On the asymptotics of wildly ramified local function field extensions

by Raphael Müller

Supervisor: Prof. Dr. Jürgen Klüners

Dissertation 2022

Institute of Mathematics
Faculty EIM

Zusammenfassung

In der vorliegenden Arbeit behandeln wir eine Fragestellung über lokale Funktionkörpererweiterungen nach dem asymptotischen Wachstum der Anzahl von Galoiserweiterungen mit fest vorgegebener nicht-abelscher Galoisgruppe und beschränkter Diskriminante. Von Hauptinteresse ist dabei der Fall, dass die Charakteristik des Körpers die Gruppenordnung teilt. In dem Falle gibt es bereits unendlich viele C_p-Erweiterungen und wir erhalten ein gänzlich anderes Verhalten als bei lokalen Zahlkörpern.

Thorsten Lagemann löste die Fragestellung für abelsche Gruppen in seiner Dissertation. Im nicht-abelschen Fall können wir in der vorliegenden Arbeit erste Resultate erzielen. Zum einen lösen wir das Problem für eine Klasse von semi-direkten Produkten der Form $(C_p)^r \rtimes C_d$, wobei $d \mid (p^r - 1)$ gilt. Das Hauptaugenmerk liegt dabei auf Untergruppen der Affinen Gruppe der Form $C_p \rtimes C_d \leq \mathrm{AGL}_1(p)$. Wir lösen außerdem das Problem für transitive Untergruppen des Kranzproduktes $C_p \wr C_p$ über p^2 Punkten. Körpertheoretisch treten diese als Galoisgruppe von Zerfällungskörpern eines Turms zweier C_p-Erweiterungen auf. Dabei geben wir eine Beschreibung aller dieser Erweiterungen an.

Wir beweisen zudem eine explizite Formel für die Anzahl aller Körpererweiterungen mit fest vorgegebener abelscher Galoisgruppe A, deren Führerexponent kleiner gleich einer vorgegebenen Schranke X ist.

Abstract

In this thesis at hand, we will study a question concerning the discriminant density of local function field extensions with a fixed non-abelian Galois group. The main interest is the case of the characteristic dividing the group order.

In this case, there are already infinitely many C_p-extensions which stands in stark contrast to p-adic fields. Lagemann solved in his Ph. D. Thesis the case of abelian groups. For non-abelian groups we prove some first results. We prove the asymptotical behaviour for an infinite class of semi-direct products $(C_p)^r \rtimes C_d$ where $d \mid (p^r - 1)$. This includes subgroups of affine group of type $C_p \rtimes C_d \leq \mathrm{AGL}_1(p)$. We moreover solve the counting problem for transitive subgroups of $C_p \wr C_p$. These extensions correspond to C_p-towers over C_p-extensions. We describe all extensions over a fixed ground field and fixed transitive subgroup of $C_p \wr C_p$.

Moreover, for given $X > 0$ and a fixed abelian group A, we give an explicit formula for the number of field extensions with Galois group isomorphic to A and with conductor exponent bounded by X.

Justice and Peace!

Our scientific power has outrun our spiritual power.
We have guided missiles and misguided men.

Dr. Martin Luther King

Multinational Corporations – Genocide of the starving Nations

Napalm Death

Contents

Introduction

The main goal of the inverse Galois problem is to determine which groups occur as Galois groups over a given field, and to construct and enumerate one or all such Galois extensions while taking into account certain properties. A classical problem is the theory of inverse Galois theory over $\mathbb{Q}$ and number fields in general. One milestone was Shafarevich's theorem proving the inverse Galois problem for every finite solvable group over a number field which was later generalised to global function fields. Although commonly expected, it is still unknown whether every finite group occurs as Galois group over $\mathbb{Q}$.

Some important milestones have been achieved through asymptotic considerations. More precisely, for a number field k and a transitive permutation group G we consider the counting function by the norm of the discriminant

$$Z(k, G; X) := \#\{K/k \ : \ \mathrm{Gal}(K/k) \cong G, \quad N_{k/\mathbb{Q}}(\mathrm{D}(K/k)) \leq X\} \quad \text{for} \quad X \in \mathbb{R}_{\geq 0}.$$

We are interested in the behaviour for $X \to \infty$. Note that $Z(k, G; X) < \infty$. Although it is not proven if every G is realisable as a Galois group over k, it is widely believed that there exist infinitely many, i.e. that the counting function $Z(k, G; X)$ is unbounded in X. Gunter Malle proposed in his well-known conjecture the asymptotic behaviour of $Z(k, G; X)$ for all number fields and finite transitive permutation groups, see [Mal02], [Mal04]. The Malle conjecture predicts explicit constants $a(G), b(K, G)$ such that

$$Z(K, G; X) \sim c(K, G) \cdot X^{a(G)} \log(X)^{b(K,G)-1} \tag{1}$$

for some constant $c(K, G) > 0$, where we mean $f \sim g \iff \lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$ for real-valued functions $f, g \colon \mathbb{R} \to \mathbb{R}_{>0}$. In general, there are no known formulas for $c(K, G)$. The Malle conjecture is a generalisation of works of Wright who determined in [Wri89] the asymptotic behaviour of $Z(k, A; X)$ for every finite abelian group A and over every global field K such that $\mathrm{char}(K) \nmid \#A$, prior to the works of Malle. This proves Malle's conjecture for all finite abelian groups. The result in [Wri89] provides evidence for a natural generalisation of Malle's conjecture (1) to every global function field k. This is supported by a heuristic by Ellenberg and Venkatesh [EV05] which connects G-extensions of a function field to rational points of covers of Hurwitz spaces $\mathbb{P}^1/\mathbb{F}_q$ for some prime power $q = p^f$ in the case $p \nmid |G|$, where the constants in Malle's conjecture reappear.

However, (1) is false if the characteristic p of the global function field divides the group order. Lagemann [Lag10] proved that for almost all non-cyclic abelian p-extensions the number of local extensions at a fixed place grows larger than (1) indicates.

One main reason is the existence of infinitely many local extensions of fixed degree over each wildly ramified place. The discriminant density of local function fields already exceeds the Malle constants, whereas in the number field case there are only finitely many local extensions of a given degree.

A local function field of characteristic p is a Laurent series ring $\mathbb{F}_q((t))$ where q is a p-power. Like in the p-adic case there exist at most finitely many fields with a given Galois group G, if the characteristic p does not divide the group order. We are interested in the exceptional case when the

characteristic divides the group order. Lagemann has already solved the asymptotics problem for abelian extensions over local fields in his thesis [Lag10], but there are no known asymptotical results for non-abelian groups in the local function field case. Our thesis addresses this problem and solves this for some infinite series of groups. We will not be able to obtain a complete answer but rather study and solve some examples of (infinite series of) finite groups and to gather different strategies to attack the problem.

As a first result in the thesis, we prove the conductor density of abelian p-groups weighted by conductor where we will give explicit formulas.

For a finite abelian group A we define the counting function by the conductor exponent

$$\mathfrak{Z}(F, A; n) := \#\{E/F \text{ Galois } : \mathrm{Gal}(E/F) \cong A \text{ and } \mathrm{N}(\mathfrak{f}(E/F)) \leq q^n\}, \quad n \in \mathbb{N}.$$

We will prove the following theorem:

Theorem A. *Let $F = \mathbb{F}_q((t))$ and A be a finite abelian p-group with exponent $\exp(A) = p^e$. Let $\alpha_p(A)$ and $\delta_A \colon \mathbb{N} \to [-\alpha_p(A), 0]$ be as defined in (2.5). Then there is a p^e-periodic and therefore bounded function $\delta_A(\cdot)$ such that:*

(a) $\mathfrak{Z}(F, A; n) = \frac{|A|}{|\mathrm{Aut}(A)|} q^{n\alpha_p(A)} q^{\delta_A(n)} \varepsilon(A, q, n)$ *for some* $\varepsilon(A, q, n)$ *with* $\lim_{n\to\infty} \varepsilon(A, q, n) = 1$.

(b) $\mathfrak{Z}(F, A; n) \sim \frac{|A|}{|\mathrm{Aut}(A)|} q^{n\alpha_p(A)} q^{\delta_A(n)}$.

(c) For fixed $i = 0, \ldots, p^e - 1$ let $f_i(n) = n \cdot p^e + i$, i.e. $f_i(n) \equiv i \mod p^e$. Then we have

$$\mathfrak{Z}(F, A; f_i(n)) \sim c_i \frac{|A|}{|\mathrm{Aut}(A)|} q^{f_i(n)\alpha_p(A)},$$

with $c_i = q^{i\alpha_p(A)+\delta_A(i)}$ and $c_0 = 1$.

We refer to Theorem 2.12 for an explicit formula for $\varepsilon(A, q, n)$ and more details. We want to highlight the periodic oscillation by δ_A in the formula for the conductor counting function. Although we even restricted to conductor exponents, we can only achieve a $\sim$-estimate when restricting to an arithmetic progression modulo p^e. For arbitrary finite abelian groups, we use the multiplicativity over the ℓ-Sylow subgroups

$$\mathfrak{Z}(F, A; n) = \prod_{\ell \in \mathbb{P}} \mathfrak{Z}(F, A_\ell; n)$$

where $\mathfrak{Z}(F, A_\ell; n)$ is bounded for $n \to \infty$ for all $\ell \neq p$.

Like in the original formulation of Malle's conjecture in [Mal02] and [Mal04], we will use the notion of a Galois group also for non-Galois extensions, i.e. as the Galois group of the corresponding Galois closure. See Paragraph 1.1.2 for details. For a finite transitive permutation group G and $X \in \mathbb{R}_{\geq 0}$ we consider the discriminant counting function

$$Z(F, G; X) := \#\left\{K/F \ : \ \mathrm{Gal}(K/F) \cong G, \ \mathrm{N}(\mathrm{D}(K/F)) \leq X\right\}.$$

If G is a group whose order is coprime to p, then there exist only finitely many G-extensions over F and the counting function $Z(F, G; X)$ is bounded for $X \to \infty$. If G is a non-trivial p-group, then there exist infinitely many G-extensions over F and it is interesting to study the asymptotic behaviour of the counting function $Z(F, G; X)$. What we expect and refer to as "solving" the asymptotics problem is to find a constant $a_p(G) \in \mathbb{R}_{\geq 0}$ such that $Z(F, G; X) \asymp X^{a_p(G)}$, that is, there exist real constants $B, c_1, c_2 > 0$ such that

$$c_1 X^{a_p(G)} \leq Z(F, G; X) \leq c_2 X^{a_p(G)} \quad \text{for all} \quad X \geq B.$$

This weaker notion is satisfactory, since even in the simple case $G = C_p$, there can not be established an asymptotic equivalence with respect to the relation $\sim$. Because the discriminants are only q-powers, the gaps between two consecutive C_p-discriminants are unbounded. Moreover, Theorem A implies that we cannot establish an asymptotic equivalence with respect to $\sim$ even when restricting to count by discriminant exponent. More details on this are given in Remark 1.37.

We solve the asymptotics problem for transitive subgroups of $C_p \wr C_p$ and subgroups of type $C_p \rtimes C_d \leq \mathrm{AGL}_1(p)$. In the latter case, we can extend the method to a larger class of groups with analogous methods.

Let $F = \mathbb{F}_q((t))$ be a local function field in characteristic p. In this thesis, we will prove:

Theorem B. *Let $d \mid (p-1)$ and $U := C_p \rtimes C_d \leq \mathrm{AGL}_1(p)$.*

(a) Consider $C_p \rtimes C_d$ as a transitive subgroup of S_p. Then we have

$$Z(F, C_p \rtimes C_d; X) \asymp X^{\frac{1}{p}}.$$

(b) Consider $C_p \rtimes C_d$ as a transitive subgroup of S_{pd}. Then we have

$$Z(F, C_p \rtimes C_d; X) \asymp X^{\frac{1}{pd}}.$$

We will generalise this result to the situation of a tower of a (tamely ramified) C_d-extension and a C_p-extension. We will describe which groups occur as Galois groups. In particular, every such group is given by a semi-direct product $U = (C_p)^k \rtimes C_d$ corresponding to a divisor $g \mid (X^d - 1)$ over $\mathbb{F}_p$ of degree $\deg(g) = k$. We prove analogous results for the counting function by discriminant as in Theorem B. We obtain $Z(F, U_{pd}; X) \asymp X^{\frac{k}{pd}}$ considered as transitive subgroup $U_{pd} \leq S_{pd}$, and $Z(F, U_{p^k d}; X) \asymp X^{\frac{(p-1)k}{pd(p^k-1)}}$ where we consider $U_{p^k d} \leq S_{p^k d}$.

Furthermore, we study the asymptotics problem for transitive subgroups of $C_p \wr C_p$. There are basically two different types of groups to consider, namely $H(p, r)$ and $\widetilde{H}(p, r)$ of order p^{r+1} which are non-isomorphic for $r < p$ and have group exponent p and p^2, respectively. For $r = p$, both constructions give the wreath product $C_p \wr C_p$.

We will considered them as permutation groups over p^2 points, indicated by the notation $H_{p^2}(p, r) \leq S_{p^2}$ and $\widetilde{H}_{p^2}(p, r) \leq S_{p^2}$, respectively.

We will prove the following main results:

Theorem C. *For $1 \leq r \leq p-1$ we have*

$$Z(F, H_{p^2}(p,r); x) \asymp x^{a_p(H_{p^2}(p,r))},$$

where $a_p(H_{p^2}(p,r)) = \begin{cases} \frac{r+1}{p(p+r)}, & r^2 < p \\ \frac{r}{p^2}, & r^2 > p. \end{cases}$

For the twisted Heisenberg group we prove the following main result:

Theorem D. *For $1 \leq r \leq p-1$ we have*

$$Z(F, \widetilde{H}_{p^2}(p,r); x) \asymp x^{a_p(\widetilde{H}_{p^2}(p,r))},$$

where $a_p(\widetilde{H}_{p^2}(p,r)) = \begin{cases} \frac{pr-r^2+r+1}{p(p^2-pr+p+r)}, & r^2 < p \\ \frac{r}{p^2}, & r^2 > p. \end{cases}$

The thesis is organised as follows: The first chapter will provide the theoretical foundation for all the other chapters. Chapters 2, 3 and 4 are independent of each other and only require results from Chapter 1.

In the first chapter, we will give the theoretical background for local function fields and Artin-Schreier theory. Artin-Schreier theory is basically an additive version of Kummer theory for elementary abelian p-extensions. The Artin-Schreier operator $\wp(x) = x^p - x$ gives a bijection between subgroups of the quotient group $F/\wp(F)$ and the set of elementary abelian p-extensions of F. We will rely on this theory immensely for constructing and counting p-extensions over local function fields of characteristic p. For instance, all Galois p-extensions K/F arise as towers of Artin-Schreier extensions, and vice versa, those towers have a p-group as its Galois group. We will recall a reasonable representative system of $J(F) = F/\wp(F)$.

We will give a constructive approach to construct G-extensions for a finite p-group which goes back to Witt [Wit36]. Furthermore, we will provide some formulas and summation techniques that we frequently use for local function field asymptotics. Particularly, we will count the C_p-extensions as an important example.

In Chapter 2, we will give exact formulas for the number of abelian local function fields up to a conductor bound. This easily implies the lower bound for the discriminant asymptotics in this way and gives a nice interpretation of the discriminant exponent in terms of the conductor exponent.

The third chapter is concerned with Theorem C and generalisations thereof. We will consider the asymptotic problem with respect to discriminant for certain subgroups of groups $\mathrm{AGL}(1,q)$ which cover all transitive subgroups of $\mathrm{AGL}(1,p)$. We will describe the Galois module $J(L) = L/\wp(L)$ for a tamely ramified cyclic extension L/F. We describe the groups which occur as Galois group in this context.

The occurring Galois groups are semi-direct products of type $U = (C_p)^{\deg(g)} \rtimes C_d$, where $g(X) \in \mathbb{F}_p[X]$ is a divisor of $X^d - 1$. In order to describe the semi-direct product, it is convenient to consider

the prime divisors of $g(X)$ and consider $(C_p)^{\deg(g)}$ as direct sum of finite fields. Let $X^d-1 = \prod_{i=1}^{\ell} f_i$ be the prime factorisation in $\mathbb{F}_p[X]$ and $I \subseteq \{1,\dots,\ell\}$ such that $g(X) = \prod_{i\in I} f_i$. Write $r_i := \deg(f_i)$. Then we can rewrite $U = \bigoplus_{i\in I} \mathbb{F}_{p^{r_i}} \rtimes C_d$, where we can interpret the action of C_d on $\mathbb{F}_{p^{r_i}}$ as a multiplication by a certain d-th root of unity in $\mathbb{F}_{p^{r_i}}$.

We solve the asymptotic problem for groups of this type over pd points and for the normal closure. Let $U := \sum_{i\in I} \mathbb{F}_{p^{r_i}} \rtimes C_d \leq \mathrm{AGL}_1(q)$ for $p \nmid d$. Then we get

$$Z(F, U_{pd}; X) \asymp X^{\frac{\deg(g)}{pd}}$$

for $U_{pd} \leq S_{pd}$ considered as transitive permutation group over pd points and we obtain

$$Z(F, U_{p^{\deg(g)}d}; X) \asymp X^{\frac{(p-1)\deg(g)}{pd\left(p^{\deg(g)}-1\right)}}$$

for $U_{p^{\deg(g)}d} \leq S_{p^{\deg(g)}d}$ considered as transitive permutation group over $p^{\deg(g)}d$ points.

