big(\theta_{P,n} \big((y_P)_n \delta_{(y_P)_n} \big)^l \Big) \ge 0$$

for all places Q' of E over Q with $Q \in \mathcal{S} \setminus \{P\}$ follows from 4.1.5 and the definition of $\theta_{P,n}$. Now

$$\begin{aligned} v_{P_n} \Big(\theta_{P,n} \big((y_P)_n \delta_{(y_P)_n} \big)^l \Big) & \\ &= v_P\big(\theta_{P,n}\big) \cdot e(P_n|P) + l \cdot v_{P_n}\big((y_P)_n\big) + l \cdot v_P\big(\delta_{(y_P)_n}\big) \cdot e(P_n|P) \\ &= sp - l \cdot v_P\big(\delta_{(y_P)_n}\big) \cdot p - l \cdot \Lambda_{P,n} + l \cdot v_P\big(\delta_{(y_P)_n}\big) \cdot p \\ &= s \cdot p - l \cdot \Lambda_{P,n} \\ &= 1, \end{aligned}$$

for all places P_n of E over P. This gives (ii) and

$$\mathcal{O}_{P_t}(E_n) = \mathcal{O}_{P_t}\Big[\theta_{P,n} \big((y_P)_n \delta_{(y_P)_n} \big)^l \Big] \tag{4.3.v}$$

for all $P_t \in \mathbb{P}_{E_t}$ with $P_t | P$. (iii) follows with 4.1.3 from (4.3.u) and (4.3.v). □

We are now left with the task to find a set of generators for each $P \in B_r$, $1 \leq r < n$. Set $t := r - 1$, i. e. E_t the inertia field of P in E_n. For each $1 \leq i \leq t$ we use Strong Approximation to find $\gamma_{P,i} \in F$ with

$$\begin{aligned} &v_P\big(\gamma_{P,i}\big) = -v_P\big(\delta_{(y_P)_i}\big) \text{ and} \\ &v_Q(\gamma_{P,i}) \geq 0 \text{ for all } Q \in \mathcal{S} \setminus \{P\}. \end{aligned}$$

We have

$$y_n^p - y_n = u_n + z_{n-1} \in E_{n-1}.$$

Let $P_{t,1}, \ldots, P_{t,r}$ be all the places of E_t, $P_{n-1,1}, \ldots, P_{n-1,r}$ be all the places of E_{n-1} and $P_{n,1}, \ldots, P_{n,r}$ be all the places of E_n above P with $P_{n,j}|P_{n-1,j}|P_{t,j}$. Since each $P_{n-1,j}$ is totally ramified in the Artin-Schreier extension E_n/E_{n-1} we know from 3.2.1 that there exists an element $\rho_{P,j}$ of E_{n-1} such that

$$v_{P_{n-1,j}}\big(u_n + z_{n-1} + (\rho_{P,j}^p - \rho_{P,j})\big) =: -m_{P,j} < 0 \tag{4.3.w}$$

with $m_{P,j} \not\equiv 0 \mod p$. Therefore we can choose $l_{P,j}$ and $s_{P,j} \in \mathbb{Z}^{\geq 0}$ such that

$$s_{P,j} \cdot p^{n-t} - l_{P,j} \cdot m_{P,j} = 1.$$

(Note that $p^{n-t} = e(P_{n,j}|P_{t,j}) = e(P_{n,j}|P)$.) Now $y_n + \rho_{P,j}$ is an Artin-Schreier generator of E_n/E_{n-1},

$$(y_n + \rho_{P,j})^p - (y_n + \rho_{P,j}) = y_n^p - y_n + \rho_{P,j}^p - \rho_{P,j} = u_n + z_{n-1} + (\rho_{P,j}^p - \rho_{P,j})$$

and

$$v_{P_{n,j}}(y_n + \rho_{P,j}) = \frac{1}{p} \cdot v_{P_{n,j}}\big(u_n + z_{n-1} + (\rho_{P,j}^p - \rho_{P,j})\big) = -m_{P,j}.$$

Select $\theta_{P,n,j} \in F$ with

$$\begin{aligned} &v_P(\theta_{P,n,j}) = s_{P,j} - l_{P,j} \cdot v_P\big(\delta_{(y_n+\rho_{P,j})}\big) \text{ and} \\ &v_Q(\theta_{P,n,j}) \geq 0 \text{ for all } Q \in \mathcal{S},\ Q \neq P. \end{aligned}$$

4.3.7 Proposition ($\mathcal{S}$-integral $\mathcal{O}_P$-generators of $\mathcal{O}_P(E)$ for $P \in B_r$, $1 \le r < n$). *Suppose we are in the situation just described. We set*

$$\Omega_P := \Big\{ (y_P)_i \delta_{(y_P)_i} \gamma_{P,i} \;\Big|\; 1 \le i \le t \Big\} \cup \Big\{ \theta_{P,n,j} \big((y_n + \rho_{P,j}) \delta_{(y_n+\rho_{P,j})} \big)^{l_{P,j}} \;\Big|\; 1 \le j \le r \Big\}. \tag{4.3.x}$$

Then

(i) $(y_P)_i \delta_{(y_P)_i} \gamma_{P,i} \in \mathcal{O}_{\mathcal{S}}(E)$ *for each* $1 \le i \le t$.

(ii) $\theta_{P,n,j} \big((y_n + \rho_{P,j}) \delta_{(y_n+\rho_{P,j})} \big)^{l_{P,j}} \in \mathcal{O}_{\mathcal{S}}(E)$ *for all* $1 \le j \le r$.

(iii) $\mathcal{O}_P(E_n) = \mathcal{O}_P\big[\Omega_P\big]$.

Proof. Like before, (i) and

$$v_{Q'} \Big(\theta_{P,n,j} \big((y_n + \rho_{P,j}) \delta_{(y_n+\rho_{P,j})} \big)^{l_{P,j}} \Big) \ge 0$$

for all places Q' of E over Q with $Q \in \mathcal{S} \setminus \{P\}$ and all $1 \le j \le r$ follow from 4.1.5 and the definition of $\gamma_{P,i}$ and $\theta_{P,n,j}$, respectively . Now

$$\begin{aligned} & v_{P_{n,j}} \Big(\theta_{P,n,j} \big((y_n + \rho_{P,j}) \delta_{(y_n+\rho_{P,j})} \big)^{l_{P,j}} \Big) \\ &= v_P\big(\theta_{P,n,j}\big) \cdot e(P_{n,j}|P) + l_{P,j} \cdot v_{P_{n,j}}\big(y_n + \rho_{P,j}\big) + l_{P,j} \cdot v_P\big(\delta_{(y_n+\rho_{P,j})}\big) \cdot e(P_{n,j}|P) \\ &= s_{P,j} p^{n-t} - l_{P,j} \cdot v_P\big(\delta_{(y_n+\rho_{P,j})}\big) \cdot p^{n-t} - l_{P,j} \cdot m_{P,j} + l_{P,j} \cdot v_P\big(\delta_{(y_n+\rho_{P,j})}\big) \cdot p^{n-t} \\ &= s \cdot p^{n-t} - l_{P,j} \cdot m_{P,j} \\ &= 1 \end{aligned}$$

for all $1 \le j \le r$. This gives (ii) and

$$\mathcal{O}_{P_{t,j}}(E_n) = \mathcal{O}_{P_{t,j}} \Big[\theta_{P,n,j} \big((y_n + \rho_{P,j}) \delta_{(y_n+\rho_{P,j})} \big)^{l_{P,j}} \Big] \tag{4.3.y}$$

for all $1 \le j \le r$. Since $v_P\big(\delta_{(y_P)_i} \gamma_{P,i}\big) = 0$ for each $1 \le i \le t$ and each place P_{i-1} of E_{i-1} over P, $\delta_{(y_P)_i} \gamma_{P,i}$ is a unit in $\mathcal{O}_P$ and therefore (by (4.3.o)) we have

$$\mathcal{O}_{P_{i-1}}(E_i) = \mathcal{O}_{P_{i-1}}\big[(y_P)_i\big] = \mathcal{O}_{P_{i-1}}\big[(y_P)_i \delta_{(y_P)_i} \gamma_{P,i}\big]. \tag{4.3.z}$$

(iii) now follows with 4.1.2 and 4.1.3 from (4.3.z) and (4.3.y). □

Like for Kummer extensions in the last section, we now summarize the above results and give an algorithm which computes for each Artin-Schreier-Witt extension E of a function field F and each $\emptyset \ne \mathcal{S} \subsetneqq \mathbb{P}_F$ a set of $\mathcal{O}_{\mathcal{S}}$-generators of $\mathcal{O}_{\mathcal{S}}(E)$:

4.3.8 Algorithm.

Input: An Artin-Schreier-Witt extension $E = F(y)/F$ and $\emptyset \neq \mathcal{S} \subsetneqq \mathbb{P}_F$.

Output: A set Ω of $\mathcal{O}_\mathcal{S}$-generators of $\mathcal{O}_\mathcal{S}(E)$.

1. Compute the set A' (see (4.3.q)).
2. Compute the sets $B_1, \ldots, B_{n+1}$ (see (4.3.k) and (4.3.l)) using algorithm 4.3.3.
3. Compute $\Omega_{A \setminus A'}$ as in Proposition 4.3.4.
4. For each $P \in A'$ compute Ω_P (see (4.3.r)) and set
$$\Omega_{A'} := \bigcup_{P \in A'} \Omega_P.$$
5. For each $P \in B$ compute Ω_P (see (4.3.s)) and set
$$\Omega_B := \bigcup_{P \in B} \Omega_P.$$
6. For each $1 \leq i \leq n$ and each $P \in B_i$ compute Ω_P (see (4.3.t) and (4.3.x)) and set
$$\Omega_{B_i} := \bigcup_{P \in B_i} \Omega_P.$$
7. **return** $\Omega := \Omega_{A \setminus A'} \cup \Omega_{A'} \cup \Omega_B \cup \Omega_{B_1} \cup \cdots \cup \Omega_{B_n}$.

The correctness of this algorithm follows from

$$\mathcal{S} = A \setminus A' \cup A' \cup B \cup B_1 \cup \cdots \cup B_n$$

and Theorem 4.1.1. We have shown that the sets $\Omega_{A \setminus A'}$, $\Omega_{A'}$, Ω_B and Ω_{B_i}, $1 \leq i \leq n$, are contained in $\mathcal{O}_\mathcal{S}(E)$. They are finite since A', B and B_i, $1 \leq i \leq n$, are finite. Therefore Ω is a finite subset of $\mathcal{O}_\mathcal{S}(E)$.

Chapter 5

Examples

In this final chapter we examine a list of examples and compare our method to compute a maximal order of a Kummer or Artin-Schreier-Witt extension E of a global function field F with the Round 2 based method.

In most of the examples we compute the finite maximal order $\mathcal{O}_E^0$ of E, in one group of examples the infinite maximal order $\mathcal{O}_E^\infty$. We list the examples in single consecutively numbered tables. We now describe the table entries whose meaning is not obvious.

T1 is the time our algorithm needed for the computation. With the implementation we used the actual calculation of the generators (which is done using algorithm 4.2.4 and 4.3.8, respectively) takes less than 1 percent of the time T1. The most part is needed for creating the order which is spanned by these generators.

$\mathrm{disc}\big(\mathcal{O}_E^0\big)$ denotes the discriminant of $\mathcal{O}_E^0$ and $\mathrm{ind}_1\big(\mathcal{O}_E^0\big)$ the index of $\mathcal{O}_E^0$ over the finite equation order $\mathcal{O}_{E,eq}^0$ of E. $\mathcal{O}_{E,eq}^0$ is defined in the following way: Let F/k be a function field with finite maximal order $\mathcal{O}_F^0$ and $E = F(y)$, $g(y) = 0$ for some irreducible polynomial

$$g(t) = t^n + \frac{a_{n-1}}{b_{n-1}} t^{n-1} + \cdots + \frac{a_0}{b_0} \in F[t],$$

where $a_i, b_i \in \mathcal{O}_F^0$. If d is a (lowest) common multiple of $b_0, \ldots, b_{n-1}$, then dy is a zero of the irreducible polynomial

$$(dt)^n + \frac{a_{n-1}}{b_{n-1}} d(dt)^{n-1} + \cdots + \frac{a_0}{b_0} d^n,$$

which has coefficients in $\mathcal{O}_F^0$. We set $\mathcal{O}_{E,eq}^0 := \mathcal{O}_F^0[dy]$. Now, T2 is the time which the Round 2 algorithm needed to compute the maximal order as an

overorder of $\mathcal{O}^0_{E,eq}$. Since in our cases $\mathrm{ind}_1\big(\mathcal{O}^0_E\big)$ is an ideal which has prime factors of fairly high degree, this method soon reaches its limits. To overcome this problem and get more realistic times to compare our algorithm with, in most of the examples we also include the time T3 which the Round 2 algorithm needed to compute $\mathcal{O}^0_E$ as an overorder of another order $\mathcal{O}^0_{E,1} \supseteq \mathcal{O}^0_{E,eq}$, whose index in $\mathcal{O}^0_E$ has less prime factors with smaller powers. We denote this index by $\mathrm{ind}_2\big(\mathcal{O}^0_E\big)$. To get $\mathcal{O}^0_{E,1}$ we set $h := \frac{gd}{t-y} \in E[t]$. Then g is a polynomial with coefficients $\beta_0, \ldots, \beta_{n-1} \in \mathcal{O}^0_E$ and

$$\mathcal{O}^0_{E,1} := \mathcal{O}^0_F[\beta_0, \ldots, \beta_{n-1}]$$

is an overorder of $\mathcal{O}^0_{E,eq}$ (see [BLP93, p. 88]).

The corresponding symbols $\mathrm{disc}\big(\mathcal{O}^\infty_E\big)$, $\mathrm{ind}_1\big(\mathcal{O}^\infty_E\big)$ and $\mathrm{ind}_2\big(\mathcal{O}^\infty_E\big)$ for the infinite maximal orders are defined in an analogous way.

We write "???" in the cases where the computation of the maximal order was not finished after more than two days.

All computations have been carried out with the computer algebra system MAGMA [C$^+$04] on a Pentium IV, 2.8 GHz, 1024 MB-RAM.

5.1 Kummer extensions

In this section we look at three groups of examples of Kummer extensions E/F. We examine the runtime of both methods with increasing degree n of the extension. We always start with a field k of p elements, p a natural prime, then adjoin a primitive n-th root of unity to k to get the field $\mathbb{F}_q$, q a power of p. In the third row of each table we print the defining equation $f(x, \rho) = 0$ of the function field $F = \mathbb{F}_q(x, \rho)$.

In the first group of examples we compute the finite maximal order $\mathcal{O}^0_E$ of E.

1.	T1 = 62 s T2 = 621 s T3 = 104 s
$q = 5^5, \quad [F : \mathbb{F}_q(x)] = 5, \quad n = 11$	
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^5 + 4\rho^4 + x^2\rho^3 + 2\rho^2 + x^5\rho + x + 1 = 0$	
$E = F(y)$: $\quad y^n - u = 0, \quad u = \frac{x^{11}+4x^{10}+x^8+4x^7+x^5+4x^4+x^2+4x+1}{x^4+4x^3+x+4}\rho^4 + \frac{1}{x^2+3}\rho + x^2$	
$\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{10}\mathfrak{p}_2^{10}\mathfrak{p}_3^{10}\mathfrak{p}_4^{10}\mathfrak{p}_5^{10}\mathfrak{p}_6^{10}\mathfrak{p}_7^{10}\mathfrak{p}_8^{10}\mathfrak{p}_9^{10}\mathfrak{p}_{10}^{10}\mathfrak{p}_{11}^{10}\mathfrak{p}_{12}^{10}\mathfrak{p}_{13}^{10}\mathfrak{p}_{14}^{10}\mathfrak{p}_{15}^{10}\mathfrak{p}_{16}^{10}\mathfrak{p}_{17}^{10}$	
$\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{45}\mathfrak{p}_2^{45}\mathfrak{p}_3^{45}\mathfrak{p}_7^{45}\mathfrak{p}_8^{45}\mathfrak{p}_{11}^{45}\mathfrak{p}_{12}^{45}\mathfrak{p}_{13}^{45}\mathfrak{p}_{14}^{45}\mathfrak{p}_{18}^{55}$	
$\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_{18}^{10}$	

2.	T1 = 69 s T2 = 570 s T3 = 146 s
$q = 5^2, \quad [F : \mathbb{F}_q(x)] = 5, \quad n = 12$	
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^5 + 4\rho^4 + x^2\rho^3 + 2\rho^2 + x^5\rho + x + 1 = 0$	
$E = F(y)$: $\quad y^n - u = 0, \quad u = \frac{x^{11}+4x^{10}+x^8+4x^7+x^5+4x^4+x^2+4x+1}{x^4+4x^3+x+4}\rho^4 + \frac{1}{x^2+3}\rho + x^2$	
$\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{11}\mathfrak{p}_2^{11}\mathfrak{p}_3^{11}\mathfrak{p}_4^{11}\mathfrak{p}_5^{11}\mathfrak{p}_6^{11}\mathfrak{p}_7^{11}\mathfrak{p}_8^{11}\mathfrak{p}_9^{11}\mathfrak{p}_{10}^{11}\mathfrak{p}_{11}^{11}\mathfrak{p}_{11}^{11}\mathfrak{p}_{13}^{11}\mathfrak{p}_{14}^{11}\mathfrak{p}_{15}^{11}\mathfrak{p}_{16}^{11}\mathfrak{p}_{17}^{11}\mathfrak{p}_{18}^{11}\mathfrak{p}_{19}^{11}\mathfrak{p}_{20}^{11}\mathfrak{p}_{21}^{11}\mathfrak{p}_{22}^{11}$	
$\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{55}\mathfrak{p}_2^{55}\mathfrak{p}_3^{55}\mathfrak{p}_4^{55}\mathfrak{p}_6^{55}\mathfrak{p}_7^{55}\mathfrak{p}_8^{55}\mathfrak{p}_{11}^{55}\mathfrak{p}_{12}^{55}\mathfrak{p}_{13}^{55}\mathfrak{p}_{15}^{55}\mathfrak{p}_{23}^{66}$	
$\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_{23}^{11}$	