Chapter 4 is concerned with proving Theorem C and Theorem D. We study subgroups of $C_p \wr C_p$ as a Galois group. These are the solutions of the group theoretic embedding problem

$$1 \to (C_p)^r \to G \to C_p \to 1$$

which we will call generalised Heisenberg groups $H(p,r)$ in the split case and twisted Heisenberg groups $\widetilde{H}(p,r)$ in the non-split case. Note that $\exp(H(p,r)) = p$ and $\exp(\widetilde{H}(p,r)) = p^2$ for $1 \leq r \leq p-1$, and $H(p,p) \cong \widetilde{H}(p,p) \cong C_p \wr C_p$. For this task, we first study the arithmetic of C_p-extensions in some detail. We will give a representative system to describe all those extensions. We solve the asymptotics problem considered as transitive permutation groups over p^2 points, i.e. counting non-Galois extensions.

Finally, in Chapter 4 we will prove Theorem C and Theorem D.

Acknowledgements

I want to express my deep gratitude to my supervisor Prof. Jürgen Klüners: For having faith in me and bringing me to Paderborn, for many fruitful discussions, for all his guidance, for our great collaboration and for leading me to my Ph.D.

I sincerely want to thank Prof. Florian Hess for his thorough review and many very helpful comments. I thank the Ph.D. Commitee Prof. Berger, Prof. Januszewski and Prof. Winkler for their time and effort, the Institute of Mathematics in Paderborn and in particular Karina Machuletz.

My deepest thanks go to my awesome colleague Anthi for her overall support, and to all my great siblings. Special thanks to the association Hilfe für Menschen in Abschiebehaft Büren e.V., to the maths department in Kaiserslautern and the band Human Remains (Trier).

Chapter 1

Local Function Fields

The local function fields are the analogue to the p-adic fields in characteristic p. A *local function field* is a formal Laurent series field $\mathbb{F}_q((t)) = \{\sum_{i=\nu}^{\infty} a_i t^i \ : \ a_i \in \mathbb{F}_q,\ \nu \in \mathbb{Z}\}$ over a finite field $\mathbb{F}_q$ with q elements. For a Laurent series $f = \sum_{i=\nu}^{\infty} a_i t^i$ we call $\sum_{i=\nu}^{0} a_i t^i \in \mathbb{F}_q[t^{-1}]$ the *main part* of f.

Throughout the thesis, we write q for a p-power with $p \in \mathbb{P}$ and $F = \mathbb{F}_q((t))$ for a local function field over the finite field $\mathbb{F}_q$.

1.1 Introduction to Local Function Fields

1.1.1 Valuation Theory

The local function field $F = \mathbb{F}_q((t))$ has a natural *normalised discrete valuation* by

$$\nu_F\left(\sum_{i=N}^{\infty} a_i t^i\right) = \begin{cases} \infty, & \sum_{i=N}^{\infty} a_i t^i = 0, \\ \min\{n \mid a_n \neq 0\}, & \text{else.} \end{cases}$$

By discrete valuation we mean that for all $\alpha, \beta \in F$ we have

- $\nu_F(0) = \infty$ and $\nu_F(\alpha) \in \mathbb{Z}$ for $\alpha \in F^\times$,
- $\nu_F(\alpha \cdot \beta) = \nu_F(\alpha) + \nu_F(\beta)$,
- $\nu_F(\alpha + \beta) \geq \inf(\nu_F(\alpha), \nu_F(\beta))$.

The valuation is moreover normalised as $\nu_F(t) = 1$ and thus $\nu_F(F^\times) = \mathbb{Z}$.

Every valuation induces an ultrametric absolute value by $|f|_F := q^{-\nu_F(f)}$. Note that F is complete with respect to the absolute value $|\cdot|$ induced by ν_F.

The valuation ν_F induces the *valuation ring* $\mathcal{O}_F = \{\alpha \in F \ : \ \nu_F(\alpha) \geq 0\}$. For a local function field we have $O_F \cong \mathbb{F}_q[[t]]$. It is a local ring whose unique maximal ideal is $\mathfrak{p}_F := \{f \in F \ : \ \nu_F(f) \geq 1\} = t \cdot \mathcal{O}_F$. The *unit group* of $\mathcal{O}_F$ is

$$U_F := \mathcal{O}_F^\times = \{f \in F^\times \ : \ \nu_F(f) = 0\}.$$

Furthermore, $\kappa_F := \mathcal{O}_F/\mathfrak{p}_F \cong \mathbb{F}_q$ denotes the *residue class field* of F.

It is well-known that $\mathcal{O}_F$ is compact with respect to $|\cdot|_F$. For our purposes, it is sufficient to only consider the exponential valuation ν_F only.

We write $\hat{F}$ for a fixed *separable closure* of F and write $G_F := \mathrm{Gal}(\hat{F}/F)$ for the *absolute Galois group* of F.

Extending Valuations in Extensions

Let E/F be a finite separable extension of degree $[E : F]$ with prime elements π_E and π_F respectively. Then ν_E is defined as the natural valuation of $E = \mathbb{F}_{\tilde{q}}((\pi_E))$ where $\kappa_E \cong \mathbb{F}_{\tilde{q}}$.

The *inertia degree* of E/F is the degree of the residue field extensions, i.e. $f_{E/F} = [\kappa_E : \kappa_F]$ and $e_{E/F} := \nu_E(\pi_F)$ is the *ramification index* of E/F.

These satisfy the well-known formula

$$[E : F] = e_{E/F} \cdot f_{E/F}, \tag{1.1}$$

see for instance [Ser79, Prop. I.10] for a proof.

Remark 1.1. Note that ν_E is not an extension of ν_F. We have the relation

$$\nu_E(x) = e_{E/F} \cdot \nu_F(x) \quad \text{for all} \ \ x \in F.$$

It is worth noting that two different prime elements lead to equal valuations.

Definition 1.2. We call a separable extension E/F of local function fields *unramified* if $e_{E/F} = 1$ and *ramified* if $e_{E/F} > 1$.

We call E/F *tamely ramified* if $p \nmid e_{E/F}$.

We call E/F *wildly ramified* if $p \mid e_{E/F}$.

We call E/F *totally ramified* if $e_{E/F} = [E : F]$.

In particular, all unramified extensions are tamely ramified extensions in our thesis.

Note that wildly ramified is the opposite of tamely ramified.

Discriminant and Conductor

Let E/F be a finite separable local extension with valuation rings $\mathcal{O}_E/\mathcal{O}_F$.

We define the conductor as in [Iwa86, p. 112]. To be more precise, the conductor exponent $c(U)$ of an open subgroup $U \leq F^\times$ of finite index is defined to be the minimal natural number n such that $1 + \mathfrak{p}_F^n \leq U$.

Let E/F be an abelian extension, then the *conductor* of the extension is defined as the conductor of its norm group: $\mathrm{N}_{E/F}(E^\times)$ is an open subgroup of U_F and $\mathrm{cond}(E/F) := c(\mathrm{N}_{E/F}(E^\times))$ is the conductor exponent, and

$$\mathfrak{f}(E/F) := \mathfrak{p}_F^{c(\mathrm{N}_{E/F}(E^\times))}$$

is called the *conductor* of E/F.

The *co-different* $\mathfrak{C}_{E/F} := \{x \in \mathcal{O}_E \ : \ \mathrm{Tr}_{E/F}(x \cdot \mathcal{O}_E) \subseteq \mathcal{O}_F\}$ is a fractional ideal of $\mathcal{O}_E$.

The *different* of E/F is the inverse ideal of the co-different, i.e.

$$\mathrm{Diff}(E/F) := \left(\mathfrak{C}_{E/F}\right)^{-1}.$$

The *discriminant ideal* is the norm ideal of the different, i.e.

$$\mathfrak{D}(E/F) = \mathrm{N}_{E/F}\left(\mathrm{Diff}(E/F)\right),$$

where $\mathrm{N}_{E/F}$ is the *ideal norm* which is a multiplicative function completely determined by $\mathrm{N}_{E/F}(\mathfrak{p}_E) = \mathfrak{p}_F^{f_{E/F}}$. It is well-known that $\mathcal{O}_E$ is a free $\mathcal{O}_F$-module (see [Iwa86, La. 2.13]). Hence $\mathcal{O}_E = \mathcal{O}_F[\alpha]$ for some $\alpha \in \mathcal{O}_E$.

Let $g(X) \in F[X]$ be the minimal polynomial of α over F, then we obtain the different through the derivative of the minimal polynomial:

$$\begin{aligned} \mathrm{Diff}(E/F) &= g'(\alpha) \cdot \mathcal{O}_E, \\ \mathfrak{D}(E/F) &= \mathrm{N}_{E/F}\left(g'(\alpha)\right) \cdot \mathcal{O}_F. \end{aligned}$$

Every ideal I of $\mathcal{O}_F$ is a power of the maximal ideal $\mathfrak{p}_F$, so

$$\mathfrak{D}(E/F) = \mathfrak{p}_F^{\mathrm{disc}(E/F)} \text{ for the integer } \mathbb{N} \ni \mathrm{disc}(E/F) = f_{E/F} \cdot \nu_E(g'(\alpha)).$$

We call $\mathrm{disc}(E/F)$ the *discriminant exponent* of E/F.

We call the natural number

$$\mathrm{D}(E/F) := |\kappa_F|^{\mathrm{disc}(E/F)}$$

the discriminant of the extension E/F.

We have $|\kappa_F| = q$ for $F = \mathbb{F}_q((t))$.

The following statement is a basic formula we will use over and over.

Theorem 1.3 (Discriminant Tower Formula)**.** *Let $K/E/F$ be finite extensions of local function fields. Then we have*

$$\mathfrak{D}(K/F) = \mathfrak{D}(E/F)^{[K:E]} \cdot \mathrm{N}_{E/F}\left(\mathfrak{D}(K/E)\right)$$

and for the discriminant exponents

$$\mathrm{disc}(K/F) = [K:E] \cdot \mathrm{disc}(E/F) + f_{E/F} \cdot \mathrm{disc}(K/E).$$

For a proof, see [Neu92, page 213].

1.1.2 Galois group and Galois closure

Definition 1.4. Let E/F be a finite separable extension E/F of degree n. Let α be a primitive element of E/F, i.e. $E = F(\alpha)$. Let ϕ_α be the minimal polynomial of α over F.

(a) We write $\mathrm{Spl}_F(E) := \mathrm{Spl}_F(\phi_\alpha)$ as the splitting field of the minimal polynomial of α over F and call this the *Galois closure* of E/F.

(b) We moreover define $\mathrm{Gal}(E/F) := \mathrm{Gal}(\phi_\alpha) \leq S_n$ as the Galois group of the minimal polynomial of α.

Note that this way, we define Galois groups also for non-Galois field extensions.

On the other hand, let $\mathrm{Spl}_F(E) = F(\beta)$ for some primitive element β and $N = [\mathrm{Spl}_F(E) : F]$. We make a distinction of $\mathrm{Gal}(E/F) = G \leq S_n$ and $\mathrm{Gal}(\mathrm{Spl}_F(E)/F) \leq S_N$ considered as transitive permutation groups over n respectively N points. Both are isomorphic as abstract groups, but not as permutation groups. Viewed as permutation groups, the former describes permutations of the roots of the n conjugates of α, while the latter describes the permutation of the N conjugates of β.

Concerning the counting function by discriminant, the discriminant weight changes quite drastically in these two situations.

1.1.3 Artin-Schreier Theory

The Artin-Schreier theory characterises all elementary abelian p-extensions over fields of characteristic p via the Artin-Schreier operator $\wp$ given by $\wp(\alpha) = \alpha^p - \alpha$ and equations of type $X^p - X - a$. An extension $E = F(\theta)$ where θ is a root of $X^p - X - \alpha$ is called an Artin-Schreier extension. Artin-Schreier theory is in the heart of our studies and is particularly interesting for p-group extensions, since any extension K/F with $\mathrm{Gal}(K/F)$ being a finite p-group can be constructed as a tower of Artin-Schreier extensions.

We start with the notations and basic results.

For any field F with $\mathrm{char}(F) = p$ the *Artin-Schreier operator* is defined as

$$\wp\colon F \to F,\ x \mapsto x^p - x.$$

The map $\wp$ is $\mathbb{F}_p$-linear with kernel $\mathrm{Ker}(\wp) = \mathbb{F}_p$. We write $J(F) := F/\wp(F)$ as the cokernel of $\wp$. We will mainly consider $\wp\colon \hat{F} \to \hat{F}$ for the algebraic closure of a local function field F or of an extension of F. The Artin-Schreier operator is a $\mathrm{Gal}(\hat{F}/F)$-module homomorphism, i.e. it commutes with all $\sigma \in \mathrm{Gal}(\hat{F}/F)$, since

$$\sigma(\wp(x)) = \sigma(x^p - x) = \sigma(x)^p - \sigma(x) = \wp(\sigma(x)) \quad \text{for all } x \in \hat{F}. \tag{1.2}$$

This way, $J(F) := F/\wp(F)$ becomes a $\mathrm{Gal}(\hat{F}/F)$-module via $\sigma \cdot (\alpha + \wp(F)) = \sigma(\alpha) + \wp(F)$.

Moreover, $\wp$ commutes with the trace map. More precisely, for every finite extension K/F we have $\mathrm{Tr}_{K/F}(\wp(\alpha)) = \wp(\mathrm{Tr}_{K/F}(\alpha))$.

For every automorphism $\sigma \in \mathrm{Gal}(\hat{F}/F)$ we get an F-linear map

$$(\sigma - 1)\colon \hat{F} \longrightarrow \hat{F}, \quad \alpha \longmapsto \sigma(\alpha) - \alpha.$$

Using $\sigma \circ \wp \overset{(1.2)}{=} \wp \circ \sigma$ we easily get

$$(\sigma - 1) \circ \wp = \wp \circ (\sigma - 1),$$

hence $\sigma - 1$ is a $\mathrm{Gal}(\hat{F}/F)$-module homomorphism.

For $a \in \hat{F}$ we write $\theta_a \in \hat{F}$ for a solution of $\wp(\theta_a) = a$. A solution θ_a of $X^p - X - a$ is unique modulo $\mathbb{F}_p$: If $\wp(\theta_a) = a$ then

$$X^p - X - a = \prod_{\lambda \in \mathbb{F}_p} (X - (\theta_a + \lambda)). \tag{1.3}$$

If $a \in F$ and $X^p - X - a$ is irreducible in $F[X]$, then we call the extension $F(\theta_a)$ an *Artin-Schreier extension* of F. Sometimes we will refer to this as a *simple Artin-Schreier extension*. Equation (1.3) implies that $X^p - X - a$ is irreducible if and only if $a \notin \wp(F)$, and so $X^p - X - a$ is either irreducible or splits completely over F.

Denote by C_n the cyclic group with n elements. It is crucial that the C_p-extensions over F are precisely the (simple) Artin-Schreier extensions and furthermore, the composite of those are precisely the elementary abelian p-extensions over F.

Lemma 1.5. *Let F be a local function field with $\mathrm{char}(F) = p$.*

(a) A field extension K/F is a C_p-extension if and only if there exists an $a \in F \setminus \wp(F)$ with $K = F(\theta_a)$.

(b) Let $a, b \in F \setminus \wp(F)$. Then $F(\theta_a) = F(\theta_b)$ if and only if $a = \lambda b + \wp(c)$ for some $\lambda \in \mathbb{F}_p^\times$ and $c \in F$.

Proofs can be found in [VS06], Theorem 5.8.4 and Proposition 5.8.6 respectively.

We will point out an obvious consequence that we will frequently use.

Remark 1.6. For all $a \in F \setminus \wp(F)$ and $\lambda \in \mathbb{F}_p^\times$, we have $F(\theta_a) = F(\theta_{\lambda a})$.

Theorem 1.7 (Main Theorem of Artin-Schreier Theory)**.** *Let F be a field with* $\mathrm{char}(F) = p$.

(a) There is a $1:1$*-correspondence*

$$\begin{aligned}\Delta\colon \{\mathbb{F}_p\text{-subspaces } U \leq F/\wp(F)\} &\longrightarrow \{\ p\text{-elementary field extensions } E/F\}\\ U &\longmapsto F(\wp^{-1}(U)).\end{aligned}$$

(b) Let $U \leq F/\wp(F)$ and $K = F(\wp^{-1}(U))$ be the corresponding extension field. Then we have a canonical isomorphism

$$U \cong \mathrm{Hom}(\mathrm{Gal}(K/F), \mathbb{F}_p), \quad a \mod \wp(F) \mapsto \chi_a,$$

where $\chi_a(\sigma) = (\sigma - 1)(\theta_a)$.

(c) Let $U \leq F/\wp(F)$ be finite and $(a_1 + \wp(F), \ldots, a_r + \wp(F))$ be an $\mathbb{F}_p$-basis of U. Then the Galois group $\mathrm{Gal}\left(F\left(\wp^{-1}(U)\right)/F\right) \cong (C_p)^r$ *is generated by the automorphisms σ_i with*

$$\sigma_i(\theta_{a_j}) = \theta_{a_j} + \delta_{i,j} \quad \text{for} \quad 1 \leq i \leq r,\ 1 \leq j \leq r,$$

where $\delta_{i,j}$ is the Kronecker-Delta.

Proof. Parts (a) and (b) are proven in Theorem IV.3.3 in [Neu92] respectively in Theorem VI.8.3 in [Lan02].