3.	T1 = 100 s T2 = 1533 s T3 = 248 s
$q = 5^4, \quad [F : \mathbb{F}_q(x)] = 5, \quad n = 13$	
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^5 + 4\rho^4 + x^2\rho^3 + 2\rho^2 + x^5\rho + x + 1 = 0$	
$E = F(y)$: $\quad y^n - u = 0, \quad u = \frac{x^{11}+4x^{10}+x^8+4x^7+x^5+4x^4+x^2+4x+1}{x^4+4x^3+x+4}\rho^4 + \frac{1}{x^2+3}\rho + x^2$	
$\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{12}\mathfrak{p}_2^{12}\mathfrak{p}_3^{12}\mathfrak{p}_4^{12}\mathfrak{p}_5^{12}\mathfrak{p}_6^{12}\mathfrak{p}_7^{12}\mathfrak{p}_8^{12}\mathfrak{p}_9^{12}\mathfrak{p}_{10}^{12}\mathfrak{p}_{11}^{12}\mathfrak{p}_{12}^{12}\mathfrak{p}_{13}^{12}\mathfrak{p}_{14}^{12}\mathfrak{p}_{15}^{12}\mathfrak{p}_{16}^{12}\mathfrak{p}_{17}^{12}\mathfrak{p}_{18}^{12}\mathfrak{p}_{19}^{12}\mathfrak{p}_{20}^{12}\mathfrak{p}_{21}^{12}$ $\mathfrak{p}_{22}^{12}\mathfrak{p}_{23}^{12}\mathfrak{p}_{24}^{12}\mathfrak{p}_{25}^{12}\mathfrak{p}_{26}^{12}\mathfrak{p}_{27}^{12}\mathfrak{p}_{28}^{12}\mathfrak{p}_{29}^{12}\mathfrak{p}_{30}^{12}\mathfrak{p}_{31}^{12}\mathfrak{p}_{32}^{12}$	
$\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{66}\mathfrak{p}_2^{66}\mathfrak{p}_3^{66}\mathfrak{p}_4^{66}\mathfrak{p}_6^{66}\mathfrak{p}_7^{66}\mathfrak{p}_8^{66}\mathfrak{p}_{11}^{66}\mathfrak{p}_{12}^{66}\mathfrak{p}_{13}^{66}\mathfrak{p}_{15}^{66}\mathfrak{p}_{16}^{66}\mathfrak{p}_{17}^{66}\mathfrak{p}_{18}^{66}\mathfrak{p}_{19}^{66}\mathfrak{p}_{20}^{66}\mathfrak{p}_{21}^{66}\mathfrak{p}_{22}^{66}\mathfrak{p}_{23}^{66}\mathfrak{p}_{24}^{66}\mathfrak{p}_{25}^{66}\mathfrak{p}_{33}^{78}$	
$\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_{33}^{12}$	

4.	T1 = 145 s T2 = 1913 s T3 = 305 s
$q = 5^6, \quad [F : \mathbb{F}_q(x)] = 5, \quad n = 14$	
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^5 + 4\rho^4 + x^2\rho^3 + 2\rho^2 + x^5\rho + x + 1 = 0$	
$E = F(y)$: $\quad y^n - u = 0, \quad u = \frac{x^{11}+4x^{10}+x^8+4x^7+x^5+4x^4+x^2+4x+1}{x^4+4x^3+x+4}\rho^4 + \frac{1}{x^2+3}\rho + x^2$	
$\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{13}\mathfrak{p}_2^{13}\mathfrak{p}_3^{13}\mathfrak{p}_4^{13}\mathfrak{p}_5^{13}\mathfrak{p}_6^{13}\mathfrak{p}_7^{13}\mathfrak{p}_8^{13}\mathfrak{p}_9^{13}\mathfrak{p}_{10}^{13}\mathfrak{p}_{11}^{13}\mathfrak{p}_{12}^{13}\mathfrak{p}_{13}^{13}\mathfrak{p}_{14}^{13}\mathfrak{p}_{15}^{13}\mathfrak{p}_{16}^{13}\mathfrak{p}_{17}^{13}\mathfrak{p}_{18}^{13}\mathfrak{p}_{19}^{13}\mathfrak{p}_{20}^{13}\mathfrak{p}_{21}^{13}$ $\mathfrak{p}_{22}^{13}\mathfrak{p}_{23}^{13}\mathfrak{p}_{24}^{13}\mathfrak{p}_{25}^{13}\mathfrak{p}_{26}^{13}$	
$\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{78}\mathfrak{p}_2^{78}\mathfrak{p}_3^{78}\mathfrak{p}_4^{78}\mathfrak{p}_5^{78}\mathfrak{p}_6^{78}\mathfrak{p}_{10}^{78}\mathfrak{p}_{11}^{78}\mathfrak{p}_{12}^{78}\mathfrak{p}_{13}^{78}\mathfrak{p}_{14}^{78}\mathfrak{p}_{15}^{78}\mathfrak{p}_{16}^{78}\mathfrak{p}_{19}^{78}\mathfrak{p}_{20}^{78}\mathfrak{p}_{27}^{91}$	
$\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_{27}^{13}$	

5.	T1 = 338 s T2 = 3441 s T3 = 603 s
$q = 5^4, \quad [F : \mathbb{F}_q(x)] = 5, \quad n = 16$	
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^5 + 4\rho^4 + x^2\rho^3 + 2\rho^2 + x^5\rho + x + 1 = 0$	
$E = F(y)$: $\quad y^n - u = 0, \quad u = \frac{x^{11}+4x^{10}+x^8+4x^7+x^5+4x^4+x^2+4x+1}{x^4+4x^3+x+4}\rho^4 + \frac{1}{x^2+3}\rho + x^2$	
$\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{15}\mathfrak{p}_2^{15}\mathfrak{p}_3^{15}\mathfrak{p}_4^{15}\mathfrak{p}_5^{15}\mathfrak{p}_6^{15}\mathfrak{p}_7^{15}\mathfrak{p}_8^{15}\mathfrak{p}_9^{15}\mathfrak{p}_{10}^{15}\mathfrak{p}_{11}^{15}\mathfrak{p}_{12}^{15}\mathfrak{p}_{13}^{15}\mathfrak{p}_{14}^{15}\mathfrak{p}_{15}^{15}\mathfrak{p}_{16}^{15}\mathfrak{p}_{17}^{15}\mathfrak{p}_{18}^{15}\mathfrak{p}_{19}^{15}\mathfrak{p}_{20}^{15}\mathfrak{p}_{21}^{15}$ $\mathfrak{p}_{22}^{15}\mathfrak{p}_{23}^{15}\mathfrak{p}_{24}^{15}\mathfrak{p}_{25}^{15}\mathfrak{p}_{26}^{15}\mathfrak{p}_{27}^{15}\mathfrak{p}_{28}^{15}\mathfrak{p}_{29}^{15}\mathfrak{p}_{30}^{15}\mathfrak{p}_{31}^{15}\mathfrak{p}_{32}^{15}$	
$\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{105}\mathfrak{p}_2^{105}\mathfrak{p}_3^{105}\mathfrak{p}_4^{105}\mathfrak{p}_6^{105}\mathfrak{p}_7^{105}\mathfrak{p}_8^{105}\mathfrak{p}_{11}^{105}\mathfrak{p}_{12}^{105}\mathfrak{p}_{13}^{105}\mathfrak{p}_{15}^{105}\mathfrak{p}_{16}^{105}\mathfrak{p}_{17}^{105}\mathfrak{p}_{18}^{105}\mathfrak{p}_{19}^{105}\mathfrak{p}_{20}^{105}\mathfrak{p}_{21}^{105}$ $\mathfrak{p}_{22}^{105}\mathfrak{p}_{23}^{105}\mathfrak{p}_{24}^{105}\mathfrak{p}_{25}^{105}\mathfrak{p}_{33}^{120}$	
$\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_{33}^{15}$	

6.	T1 = 843 s T2 = 10209 s T3 = 1305 s
$q = 5^2, \quad [F : \mathbb{F}_q(x)] = 5, \quad n = 24$	
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^5 + 4\rho^4 + x^2\rho^3 + 2\rho^2 + x^5\rho + x + 1 = 0$	
$E = F(y)$: $\quad y^n - u = 0, \quad u = \frac{x^{11}+4x^{10}+x^8+4x^7+x^5+4x^4+x^2+4x+1}{x^4+4x^3+x+4}\rho^4 + \frac{1}{x^2+3}\rho + x^2$	
$\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{23}\mathfrak{p}_2^{23}\mathfrak{p}_3^{23}\mathfrak{p}_4^{23}\mathfrak{p}_5^{23}\mathfrak{p}_6^{23}\mathfrak{p}_7^{23}\mathfrak{p}_8^{23}\mathfrak{p}_9^{23}\mathfrak{p}_{10}^{23}\mathfrak{p}_{11}^{23}\mathfrak{p}_{12}^{23}\mathfrak{p}_{13}^{23}\mathfrak{p}_{14}^{23}\mathfrak{p}_{15}^{23}\mathfrak{p}_{16}^{23}\mathfrak{p}_{17}^{23}\mathfrak{p}_{18}^{23}\mathfrak{p}_{19}^{23}\mathfrak{p}_{20}^{23}\mathfrak{p}_{21}^{23}\mathfrak{p}_{22}^{23}$	
$\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{253}\mathfrak{p}_2^{253}\mathfrak{p}_3^{253}\mathfrak{p}_4^{253}\mathfrak{p}_5^{253}\mathfrak{p}_6^{253}\mathfrak{p}_7^{253}\mathfrak{p}_8^{253}\mathfrak{p}_9^{253}\mathfrak{p}_{10}^{253}\mathfrak{p}_{11}^{253}\mathfrak{p}_{12}^{253}\mathfrak{p}_{13}^{253}\mathfrak{p}_{14}^{253}\mathfrak{p}_{15}^{253}\mathfrak{p}_{23}^{276}$	
$\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_{23}^{23}$	

The difference between the next examples and the previous is that the indices $\operatorname{ind}_1(\mathcal{O}_E^0)$ and $\operatorname{ind}_2(\mathcal{O}_E^0)$ have prime factors of higher degree. Here we observe that our method yields much better results compared to the Round 2 algorithm.

7.	T1 = 5 s T2 = 2581 s T3 = 539 s
$q = 3^6, \quad [F : \mathbb{F}_q(x)] = 2, \quad n = 28$	
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^2 + 2\rho + x^3 + x + 1 = 0$	
$E = F(y)$: $\quad y^n - u = 0, \quad u = \frac{1}{x^2}\rho + x^2$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{24}\mathfrak{p}_2^{27}\mathfrak{p}_3^{27}\mathfrak{p}_4^{27}\mathfrak{p}_5^{27}\mathfrak{p}_6^{27}\mathfrak{p}_7^{27}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{1446}$ $\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_1^{42}$	

8.	T1 = 14 s T2 = 15989 s T3 = 4160 s
$q = 3^{30}, \quad [F : \mathbb{F}_q(x)] = 2, \quad n = 31$	
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^2 + 2\rho + x^3 + x + 1 = 0$	
$E = F(y)$: $\quad y^n - u = 0, \quad u = \frac{1}{x^2}\rho + x^2$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{30}\mathfrak{p}_2^{30}\mathfrak{p}_3^{30}\mathfrak{p}_4^{30}\mathfrak{p}_5^{30}\mathfrak{p}_6^{30}\mathfrak{p}_7^{30}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{1785}$ $\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_1^{45}$	

9.	T1 = 15 s T2 = 6894 s T3 = 1720 s
$q = 3^4, \quad [F : \mathbb{F}_q(x)] = 2, \quad n = 40$	
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^2 + 2\rho + x^3 + x + 1 = 0$	
$E = F(y)$: $\quad y^n - u = 0, \quad u = \frac{1}{x^2}\rho + x^2$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{36}\mathfrak{p}_2^{39}\mathfrak{p}_3^{39}\mathfrak{p}_4^{39}\mathfrak{p}_5^{39}\mathfrak{p}_6^{39}\mathfrak{p}_7^{39}\mathfrak{p}_8^{39}\mathfrak{p}_9^{39}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{3024}$ $\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_1^{60}$	

10. T1 = 37 s T2 = ??? T3 = 29264 s
$q = 3^{10}, \quad [F : \mathbb{F}_q(x)] = 2, \quad n = 61$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^2 + 2\rho + x^3 + x + 1 = 0$
$E = F(y)$: $\quad y^n - u = 0, \quad u = \frac{1}{x^2}\rho + x^2$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{60}\mathfrak{p}_2^{60}\mathfrak{p}_3^{60}\mathfrak{p}_4^{60}\mathfrak{p}_5^{60}\mathfrak{p}_6^{60}\mathfrak{p}_7^{60}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{7170}$ $\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_1^{90}$

11. T1 = 975 s T2 = ??? T3 = ???
$q = 3^{20}, \quad [F : \mathbb{F}_q(x)] = 2, \quad n = 100$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^2 + 2\rho + x^3 + x + 1 = 0$
$E = F(y)$: $\quad y^n - u = 0, \quad u = \frac{1}{x^2}\rho + x^2$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{96}\mathfrak{p}_2^{99}\mathfrak{p}_3^{99}\mathfrak{p}_4^{99}\mathfrak{p}_5^{99}\mathfrak{p}_6^{99}\mathfrak{p}_7^{99}\mathfrak{p}_8^{99}\mathfrak{p}_9^{99}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{19554}$

12. T1 = 367 s T2 = ??? T3 = ???
$q = 3^{10}, \quad [F : \mathbb{F}_q(x)] = 2, \quad n = 122$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^2 + 2\rho + x^3 + x + 1 = 0$
$E = F(y)$: $\quad y^n - u = 0, \quad u = \frac{1}{x^2}\rho + x^2$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{120}\mathfrak{p}_2^{121}\mathfrak{p}_3^{121}\mathfrak{p}_4^{121}\mathfrak{p}_5^{121}\mathfrak{p}_6^{121}\mathfrak{p}_7^{121}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{29222}$

13. T1 = 1751 s T2 = ??? T3 = ???
$q = 3^{12}, \quad [F : \mathbb{F}_q(x)] = 2, \quad n = 140$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^2 + 2\rho + x^3 + x + 1 = 0$
$E = F(y)$: $\quad y^n - u = 0, \quad u = \frac{1}{x^2}\rho + x^2$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{136}\mathfrak{p}_2^{139}\mathfrak{p}_3^{139}\mathfrak{p}_4^{139}\mathfrak{p}_5^{139}\mathfrak{p}_6^{139}\mathfrak{p}_7^{139}\mathfrak{p}_8^{139}\mathfrak{p}_9^{139}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{38574}$

14. T1 = 3276 s T2 = ??? T3 = ???
$q = 3^8, \quad [F : \mathbb{F}_q(x)] = 2, \quad n = 160$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^2 + 2\rho + x^3 + x + 1 = 0$
$E = F(y)$: $\quad y^n - u = 0, \quad u = \frac{1}{x^2}\rho + x^2$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{156}\mathfrak{p}_2^{159}\mathfrak{p}_3^{159}\mathfrak{p}_4^{159}\mathfrak{p}_5^{159}\mathfrak{p}_6^{159}\mathfrak{p}_7^{159}\mathfrak{p}_8^{159}\mathfrak{p}_9^{159}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{50484}$

In the last group of examples in this section we compute the infinite maximal order $\mathcal{O}_E^\infty$ of the Kummer extension E.

15. T1 = 1 s T2 = 33 s T3 = 8 s
$q = 3^4, \quad [F : \mathbb{F}_q(x)] = 3, \quad n = 5$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^n - u = 0, \quad u = (x^3+2)\rho^2 + (x^2+1)\rho + 1$ $\operatorname{disc}(\mathcal{O}_E^\infty) = \mathfrak{p}_1^4$ $\operatorname{ind}_1(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{170}$ $\operatorname{ind}_2(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{44}$

16. T1 = 3 s T2 = 437 s T3 = 43 s
$q = 3^4, \quad [F : \mathbb{F}_q(x)] = 3, \quad n = 10$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^n - u = 0, \quad u = (x^3+2)\rho^2 + (x^2+1)\rho + 1$ $\operatorname{disc}(\mathcal{O}_E^\infty) = \mathfrak{p}_1^9$ $\operatorname{ind}_1(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{855}$ $\operatorname{ind}_2(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{99}$

17. T1 = 12 s T2 = 3459 s T3 = 212 s
$q = 3^4, \quad [F : \mathbb{F}_q(x)] = 3, \quad n = 16$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^n - u = 0, \quad u = (x^3+2)\rho^2 + (x^2+1)\rho + 1$ $\mathrm{disc}(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{15}$ $\mathrm{ind}_1(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{2370}$ $\mathrm{ind}_2(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{165}$

18. T1 = 18 s T2 = 6400 s T3 = 283 s
$q = 3^4, \quad [F : \mathbb{F}_q(x)] = 3, \quad n = 20$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^n - u = 0, \quad u = (x^3+2)\rho^2 + (x^2+1)\rho + 1$ $\mathrm{disc}(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{19}$ $\mathrm{ind}_1(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{3800}$ $\mathrm{ind}_2(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{209}$

19. T1 = 385 s T2 = 32722 s T3 = 1645 s
$q = 3^{11}, \quad [F : \mathbb{F}_q(x)] = 3, \quad n = 23$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^n - u = 0, \quad u = (x^3+2)\rho^2 + (x^2+1)\rho + 1$ $\mathrm{disc}(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{22}$ $\mathrm{ind}_1(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{5093}$ $\mathrm{ind}_2(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{246}$

20. T1 = 2060 s T2 = ??? T3 = 12302 s
$q = 3^{28}, \quad [F : \mathbb{F}_q(x)] = 3, \quad n = 29$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^n - u = 0, \quad u = (x^3+2)\rho^2 + (x^2+1)\rho + 1$ $\operatorname{disc}(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{28}$ $\operatorname{ind}_1(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{8246}$ $\operatorname{ind}_2(\mathcal{O}_E^\infty) = \mathfrak{p}_1^{308}$

5.2 Artin-Schreier-Witt Extensions

In the first group of examples (1. - 10.) we compute the finite maximal order of different Artin-Schreier extensions. In every step we increase the degree p of the extension.