Concerning part (c), it is clear by part (a) that σ_i indeed define automorphisms for $1 \leq i \leq r$. Moreover, for all $\lambda_1, \ldots, \lambda_r \in \mathbb{F}_p$ and $1 \leq i \leq r$ we get

$$\left(\sum_{i=1}^{r} \lambda_i \sigma_i\right)(\theta_{a_i}) = \theta_{a_i} + \lambda_i,$$

hence $\sum_{i=1}^{r} \lambda_i \sigma_i = \mathrm{id}$ if and only if $0 = \lambda_i$ for all i. Hence, $\sigma_1, \ldots, \sigma_r$ forms an $\mathbb{F}_p$-basis of $\mathrm{Gal}\left(F\left(\wp^{-1}(U)\right)/F\right)$. □

In the situation of Theorem 1.7(c), we call $E = F(\theta_{a_1}, \ldots, \theta_{a_r})$ an *Artin-Schreier extension* with generators $\theta_{a_1}, \ldots, \theta_{a_r}$. If $r = 1$ we call E/F a *simple Artin-Schreier extension.*

Remark 1.8.
Let $F = \mathbb{F}_q((t))$ and $U \leq F/\wp(F)$ be an $\mathbb{F}_p$-subspace of $J(F)$. Set $V := \mathrm{Span}_{\mathbb{F}_p}(U, \wp(F))$.

(a) Every subspace $U \leq F/\wp(F)$ corresponds to a subspace

$$\wp(F) \subseteq V \leq F.$$

(b) Let $K := F(\wp^{-1}(U))$ be the corresponding Artin-Schreier extension. Then we have $\wp(K) \cap F = V$ and equivalently, $(\wp(K) \cap F)/\wp(F) = U$.

Proof. The first part is common knowledge from algebra.

Let $\alpha \in \wp(K) \cap F$ and consider $\widetilde{U} := \mathrm{Span}_{\mathbb{F}_p}(U, \alpha + \wp(F)) \leq F/\wp(F)$. Then we have $\wp^{-1}(\alpha) \subseteq K$ and thus $\wp^{-1}(\widetilde{U}) \leq K$, hence

$$K = F\left(\wp^{-1}(U)\right) \leq F\left(\wp^{-1}(\widetilde{U})\right) \leq K$$

which proves $F\left(\wp^{-1}(\widetilde{U})\right) = K$. Using the one-to-one correspondence in Theorem 1.7 we get $\widetilde{U} = U$.

Using the same reasoning for all $\alpha \in \wp(K) \cap F$ we obtain

$$U + \left(\wp(K) \cap F + \wp(F)\right)/\wp(F) = U = V/\wp(F),$$

hence $V \leq \wp(K)$ and $V \leq F$ by construction showing $V \leq \wp(K) \cap F$.

Concerning the other direction, the polynomial $X^p - X - u$ has a root in K for all $u \in V$ by definition of K, hence $\wp(K) \cap F \leq V$. □

Theorem 1.9. *Let K/F be a finite Galois extension with $G = \mathrm{Gal}(K/F)$ and $U \leq K/\wp(K)$ be an $\mathbb{F}_p$-subspace. Then $K(\wp^{-1}(U))/F$ is Galois if and only if $\sigma(U) = U$ for all $\sigma \in G$.*

Proof. Let $L = K(\wp^{-1}(U))$ and let $V \leq K$ with $\wp(K) \subseteq V$ such that $V/\wp(K) = U$. Assume that the extension L/F is Galois. Then the polynomials

$$X^p - X - \sigma(v) \text{ split in } L \quad \text{for all} \quad v \in V, \sigma \in G.$$

Thus $\sigma(v) \in \wp(L) \cap K = V$ for all $\sigma \in G$ and $v \in V$, thus $\sigma(V) = V$ and $\sigma(U) = U$.

On the other hand, assume $\sigma(U) = U$ for all $\sigma \in G$ which directly implies $\sigma(V) = V$. Let $\tilde{\sigma} \colon L \to \hat{F}$ be a field homomorphism with $\tilde{\sigma}|_K = \sigma$. We have $L = K(\theta_v \mid v \in V)$ by definition, and we have that

$$\tilde{\sigma}(\theta_v) \text{ is a root of } X^p - X - \sigma(v) \quad \text{for all} \quad v \in V,$$

and by $\sigma(V) = V$ we have $\tilde{\sigma}(\theta_v) = \theta_{\sigma(v)} \in \wp^{-1}(V) \leq L$. This proves that indeed $\tilde{\sigma}(L) = L$.

Conclusively, we obtain $|G| \cdot [L : K] = [L : F]$ many field homomorphisms $L \to \hat{F}$ with $\tilde{\sigma}(L) = L$, and hence L/F is a Galois extension. □

Definition 1.10. We call a finite field extension L/F an *Artin-Schreier tower* if there exists a chain of subfields $L_0 := F \leq L_1 \leq \ldots \leq L_r = L$ such that L_i/L_{i-1} is a simple Artin-Schreier extension for all $1 \leq i \leq r$, i.e. such that $L_i = L_i(\theta_{\alpha_i})$ for some $\alpha_i \in L_{i-1}$.

It is worth pointing out that this way, we define the Galois group for non-Galois extensions as well.

Theorem 1.11. *Let $M/L/K$ be a tower of fields such that M/L and L/K are Galois and $H_1 = \mathrm{Gal}(M/L)$ and $H_2 = \mathrm{Gal}(L/K)$. Then $\mathrm{Gal}(M/K)$ is isomorphic to a subgroup of the wreath product $H_1 \wr H_2$.*

For a proof we refer the reader to Satz 1.10 in Geissler's Ph.D. Thesis [Gei03].

Proposition 1.12. *Let K/F be a (possibly non-Galois) finite separable extension. Then $\mathrm{Gal}(K/F)$ is a p-group if and only if K/F is an Artin-Schreier tower.*

Proof. Write $L := \mathrm{Spl}_F(K)$ as the normal closure of K/F and $H = \mathrm{Gal}(L/K)$. Note that each proper subgroup $H \lneq G$ of a p-group is contained in a maximal normal subgroup N of index p, see [AB95, Corollary 8.4, p. 74]. The fixed field $E := \mathrm{Fix}(N)$ of N is a subfield of K by construction and satisfies $\mathrm{Gal}(E/F) \cong G/N \cong C_p$. Thus E/F is an Artin-Schreier extension according to Lemma 1.5 and $\mathrm{Gal}(K/E)$ is a p-group. Hence by induction K/E is a tower of Artin-Schreier extensions and so is K/F.

For the inverse direction "$\Longleftarrow$" we consider a tower of fields $F = K_0 \leq K_1 \leq \ldots \leq K_r = K$ such that K_i/K_{i-1} is a simple Artin-Schreier extension.

Set $L_{r-1} := \mathrm{Spl}_F(K_{r-1})$ and consider the composite field $M := L_{r-1}K_r$. Theorem 1.11 inductively shows that $\mathrm{Gal}(L_{r-1}/F)$ and thus $\mathrm{Gal}(L_{r-1}/K_{r-1})$ are p-groups. By Theorem 1.11 we have

$$\mathrm{Gal}(M/K_{r-1}) \leq \mathrm{Gal}(M/L_{r-1}) \wr \mathrm{Gal}(L_{r-1}/K_{r-1}) \cong C_p \wr \mathrm{Gal}(L_{r-1}/K_{r-1}).$$

The wreath product of p-groups is a p-group again hence $\mathrm{Gal}(M/K_{r-1})$ and $\mathrm{Gal}(K_{r-1}/F)$ are p-groups and thus $\mathrm{Gal}(M/F)$ is a p-group since $\mathrm{Gal}(L_{r-1}/K_{r-1})$ and C_p are p-groups. Finally, $\mathrm{Gal}(M/F) = \mathrm{Gal}(\mathrm{Spl}_F(K_{r-1})K_r/F)$ completes the proof. □

Remark 1.13. Artin-Schreier theory can be considered as the analogue of Kummer theory of degree p extensions of characteristic p:

Artin-Schreier Theory	$\mathrm{char}(K) = p$	$\wp$	θ_a	$K/\wp(K)$
Kummer Theory	$\zeta_p \in K$	$\sqrt[p]{\ }$	$\sqrt[p]{a}$	$K^\times/K^{\times p}$

1.1.4 System of Representatives of $J(F)$

Recall $J(F) = F/\wp(F)$ which is the $\mathbb{F}_p$-vector space characterising all elementary abelian p-extensions of F. For an element $a \in F$ we will write

$$[a] := a + \wp(F) \in J(F).$$

There is a well-known relation between the discriminant of a simple Artin-Schreier extension $E = F(\theta_a)$ and the value

$$\max_{f \in F}(\nu_F(a + \wp(f))).$$

We want to construct a system of representatives of $J(F)$ so that this value is simply $\nu_F(a)$.

Definition 1.14. We set $\nu_{J(F)}([0]) := \infty$ and for all $a \in F \setminus \wp(F)$ we define

$$\nu_{J(F)}([\alpha]) := \max\{\nu_F(a + \wp(x)) \ : \ x \in F\}$$

to be the *reduced valuation* of a in F. If $\nu_F(a) = \nu_{J(F)}([a])$ we call the element $a \in F$ *reduced*. A reduced element $\beta \in F$ such that $a - \beta \in \wp(F)$ is called a *reduction of* a in F.

Clearly, a reduction of an element a in F is far from being unique: If α is any reduction of a, then so is $\alpha + \beta$ for all $\beta \in F$ with $\nu_F(\beta) > 0$.

Remark 1.15. For the map $\nu_{J(E)} \colon J(E) \to \mathbb{Z}_{\leq 0} \cup \{\infty\}$ and for all $\alpha, \beta \in J(E)$ we have

$$\nu_{J(E)}([\alpha + \beta]) \geq \min\left\{\nu_{J(E)}([\alpha]), \nu_{J(E)}([\beta])\right\}$$

and

$$\nu_{J(E)}([\alpha + \beta]) = \min\left\{\nu_{J(E)}([\alpha]), \nu_{J(E)}([\beta])\right\} \quad \text{if} \quad \nu_{J(E)}([\alpha]) \neq \nu_{J(E)}([\beta]).$$

Proof. Let π be a prime element of E. Let $\widetilde{\alpha} = \alpha + \wp(x) \in [\alpha]$ and $\widetilde{\beta} = \beta + \wp(y) \in [\beta]$ with $x, y \in E$ such that $\nu_{J(E)}([\alpha]) = \nu_E(\widetilde{\alpha})$ and $\nu_{J(E)}([\beta]) = \nu_E(\widetilde{\beta})$.

Then we have $\widetilde{\alpha} + \widetilde{\beta} = \alpha + \beta + \wp(x + y) \in [\alpha + \beta]$. By the ultra-metric triangle-inequality of ν_E we have

$$\nu_{J(E)}([\alpha + \beta]) \geq \nu_E(\widetilde{\alpha} + \widetilde{\beta}) \geq \min\left\{\nu_E(\widetilde{\alpha}),\ \nu_E(\widetilde{\beta}\right\} = \min\left\{\nu_{J(E)}([\alpha]),\ \nu_{J(E)}([\beta])\right\}.$$

For the second equation we can without loss of generality assume

$$\nu_E(\widetilde{\alpha}) = \nu_{J(E)}([\alpha]) < \nu_{J(E)}([\beta]) = \nu_E(\widetilde{\beta}).$$

For any $\gamma \in [\alpha + \beta]$ there is some $z \in E$ such that $\gamma = \alpha + \beta + \wp(z)$. Then we have

$$\begin{aligned}\nu_E(\gamma) = \nu_E(\alpha + \beta + \wp(z)) = \nu_E(\widetilde{\alpha} + \wp(z - x - y) + \widetilde{\beta}) &\overset{\triangle\text{-ineq.}}{=} \min\left\{\nu_E(\widetilde{\alpha} + \wp(z - x - y),\ \nu_E(\widetilde{\beta})\right\} \\ = \nu_E(\widetilde{\beta})) &= \min\left\{\nu_{J(E)}([\alpha]),\ \nu_{J(E)}([\beta])\right\}.\end{aligned}$$

This is true for all $\gamma \in [\alpha + \beta]$, thus

$$\nu_{J(E)}([\alpha + \beta]) = \max_{\gamma \in [\alpha+\beta]}(\nu_E(\gamma)) = \min\left\{\nu_{J(E)}([\alpha]),\ \nu_{J(E)}([\beta])\right\}. \qquad \square$$

It should be noted that there are reduced elements $\alpha, \beta \in F$ such that $\alpha + \beta$ is not reduced. This is demonstrated in the following example.

Example 1.16.

(a) Take for instance $F = \mathbb{F}_2((t))$ and $\alpha = t^{-3} + t^{-2}$ and $\beta := t^{-3}$, then $\alpha + \beta = t^{-2}$ is not reduced.

(b) Note that the multiplication of E does not lead to a well-defined multiplication of $J(E)$ as there exist $\alpha, \beta \in E$ such that $\alpha \cdot \wp(\beta) \notin \wp(E)$.

For instance in $E := \mathbb{F}_5((t))$ we have

$$t \in \wp(E), t^{-1} = t \cdot t^{-2} \notin \wp(F), \qquad [t^{-3}] = [t^{-1} \cdot t^{-2}] \neq [(t^{-1} + t)t^{-2}].$$

Moreover, there exist $\lambda \in \mathbb{F}_q^\times$ and $\alpha \in E$ such that $\nu_{J(E)}([\lambda \cdot \alpha]) \neq \nu_{J(E)}([\alpha])$ for instance if $q > p$ and $\lambda \in \wp(\mathbb{F}_q) \setminus \wp(\mathbb{F}_p)$, $\alpha = 1 \in \wp(E)$.

Considering the conductor and discriminant exponent of Artin-Schreier extensions, the following definitions and notations are helpful.

Definition 1.17. Let $a \in F \setminus \wp(F)$. Then we define

$$\operatorname{cond}([a]) := \begin{cases} 0, & \nu_{J(F)}([a]) = 0, \\ |\nu_{J(F)}([a])| + 1, & \nu_{J(F)}([a]) \neq 0. \end{cases}$$

and

$$\operatorname{disc}([a]) := (p-1)\operatorname{cond}([a]) = \begin{cases} 0, & \nu_{J(F)}([a]) = 0, \\ (p-1)\left(|\nu_{J(F)}([a])| + 1\right), & \nu_{J(F)}([a]) \neq 0. \end{cases}$$

We occasionally use the notation $d_a := \operatorname{disc}([a])$.

Proposition 1.18. *Let $a \in F \setminus \wp(F)$ and $E = F(\theta_a)$. Then:*

(a) Either $\nu_{J(F)}([a]) = 0$ or $\left(\nu_{J(F)}([a]) < 0 \text{ and } p \nmid \nu_{J(F)}([a])\right)$.
Moreover, E/F is ramified if and only if $\nu_{J(F)}([a]) < 0$.

(b) We get $\nu_E(\theta_a) = \nu_F(a)$.

(c) We have $\operatorname{cond}(E/F) = \operatorname{cond}([a])$ for the conductor exponent.

(d) For the discriminant exponent we have

$$\operatorname{disc}(E/F) = d_a = \begin{cases} 0, & \nu_{J(F)}([a]) = 0, \\ (p-1)(|\nu_{J(F)}([a])| + 1), & \nu_{J(F)}([a]) < 0. \end{cases}$$

(e) We have $\operatorname{disc}(E/F) \not\equiv -1 \pmod{p}$.

Proof. The first statement of (a) is Theorem 5.8.10 in [VS06] and the second statement is clear by (d).

For (b), we can immediately check

$$\nu_E(\theta_a^p) = \nu_E(\theta_a - a) = \nu_E(a) \overset{(a)}{=} \begin{cases} 0, & \nu_{J(F)}([a]) = 0, \\ p\nu_F(a), & \nu_{J(F)}([a]) < 0. \end{cases}$$

Part (d) is Theorem 5.8.11 in [VS06]. Part (c) follows by (d) and the Conductor-Discriminant Formula. Finally, note for part (e) that $\operatorname{disc}([a]) = 0$ or $p \nmid \nu_{J(F)}([a])$ in which case

$$\operatorname{disc}([a]) = (p-1)\left(|\nu_{J(F)}([a])| + 1\right) \not\equiv p - 1 \equiv -1 \mod p. \qquad \square$$

Hence to study the discriminants of Artin-Schreier extensions it is useful to consider reduced valuations and reductions of Artin-Schreier generators.

A reduction is not unique. For this purpose we will construct some nice system of representatives of reduced elements.

Definition 1.19. Let $V \leq F$ be an $\mathbb{F}_p$-subspace with $\wp(F) \leq V \leq F$.

We call an $\mathbb{F}_p$-complement R_V with $F = R_V \oplus V$ a *reduced complement* if all elements $0 \neq \alpha \in R_V$ are reduced, that is

$$x \in R_V \iff x = 0 \text{ or } \nu_F(x) = \max\{\nu_F(a) \ : \ a \in x + V\}.$$

Such a complement R_V describes the factor space F/V and serves as a reduction of elements in F: Every $\alpha = r + v$ is representable in a unique way with $r \in R_V$ and $v \in V$, where $\alpha \equiv r \mod \wp(F)$ and the emphasis on R_V being reduced simply means that $\nu_F(r)$ describes the field discriminant of $F(\theta_\alpha)/F$.

The main examples are

$$V = \wp(F) \quad \text{or} \quad V = \wp(K) \cap F \text{ for a separable field extension } K/F.$$

Now we construct a reduced system of representatives of $J(F)$. This can be used to construct a reduced system of representatives for all $V \leq J(F)$.

Fix an $\mathbb{F}_p$-basis $\{\omega_1, \ldots, \omega_r\}$ of $\mathbb{F}_q$ such that $\omega_1 \notin \wp(\mathbb{F}_q)$. Thus, $R_q := \mathbb{F}_p \cdot \omega_1$ is an $\mathbb{F}_p$-complement of $\wp(\mathbb{F}_q)$ in $\mathbb{F}_q$.

Lemma 1.20. *Let F be a local function field with $\operatorname{char}(F) = p$.*

(a) If $\alpha \in F$ with $\nu_F(\alpha) > 0$, then $\alpha \in \wp(F)$.

(b) For every prime element π of F and $\omega_1 \in \mathbb{F}_q \setminus \wp(\mathbb{F}_q)$, the set

$$R_F(\pi, \omega_1) := \left\{ a_0\omega_1 + \sum_{\substack{i=n_0 \\ p \nmid i}}^{-1} b_i \pi^i \ \middle| \ a_0 \in \mathbb{F}_p;\ b_i \in \mathbb{F}_q,\ n_0 \in \mathbb{Z}_{<0} \right\}$$

is a reduced complement of $\wp(F)$ in F.

(c) We have $J(F) \cong \mathbb{F}_p \bigoplus_{\substack{n<0 \\ p \nmid n}} \mathbb{F}_q$ as an $\mathbb{F}_p$-vector space.

Proof. For (a) let $\alpha = \sum_{n=1}^{\infty} a_n \pi^n$ with $a_n \in \mathbb{F}_q$. Then we obtain

$$\wp\left(\sum_{n=1}^{\infty}\sum_{k=0}^{\infty} -a_n^{p^k}\pi^{np^k}\right) = \sum_{n=1}^{\infty} a_n\pi^n = \alpha$$

since for all $n \geq 1$ we have:

$$\begin{aligned}\wp\left(\sum_{k=0}^{\infty} -a_n^{p^k}\pi^{np^k}\right) &= \sum_{k=0}^{\infty}(-1)^p a_n^{p^{k+1}}\pi^{np^{k+1}} - \sum_{k=0}^{\infty} -a_n^{p^k}\pi^{np^k} \\ &\overset{(-1)^p=-1}{=} \sum_{k=1}^{\infty} -a_n^{p^k}\pi^{np^k} + \sum_{k=0}^{\infty} a_n^{p^k}\pi^{np^k} \\ &= a_n\pi^n + \sum_{k=1}^{\infty}\left(-a_n^{p^k} + a_n^{p^k}\right)\pi^{np^k} \\ &= a_n\pi^n + 0 = a_n\pi^n.\end{aligned}$$

Note for $p = 2$ we simply have $-1 = 1$. Now for (b), let $\phi\colon \mathbb{F}_q \to \mathbb{F}_q, a \mapsto a^{q/p}$, which is a field isomorphism as the inverse of the Frobenius automorphism. Let $n = -ip^k < 0$ with $a \in \mathbb{F}_q^\times$, $p \nmid i$ and $k \geq 1$. Then

$$\wp\left(\phi(a)\cdot\pi^{-ip^{k-1}}\right) = a\pi^{-ip^k} - \phi(a)\cdot\pi^{ip^{k-1}},$$

hence inductively $a\pi^{-ip^k} \equiv \widetilde{a}\pi^{-i} \mod \wp(F)$ for some $\widetilde{a} \in \mathbb{F}_q^\times$. Thus, every $\alpha \in \mathbb{F}_q((t))$ is equivalent to a Laurent series

$$\sum_{\substack{n=\nu \\ \gcd(n,p)=1}}^{-1} a_n\pi^n + a_0.$$

By $\mathbb{F}_p \cong \mathbb{F}_q/\wp(\mathbb{F}_q)$ and $\omega_1 + \wp(\mathbb{F}_q) \neq \wp(\mathbb{F}_q)$, the constant term a_0 can be easily reduced to an element in $\mathbb{F}_p \cdot \omega_1$. Therefore, for all $\alpha \in F$ exists $\beta \in R_F(\pi, \omega_1)$ such that $\alpha - \beta \in \wp(F)$ which shows $F = \wp(F) + R_F(\pi, \omega_1)$.

Concerning directness, assume $0 \neq \alpha \in R_F(\pi, \omega_1) \cap \wp(F)$. Then $\alpha \in \wp(F)$ implies $\nu_F(\alpha) \geq 0$ or $p \mid \nu_F(\alpha)$.

On the other hand, $\alpha \in R_F(\pi, \omega_1)$ implies $\nu_F(\wp(\alpha)) \geq 0 \quad$ or $\quad p \mid \nu_F(\wp(\alpha))$. Thus $\nu_F(\alpha) = 0$ so that $\alpha \in \wp(F) \cap \mathbb{F}_q = \wp(\mathbb{F}_q)$. By construction of the set $R_F(\pi, \omega_1)$ we have $R_F(\pi, \omega_1) \cap \wp(\mathbb{F}_q) = \{0\}$, thus we have $\alpha = 0$. Hence $R_F(\pi, \omega_1) \cap \wp(F) = 0$ and $R_F(\pi, \omega_1) + \wp(F) = F$ which proves (b).

Part (c) is now obvious as

$$J(F) \cong R_F(\pi, \omega_1) \cong \mathbb{F}_p \cdot \omega_1 \bigoplus_{n<0,\ p\nmid n} \mathbb{F}_q \cdot \pi^n$$

is a direct sum of $\mathbb{F}_p$-subspaces. □

Usually we simply write R_F instead of $R_F(\pi, \omega_1)$. Sometimes, as in Chapter 3, it will be important to choose π and ω_1 carefully.

Remark 1.21. We will regularly use the following easy observation: Let $\alpha, \beta \in R_F \setminus \{0\}$. Then we have

$$\operatorname{disc}([\alpha]) \geq \operatorname{disc}([\beta]) \iff |\nu_F(\alpha)| \geq |\nu_F(\beta)| \iff \nu_F(\alpha) \leq \nu_F(\beta), \tag{1.4}$$

as the reduced valuations are ≤ 0.

Remark 1.22.

(a) Let $a \in R_F$ and $E := F(\theta_a)$ then we have

$$V_a := \wp(E) \cap F = \wp(F) + \mathbb{F}_p \cdot a.$$

We define $R_{V_a} \leq R_F$ to be a complement of $\mathbb{F}_p a \in R_F$, i.e. such that

$$F = \wp(F) \oplus \mathbb{F}_p \cdot a \oplus R_{V_a} = V_a \oplus R_{V_a}.$$

Then, obviously R_{V_a} is a reduced complement of V_a.

(b) For any $\mathbb{F}_p$-subspace with $\wp(F) \leq V \leq F$ we can analogously construct a reduced system of representatives $R_V \subseteq R_F$ for the quotient space F/V.

Remark 1.23. Let $E = F(\theta_a)$ for $a \in R_F$ be a simple Artin-Schreier extension. Here we briefly give a construction of a prime element of E.

If E/F is unramified, then t is a prime element of E.

If E/F is ramified, then $\nu_F(a) < 0$ is not divisible by p. Let $i, s \in \mathbb{N}$ such that $\nu_F(a)i + ps = 1$. Then $\pi = \theta_a^i t^s$ is a prime element of R.

More generally, let L/F be a tower of Artin-Schreier extensions, i.e. there exists a chain

$$L = L_r/L_{r-1}/\ldots/L_0 = F$$

such that $L_i = L_{i-1}(\theta_{\gamma_i})$ for $\gamma_i \in L_{i-1}$ for $1 \leq i \leq r$. Then we can construct a prime element of L_n inductively by means of this procedure.

1.1.5 Ramification Theory

Here we follow [Ser79, IV.1, IV.2]. Let K/F be a Galois extension of local fields with prime ideals $\mathfrak{p}_K$ and $\mathfrak{p}_F$ respectively. Let $G := \operatorname{Gal}(K/F)$ be the Galois group of K/F, and let π_K respectively π_F be prime elements of $\mathfrak{p}_K$ respectively $\mathfrak{p}_F$. We define the following subgroups:

Definition 1.24. For $\sigma \in G$, we define $i_{K/F}(\sigma) := \nu_K(\sigma(\pi_K) - \pi_K)$.

The *n-th ramification group* of K/F for $n \in \mathbb{N}_0$ is

$$G_n := \{\sigma \in G \ : \ \nu_K(\sigma(\pi_K) - \pi_K) \geq n+1\}.$$

A natural number $n \in \mathbb{N}_0$ is called a *(lower) ramification break* if $G_n \neq G_{n+1}$.

The number $i_{K/F}(\sigma)$ is well-defined, as the valuation $\nu_K(\sigma(\pi) - \pi)$ is independent of the chosen prime element π.

The n-th ramification group G_n can be constructed as follows: Let $\sigma \in G$. As $\sigma(\mathcal{O}_K) = \mathcal{O}_K$ and $\sigma(\mathfrak{p}_K) = \mathfrak{p}_K$ we have for all $n \in \mathbb{N}$ an automorphism $\sigma_n \colon \mathcal{O}_K/\mathfrak{p}_K^{n+1} \to \mathcal{O}_K/\mathfrak{p}_K^{n+1}$. This defines a homomorphism

$$\Psi_n \colon G \longrightarrow \mathrm{Aut}(\mathcal{O}_K/\mathfrak{p}_K^{n+1}), \quad \sigma \longmapsto \sigma_n$$

with $\mathrm{Ker}(\Psi_n) = G_n$.

Theorem 1.25. *Let E/F be a finite Galois extension of local fields with $\mathrm{char}(\kappa_F) = p$ and $G = \mathrm{Gal}(E/F)$.*

(a) The ramification groups form a descending chain that becomes stationary.

(b) $G_i \trianglelefteq G$ for all $i \geq 0$ and G_i is a p-group for each $i \geq 1$.

(c) $G/G_0 \cong \mathrm{Gal}(\kappa_K/\kappa_F)$ is cyclic of order $f_{K/F}$ and $|G_0| = e_{K/F}$.

(d) G_0/G_1 is cyclic and G_i/G_{i+1} is p-elementary abelian for $i \geq 1$. In particular $|G_1| = p^{\nu_p(e)}$.

(e) For each $i \geq 0$ we have an injective homomorphism

$$G_i/G_{i+1} \longrightarrow (1+\mathfrak{p}^i)/(1+\mathfrak{p}^{i+1}), \quad \sigma \longmapsto \frac{\sigma(\pi_K)}{\pi_K}.$$

Proofs for these facts are contained in [Ser79, p. 65-67].

Theorem 1.26. *Let $\sigma \in G_0$ s.th. $\sigma^{p^n} \neq \mathrm{id}$. Then*

$$i_{K/F}(\sigma^{p^{n-1}}) \equiv i_{K/F}(\sigma^{p^n}) \mod p^n.$$

For a proof see [Sna94, Prop. 6.1.34].

The ramification groups are closely connected to the discriminant of K/F:

Theorem 1.27. *Let K/F be a finite Galois extension of local function fields with inertia degree $f_{K/F}$. Then:*

(a) $\nu_K(\mathrm{Diff}(K/F)) = \sum\limits_{\sigma \neq \mathrm{id}} i_{K/F}(\sigma) = \sum\limits_{i=0}^{\infty} (|G_i| - 1)$,

(b) $\mathrm{disc}(K/F) = f_{K/F} \cdot \left(\sum\limits_{i=0}^{\infty} |G_i| - 1 \right)$.

See [Ser79, Prop. IV.4].

1.1.6 Abelian Conductor-Discriminant-Formula

Here we follow [Iwa86, p.113].

Let E/F be an abelian extension of local fields and χ be a character of $\mathrm{Gal}(E/F) = G$. We write $E_\chi := \mathrm{Fix}(\mathrm{Ker}(\chi))$ and define the conductor of χ via

$$\mathfrak{f}(\chi) := \mathfrak{f}(E_\chi/F).$$

Theorem 1.28 (Conductor-Discriminant Formula)**.** *Let E/F be an abelian extension of local fields. Then*

$$\mathfrak{D}(E/F) = \prod_{\chi \text{ irr. character}} \mathfrak{f}(\chi).$$

A proof is given in [Iwa86, Thm. 7.15].

We use this to prove the discriminant formula for C_p^r-extensions which is central for the discriminant calculations throughout the thesis.

Example 1.29. *Let E/F be a C_p-extension. Let $\chi \in \mathrm{Gal}(E/F)^*$. If $\chi = 1$, then $\mathrm{Ker}(\chi) = C_p$ and $E_\chi = \mathrm{Fix}\left(\mathrm{Ker}(\chi)\right) = F$. Hence $\mathfrak{f}(1) = \mathfrak{f}(F/F) = 1$.*

If $\chi \neq 1$, then $\mathrm{Ker}(\chi) = 1$ and $E_\chi = \mathfrak{f}\left(\mathrm{Fix}\left(\mathrm{Gal}(E/F)\right)/F\right) = \mathfrak{f}\left(E/F\right)$, hence

$$\mathfrak{D}(E/F) = \prod_{\chi \in \mathrm{Gal}(E/F)^*} \mathfrak{f}(\chi) = 1 \cdot \prod_{\chi \neq 1} \mathfrak{f}(E/F) = \mathfrak{f}(E/F)^{p-1}.$$

Proposition 1.30. *Let E/F be an elementary abelian extension with Galois group $\mathrm{Gal}(E/F) \cong (C_p)^r$.*

(a) Then for the discriminant ideal, we have

$$\mathfrak{D}(E/F) = \prod_{\substack{Z \leq E \\ Z/F \text{ cyclic}}} \mathfrak{f}(Z/F)^{p-1} = \prod_{\substack{Z \leq E \\ Z/F \text{ cyclic}}} \mathfrak{D}(Z/F),$$

(b) Concerning the discriminant norm, there exist C_p-subfields $E_1, \ldots, E_r \leq E$ such that $D(E_r/F) \geq D(E_{r-1}/F) \geq \ldots \geq D(E_1/F)$ and

$$\mathrm{D}(E/F) = \prod_{i=1}^{r} \mathrm{D}(E_i/F)^{p^{i-1}}.$$

Proof. Let $U := (\wp(E) \cap F)/\wp(F)$. Then by the conductor-discriminant formula we have

$$\mathfrak{D}(E/F) = \prod_{\chi \in \mathrm{Gal}(E/F)^*} \mathfrak{f}(\mathrm{Ker}(\chi)) \overset{\text{Theorem 1.7(b)}}{=} \prod_{a \in U} \mathfrak{f}(\mathrm{Ker}(\chi_a))$$
$$= \prod_{a \in U} \mathfrak{f}(F(\theta_a)/F) = \prod_{\langle a \rangle \leq U} \mathfrak{f}(F(\theta_a)/F)^{p-1},$$

where the last product runs over all cyclic subgroups. Applying Example 1.29, for a fixed C_p-extension $F(\theta_a)/F$ we have $\mathfrak{D}(F(\theta_a)/F) = \mathfrak{f}(F(\theta_a)/F)^{p-1}$.

For part (b), we consider for every $x \in \mathbb{R}$ the set

$$U_x := [0] \cup \left\{ u \in U \mid \nu_{J(F)}(u) \geq x \right\}$$

which clearly forms an $\mathbb{F}_p$-subspace of U.

Consider the ordered set $\{\lambda_1 > \lambda_2 > \ldots > \lambda_s\} = \{\nu_{J(F)}(u) : 0 \neq u \in U\}$. Let $d_i := \dim_{\mathbb{F}_p}(U_{\lambda_i})$.

Now choose a basis of the flag $U_{\lambda_1} < U_{\lambda_2} < \ldots < U_{\lambda_s}$, i.e choose a basis $v_1, \ldots, v_{d_1}$ of U_{λ_1}, supplement with vectors of U_{λ_2} so that $v_1, \ldots, v_{d_1}, v_{d_1+1}, \ldots, v_{d_2}$ forms a basis of U_{λ_2} etc. The basis $(v_1, \ldots, v_r)$ built this way has the property

$$\nu_{J(F)}\left(\sum_{i=1}^{r} \mu_i v_i\right) = \max_{\substack{1 \leq j \leq r \\ \mu_j \neq 0}} (\nu_{J(F)}(v_j)) \qquad \text{for all } (\mu_1, \ldots, \mu_r) \in \mathbb{F}_p^r \setminus 0.$$

Using $\mathfrak{f}(F(\theta_a)/F) = \mathfrak{p}_F^{\mathrm{cond}([a])}$, we get

$$\mathrm{D}(E/F) = \prod_{0 \neq u \in U} \mathfrak{f}(F(\theta_u)/F) = \prod_{i=1}^{r} \mathfrak{f}(F(\theta_{v_i})/F)^{(p-1)\cdot p^{r-i-1}} = \prod_{i=1}^{r} \mathrm{D}(F(\theta_{v_i})/F)^{p^{r-i-1}}.$$

The corresponding C_p-subfields $E_i := F(\wp^{-1}(v_i))$ fulfil the claim. □

Example 1.31. *Let $F = \mathbb{F}_q((t))$ be a local function field with $\mathrm{char}(F) = p$. Let $a, b \in R_F$ be $\mathbb{F}_p$-linearly independent such that $K = F(\theta_a, \theta_b)$ defines a $C_p \times C_p$-extension. The corresponding module is*

$$U := \mathrm{Span}_{\mathbb{F}_p}(a + \wp(F), b + \wp(F)) \leq F/\wp(F).$$

The C_p-subfields of K correspond to $\mathbb{P}^1(\mathbb{F}_p)$. The non-trivial conductors correspond to the non-zero vectors of U. We have

$$\mathrm{disc}(K/F) = \sum_{0 \neq u \in U} \mathrm{cond}(u) = \sum_{(\lambda,\mu) \in \mathbb{F}_p^2 \setminus \{(0,0)\}} \mathrm{cond}([\lambda a + \mu b]).$$

Let $E_1, \ldots, E_{p+1} \leq K$ the C_p-subfields such that E_{p+1} has minimal discriminant. Then we have

$$\mathrm{disc}(K/F) = p\,\mathrm{disc}(E_1/F) + \mathrm{disc}(E_{p+1}/F).$$

Starting with a and b, there are three cases:

(1) Let $\nu_F(a) \neq \nu_F(b)$ and assume without loss of generality $|\nu_F(a)| > |\nu_F(b)|$. Then we have

$$\operatorname{disc}(K/F) = p \operatorname{disc}(F(\theta_a)/F) + \operatorname{disc}(F(\theta_b)/F) = p \cdot d_a + d_b.$$

(2) If $\nu_F(a) = \nu_F(b)$ and $\nu_F(a + \lambda \cdot b) = \nu_F(a)$ for all $\lambda \in \mathbb{F}_p^\times$, then $\operatorname{disc}(E_1)/F = \operatorname{disc}(E_i/F)$ for all $1 \leq i \leq p+1$ and we get

$$\operatorname{disc}(K/F) = (p+1) \operatorname{disc}(E_1/F) = (p+1) \cdot d_a.$$

Note that this case is only possible if $q \neq p$.