1. T1 = 3 s T2 = 22 s T3 = 16 s
$p = 5, \quad q = 5, \quad [F : \mathbb{F}_q(x)] = 3,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^8\mathfrak{p}_2^8\mathfrak{p}_3^8\mathfrak{p}_4^8\mathfrak{p}_5^8\mathfrak{p}_6^8\mathfrak{p}_7^8\mathfrak{p}_8^8\mathfrak{p}_9^8\mathfrak{p}_{10}^8\mathfrak{p}_{11}^8$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{46}\mathfrak{p}_2^{46}\mathfrak{p}_3^{46}\mathfrak{p}_4^6\mathfrak{p}_5^6\mathfrak{p}_6^6\mathfrak{p}_7^6\mathfrak{p}_8^6\mathfrak{p}_9^6\mathfrak{p}_{10}^6\mathfrak{p}_{11}^6\mathfrak{p}_{12}^{10}$ $\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_1^{16}\mathfrak{p}_2^{16}\mathfrak{p}_3^{16}\mathfrak{p}_{12}^4$

2. T1 = 4 s T2 = 77 s T3 = 18 s
$p = 7, \quad q = 7, \quad [F : \mathbb{F}_q(x)] = 3,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{36}\mathfrak{p}_2^{36}\mathfrak{p}_3^{36}\mathfrak{p}_4^{12}\mathfrak{p}_5^{12}\mathfrak{p}_6^{12}\mathfrak{p}_7^{12}\mathfrak{p}_8^{12}\mathfrak{p}_9^{12}\mathfrak{p}_{10}^{12}\mathfrak{p}_{11}^{18}\mathfrak{p}_{12}^{12}\mathfrak{p}_{13}^{12}\mathfrak{p}_{14}^{12}\mathfrak{p}_{15}^{12}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{87}\mathfrak{p}_2^{87}\mathfrak{p}_3^{87}\mathfrak{p}_4^{15}\mathfrak{p}_5^{15}\mathfrak{p}_6^{15}\mathfrak{p}_7^{15}\mathfrak{p}_8^{15}\mathfrak{p}_9^{15}\mathfrak{p}_{10}^{15}\mathfrak{p}_{11}^{33}\mathfrak{p}_{12}^{15}\mathfrak{p}_{13}^{15}\mathfrak{p}_{14}^{15}\mathfrak{p}_{15}^{15}$ $\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_1^{12}\mathfrak{p}_2^{12}\mathfrak{p}_3^{12}\mathfrak{p}_{11}^3$

3.	T1 = 5 s T2 = 499 s T3 = 63 s
$p = 11, \quad q = 11, \quad [F : \mathbb{F}_q(x)] = 3,$	
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$	
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{60}\mathfrak{p}_2^{60}\mathfrak{p}_3^{60}\mathfrak{p}_4^{20}\mathfrak{p}_5^{20}\mathfrak{p}_6^{20}\mathfrak{p}_7^{20}\mathfrak{p}_8^{20}\mathfrak{p}_9^{20}\mathfrak{p}_{10}^{20}\mathfrak{p}_{11}^{20}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{245}\mathfrak{p}_2^{245}\mathfrak{p}_3^{245}\mathfrak{p}_4^{45}\mathfrak{p}_5^{45}\mathfrak{p}_6^{45}\mathfrak{p}_7^{45}\mathfrak{p}_8^{45}\mathfrak{p}_9^{45}\mathfrak{p}_{10}^{45}\mathfrak{p}_{11}^{45}$ $\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_1^{20}\mathfrak{p}_2^{20}\mathfrak{p}_3^{20}$	

4.	T1 = 20 s T2 = 15073 s T3 = 1829 s
$p = 23, \quad q = 23, \quad [F : \mathbb{F}_q(x)] = 3,$	
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$	
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{132}\mathfrak{p}_2^{132}\mathfrak{p}_3^{132}\mathfrak{p}_4^{44}\mathfrak{p}_5^{44}\mathfrak{p}_6^{44}\mathfrak{p}_7^{44}\mathfrak{p}_8^{44}\mathfrak{p}_9^{44}\mathfrak{p}_{10}^{44}\mathfrak{p}_{11}^{44}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{1199}\mathfrak{p}_2^{1199}\mathfrak{p}_3^{1199}\mathfrak{p}_4^{231}\mathfrak{p}_5^{231}\mathfrak{p}_6^{231}\mathfrak{p}_7^{231}\mathfrak{p}_8^{231}\mathfrak{p}_9^{231}\mathfrak{p}_{10}^{231}\mathfrak{p}_{11}^{231}$ $\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_1^{44}\mathfrak{p}_2^{44}\mathfrak{p}_3^{44}$	

5.	T1 = 36 s T2 = 57512 s T3 = 4240 s
$p = 31, \quad q = 31, \quad [F : \mathbb{F}_q(x)] = 3,$	
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$	
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{180}\mathfrak{p}_2^{180}\mathfrak{p}_3^{180}\mathfrak{p}_4^{60}\mathfrak{p}_5^{60}\mathfrak{p}_6^{60}\mathfrak{p}_7^{60}\mathfrak{p}_8^{60}\mathfrak{p}_9^{60}\mathfrak{p}_{10}^{60}\mathfrak{p}_{11}^{60}\mathfrak{p}_{12}^{60}\mathfrak{p}_{13}^{60}\mathfrak{p}_{14}^{60}\mathfrak{p}_{15}^{60}\mathfrak{p}_{16}^{60}\mathfrak{p}_{17}^{60}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{2235}\mathfrak{p}_2^{2235}\mathfrak{p}_3^{2235}\mathfrak{p}_4^{435}\mathfrak{p}_5^{435}\mathfrak{p}_6^{435}\mathfrak{p}_7^{435}\mathfrak{p}_8^{435}\mathfrak{p}_9^{435}\mathfrak{p}_{10}^{435}\mathfrak{p}_{11}^{435}\mathfrak{p}_{12}^{435}\mathfrak{p}_{13}^{435}\mathfrak{p}_{14}^{435}\mathfrak{p}_{15}^{435}\mathfrak{p}_{16}^{435}\mathfrak{p}_{17}^{435}$ $\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_1^{60}\mathfrak{p}_2^{60}\mathfrak{p}_3^{60}$	

6.	T1 = 475 s T2 = 691322 s T3 = 35290 s
$p = 53, \quad q = 53, \quad [F : \mathbb{F}_q(x)] = 3,$	
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$	
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{312}\mathfrak{p}_2^{312}\mathfrak{p}_3^{312}\mathfrak{p}_4^{104}\mathfrak{p}_5^{104}\mathfrak{p}_6^{104}\mathfrak{p}_7^{104}\mathfrak{p}_8^{104}\mathfrak{p}_9^{104}\mathfrak{p}_{10}^{104}\mathfrak{p}_{11}^{104}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{6734}\mathfrak{p}_2^{6734}\mathfrak{p}_3^{6734}\mathfrak{p}_4^{1326}\mathfrak{p}_5^{1326}\mathfrak{p}_6^{1326}\mathfrak{p}_7^{1326}\mathfrak{p}_8^{1326}\mathfrak{p}_9^{1326}\mathfrak{p}_{10}^{1326}\mathfrak{p}_{11}^{1326}$ $\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_1^{104}\mathfrak{p}_2^{104}\mathfrak{p}_3^{104}$	

7.	T1 = 300 s T2 = ??? T3 = 79350 s
$p = 61, \quad q = 61, \quad [F : \mathbb{F}_q(x)] = 3,$	
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$	
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{360}\mathfrak{p}_2^{360}\mathfrak{p}_3^{360}\mathfrak{p}_4^{120}\mathfrak{p}_5^{120}\mathfrak{p}_6^{120}\mathfrak{p}_7^{120}\mathfrak{p}_8^{120}\mathfrak{p}_9^{120}\mathfrak{p}_{10}^{120}\mathfrak{p}_{11}^{120}\mathfrak{p}_{12}^{120}\mathfrak{p}_{13}^{120}\mathfrak{p}_{14}^{120}\mathfrak{p}_{15}^{120}\mathfrak{p}_{16}^{120}\mathfrak{p}_{17}^{120}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{8970}\mathfrak{p}_2^{8970}\mathfrak{p}_3^{8970}\mathfrak{p}_4^{1770}\mathfrak{p}_5^{1770}\mathfrak{p}_6^{1770}\mathfrak{p}_7^{1770}\mathfrak{p}_8^{1770}\mathfrak{p}_9^{1770}\mathfrak{p}_{10}^{1770}\mathfrak{p}_{11}^{1770}\mathfrak{p}_{12}^{1770}\mathfrak{p}_{13}^{1770}$ $\mathfrak{p}_{14}^{1770}\mathfrak{p}_{15}^{1770}\mathfrak{p}_{16}^{1770}\mathfrak{p}_{17}^{1770}$ $\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_1^{120}\mathfrak{p}_2^{120}\mathfrak{p}_3^{120}$	