(3) Otherwise, we have $\nu_F(a) = \nu_F(b)$ and there exists $\lambda \in \mathbb{F}_p^\times$ such that $c := a + \lambda \cdot b$ has valuation strictly larger than the valuation of a. Thus $E_{p+1} = F(\theta_c)$ has minimal discriminant, and we obtain

$$\operatorname{disc}(K/F) = p \operatorname{disc}(E_1/F) + \operatorname{disc}(F(\theta_c)/F) = p \cdot d_a + d_c.$$

1.2 Asymptotics and Tauberian Theorems

In this section we introduce some tools that we use to attack the asymptotics problem. We frequently have to deal with geometric series with a periodic twist. There is a Tauberian theorem occurring in Ellenberg-Venkatesh we frequently use. Moreover, some formulas for counting C_p-extensions are crucial for the whole thesis and are highlighted here.

1.2.1 Big O-Notation

For two real-valued functions $f,\ g\colon \mathbb{R} \to \mathbb{R}$ we use the following notations:

$$\begin{aligned}
f = O(g) &\iff \exists B > 0, c > 0 \ : \ |f(x)| \leq c \cdot |g(x)| \quad \text{for all} \quad x \geq B, \\
f = o(g) &\iff \lim_{x\to\infty} \frac{f(x)}{g(x)} = 0, \\
f \sim g &:\iff \lim_{x\to\infty} \frac{f(x)}{g(x)} = 1, \\
f \asymp g &:\iff \exists B, c_1, c_2 > 0 \ \ c_1 f(x) \leq g(x) \leq c_2 f(x) \quad \text{for all} \ \ x \geq B.
\end{aligned}$$

We will occasionally write

$$f \ll g : \iff f = o(g)$$

to express that f is of strictly smaller order than g.

It is straightforward to show that $\sim$ and $\asymp$ are equivalence relations.

Discriminant Counting Function

Our main goal is to achieve a similar result as the so-called weak Malle conjecture: Let F be a local function field with constant field $\mathbb{F}_q$ and let G be a finite group. We define the counting function

$$Z(F,G;X) := \#\{E/F \ : \ \mathrm{Gal}(E/F) \cong G, \quad \mathrm{D}(E/F) \leq X\}.$$

Our goal is to find a constant $\alpha_p(G) \in \mathbb{R}_{\geq 0}$ such that

$$Z(F,G;X) \asymp X^{\alpha_p(G)}.$$

In order to obtain a reasonable stronger version, we try to find a periodic function δ_G such that

$$Z(F,G;X) \sim \delta_G(X) X^{\alpha_p(G)}$$

or could prove a $\sim$-asymptotics for a suitable arithmetic progression $X_n = n \cdot D + k$.

The problem is only interesting for $p \mid \#G$. In the case $\#G$ being coprime to p, there exist only finitely many extensions. Thus, there is a bound $B > 0$ such that $Z(F,G;X) \leq B$ for all $X \in \mathbb{R}$ and we always have $a_p(G) = 0$.

1.2.2 Counting C_p-extensions over Local Function Fields

As a first and crucial example we count C_p-extensions over $F = \mathbb{F}_q((t))$. For $x \in \mathbb{R}$, we denote the truncation function

$$\lfloor x \rfloor := \max\{z \in \mathbb{Z} \ : \ z \leq x\}.$$

Definition 1.32. Let $p \in \mathbb{P}$ and $q = p^r$ be a p-power.

For $x \in \mathbb{R}$ we define

$$T_p(x) := \#\{1 \leq i \leq |x| \ : \ i \in \mathbb{N}, \ p \nmid i\}.$$

Let moreover

$$\Gamma_q(x) := \#\{\alpha \in R_F \ : \ |\nu_F(\alpha)| \leq |x|\}$$

and

$$\gamma_q(x) := \#\{\alpha \in R_F \ : \ |\nu_F(\alpha)| = |x|\}.$$

Define $\{x\} := x - \lfloor x \rfloor \in [0,1)$ for $x \in \mathbb{R}$.

For $x \in \mathbb{R}$, we have

$$T_p(x) := \lfloor |x| \rfloor - \lfloor \frac{|x|}{p} \rfloor.$$

Moreover, we have

$$T_p(n) = \lceil n \cdot \frac{p-1}{p} \rceil \quad \text{for all} \ \ n \in \mathbb{N} \tag{1.5}$$

since $n\frac{p-1}{p} = n - \frac{n}{p} = n - \lceil \frac{n}{p} \rceil$ if $p \mid n$, and if $p \nmid n$ we have

$$n - \frac{n}{p} < n - \lfloor \frac{n}{p} \rfloor \leq n - \frac{n}{p} + 1 \Longrightarrow T_p(n) = n - \lfloor \frac{n}{p} \rfloor = \lceil n\frac{p-1}{p} \rceil.$$

Lemma 1.33.
For every $p \in \mathbb{P}$ there is a bounded periodic function $\epsilon_p \colon \mathbb{R}_{\geq 0} \to [-\frac{p-1}{p}, \frac{p-1}{p}]$ of period p such that

$$T_p(x) = \frac{p-1}{p} \cdot x + \epsilon_p(x) \qquad \textit{for all } \; x \in \mathbb{R}_{\geq 0}.$$

Proof. Write $x = pN(x) + r(x) + \{x\}$ where $0 \leq r(x) \leq p-1$, $N(x) \in \mathbb{N}$ and $\{x\} \in [0,1)$ as defined above. With respect to these notations we set

$$\epsilon_p \colon \mathbb{R}_{\geq 0} \to [-\frac{p-1}{p}, \frac{p-1}{p}], \quad x \longmapsto \frac{r(x)}{p} - \frac{(p-1)\{x\}}{p}. \tag{1.6}$$

Indeed, we have

$$\begin{aligned} T_p(x) &= \#\{1 \leq i \leq p \cdot N(x) + r(x) + \{x\} \;\; : \;\; i \in \mathbb{N}, \; p \nmid i\} \\ &= (p-1)N(x) + r(x) \\ &= \frac{p-1}{p}(pN(x) + r(x)) + \frac{r(x)}{p} + \{x\}\frac{p-1}{p} - \{x\}\frac{p-1}{p} \\ &= \frac{p-1}{p}x + \frac{r(x)}{p} - \{x\}\frac{p-1}{p} \\ &= \frac{p-1}{p}x + \epsilon_p(x). \end{aligned} \tag{1.7}$$

By $0 \leq \{x\} < 1$ and $0 \leq r(x) \leq (p-1)$ we immediately get

$$-(p-1) \leq r(x) - (p-1)\{x\} \leq p-1 \Longrightarrow -\frac{p-1}{p} \leq \epsilon_p(x) \leq \frac{p-1}{p}.$$

Finally $r(x+p) = r(x)$ by construction and $\{x+p\} = \{x\}$ as $p \in \mathbb{N}$, hence ϵ_p is a periodic function with period p. □

Lemma 1.34. *Let $p \in \mathbb{P}$ and $q = p^r$ be a p-power.*

(a) For all $x \in \mathbb{R}_{\geq 0}$ we have

$$\Gamma_q(x) = p \cdot q^{T_p(x)}.$$

Moreover, there is a periodic function $\Delta_q \colon \mathbb{R}_{\geq 0} \to [\frac{p}{q}, pq]$ of period p such that

$$\Gamma_q(x) = q^{\frac{p-1}{p}x} \cdot \Delta_q(x).$$

(b) For all $n \in \mathbb{N}$ we have

$$\gamma_q(n) = \begin{cases} p-1, & n = 0 \\ p(q-1)q^{T_p(n)-1}, & p \nmid n \\ 0, & \text{else.} \end{cases}$$

(c) We have $T_p(p \cdot k + r) = (p-1)k + r$ for $k, r \in \mathbb{N}$, $0 \le r < p$, and there is a p-periodic function

$$\delta_q \colon \mathbb{N} \to [0, p\frac{q-1}{q^{1/p}}] \quad \text{with} \quad \delta_q(0) := 0, \quad \delta_q(i) := p\frac{q-1}{q^{1-i/p}} \quad \text{for } i = 1, \dots, p-1$$

such that

$$\gamma_q(n) = q^{\frac{p-1}{p}n}\delta_q(n).$$

Proof. Set $M_x := \{k \in \mathbb{Z}_{<0} \ : \ 1 \le |k| \le x, \ \ p \nmid k\}$. Clearly, we have

$$|M_x| = \lfloor x \rfloor - \#\{p, \dots, \lfloor \frac{x}{p} \rfloor \cdot p\} = T_p(x).$$

Thus, we obtain

$$\begin{aligned} \Gamma_q(x) &= \#\{\alpha \in R_F \ : \ |\nu_F(\alpha)| \le x\} = \#\{\lambda\omega_0 + \sum_{\substack{-|x| \ge i \ge -1 \\ p \nmid i}} a_i t^i \ : \ \lambda \in \mathbb{F}_p, a_i \in \mathbb{F}_q\} \\ &= \#\{\lambda\omega_0 + \sum_{i \in M_x} a_i t^i \ : \ \lambda \in \mathbb{F}_p, a_i \in \mathbb{F}_q\} \\ &= p \cdot q^{|M_x|} = p \cdot q^{T_p(x)}. \end{aligned} \tag{1.8}$$

Define $\Delta_q(x) := p \cdot q^{\epsilon_p(x)}$ with $\epsilon_p(x)$ as defined in (1.6). With (1.7), we get

$$\Gamma_q(x) = p \cdot q^{T_p(x)} \overset{(1.7)}{=} pq^{\frac{p-1}{p}x + \epsilon_q(x)} = q^{\frac{p-1}{p}x} \cdot \Delta_q(x).$$

By $-1 < -\frac{p-1}{p} \le \epsilon_q(x) < \frac{p-1}{p} < 1$ we have $p \cdot q^{-1} \le pq^{\epsilon_p(x)} = \Delta_q(x) \le pq$, completing the proof of (a).

Analogously to (1.8), we have

$$\begin{aligned} \gamma_q(n) &= \#\{\lambda\omega_0 + \sum_{i \in M_n} a_i t^i \ : \ \lambda \in \mathbb{F}_p, a_i \in \mathbb{F}_q, \ a_n \neq 0\} \\ &= \begin{cases} |\mathbb{F}_p^\times| = p-1, & n = 0 \\ |\mathbb{F}_q^\times| pq^{|M_n|-1} = p(q-1)q^{T_p(n)-1}, & p \nmid n \\ 0, & p \mid n, \ n \neq 0. \end{cases} \end{aligned}$$

Lastly $n \in M_n$ is equivalent to $n = 0$ or $p \nmid n$ completing the second assertion. □

Combining these two results, we obtain the following:

Corollary 1.35. *Let q be a p-power, then there exist periodic functions $\delta_q\colon \mathbb{R}_{\geq 0} \to [0, pq]$ and $\Delta_q\colon \mathbb{R} \to [pq^{-1}, pq]$ with period length p such that for all $x \in \mathbb{R}_{\geq 0}$ we have*

$$\gamma_q(x) = \delta_q(x) \cdot q^{\frac{p-1}{p}x} \quad \text{and} \quad \Gamma_q(x) = \Delta_q(x) \cdot q^{\frac{p-1}{p}x}.$$

Theorem 1.36. *Let $p \in \mathbb{P}$ and $q = p^r$ for some $r \geq 1$ and $F = \mathbb{F}_q((t))$. Then we have*

$$Z(F, C_p; X) \asymp X^{\frac{1}{p}}.$$

Proof. For every C_p-extension E/F there is an $a \in F \setminus \wp(F)$ such that $E = F(\theta_a)$.

Moreover, there exists a unique $\alpha \in R_F$ such that $a + \wp(F) = \alpha + \wp(F)$.

By Lemma 1.5(b) there exist $(p-1)$ elements $\alpha_1, \ldots, \alpha_{p-1}$ defining the same field, given by $\alpha_i := i \cdot \alpha$ for $i \in \mathbb{F}_p^\times$. The discriminant is given by the formula

$$\operatorname{disc}(E/F) = \begin{cases} (p-1)(|\nu_F(\alpha)| + 1), & \nu_F(\alpha) < 0 \\ 0, & \nu_F(\alpha) = 0. \end{cases}$$

Let $y = \log_q(X)$, i.e. $X = q^y$. Then we get

$$Z(F, C_p; X) = Z(F, C_p; q^y) = \Gamma_q\left(\frac{y}{p-1} - 1\right) \overset{\text{La. 1.34}}{=} pq^{T_p(\frac{y}{p-1} - 1)} - 1 \quad \text{for all } \ y \in \mathbb{R}_{\geq 0}.$$

The zero-element in R_F does not define a C_p-extension and we have to subtract it. Using Lemma 1.33 we get $\frac{p-1}{p}(y-p) \leq T_p(y) \leq \frac{p-1}{p}(y+p)$. Thus

$$pq^{\frac{p-1}{p}(\frac{y}{p-1} - p - 1)} \leq pq^{T_p(\frac{y}{p-1} - 1)} = Z(F, C_p; q^y) \leq pq^{\frac{p-1}{p}(\frac{y}{p-1} + p - 1)}.$$

Hence, we obtain $Z(F, C_p; q^y) \asymp q^{y \cdot \frac{p-1}{p}\frac{1}{p-1}} = q^{y\frac{1}{p}} = X^{\frac{1}{p}}$. □

Remark 1.37. Set $U(N) := Z(F, C_p; q^{(p-1)(N+1)})$ and write $N := q(N) \cdot p + r(N)$, where $0 \leq r(N) < p$ and $r(N),\ q(N) \in \mathbb{N}$. Writing $\delta(N) := pq^{r(N)}$ defines a period function of period length p which satisfies

$$\begin{aligned} U(N) &= q^{\frac{1}{p}(p-1)N} \cdot pq^{\frac{r(N)}{p}} \\ &= q^{\frac{1}{p}(p-1)N} \cdot \delta(N). \end{aligned}$$

We conclude that $\frac{U(N)}{q^{N/p}}$ does not converge and in particular

$$Z(F, C_p; X) \not\asymp c \cdot X^{\frac{1}{p}} \quad \text{for all } \ c \in \mathbb{R}_{>0}.$$

One general issue is that $Z(F, G; q^N) = Z(F, G; q^{N+1} - 1)$ which makes it impossible to establish a $\sim$-equivalence of type

$$Z(F, G; X) \sim c \cdot X^a$$

for any $c > 0$ and $a > 0$, as

$$\lim_{n\to\infty} \frac{Z(F,G;q^{n+1}-1)}{c\cdot(q^{n+1}-1)^a} = \frac{1}{q^a}\cdot \lim_{n\to\infty} \frac{Z(F,G;q^n)}{c\cdot q^{an}}.$$

Another problem arises from oscillation effects, so that $Z(F, C_p; q^{(pN+k)(p-1)})$ considered as a function in N has a different behaviour depending on the arithmetic progression $pN + k$.

However for any $k \in \{0, \dots, p-1\}$ we have the convergence result

$$U(pN + k) \sim \delta(k)q^N$$

and combined, we have

$$U(N) \sim \delta(N)q^{N/p}.$$

This demonstrates why we can at best expect to find a periodic function $\delta_G \colon \mathbb{N}_0 \to \mathbb{R}_{\geq 0}$ such that

$$Z(F,G;q^N) \sim \delta(N)\cdot q^{\alpha_G\cdot N}.$$

Mostly, we will be satisfied with establishing an $\asymp$-equivalence in our context.

1.2.3 Analytic Framework

Here we collect some basic computational methods we will frequently use. In particular we will introduce and consider certain types of functions which play a key role in our counting. They will involve summation over periodic functions.

Theorem 1.38 (Tauberian Theorem)**.** *Suppose $(a_n)_{n\in\mathbb{N}}$ is a sequence of non-negative real numbers with $a_n = 0$ whenever n is not a power of q, and suppose that the formal power series*

$$\Phi(u) := \sum_{r=0}^{\infty} a_{q^r} u^{-r}$$

is a rational function in $u = q^s$. Let $B \in \mathbb{R}_{>0}$. If $\Phi(u)$ has no poles with $|u| \geq q^B$, then

$$\sum_{1\leq n\leq X} a_n \ll X^B.$$

If $\Phi(u)$ has a pole at $u = q^a$ of order b and no other poles with $|u| \geq q^a$, then:

$$\sum_{1\leq n\leq X} a_n \asymp X^a(\log X)^{b-1}.$$

See [EV05, Lemma 2.3]. A complete proof is given in [Lag12, Lemma A.4].

Our main application is the following Dirichlet series. Consider $F = \mathbb{F}_q((t))$ and a transitive permutation group G. Let

$$a_n := \#\{K/F \mid \mathrm{Gal}(K/F) \cong G,\ \mathrm{D}(K/F) = n\} \quad \text{for} \quad n \in \mathbb{N}.$$

Here, we mean by $\cong$ that there is an isomorphism of permutation groups $\mathrm{Gal}(K/F) \cong G$.

Then we get a sequence $(a_n)_{n\in\mathbb{N}} \geq 0$ with $a_n = 0$ if n is not a power of q. Consider the Dirichlet series

$$\Phi_{F,G}(s) := \sum_{\substack{K/F \\ \mathrm{Gal}(K/F)\cong G}} \mathrm{D}(K/F)^{-s} = \sum_{k\geq 0} a_k k^{-s}.$$

To apply Theorem 1.38 we set $u = q^s$, and we obtain a new power series

$$\Psi_{F,G}(u) = \sum_{k=0}^{\infty} a_{q^k} u^{-k}.$$

Now let us assume that the series $\Psi_{F,G}$ is a rational function with a simple pole at $a \in \mathbb{R}$ and no poles for $\mathrm{Re}(u) > a$. Then we obtain for $X \in \mathbb{R}_{\geq 0}$ that

$$\begin{aligned}\sum_{1\leq n\leq X} a_n &= \sum_{n\leq X} \#\{K/F \mid \mathrm{Gal}(K/F) \cong G,\ \mathrm{D}(K/F) = n\} \\ &= Z(F,G;X) \overset{1.38}{\asymp} X^a.\end{aligned}$$

The most obvious example is given by a geometric series.

Example 1.39. *Let $\lambda \in \mathbb{R}$ and $a_{q^r} = q^{\lambda r}$ for $r \in \mathbb{N}$. Setting $u = q^s$, we get a geometric series*

$$\Phi(u) = \sum_{r\geq 0} a_{q^r} u^{-r} = \sum_{r\geq 1} a_{q^{\lambda r}} q^{-rs} = \sum_{r\geq 1} q^{r(\lambda - s)} = \frac{1}{1-q^{\lambda-s}} = \frac{1}{1-q^{\lambda}q^{-s}},$$

which is a rational function in $u = q^s$. It has a simple pole at $u = q^\lambda$ and no poles with $|u| > q^\lambda$, thus Theorem 1.38 yields as expected

$$\sum_{n\leq X} a_n \asymp X^{\lambda}.$$

Periodic twist of a geometric series Some of the counting functions we consider are geometric series twisted with a periodic function:

Notation 1.40. Let $\delta\colon \mathbb{N}_0 \to \mathbb{R}_{\geq 0}$ be a periodic function with period $D > 0$, $D \in \mathbb{N}$ and $\delta \neq 0$.

Moreover, let $\alpha_0, \alpha_1 \in \mathbb{R}$ and $\alpha\colon \mathbb{C} \to \mathbb{C}, s \mapsto \alpha_0 + \alpha_1 \cdot s$ be an affine function. We have the interpretation in mind that $q^{\alpha_1 \cdot n}$ is a discriminant with discriminant exponent $\alpha_1 \cdot n$.

For $s \in \mathbb{C}$ we write

$$S_{\delta,\alpha,s}(N) := \sum_{n=1}^{N} \delta(n) \cdot q^{\alpha(s)\cdot n}, \quad \Phi_{\delta,\alpha}(s) = \sum_{n=1}^{\infty} \delta(n) \cdot q^{\alpha(s)\cdot n}.$$

Moreover, we define

$$T_{\delta,\alpha,s}\colon \mathbb{N}_0 \to \mathbb{C}, \quad T_{\delta,\alpha,s}(N) := S_{\delta,\alpha,s}(D \cdot N). \tag{1.9}$$

The summation in $T_{\delta,s}$ reflects the arithmetic progression $(a_n)_{n\in\mathbb{N}} := (D \cdot n)_{n\in\mathbb{N}}$. We define

$$\Delta(\delta, \alpha, s) = \sum_{j=1}^{D} \delta(j) q^{\alpha(s)\cdot j} \tag{1.10}$$

and

$$\Phi^T_{\delta,\alpha}(s) := \sum_{n=0}^{\infty} \left(\sum_{j=1}^{D} \delta(j) q^{-\alpha(s)j} \right) \cdot q^{-sDn} = \sum_{n=0}^{\infty} \Delta(\delta, \alpha, s) \cdot q^{-sDn}.$$

Lemma 1.41. *Let $\delta\colon \mathbb{N}_0 \to \mathbb{C}$ be a periodic function of length $D \in \mathbb{N}$. Let $\alpha_0, \alpha_1 \in \mathbb{R}$ with $\alpha_1 > 0$ and $\alpha\colon \mathbb{C} \to \mathbb{C}, z \mapsto \alpha_0 - \alpha_1 \cdot z$. Let $0 \neq s \in \mathbb{C}$ and $T_{\delta,\alpha,s}$ as in (1.9) and $\Delta_{\delta,\alpha,s}$ as in (1.10).*

(a) For all $N \in \mathbb{N}$ we have

$$T_{\delta,\alpha(s)}(N) = \Delta(\delta, \alpha, s) \cdot \frac{1 - q^{-\alpha(s)\cdot DN}}{1 - q^{-\alpha(s)\cdot D}}.$$

(b) For $\mathrm{Re}(s) > \frac{\alpha_0}{\alpha_1}$ the sequence $(T_{\delta,\alpha,s}(N))_{N\in\mathbb{N}}$ converges absolutely and

$$\Phi^T_{\delta,\alpha}(s) = \Delta(\delta, \alpha, s) \cdot \frac{1}{1 - q^{-\alpha(s)D}} \qquad \textit{is in particular rational.}$$

Proof. For $N \in \mathbb{N}$ we have

$$\begin{aligned} T_{\delta,\alpha,s}(N) &= \sum_{n=1}^{DN} \delta(n) \cdot q^{\alpha(s)\cdot n} \\ &= \sum_{k=0}^{N-1} \sum_{j=1}^{D} \delta(j) \cdot q^{\alpha(s)(D\cdot k + j)} \\ &= \sum_{k=0}^{N-1} \Delta(\delta, \alpha, s) q^{\alpha(s)\cdot Dk} \\ &= \Delta(\delta, \alpha, s) \cdot \sum_{k=0}^{N-1} q^{\alpha(s)Dk} \\ &= \Delta(\delta, \alpha, s) \frac{1 - q^{DN\cdot\alpha(s)}}{1 - q^{D\cdot\alpha(s)}}. \end{aligned} \tag{1.11}$$

In particular $\Phi^T_{\delta,\alpha}(s)$ is a rational function in q^s.

By assumption we have $\delta \neq 0$ and $\delta(n) \geq 0$ for all $n \in \mathbb{N}$. Thus for all $s \in \mathbb{R}$ we have $\alpha(s) > 0$ and $\Delta(\delta, \alpha, s) > 0$. Thus we have a pole at $s = \frac{\alpha_0}{\alpha}$ which is the unique root of α. □

The next example is a useful summation for the discriminant counting function over local function fields.

Proposition 1.42. *Let $q = p^r$, $\lambda \in \mathbb{R}$, $\mu \in \mathbb{R} \setminus \{0\}$ and $X \in \mathbb{R}_{\geq 0}$. Then we have*

$$\sum_{\substack{a \in R_F \\ q^{\mu \cdot |\nu_F(a)|} \leq X}} q^{\lambda \cdot |\nu_F(a)|} \asymp X^{\frac{\lambda + (p-1)/p}{\mu}}.$$

Proof. The condition $q^{\mu \cdot |\nu_F(a)|} \leq X$ is equivalent to $|\nu_F(a)| \leq \frac{1}{\mu} \cdot \log_q(X)$, hence to

$$|\nu_F(a)| \leq \lfloor \frac{1}{\mu} \cdot \log_q(X) \rfloor \tag{1.12}$$

since $|\nu_F(a)| \in \mathbb{N}_0$. Moreover, we have

$$q^{\lambda \cdot n} = q^{\frac{\lambda}{\mu} \cdot \mu n} = \left(q^{\frac{\lambda}{\mu}}\right)^{\mu \cdot n} \quad \text{for all} \quad n \in \mathbb{N}_0. \tag{1.13}$$

We use the formula

$$\gamma_q(n) \overset{\text{Cor. 1.35}}{=} \delta_q(n) q^{\frac{p-1}{p} n}, \tag{1.14}$$

where δ_q is periodic of period length p and in particular a bounded function. We obtain

$$\begin{aligned}
\sum_{\substack{a \in R_F \\ q^{\mu \cdot |\nu_F(a)|} \leq X}} q^{\lambda \cdot |\nu_F(a)|} &\overset{(1.12)}{=} \sum_{\substack{a \in R_F \\ |\nu_F(a)| \leq \frac{\log_q(X)}{\mu}}} q^{\lambda \cdot |\nu_F(a)|} \\
&\overset{(1.14)}{=} \sum_{n \leq \frac{\log_q(X)}{\mu}} \delta_q(n) \cdot q^{\frac{p-1}{p} n} q^{\lambda \cdot n} \\
&\overset{(1.13)}{=} \sum_{n \leq \frac{\log_q(X)}{\mu}} \delta_q(n) \cdot \left(q^{\frac{p-1}{p \cdot \mu} + \frac{\lambda}{\mu}}\right)^{\mu \cdot n} \\
&\overset{\text{La. 1.41}}{\asymp} \frac{\left(q^{\frac{p-1}{p\mu} + \frac{\lambda}{\mu}}\right)^{\mu \cdot \lceil \frac{\log_q(X)}{\mu} \rceil} - 1}{q^{\frac{p-1}{p\mu} + \frac{\lambda}{\mu}} - 1} \\
&\asymp X^{\frac{\lambda + (p-1)/p}{\mu}}.
\end{aligned}$$

□

Example 1.43. *Here we continue the example of counting C_p-extensions from Remark 1.37. For $n \in \mathbb{N}_0$, we write $n = pN + r(n)$ with $0 \leq r(n) \leq p-1$ as in the proof of Lemma 1.33. with $q = p^r$ and the periodic function*

$$\delta_q(n) = p \frac{q-1}{q} \cdot q^{\frac{r(n)}{p}} \qquad \text{of length } p.$$

(a) For C_p-extensions we can apply Lemma 1.41 with $\alpha_0 = \frac{p-1}{p}$ and $\alpha_1 = (p-1)$ to obtain the critical pole at $s = \frac{\alpha_0}{\alpha_1} = \frac{1}{p}$.

(b) We can also apply Proposition 1.42 with $\lambda = 0$ and $\mu = (p-1)$ and obtain the exponent

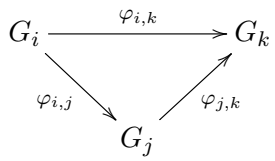
$$s = \frac{\lambda + \frac{p-1}{p}}{\mu} = \frac{\frac{p-1}{p}}{p-1} = \frac{1}{p}.$$

1.3 Cohomology and Explicit Construction

1.3.1 The Absolute Galois Group of Local Function Fields

The absolute Galois group of local fields is well understood. We will give a brief description here and draw some conclusions concerning embedding problems. We follow the book of Ribes and Zaleskii for notations (see [RZ00]) and collect some results from [NSW08].

Definition 1.44. An *inductive system* of finite groups consists of a directed partially-ordered[1] index set $(I, \leq)$, a family of finite groups $(G_i)_{i\in I}$ and a family of morphisms $(\varphi_{i,j}\colon G_i \to G_j)_{i\geq j}$ which are compatible, i.e. for all $i \geq j \geq k$ in I the following diagram commutes:



Definition 1.45. A projective limit of an inductive system of finite groups is called a *profinite group*. It is called a pro-p-group or pro-solvable group respectively if the inductive system consists of finite p-groups or solvable groups respectively.
Let $\mathfrak{c}$ be a class of finite groups which is closed under subgroups, quotients and extensions. Then a pro-$\mathfrak{c}$-group is a projective limit of an inductive system of groups in $\mathfrak{c}$.

Definition 1.46. A pro-$\mathfrak{c}$-group G is called *free* if there exists a set $X \subseteq G$ and a map $i\colon X \to G$ such that

1.) each open normal subgroup of G contains almost all elements of X and

2.) for each pro-$\mathfrak{c}$-group $\widetilde{G}$ and map $j\colon X \to \widetilde{G}$ exists $\exists!$ $\psi\colon G \to \widetilde{G}$ continuous homomorphism such that $\psi \circ i = j$.

$|X|$ is called the rank of G and $i(X)$ is called a basis of G.

Next we collect some important results on the structure of the absolute Galois group of a local function field. For this, let F be a local function field with constant field κ_F of cardinality q and $\mathrm{char}(F) = p$. Denote by G_F the absolute Galois group of F. Its structure is completely determined by the following theorem:

Theorem 1.47 (Absolute Galois group)**.**
Let $F = \mathbb{F}_q((t))$ be a local function field with $\mathrm{char}(F) = p$ and absolute Galois group G_F.

(a) For F_{unr}, the maximal unramified extension, we have $G_{\mathrm{unr}} = \mathrm{Gal}(F_{\mathrm{unr}}/F) \cong \mathrm{Gal}(\widehat{\mathbb{F}_q}/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$ where the Frobenius automorphism is a topological generator.

[1] I.e. $\leq$ is an ordering such that additionally holds: $\forall i, j \in I\ \exists k \in I$ with $i \leq k$ and $j \leq k$.

(b) Let F_{tr} be the maximal tamely ramified extension of F. We have

$$G_{\mathrm{tr}} = \mathrm{Gal}(F_{\mathrm{tr}}/F) = \prod_{\ell \neq p} \mathbb{Z}_\ell \rtimes G_{\mathrm{unr}} = \langle \sigma, \tau \mid \sigma\tau\sigma^{-1} = \tau^q \rangle$$

as a profinite group.

(c) For the absolute Galois group we get $G_F \cong G_p \rtimes G_{\mathrm{tr}}$, where G_p is a free pro-p-group of countably infinite rank.

For a proof see [NSW08], Theorem VII.5.13.

For our work, we are particularly interested in the maximal pro-p-quotient of G_F. The maximal p-extension $F(p)$ of F is defined as the composite of all Galois extensions of F of p-power degree. Write $G_F(p) := \mathrm{Gal}(F(p)/F)$ which is the maximal pro-p-factor group of G_F, see [NSW08, p.414].

Theorem 1.48. *Let F be a local field with $\mathrm{char}(F) = p$. Let G_F be the absolute Galois group of F and $G_F(p)$ be the maximal pro-p-factor group of G_F.*

Then $G_F(p)$ is a free pro-p-group of countably infinite rank.

For a proof see [NSW08], Theorem VII.5.10.

Our main interest is the following consequence:

Corollary 1.49. *Let F be a local function field with $\mathrm{char}(F) = p$. Each finite p-group H is a quotient of G_F, in particular, there exists a field extension K/F with $\mathrm{Gal}(K/F) \cong H$.*

Proof. Let $X = \{x_1, x_2, \ldots\} \subseteq G_F(p)$ and $i\colon X \to G_F(p)$ satisfying the conditions of Definiton 1.46. Consider a numbering $H = \{h_1, \ldots, h_{|H|}\}$ of the elements and consider the map

$$j\colon X \longrightarrow H,\ x_k \longmapsto \begin{cases} h_k, & k \leq |H| \\ h_1, & k > |H|. \end{cases}$$

The induced continuous homomorphism $\phi\colon G_F(p) \to H$ is clearly surjective. Setting $\phi(x) = \mathrm{id}_H$ for $x \in G_{\mathrm{tr}}$ defines a surjective homomorphism $\phi\colon G_F \to H$ as claimed. □

Remark 1.50. We briefly compare this to the absolute Galois group of a p-adic field: While the p'-part is isomorphic to the p'-part in the function field case, the p-part of the absolute Galois group of a p-adic field is a pro-p-group of finite rank, which is free or has one relation. The relation occurs if and only if the p-adic field contains p-th roots of unity.

Hence, there is a drastic difference concerning the p-part. Consequently, there are infinitely many extensions of degree p^n over a local function field for $n \geq 1$, while there are only finitely many degree-n-extensions over a p-adic field for any $n \in \mathbb{N}$.

1.3.2 Central Embedding Problems

A *group extension* ϵ with *kernel* N is an exact sequence of groups

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} H \longrightarrow 1.$$

It is called *central* if $i(N) \subseteq Z(G)$ and it is called *split* if there exists a homomorphism $s\colon H \to G$ such that $\pi \circ s = \mathrm{id}_H$. Otherwise we call it *non-split*. Note that the extension is split if and only if $G \cong N \rtimes H$ is a semi-direct product.

Given a Galois extension K/F with $\mathrm{Gal}(K/F) \cong H$ the embedding problem for K is to find a field extension L/K such that

$$\mathrm{Gal}(L/K) \cong N \quad \text{and} \quad \mathrm{Gal}(L/F) \cong G$$

and such that the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(L/K) & \xrightarrow{\sigma\mapsto\sigma} & \mathrm{Gal}(L/F) & \xrightarrow{\sigma\mapsto\sigma|_K} & \mathrm{Gal}(K/F) & \longrightarrow & 1 \\ & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \\ 1 & \longrightarrow & N & \xrightarrow{\iota} & G & \xrightarrow{\pi} & H & \longrightarrow & 1 \end{array}$$

commutes. We refer to this situation as the embedding problem of the group extension over K and in short, as "embedding problem of G over K".