8.	T1 = 488 s T2 = ??? T3 = ???
$p = 71, \quad q = 71, \quad [F : \mathbb{F}_q(x)] = 3,$	
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$	
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{420}\mathfrak{p}_2^{420}\mathfrak{p}_3^{420}\mathfrak{p}_4^{140}\mathfrak{p}_5^{140}\mathfrak{p}_6^{140}\mathfrak{p}_7^{140}\mathfrak{p}_8^{140}\mathfrak{p}_9^{140}\mathfrak{p}_{10}^{140}\mathfrak{p}_{11}^{140}\mathfrak{p}_{12}^{140}\mathfrak{p}_{13}^{140}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{12215}\mathfrak{p}_2^{12215}\mathfrak{p}_3^{12215}\mathfrak{p}_4^{2415}\mathfrak{p}_5^{2415}\mathfrak{p}_6^{2415}\mathfrak{p}_7^{2415}\mathfrak{p}_8^{2415}\mathfrak{p}_9^{2415}\mathfrak{p}_{10}^{2415}\mathfrak{p}_{11}^{2415}\mathfrak{p}_{12}^{2415}\mathfrak{p}_{13}^{2415}$	

9. T1 = 1859 s T2 = ??? T3 = ???
$p = 83, \quad q = 83, \quad [F : \mathbb{F}_q(x)] = 3,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{492}\mathfrak{p}_2^{492}\mathfrak{p}_3^{492}\mathfrak{p}_4^{164}\mathfrak{p}_5^{164}\mathfrak{p}_6^{164}\mathfrak{p}_7^{164}\mathfrak{p}_8^{164}\mathfrak{p}_9^{164}\mathfrak{p}_{10}^{164}\mathfrak{p}_{11}^{164}\mathfrak{p}_{12}^{164}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{16769}\mathfrak{p}_2^{16769}\mathfrak{p}_3^{16769}\mathfrak{p}_4^{3321}\mathfrak{p}_5^{3321}\mathfrak{p}_6^{3321}\mathfrak{p}_7^{3321}\mathfrak{p}_8^{3321}\mathfrak{p}_9^{3321}\mathfrak{p}_{10}^{3321}\mathfrak{p}_{11}^{3321}\mathfrak{p}_{12}^{3321}$

10. T1 = 62226 s T2 = ??? T3 = ???
$p = 97, \quad q = 97, \quad [F : \mathbb{F}_q(x)] = 3,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{576}\mathfrak{p}_2^{576}\mathfrak{p}_3^{576}\mathfrak{p}_4^{192}\mathfrak{p}_5^{192}\mathfrak{p}_6^{192}\mathfrak{p}_7^{192}\mathfrak{p}_8^{192}\mathfrak{p}_9^{192}\mathfrak{p}_{10}^{192}\mathfrak{p}_{11}^{192}\mathfrak{p}_{12}^{192}\mathfrak{p}_{13}^{192}\mathfrak{p}_{14}^{192}\mathfrak{p}_{15}^{192}\mathfrak{p}_{16}^{192}\mathfrak{p}_{17}^{192}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{22992}\mathfrak{p}_2^{22992}\mathfrak{p}_3^{22992}\mathfrak{p}_4^{4560}\mathfrak{p}_5^{4560}\mathfrak{p}_6^{4560}\mathfrak{p}_7^{4560}\mathfrak{p}_8^{4560}\mathfrak{p}_9^{4560}\mathfrak{p}_{10}^{4560}\mathfrak{p}_{11}^{4560}\mathfrak{p}_{12}^{4560}\mathfrak{p}_{13}^{4560}$ $\mathfrak{p}_{14}^{4560}\mathfrak{p}_{15}^{4560}\mathfrak{p}_{16}^{4560}\mathfrak{p}_{17}^{4560}$

In the next examples (11. - 17.) we consider a fixed Artin-Schreier extension E/F and compute the finite maximal order of constant field extensions of E.

11. T1 = 9 s T2 = 1141 s T3 = 192 s
$p = 13, \quad q = 13, \quad [F : \mathbb{F}_q(x)] = 3,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{72}\mathfrak{p}_2^{72}\mathfrak{p}_3^{72}\mathfrak{p}_4^{24}\mathfrak{p}_5^{24}\mathfrak{p}_6^{24}\mathfrak{p}_7^{24}\mathfrak{p}_8^{24}\mathfrak{p}_9^{24}\mathfrak{p}_{10}^{24}\mathfrak{p}_{11}^{24}\mathfrak{p}_{12}^{24}\mathfrak{p}_{13}^{24}\mathfrak{p}_{14}^{24}\mathfrak{p}_{15}^{24}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{354}\mathfrak{p}_2^{354}\mathfrak{p}_3^{354}\mathfrak{p}_4^{66}\mathfrak{p}_5^{66}\mathfrak{p}_6^{66}\mathfrak{p}_7^{66}\mathfrak{p}_8^{66}\mathfrak{p}_9^{66}\mathfrak{p}_{10}^{66}\mathfrak{p}_{11}^{66}\mathfrak{p}_{12}^{66}\mathfrak{p}_{13}^{66}\mathfrak{p}_{14}^{66}\mathfrak{p}_{15}^{66}\mathfrak{p}_{16}^{78}$ $\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_{13}^{24}\mathfrak{p}_{14}^{24}\mathfrak{p}_{15}^{24}\mathfrak{p}_{16}^{12}$

12. T1 = 14 s T2 = 2958 s T3 = 226 s
$p = 13, \quad q = 13^5, \quad [F : \mathbb{F}_q(x)] = 3,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{72}\mathfrak{p}_2^{72}\mathfrak{p}_3^{72}\mathfrak{p}_4^{24}\mathfrak{p}_5^{24}\mathfrak{p}_6^{24}\mathfrak{p}_7^{24}\mathfrak{p}_8^{24}\mathfrak{p}_9^{24}\mathfrak{p}_{10}^{24}\mathfrak{p}_{11}^{24}\mathfrak{p}_{12}^{24}\mathfrak{p}_{13}^{24}\mathfrak{p}_{14}^{24}\mathfrak{p}_{15}^{24}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{354}\mathfrak{p}_2^{354}\mathfrak{p}_3^{354}\mathfrak{p}_4^{66}\mathfrak{p}_5^{66}\mathfrak{p}_6^{66}\mathfrak{p}_7^{66}\mathfrak{p}_8^{66}\mathfrak{p}_9^{66}\mathfrak{p}_{10}^{66}\mathfrak{p}_{11}^{66}\mathfrak{p}_{12}^{66}\mathfrak{p}_{13}^{66}\mathfrak{p}_{14}^{66}\mathfrak{p}_{15}^{66}\mathfrak{p}_{16}^{78}$ $\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_{13}^{24}\mathfrak{p}_{14}^{24}\mathfrak{p}_{15}^{24}\mathfrak{p}_{16}^{12}$

13. T1 = 54 s T2 = 8990 s T3 = 559 s
$p = 13, \quad q = 13^{10}, \quad [F : \mathbb{F}_q(x)] = 3,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{72}\mathfrak{p}_2^{72}\mathfrak{p}_3^{72}\mathfrak{p}_4^{24}\mathfrak{p}_5^{24}\mathfrak{p}_6^{24}\mathfrak{p}_7^{24}\mathfrak{p}_8^{24}\mathfrak{p}_9^{24}\mathfrak{p}_{10}^{24}\mathfrak{p}_{11}^{24}\mathfrak{p}_{12}^{24}\mathfrak{p}_{13}^{24}\mathfrak{p}_{14}^{24}\mathfrak{p}_{15}^{24}\mathfrak{p}_{16}^{24}\mathfrak{p}_{17}^{24}\mathfrak{p}_{18}^{24}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{354}\mathfrak{p}_2^{354}\mathfrak{p}_3^{354}\mathfrak{p}_4^{66}\mathfrak{p}_5^{66}\mathfrak{p}_6^{66}\mathfrak{p}_7^{66}\mathfrak{p}_8^{66}\mathfrak{p}_9^{66}\mathfrak{p}_{10}^{66}\mathfrak{p}_{11}^{66}\mathfrak{p}_{12}^{66}\mathfrak{p}_{13}^{66}\mathfrak{p}_{14}^{66}\mathfrak{p}_{15}^{66}\mathfrak{p}_{16}^{66}\mathfrak{p}_{17}^{66}\mathfrak{p}_{18}^{66}\mathfrak{p}_{19}^{78}$ $\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_{16}^{24}\mathfrak{p}_{17}^{24}\mathfrak{p}_{18}^{24}\mathfrak{p}_{19}^{12}$

14. T1 = 81 s T2 = 20004 s T3 = 1148 s
$p = 13, \quad q = 13^{20}, \quad [F : \mathbb{F}_q(x)] = 3,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$ $\operatorname{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{72}\mathfrak{p}_2^{72}\mathfrak{p}_3^{72}\mathfrak{p}_4^{24}\mathfrak{p}_5^{24}\mathfrak{p}_6^{24}\mathfrak{p}_7^{24}\mathfrak{p}_8^{24}\mathfrak{p}_9^{24}\mathfrak{p}_{10}^{24}\mathfrak{p}_{11}^{24}\mathfrak{p}_{12}^{24}\mathfrak{p}_{13}^{24}\mathfrak{p}_{14}^{24}\mathfrak{p}_{15}^{24}\mathfrak{p}_{16}^{24}\mathfrak{p}_{17}^{24}\mathfrak{p}_{18}^{24}$ $\operatorname{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{354}\mathfrak{p}_2^{354}\mathfrak{p}_3^{354}\mathfrak{p}_4^{66}\mathfrak{p}_5^{66}\mathfrak{p}_6^{66}\mathfrak{p}_7^{66}\mathfrak{p}_8^{66}\mathfrak{p}_9^{66}\mathfrak{p}_{10}^{66}\mathfrak{p}_{11}^{66}\mathfrak{p}_{12}^{66}\mathfrak{p}_{13}^{66}\mathfrak{p}_{14}^{66}\mathfrak{p}_{15}^{66}\mathfrak{p}_{16}^{66}\mathfrak{p}_{17}^{66}\mathfrak{p}_{18}^{66}\mathfrak{p}_{19}^{78}$ $\operatorname{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_{16}^{24}\mathfrak{p}_{17}^{24}\mathfrak{p}_{18}^{24}\mathfrak{p}_{19}^{12}$