We call the embedding problem *solvable* if such an extension field L exists.

A solution with minimal discriminant is called a *minimal solution*. Its discriminant over F is called the *minimal discriminant* of the embedding problem. The embedding problem is called *split* or *central*, if the corresponding group extension is split or central, respectively.

The solutions of central embedding problems with kernel $N = C_p$ have a particularly nice structure. If we have one solution, then all solutions are parametrised by C_p-extensions.

Proposition 1.51.
Let F be a local function field of characteristic p. Further, let H and G be finite groups and

$$1 \longrightarrow C_p \longrightarrow G \longrightarrow H \longrightarrow 1 \tag{1.15}$$

be a central non-split embedding problem.

(a) If H is a p-group, then the embedding problem is solvable.

(b) If $M = K(\theta_a)$ is any solution of the embedding problem of type (1.15) then each solution of the embedding problem is of type $M_c := K(\theta_{a+c})$ for some $c \in R_F$.

For a proof see [JLY02, App. A].

The following lemma is useful for determining minimal discriminants.

Lemma 1.52. *Assume* $\operatorname{disc}(K(\theta_\alpha)/F) \notin \{\operatorname{disc}(K(\theta_c)/F) \mid c \in F\}$, *then* $K(\theta_\alpha)/F$ *is a minimal extension.*

Proof. Suppose

$$\operatorname{disc}(K(\theta_{\alpha+c})/F) < \operatorname{disc}(K(\theta_\alpha)/F) \quad \text{for some} \quad c \in F. \tag{1.16}$$

Both fields $K(\theta_\alpha)$ and $K(\theta_{\alpha+c})$ are subfields of the field compositum $L := K(\theta_\alpha, \theta_c)$ with $\operatorname{Gal}(L/K) \cong C_p \times C_p$. Clearly, $\operatorname{disc}(K(\theta_\alpha)/K) > \operatorname{disc}(K(\theta_{\alpha+c})/K)$ by (1.16). Using Example 1.31(1) then yields

$$\operatorname{disc}(L/K) = p \operatorname{disc}(K(\theta_\alpha)/K) + \operatorname{disc}(K(\theta_{\alpha+c})/K).$$

We have $K(\theta_c) \leq L$ with $K(\theta_c) \neq K(\theta_{\alpha+c})$. Hence, Example 1.31(1) and Proposition 1.30 give

$$\operatorname{disc}(K(\theta_c)/K) = \operatorname{disc}(K(\theta_\alpha)/K)$$

and thus $\operatorname{disc}(K(\theta_c)/F) = \operatorname{disc}(K(\theta_\alpha)/F)$ in contradiction to our assumption. Thus $K(\theta_\alpha)$ is a minimal extension. □

Theorem 1.53. *Let* F *be a local function field of characteristic* p *and* G *be a finite group.*

(a) For each finite p*-group* $G \neq \mathbf{1}$, *there are infinitely many* G*-extensions of* F.

(b) If $U \leq Z(G)$ *is a subgroup with* p *elements and there is a* G/U*-extension* K *over* F, *then there are infinitely many extensions with Galois group* G *containing* K.

(c) Let H *be a finite group such that there is a field extension* K/F *with* $\operatorname{Gal}(K/F) \cong H$ *and* $G \neq \mathbf{1}$ *be a finite* p*-group. Then there are infinitely many* $G \times H$*-extensions over* F.

Proof. For (a) we use Proposition 1.51(a) to prove the existence and 1.51(b) for the existence of infinitely many G-extensions. Similarly, (b) follows by 1.51(b).

For (c) note that any finite non-trivial p-group has non-trivial center. Hence using $1 \to C_p \to H \times C_p \to H \to 1$ and induction one obtains infinitely many $H \times G$-extensions by Theorem 1.51(b). □

The following example shows the existence of finite groups G with $p \mid |G|$ such that there exist only finitely many but more than zero extensions K/F with Galois group G.

Example 1.54.

(a) We consider $F = \mathbb{F}_2((t))$ *and* $G = S_3$. *We show here that there is an extension* L/F *with* $\operatorname{Gal}(L/F) \cong S_3$, *but there are only finitely many* S_3*-extensions over* F, *although* $2 = \operatorname{char}(F) \mid |S_3|$.

To affirm the existence part, take for instance $L := F(\sqrt[3]{t}, \zeta_3)$. *This is the splitting field of* $K := F(\sqrt[3]{t})$ *as* $\zeta_3 \notin \mathbb{F}_2$. *As the extension* K/F *is not Galois, we have that* $\operatorname{Gal}(L/F)$ *is non-abelian, hence* $\operatorname{Gal}(L/F) \cong S_3$.

On the other hand, let L/F be any S_3-extension. There are three subfields $K_i \leq L$ with $[K_i : F] = 3$ and $L = K_1K_2$. There are only finitely many degree-3-extensions of F as they are all tamely ramified. Hence, there are only finitely many S_3-extensions over F.

This shows that the statement in Theorem 1.53(c) can not be improved to semi-direct products $G \rtimes H$, as $S_3 = C_3 \rtimes C_2$ and $2 = \mathrm{char}(F) \mid 6 = |S_3|$ demonstrate.

(b) *If $F = \mathbb{F}_4((t))$, then $\zeta_3 \in F$ and there does not exist an S_3-extension over F, as every degree-3-extension K/F is at most tamely ramified and therefore a radical extension which is a Galois extension due to $\zeta_3 \in F$.*

(c) *Now let $p = 3$ and $F = \mathbb{F}_3((t))$. Let $K := F(\omega) := \mathbb{F}_9((t))$ be the unramified C_2-extension of F. We will show in Chapter 3 that the infinite series of fields*

$$L_n := K(\theta_{\wp(t^{-3n-1})\omega}), \qquad n \in \mathbb{N},$$

is a series of non-isomorphic field extensions with $\mathrm{Gal}(L_n/F) \cong S_3$. The fields are non-isomorphic as the discriminant exponents $\mathrm{disc}(L_n/K) = 2 \cdot ((3n+1)+1)$ are pairwise different.

Generalising Example 1.54(a), we obtain:

Lemma 1.55. *Let F be a local function field with $\mathrm{char}(F) = p$ and $G \leq S_n$ be a transitive permutation group over n points with $p \nmid n$. Then there are only finitely many G-extensions of F.*

Proof. Let K/F be a extension of degree n with $\mathrm{Gal}(K/F) = G \leq S_n$ and let L/F be the Galois closure of K/F. Then, L is the splitting field of K/F. As

$$n = [K : F] \overset{(1.1)}{=} e_{K/F} \cdot f_{K/F} \quad \text{and} \quad p \nmid n,$$

we have that K/F is tamely ramified. Thus, L/F is tamely ramified as the composite of tamely ramified extensions. Thus, there are only finitely many tamely ramified extensions of degree $|G|$, which proves the statement of the Lemma. □

1.3.3 Cohomology of Groups

Here we simply recall definitions and some basic results we need. These standard definitions are taken from [NSW08, p. 15ff].

Let G be a finite group. We call an abelian group A a *G-module* if G is acting on A. We will write $(G, \cdot)$ multiplicatively and $(A, +)$ additively. We are mainly interested in the 0-th, 1-st and 2-nd cohomology group and their interpretations.

Definition 1.56. Let G be a finite group and A be a G-module.

(a) The 0-th cohomology group is

$$H^0(G, A) := \mathrm{Fix}_G(A) = \{a \in A \mid a^g = a \ \forall g \in G\}.$$

(b) A map $f\colon G \to A$ with $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$ for all $\sigma, \tau \in G$ is called a 1-cocycle[2] and $Z^1(G, A)$ is the set of all 1-cocycles.

A 1-coboundary[3] is a map

$$G \longrightarrow A, \quad \sigma \longmapsto \sigma \cdot a - a$$

for a fixed $a \in A$. $B^1(G, A)$ is the set of all 1-coboundaries.

(c) $Z^1(G, A)$ forms an abelian group via

$$f_1 \cdot f_2\colon G \to A, \quad \sigma \mapsto f_1(\sigma) + f_2(\sigma)$$

and $B^1(G, A) \leq Z^1(G, A)$ forms a subgroup.

The quotient group $H^1(G, A) := Z^1(G, A)/B^1(G, A)$ is the first cohomology group.

Similarly, we define in the following definition the second cohomology group $H^2(G, A)$ as the quotient of cocycles modulo coboundaries. $H^2(G, A)$ characterises the group extensions $1 \longrightarrow A \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$.

Definition 1.57. Let G be a finite group acting on an abelian group $(A, +)$.

(a) Let $f\colon G \times G \to A$ and write $f_{\sigma,\tau} := f(\sigma, \tau)$. The map f is called a 2-cocycle[4] if

$$f(\rho, \sigma) + f(\rho\sigma, \tau) = \rho \cdot f(\sigma, \tau) + f(\rho, \sigma\tau) \quad \text{for all} \quad \rho, \sigma, \tau \in G$$

and $Z^2(G, A)$ is the set of all 2-cocycles.

(b) For any map $a\colon G \to A, \sigma \mapsto a_\sigma$ the associated function

$$G \times G \to A, \quad (\sigma, \tau) \mapsto a_\sigma + \sigma a_\tau - a_{\sigma\tau}$$

is called a 2-coboundary[5] and $B^2(G, A)$ is the set of all 2-coboundaries.

(c) $Z^2(G, A)$ forms a group with pairwise multiplication, i.e.

$$(f_1 \cdot f_2)(\sigma, \tau) := f_1(\sigma, \tau) + f_2(\sigma, \tau).$$

The quotient group $H^2(G, A) := Z^2(G, A)/B^2(G, A)$ is called the second cohomology group.

Definition 1.58. Let A be an abelian group and

$$1 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1$$

be an exact sequence of finite groups. For all $\sigma \in G$ let s_σ be a fixed pre-image under π. Then G acts on A via

$$\sigma \cdot a := s_\sigma \iota(a) s_\sigma^{-1} \quad \text{for all} \quad \sigma \in G, \quad a \in A.$$

The second cohomology group $H^2(G, A)$ with respect to this G-action is also called "the cohomology group" of the group extension.

[2] or *crossed homomorphism*
[3] or *principal crossed homomorphism*
[4] or *factor system*
[5] or *splitting factor system*

Remark 1.59. (a) Note that A being abelian is crucial so that $Z^i(G,A)$, $B^i(G,A)$ and $H^i(G,A)$ indeed form groups.

(b) If the group extension $1 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1$ is central, then the induced G-module on A is trivial.

Example 1.60. *Let L/F be a finite Galois extension of (local) function fields and $G = \mathrm{Gal}(L/F)$.*

(a) Let $A = (L,+)$, then $H^0(G,L) = \mathrm{Fix}_G(L) = F$ is the fixed field.

Moreover, we get a 1-cocycle

$$f_\gamma \colon G \to L, \quad \sigma \mapsto (\sigma - 1)(\gamma)$$

for all $\gamma \in L$.

(b) For any 2-coboundary $a \colon G \to \mathbb{F}_p$ with coefficients in $\mathbb{F}_p$ the map

$$(\wp(a_\sigma))_{\sigma \in G} := (a_\sigma^p - a_\sigma)_{\sigma \in G}$$

forms a 1-cocycle. This holds as $\wp$ commutes with $\sigma \in G$ and $y^p - y = 0$ for all $y \in \mathbb{F}_p$.

Theorem 1.61. *Let L/K be a finite Galois extension with $G = \mathrm{Gal}(L/K)$. Then:*

(a) $H^1(G, L^\times) = 0$ is trivial.

(b) $H^1(G,L) = 0$ and $H^2(G,L) = 0$.

A proof is given in [Led05, p. 32].

Note that in general $H^2(G, L^\times)$ does not have to be trivial.

1.3.4 Construction of p-Extensions in Characteristic p

Finally, we state a classical construction by Witt [Wit36] for all solutions of a central embedding problem of finite p-groups with elementary abelian kernel in characteristic p. Although we do not use it directly in this thesis, we want to highlight this construction as it is highly useful in the context of constructions of p-group extensions over local function fields. We used this construction to construct some D_4-extensions, Q_8-extensions, $H(p,2)$-extensions and $\widetilde{H}(p,2)$-extensions. This is very useful because one solution automatically gives us all solutions to such a central embedding problem.

We will give the construction for the kernel C_p first.

Preliminaries Let $1 \longrightarrow (C_p, +) \xrightarrow{\iota} G \xrightarrow{\pi} H \longrightarrow 1$ be a central embedding problem of p-groups and let K/F be a field extension with $\mathrm{Gal}(K/F) = H$.

Moreover, we identify $\chi\colon C_p \longrightarrow \mathbb{F}_p \subseteq K$, i.e. $\chi(C_p)$ is the prime field of K.

(i) Let R be a fixed representative system of $G/\iota(C_p)$,

(ii) Let $r_\sigma \in R$ be a fixed pre-image of $\sigma \in H$ under π,

(iii) Let $g_{\sigma,\tau} \in C_p$ be satisfying $r_\sigma r_\tau = r_{\sigma\tau}\iota(g_{\sigma,\tau})$ for all $\sigma, \tau \in H$.

Conclusions:

(1) $(g_{\sigma,\tau})_{\sigma,\tau}$ forms a 2-cocycle, i.e. $g \in Z^2(H, C_p)$ and

$$\mathbb{F}_p \ni \chi(g_{\sigma,\tau}) + \chi(g_{\rho,\sigma\tau}) = \chi(g_{\rho,\sigma}) + \chi(g_{\rho\sigma,\tau}) \qquad \text{for all } \rho, \sigma, \tau \in H.$$

Moreover, $g \in Z^2(H, K)$ forms a factor system over K via the inclusion $C_p \hookrightarrow K$, more precisely via the canonical map

$$H^2(H, \mathbb{F}_p) \to H^2(H, K).$$

(2) Let $\alpha \in K$ such that $\mathrm{Tr}_{K/F}(\alpha) \neq 0$ and set

$$a_\sigma := \frac{1}{\mathrm{Tr}_{K/F}(\alpha)} \cdot \sum_{\tau \in G} g_{\sigma,\tau} \cdot \sigma\tau(\alpha) \quad \text{for } \sigma \in H.$$

Then $(a_\sigma)_{\sigma \in H} \subseteq K$ satisfies

$$g_{\sigma,\tau} = a_\sigma + \sigma a_\tau - a_{\sigma\tau} \quad \text{for all } \sigma, \tau \in H.$$

That is, the factor system is splitting over K.

(3) $(\wp(a_\sigma))_{\sigma \in H}$ forms a crossed homomorphism (or a 1-cocycle).

(4) Using $\mathrm{Tr}_{K/F}(\alpha) \neq 0$ and the choice

$$\gamma := \frac{1}{\mathrm{Tr}_{K/F}(\alpha)} \cdot \sum_{\tau \in G} a_\tau \cdot \tau(\alpha)$$

we get

$$\wp(a_\sigma) = a_\sigma^p - a_\sigma = \sigma(\gamma) - \gamma \quad \text{for all } \sigma \in H.$$

(5) Let θ_γ be a zero of $X^p - X - \gamma$. Then $L = K(\theta_\gamma)$ is a solution of the embedding problem, i.e. $\mathrm{Gal}(L/F) \cong G$.

(6) For each solution $\tilde{L}/F$, there is $f \in F$ satisfying $\tilde{L} = K(\theta_{\gamma+f})$.

Proof: The proof is mainly done in two papers of Witt ([Wit35], [Wit36]).

(1) This is a well-known result in extension theory, see for instance [NSW08] or [Led05].

(2) We have $H^2(H,K) = 0$, see [Led05, Ch. 4.2]. Hence $H^2(H,C_p) \to H^2(H,K)$ is the zero-map and there exist $a_\sigma \in K,\ \sigma \in H$ such that

$$a_\sigma + \sigma a_\tau - a_{\sigma\tau} = g_{\sigma,\tau} \quad \text{for all } \sigma,\tau \in H.$$

An explicit construction can be found in [Wit35, I.(3)]: Take an element $\alpha \in K$ such that $\mathrm{Tr}_{K/F}(\alpha) \neq 0$. Then a solution for $(a_\sigma)_{\sigma\in G} \in K$ is given via

$$a_\sigma := \frac{1}{\mathrm{Tr}_{K/F}(\alpha)} \cdot \sum_{\tau\in G} g_{\sigma,\tau} \cdot \sigma\tau(\alpha).$$

(3) $\phi\colon H \to K, \sigma \mapsto \wp(a_\sigma)$ forms a 1-cocycle: Firstly $\wp(g_{\sigma,\tau}) = 0$ as $g_{\sigma,\tau} \in \mathbb{F}_p$. Moreover, we have for all $\sigma,\tau \in H$:

$$\phi(\sigma\tau) = \wp(a_{\sigma\tau}) = \wp(a_\sigma + \sigma a_\tau) = \wp a_\sigma + \sigma\wp a_\tau = \phi(\sigma) + \sigma\phi(\tau).$$

(4) It is well-known that $H^1(H,K) = 0$. One explicit construction is given in [Wit35, I.(2)] via $\mathrm{Tr}_{K/F}(\alpha) \neq 0$ and

$$\gamma := \frac{1}{\mathrm{Tr}_{K/F}(\alpha)} \cdot \sum_{\tau\in G} a_\tau \cdot \tau(\alpha).$$

Thus there is a $\gamma \in K$ such that $(\sigma - 1)(\gamma) = \wp(a_\sigma)$ for all $\sigma \in H$.