15. T1 = 163 s T2 = ??? T3 = 1708s
$p = 13, \quad q = 13^{30}, \quad [F : \mathbb{F}_q(x)] = 3,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$
$\mathrm{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{72}\mathfrak{p}_2^{72}\mathfrak{p}_3^{72}\mathfrak{p}_4^{24}\mathfrak{p}_5^{24}\mathfrak{p}_6^{24}\mathfrak{p}_7^{24}\mathfrak{p}_8^{24}\mathfrak{p}_9^{24}\mathfrak{p}_{10}^{24}\mathfrak{p}_{11}^{24}\mathfrak{p}_{12}^{24}\mathfrak{p}_{13}^{24}\mathfrak{p}_{14}^{24}\mathfrak{p}_{15}^{24}\mathfrak{p}_{16}^{24}\mathfrak{p}_{17}^{24}\mathfrak{p}_{18}^{24}\mathfrak{p}_{19}^{24}\mathfrak{p}_{20}^{24}$
$\mathrm{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{354}\mathfrak{p}_2^{354}\mathfrak{p}_3^{354}\mathfrak{p}_4^{66}\mathfrak{p}_5^{66}\mathfrak{p}_6^{66}\mathfrak{p}_7^{66}\mathfrak{p}_8^{66}\mathfrak{p}_9^{66}\mathfrak{p}_{10}^{66}\mathfrak{p}_{11}^{66}\mathfrak{p}_{12}^{66}\mathfrak{p}_{13}^{66}\mathfrak{p}_{14}^{66}\mathfrak{p}_{15}^{66}\mathfrak{p}_{16}^{66}\mathfrak{p}_{17}^{66}\mathfrak{p}_{18}^{66}\mathfrak{p}_{19}^{66}\mathfrak{p}_{20}^{66}\mathfrak{p}_{21}^{78}$
$\mathrm{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_{18}^{24}\mathfrak{p}_{19}^{24}\mathfrak{p}_{20}^{24}\mathfrak{p}_{21}^{12}$

16. T1 = 247 s T2 = ??? T3 = 2499 s
$p = 13, \quad q = 13^{40}, \quad [F : \mathbb{F}_q(x)] = 3,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$
$\mathrm{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{72}\mathfrak{p}_2^{72}\mathfrak{p}_3^{72}\mathfrak{p}_4^{24}\mathfrak{p}_5^{24}\mathfrak{p}_6^{24}\mathfrak{p}_7^{24}\mathfrak{p}_8^{24}\mathfrak{p}_9^{24}\mathfrak{p}_{10}^{24}\mathfrak{p}_{11}^{24}\mathfrak{p}_{12}^{24}\mathfrak{p}_{13}^{24}\mathfrak{p}_{14}^{24}\mathfrak{p}_{15}^{24}\mathfrak{p}_{16}^{24}\mathfrak{p}_{17}^{24}\mathfrak{p}_{18}^{24}$
$\mathrm{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{354}\mathfrak{p}_2^{354}\mathfrak{p}_3^{354}\mathfrak{p}_4^{66}\mathfrak{p}_5^{66}\mathfrak{p}_6^{66}\mathfrak{p}_7^{66}\mathfrak{p}_8^{66}\mathfrak{p}_9^{66}\mathfrak{p}_{10}^{66}\mathfrak{p}_{11}^{66}\mathfrak{p}_{12}^{66}\mathfrak{p}_{13}^{66}\mathfrak{p}_{14}^{66}\mathfrak{p}_{15}^{66}\mathfrak{p}_{16}^{66}\mathfrak{p}_{17}^{66}\mathfrak{p}_{18}^{78}\mathfrak{p}_{19}^{78}$
$\mathrm{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_{16}^{24}\mathfrak{p}_{17}^{24}\mathfrak{p}_{18}^{24}\mathfrak{p}_{19}^{12}$

17. T1 = 6016 s T2 = ??? T3 = 16860 s
$p = 13, \quad q = 13^{50}, \quad [F : \mathbb{F}_q(x)] = 3,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - (x+1)\rho^2 + 2x\rho - x^5 = 0$
$E = F(y)$: $\quad y^p - y = u, \quad u = \frac{x^5}{x^3-1}\rho^2 + \frac{x^6+x^2+1}{x^6-1}\rho + \frac{1}{x^5}$
$\mathrm{disc}(\mathcal{O}_E^0) = \mathfrak{p}_1^{72}\mathfrak{p}_2^{72}\mathfrak{p}_3^{72}\mathfrak{p}_4^{24}\mathfrak{p}_5^{24}\mathfrak{p}_6^{24}\mathfrak{p}_7^{24}\mathfrak{p}_8^{24}\mathfrak{p}_9^{24}\mathfrak{p}_{10}^{24}\mathfrak{p}_{11}^{24}\mathfrak{p}_{12}^{24}\mathfrak{p}_{13}^{24}\mathfrak{p}_{14}^{24}\mathfrak{p}_{15}^{24}\mathfrak{p}_{16}^{24}\mathfrak{p}_{17}^{24}\mathfrak{p}_{18}^{24}$
$\mathrm{ind}_1(\mathcal{O}_E^0) = \mathfrak{p}_1^{354}\mathfrak{p}_2^{354}\mathfrak{p}_3^{354}\mathfrak{p}_4^{66}\mathfrak{p}_5^{66}\mathfrak{p}_6^{66}\mathfrak{p}_7^{66}\mathfrak{p}_8^{66}\mathfrak{p}_9^{66}\mathfrak{p}_{10}^{66}\mathfrak{p}_{11}^{66}\mathfrak{p}_{12}^{66}\mathfrak{p}_{13}^{66}\mathfrak{p}_{14}^{66}\mathfrak{p}_{15}^{66}\mathfrak{p}_{16}^{66}\mathfrak{p}_{17}^{66}\mathfrak{p}_{18}^{66}\mathfrak{p}_{19}^{78}$
$\mathrm{ind}_2(\mathcal{O}_E^0) = \mathfrak{p}_{16}^{24}\mathfrak{p}_{17}^{24}\mathfrak{p}_{18}^{24}\mathfrak{p}_{19}^{12}$

In the last examples we compute the finite maximal order of Artin-Schreier-Witt Extensions E/F of degree p^2, $p = 3, 5, 7$ and p^3, $p = 2, 3$, respectively. Here $\wp : W_n(\bar{F}) \to W_n(\bar{F})$, $n = 2, 3$, is the Artin-Schreier-Witt map which was defined in Proposition 3.2.3.

18. T1 = 3 s T2 = 33 s
$p = 3, \quad q = 3, \quad [F : \mathbb{F}_q(x)] = 2,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^2 + x^3 + x + 1 = 0$
$E = F\big((y_1, y_2)\big)$: $\quad \wp\big((y_1, y_2)\big) = \big(\frac{1}{x^2}\rho + x^2, \frac{1}{x-1}\rho + x\big)$ $\mathrm{disc}\big(\mathcal{O}_E^0\big) = \mathfrak{p}_1^{48}\mathfrak{p}_2^{12}$ $\mathrm{ind}_1\big(\mathcal{O}_E^0\big) = \mathfrak{p}_1^{444}\mathfrak{p}_2^{138}\mathfrak{p}_3^{3}\mathfrak{p}_4^{3}\mathfrak{p}_5^{3}\mathfrak{p}_6^{3}\mathfrak{p}_7^{12}\mathfrak{p}_8^{12}\mathfrak{p}_9^{12}$

19. T1 = 658 s T2 = 2175s
$p = 5, \quad q = 5, \quad [F : \mathbb{F}_q(x)] = 2,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^2 + x^3 + x + 1 = 0$
$E = F\big((y_1, y_2)\big)$: $\quad \wp\big((y_1, y_2)\big) = \big(\frac{1}{x^2+3}\rho + x^2, \frac{1}{x-1}\rho + x\big)$

20. T1 = 542 s T2 = ???
$p = 7, \quad q = 7, \quad [F : \mathbb{F}_q(x)] = 2,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^2 + x^3 + x + 1 = 0$
$E = F\big((y_1, y_2)\big)$: $\quad \wp\big((y_1, y_2)\big) = \big(\frac{1}{x^2+3}\rho + x^2, \frac{1}{x-1}\rho + x\big)$

21. T1 = 451 s T2 = ???
$p = 2, \quad q = 2, \quad [F : \mathbb{F}_q(x)] = 3,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^3 - \rho^2 + 2x\rho - x^5 = 0$
$E = F\big((y_1, y_2, y_3)\big)$: $\wp\big((y_1, y_2, y_3)\big) = \big((x+1)\rho^2 + \frac{1}{x^2+1}\rho + x^2, (x^3+x^2)\rho^2 + \frac{1}{x+1}\rho + x, \frac{1}{x^2+1}\rho^2 + (x^6+1)\rho + \frac{1}{x^{12}}\big)$

22. T1 = 34586 s T2 = ???
$p = 3, \quad q = 3, \quad [F : \mathbb{F}_q(x)] = 2,$
$F = \mathbb{F}_q(x, \rho)$: $\quad \rho^2 + x^3 + x + 1 = 0$
$E = F\big((y_1, y_2, y_3)\big)$: $\wp\big((y_1, y_2, y_3)\big) = \big((x+2)\rho + \frac{1}{x^2}, (x^3+x^2)\rho + \frac{1}{x+2}, \frac{1}{x^2}\rho + x^6 + 2\big)$

List of Symbols

k	field
$k(x)$	rational function field
F, F/k	function field
E, E/F	function field extension
$\mathcal{O}$	valuation ring
P, Q	places of a function field
$P'\|P$	extension of places
$\mathbb{P}_F$	set of places of F
v	valuation
v_P	valuation for the place P
$\mathcal{O}_P$	valuation ring of P
$\overline{\mathcal{O}_P}$	residue class field $\mathcal{O}_P/P$ of P
$e(P'\|P)$	ramification index of $P'\|P$
$f(P'\|P)$	relative degree of $P'\|P$
$\mathcal{C}l(R, F)$	the integral closure of the ring R in F
$\mathcal{S}$	subset of $\mathbb{P}_F$
$\mathcal{O}_\mathcal{S}$	holomorphy ring
$\mathcal{O}_P(E)$	$\mathcal{C}l(\mathcal{O}_P, E)$
$\mathcal{O}_\mathcal{S}(E)$	$\mathcal{C}l(\mathcal{O}_\mathcal{S}, E)$
$\chi_{(y,\, E/F)}(T)$	the the minimal polynomial of $y \in E$ over F
$\mathbb{Z}$	rational integers

$\mathbb{F}_q$	finite field of q elements
p	rational prime
$\mathcal{F}$	Frobenius map
$W(E)$	ring of Witt vectors over E
$W_n(E)$	ring of Witt vectors of length n over E
$\mathrm{Fix}_{L/F}(H)$	the fixed field of the subgroup H of the Galois group of the extension L/F
$\mathrm{Gal}_{L/F}(E)$, $\mathrm{Gal}(L/E)$	the Galois group of the subfield E of the Galois extension L/F
$\lvert G\rvert$	the order of the (finite) group G
gcd	greatest common divisor
$\prod$	outer direct product
$\coprod$	inner direct product
$\bigoplus$	direct sum
A^H	see (2.1.a)
G_B	see (2.1.b)
$F(B)$	see (2.1.c)
A_E	see (2.1.d)
N_{E_2/E_1}	norm map
Tr_{E_2/E_1}	trace map
$\wp$	surjective G-homomorphism, see (2.1.h)
$\mu_\wp$	the kernel of $\wp$
Δ_U, Δ_u	see definition on p. 21
$\overline{\Delta}$	see definition in the proof of Theorem 2.3.1
$\iota_{\_,1}$	see (2.2.a)
$\iota_{\_,2}$	see (2.2.b)
$\phi_{\_,1}$	see (2.2.c)
$\phi_{\_,2}$	see (2.2.d)
$\lambda_P(u)$	see (3.2.1)(i)

Index

L

M

P

R

S

U

V

W

Bibliography

[AB74] M. Auslander and D. A. Buchsbaum, *Groups, rings, modules*, Harper & Row, New York, 1974. 1, 2, 3

[AS27] E. Artin and O. Schreier, *Über eine Kennzeichnung der reell abgeschlossenen Körper*, Abh. Math. Sem. Hamburg **5** (1927). 37

[BLP93] J. P. Buhler, H. W. Lenstra, Jr., and Carl Pomerance, *Factoring integers with the number field sieve*, The development of the number field sieve, Lecture Notes in Math., vol. 1554, Springer, Berlin, 1993, pp. 50–94. MR 1 321 221 72

[C+04] J. Cannon et al., *The computer algebra system Magma*, University of Sydney, 2004, `http://magma.maths.usyd.edu.au/magma/`. vii, 72

[Cas86] J. W. S. Cassels, *Local fields*, Cambridge University Press, Cambridge, 1986. 50

[Coh99] H. Cohen, *Advanced topics in computational number theory*, Springer Verlag, New York, 1999. 19

[Dab95] M. Daberkow, *Über die Bestimmung der ganzen Elemente in Radikalerweiterungen algebraischer Zahlkörper*, Dissertation, TU - Berlin, 1995. vi

[Fri97] C. Friedrichs, *Bestimmung relativer Ganzheitsbasen mit dem Round-2-Algorithmus*, Diplomarbeit, Technische Universität Berlin, 1997. vi

[Fri00] ———, *Berechnung von Maximalordnungen über Dedekindringen*, Dissertation, Technische Universit"at Berlin, 2000. vi

[Gop81] V. D. Goppa, *Codes on algebraic curves*, Dokl. Akad. Nauk SSSR **259** (1981), no. 6, 1289–1290. v

[Gop88] ———, *Geometry and codes*, Mathematics and its Applications (Soviet Series), vol. 24, Kluwer Academic Publishers Group, Dordrecht, 1988, Translated from the Russian by N. G. Shartse. v

[Has34] H. Hasse, *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper*, J. Reine Angew. Math. **172** (1934), 37–54. 37

[Has80] ———, *Number theory*, Springer Verlag, Berlin - Heidelberg - New York, 1980. 14, 15

[Hes02] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445. 12

[Jan73] G.J. Janusz, *Algebraic number fields*, Academic Press, New York and London, 1973. 35

[Lor90] Falko Lorenz, *Einführung in die Algebra. Teil II*, Bibliographisches Institut, Mannheim, 1990. 14, 15

[Neu92] J. Neukirch, *Algebraische Zahlentheorie*, Springer Verlag, Berlin - Heidelberg - New York, 1992. 19

[PZ89] M. E. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, 1989. vi

[Sch36a] H. L. Schmid, *Zur Arithmetik der zyklischen p-Körper*, J. reine angew. Math. 176, 161-167 (1936). 14

[Sch36b] ———, *Zyklische algebraische Funktionenkörper vom Grade p^n über endlichem Konstantenkörper der Charakteristik p*, J. reine angew. Math. 175, 108-123 (1936). 14

[Sti93] H. Stichtenoth, *Algebraic function fields and codes*, Springer Verlag, Berlin - Heidelberg - New York, 1993. 3, 11, 38

[Wit36] E. Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n.*, J. Reine Angew. Math. 176, 126-140 (1936). 14

Abstract

Let F be a field and L be an arbitrary (finite or infinite) Galois extension of F with Galois group G. We give a detailed presentation of general Kummer theory, which gives us an abstract tool to characterize all Abelian extensions E of F with $E \subseteq L$: Let A be a subset of L^m which has a group structure which is compatible with the coordinatewise operation of G on A. Then A is called a G-module. Furthermore let $\wp : A \to A$ be a surjective G-homomorphism with finite cyclic kernel $\mu_\wp$. Then there is a bijection between the set of subgroups Δ of A with $\wp(A \cap F^m) \subseteq \Delta \subseteq A \cap F^m$ and the set of Abelian extensions E of F of exponent $|\mu_\wp|$ (with $E \subseteq L$).

We then use general Kummer theory to describe Kummer and Artin-Schreier-Witt extensions. Suppose F contains the set of all n-th roots of unity, where the characteristic of F is zero or coprime to n. Then a Kummer extension of F is an Abelian extension of exponent n. Abelian extensions F of exponent p^r, where $p > 0$ is the characteristic of F, are called Artin-Schreier-Witt extensions.

Let k be a finite (in particular perfect) field and F/k be an algebraic function field over k, i. e.

$$F = k(x, \rho) \text{ with } f(x, \rho) = 0$$

for some irreducible polynomial $f \in k[x, t]$ which is monic and separable with respect to t. Let $\emptyset \neq \mathcal{S}$ be a proper subset of the set of places $\mathbb{P}_F$ of F and E a cyclic Kummer or Artin-Schreier-Witt extension of F. The main result of this thesis is the development of a procedure to compute the ring $\mathcal{O}_\mathcal{S}(E)$ of elements of E which are integral at all places of S. We present algorithms which determine a set Ω of $\mathcal{O}_\mathcal{S}$-generators of $\mathcal{O}_\mathcal{S}(E)$.

This is done by computing for each P in $\mathcal{S}$ a set Ω_P of $\mathcal{S}$-integral generators of $\mathcal{O}_P(E)$ over $\mathcal{O}_P$. The set which consists of the union of all Ω_P is the sought-after set Ω of $\mathcal{O}_\mathcal{S}$-generators of $\mathcal{O}_\mathcal{S}(E)$. Ω is finite since the sets Ω_P are equal for all but finitely many $P \in \mathcal{S}$.

At the end we give examples which demonstrate the efficiency of our method for computing integral closures by comparing it with a general method, which is based on the Round 2 algorithm.