(5) This assertion is proven in [Wit36, III. Konstruktion] with the verification of formulas (7) - (13b) in that paper.

Let $\theta := \theta_\gamma$ be a root of $x^p - x - \gamma$. Note that the extension $K(\theta)/F$ is Galois as

$$\sigma(\gamma) = \gamma + \wp(a_\sigma) \quad \Longrightarrow \quad \theta + a_\sigma \text{ is a root of } x^p - x - \sigma(\gamma).$$

Moreover, we define $u_\sigma \in \mathrm{Gal}(K(\theta)/F)$ for $\sigma \in H$ via

$$u_\sigma(\theta) = \theta + a_\sigma, \quad u_\sigma(k) = \sigma(k) \quad \text{for all } k \in K$$

and for all $g \in C_p$

$$\tilde{g} \in \mathrm{Gal}(K(\theta)/F), \quad \tilde{g}(\theta) = \theta + \chi(g), \quad \tilde{g}(k) = k \ \text{ for all } \ k \in K.$$

These automorphisms satisfy

$$\begin{aligned} u_\sigma u_\tau &= \tilde{g}_{\sigma,\tau} u_{\sigma\tau}, \\ u_\sigma \tilde{g} &= \tilde{g} u_\sigma. \end{aligned}$$

Thus, we conclude $\mathrm{Gal}(K(\theta)/F) \cong G$.

(6) This is Proposition 1.51.

Example 1.62. *Consider the group extension*

$$1 \to C_p \to C_{p^{n+1}} \to C_{p^n} \to 1.$$

Let $C_{p^n} = \langle \sigma \rangle$. *Then we have a factor system*

$$g_{\sigma^i,\sigma^j} = \begin{cases} 1, & i+j \geq p^n, \\ 0, & i+j < p^n. \end{cases}$$

Let K_n/F *be a* C_{p^n}*-extension. Then every element* $a_\sigma \in K_n$ *such that* $\mathrm{Tr}_{K_n/F}(a_\sigma) = 1$ *describes a splitting factor system via*

$$a_1 = 0, \quad a_\sigma^i = a_\sigma + \sigma(a_{\sigma^{i-1}}) \ \text{ for all } \ 1 \leq i \leq p^n - 1.$$

Let K_i *be the unique subextension with* $[K_i : F] = p^i$ *and* $K_i = K_{i-1}(\theta_i)$. *One choice for* a_σ *is given by*

$$a_\sigma := (-1)^n(\theta_1 \cdots \theta_n)^{p-1}.$$

If $\gamma_{n+1} \in K_n$ *is a solution of*

$$(\sigma - 1)(\gamma_n) = \wp(a_\sigma)$$

then $K_{n+1} := K_n(\theta_{\gamma_n})/F$ *is a* $C_{p^{n+1}}$*-extension. The automorphism* $\tilde{\sigma} \in \mathrm{Gal}(K_{n+1}/F)$ *given by*

$$\tilde{\sigma}(\theta_{n+1}) := \theta_{n+1} + a_\sigma, \quad \tilde{\sigma}|_{K_n} = \sigma$$

is a generator of $\mathrm{Gal}(K_{n+1}/F)$.

Construction with Elementary Abelian Kernel

More generally we can use an analogous construction when considering a central extension of finite p-groups of type

$$1 \to C_p^r \to G \to H \to 1.$$

Let $\chi_1, \ldots, \chi_r \in \chi(C_p^r) = \mathrm{Hom}(C_p^r, \mathbb{F}_p)$ be a basis of the characters of C_p^r. Then we get a factor system $\chi_i(g)$ for each $1 \leq i \leq r$ given by

$$(\chi_i(g))_{\sigma,\tau} := \chi_i(g_{\sigma,\tau}).$$

We solve each factor system with the approach above:

- Take $(a_\sigma^{(i)})_{\sigma \in H} \in K a_\sigma^{(i)} + \sigma a_\tau^{(i)} - a_{\sigma\tau}^{(i)} = \chi_i(g_{\sigma,\tau})$,
- Let $\gamma_i \in K$ such that

$$(\sigma - 1)(\gamma_i) = \wp(a_\sigma^{(i)}) \quad \text{for all } \ 1 \leq i \leq n,$$

- Let $\theta_i \in \hat{K}$ such that $\wp(\theta_i) = \gamma_i$ and define $L := K(\theta_1, \ldots, \theta_r)$.
- Then L/F is Galois and $\mathrm{Gal}(L/F)$ is generated by the automorphisms

$$\bar{g} \cdot \theta_i = \chi_i(g), K \leq \mathrm{Fix}(\bar{g}); \qquad u_\sigma(\theta_i) = \theta_i + a_\sigma^{(i)}, \quad u_\sigma|_K = \sigma$$

  for all $g \in C_p^r,\ \sigma \in H$.

Then $\mathrm{Gal}(K(\theta)/F) \cong G$, more precisely $g \in C_p^r$ and $\sigma, \tau \in H$ satisfy the relations

$$\begin{aligned} u_\sigma u_\tau &= \tilde{g}_{\sigma,\tau} u_{\sigma\tau}, \\ u_\sigma \tilde{g} &= \tilde{g} u_\sigma. \end{aligned}$$

Chapter 2

Conductor Density of Abelian Extensions

All the results of this chapter were published in a paper with J. Klüners, see [KM20]. Here we explicitly count all extensions of a local function field with a fixed abelian Galois group up to a conductor bound. Let G be a finite abelian group and F be a local function field of characteristic p. The main object is the counting function

$$\mathfrak{Z}(F, G; n) := \#\{E/F \text{ Galois } : \mathrm{Gal}(E/F) \cong G \text{ and } \mathrm{N}(\mathfrak{f}(E/F)) \leq q^n\},$$

where $\mathrm{N}(\mathfrak{f}(E/F))$ is the norm of the conductor. Note that we count with respect to conductor exponent here. We will establish explicit formulas and analyse its asymptotic behaviour. The main difficulty is the p-part of G which will be handled first.

By class field theory, all extensions of F with Galois group G are in bijection with quotient groups of the unit group $F^\times$. For a conductor bound n, we can restrict this to a finite quotient group X_n of $F^\times$. In a first step, we construct these quotient groups X_n and we compute the p^i-ranks of these groups. Secondly, we need to count all quotient groups of X_n isomorphic to G, which is equivalent to computing the number of subgroups of X_n that are isomorphic to G. We apply well-known formulas and obtain an explicit description of the conductor counting function.

Note that the problem of determining the conductor density is significantly easier than the problem of determining the discriminant density. As by the conductor-discriminant formula, we need to know the conductor of all subfields, in contrast to only knowing the maximal conductor of any subfield. Nevertheless, we apply the result on the conductor density to establish a lower bound on the discriminant density of abelian groups which Lagemann proved in [Lag10] and we obtain an interpretation of the discriminant asymptotics exponent.

2.1 Certain Quotient Groups of the Unit Group

Let again $\mathbb{F}_q$ be a finite field with $q = p^f$ elements and $F = \mathbb{F}_q((t))$ be the Laurent series ring over $\mathbb{F}_q$. Let $\mathcal{O}_F = \mathbb{F}_q[[t]]$ be the local ring with maximal ideal $\mathfrak{p} = t\mathcal{O}_F$. By the main theorem of local

class field theory, we get a one-to-one correspondence of abelian extensions E/F and norm groups $U := \mathrm{N}_{E/F}(E^\times)$ in $F^\times$. Recall from Chapter 1 the definition of the conductor

$$\mathfrak{f}(E/F) = \mathfrak{p}^{c(\mathrm{N}_{E/F}(E^\times))}$$

with $c(U)$ being the minimal natural number n such that $1 + \mathfrak{p}^n \leq U$.

Theorem 2.1. *The mapping $E \mapsto \mathrm{N}_{E/F}(E^\times)$ defines a bijection between finite abelian extensions of F and open subgroups of $F^\times$ of finite index.*

Moreover, the Galois group $\mathrm{Gal}(E/F)$ is isomorphic to the quotient group $F^\times/U$.

For a proof, see [FV02, Theorem 6.2., p. 154].

Let G be a finite abelian group of exponent $\exp(G)$. Recall $F^\times \cong \mathbb{Z} \times \mathbb{F}_q^\times \times (1+\mathfrak{p})$, see Hasse ([Has69, Ch. 15]). We define

$$U_n := (1+\mathfrak{p})/(1+\mathfrak{p}^n) \quad \text{and} \quad X_n(G) := \mathbb{Z}/\exp(G)\mathbb{Z} \times \mathbb{F}_q^\times \times U_n.$$

By class field theory, the counting problem reduces to count the number of open subgroups $U \leq F^\times$ with $F^\times/U$ isomorphic to G. The conductor bound $\mathrm{N}(\mathfrak{F}(E/F)) \leq q^n$ is equivalent to $1 + \mathfrak{p}^n \leq U$. Moreover, $F^\times/U \cong G$ implies that $\exp(G)$ annihilates $F^\times/U$. So for our counting problem it is sufficient to consider the subgroups of $F^\times$ containing

$$\exp(G)\mathbb{Z} \times 1 \times (1+\mathfrak{p}^n)$$

which correspond to the subgroups of $X_n(G)$.

By dualising, the number of subgroups of $F^\times$ with quotient isomorphic to G is exactly the number of subgroups of $X_n(G)$ isomorphic to G. Thus we reduce our counting problem to counting subgroups in certain finite abelian groups.

In establishing our desired formula, we first study higher unit groups, and consider formulas on subgroups of finite abelian groups depending on the p^k-ranks of the groups.

In general, for a finite abelian group and $n \in \mathbb{N}$, we get the subgroups

$$G^n := \{g^n \mid g \in G\}$$

and the n-th torsion subgroup

$$G[n] := \{g \in G \mid g^n = 1\}.$$

For a prime $p \in \mathbb{P}$, we set the p^n-rank of G as

$$\mathrm{rk}_{p^n}(G) := \log_p \left(\frac{|G^{p^{n-1}}|}{|G^{p^n}|} \right).$$

In the following, we will fix some notations and abbreviations for an abelian p-group.

Definition 2.2. Let G be a finite abelian p-group and $k \in \mathbb{N}$.

We set $r_k(G) := \mathrm{rk}_{p^k}(G)$.

Moreover, we set $\tilde{r}_k(G) := r_k(G) - r_{k+1}(G)$.

A sequence of elements $(g_1, \ldots, g_r)$ is called a *group-basis* of G if each element $g \in G$ has a unique representation

$$g = g_1^{i_1} \cdots g_r^{i_r}, \quad 0 \le i_j < \mathrm{ord}(g_j).$$

Remark 2.3. Let G be a finite abelian p-group of exponent p^e. If $(g_1, \ldots, g_r)$ is a group-basis of G, then $\tilde{r}_k(G)$ is the number of generators with $\mathrm{ord}(g_j) = p^k$, i.e. it is the number of cyclic factors of G isomorphic to C_{p^k}.

$r_k(G)$ is the number of generators of order $\ge p^k$.

We have the decomposition

$$G \cong (C_p)^{\tilde{r}_1(G)} \times (C_{p^2})^{\tilde{r}_2(G)} \times \cdots \times (C_{p^e})^{\tilde{r}_e(G)}.$$

Lemma 2.4. *Let $(v_1, \ldots, v_f)$ be an $\mathbb{F}_p$-basis of $\mathbb{F}_q$. Then the following holds:*

(a) $1 + \mathfrak{p}$ has a $\mathbb{Z}_p$-basis

$$\{1 + v_i t^k : k \in \mathbb{N}, p \nmid k, 1 \le i \le f\} \quad \text{and}$$

$$\{\overline{1 + v_i t^k} : 1 \le i \le f, k \le n-1, p \nmid k\} \quad \text{is a group-basis of } U_n.$$

(b) For each $v \in \mathbb{F}_q^\times$ and $i \ge 1$ we have $\mathrm{ord}(\overline{1 + vt^i}) = p^{\lceil \log_p(n/i) \rceil}$ in U_n.

(c) For all $j \in \mathbb{N}$, the torsion group $U_n[p^j]$ is generated by

$$\{1 + v_i t^k : 1 \le i \le f, p \nmid k, \lceil n/p^j \rceil \le k \le n-1\}.$$

(d) For all $k \in \mathbb{N}$ we have

$$r_k(U_n) = f\left(\lfloor \frac{n-1}{p^{k-1}} \rfloor - \lfloor \frac{n-1}{p^k} \rfloor\right), \qquad \mathrm{rk}_{p^k}(X_n(G)) = r_k(U_n) + 1.$$

Proof. (a) The first assertion on the $\mathbb{Z}_p$-basis is shown in [Has69, p. 227].

The second assertion concerning the group basis follows, using the elements of the $\mathbb{Z}_p$-generators of $\mathbb{Z}_p$ whose residue is non-zero in $U_n = (1+\mathfrak{p})/(1+\mathfrak{p})^n$ and the fact that

$$\prod_{i=1}^{r} \prod_{p \nmid k} \left(1 + v_i t^k\right)^{e_{i,k}} \in 1 + \mathfrak{p}^n \iff \left(1 + v_i t^k\right)^{e_{i,k}} \in 1 + \mathfrak{p}^n \text{ for all } 1 \le i \le r,\ p \nmid k.$$

(b) U_n is a p-group of order q^{n-1} since $\langle 1+\mathfrak{p}^i\rangle/\langle 1+\mathfrak{p}^{i+1}\rangle \cong \mathbb{F}_q$ for all $i \geq 1$. Let $i \leq n$ and put $\alpha := \overline{1+vt^i} \in \langle 1+\mathfrak{p}\rangle/\langle 1+\mathfrak{p}^n\rangle$ with $v \in \mathbb{F}_q^\times$ and $k \in \mathbb{N}$. Then:

$$\begin{aligned}\overline{1+vt^i}^{p^k} = 1 &\iff v^{p^k}t^{ip^k} \in \mathfrak{p}^n \iff ip^k \geq n \\ &\iff p^k \geq \frac{n}{i} \overset{k\in\mathbb{N}}{\iff} k \geq \lceil \log_p(\frac{n}{i})\rceil.\end{aligned}$$

(c) This is (a) and (b) with $\lceil \log_p(n/k)\rceil \leq j \iff n/k \leq p^j \iff k \geq n/p^j$.

(d) By (a), $\mathscr{B} = \{\overline{1+v_jt^i} : 1 \leq i < n \text{ and } p \nmid i\}$ is a group-basis of $X_n(G)$. Then

$$r_k(X_n(G)) = |\{g \in \mathscr{B} : \operatorname{ord}(g) \geq p^k\}|.$$

By (b), we have $\operatorname{ord}(\overline{1+v_jt^i}) \geq p^k \iff ip^{k-1} < n \iff ip^{k-1} \leq n-1$, hence

$$r_k(U_n) = f \cdot |\{i : i \leq \lfloor \frac{n-1}{p^{k-1}}\rfloor, p \nmid i\}| = f(\lfloor \frac{n-1}{p^{k-1}}\rfloor - \lfloor \frac{n-1}{p^k}\rfloor).$$

Note that $r_k(X_n(G)) = r_k(U_n) + 1$ since $p \nmid |\mathbb{F}_q^\times|$. □

2.2 Conductor Density of Abelian p-groups

For a finite abelian group G let $G_p = \{g \in G : \operatorname{ord}(g) = p^a \text{ for some } a \in \mathbb{N}_0\}$ be the p-Sylow subgroup of G and let $G_{p'}$ denote the coprime to p part of G. For finite abelian groups G and A we define

$$\operatorname{Inj}(G,A) := \{\phi : G \to A \text{ monomorphism}\}, \quad \alpha_G(A) := |\{U \leq A : U \cong G\}|.$$

We immediately get

$$\alpha_G(A) \cdot |\operatorname{Aut}(G)| = |\operatorname{Inj}(G,A)|. \tag{2.1}$$

We start with the following reduction to p-groups.

Lemma 2.5. *We have the decompositions*

$$\operatorname{Inj}(G,A) \cong \prod_{\ell\in\mathbb{P}} \operatorname{Inj}(\mathrm{G}_\ell, \mathrm{A}_\ell) \quad \textit{and} \quad \alpha_G(A) = \prod_{\ell\in\mathbb{P}} \alpha_{G_\ell}(A_\ell).$$

In particular $\alpha_G(A) = \alpha_{G_p}(A_p) \cdot \alpha_{G_{p'}}(A_{p'})$ *and* $|\operatorname{Inj}(G,A)| = |\operatorname{Inj}(G_p(A_p))| \cdot |\operatorname{Inj}(G_{p'}, A_{p'})|$.

Proof. The structure theorem of finite abelian groups gives decompositions $G = \prod_{\ell\in\mathbb{P}} G_\ell$ and $A = \prod_{\ell\in\mathbb{P}} A_\ell$, where only finitely many factors are non-trivial. So every element $g \in G$ can uniquely be written as $g = (g_\ell)_{\ell\in\mathbb{P}}$ for $g_\ell \in G_\ell$, and with this we can define

$$\Psi\colon \prod_{\ell\in\mathbb{P}} \operatorname{Inj}(\mathrm{G}_\ell, \mathrm{A}_\ell) \longrightarrow \operatorname{Inj}(G,A), \quad (\phi_\ell) \longmapsto \left(g \mapsto \sum_{\ell\in\mathbb{P}} \phi_\ell(g_\ell)\right).$$

The sum is finite and $\Psi((\phi_\ell)_{\ell\in\mathbb{P}})$ is injective by the Chinese Remainder Theorem.

The map Ψ has an inverse mapping given by

$$\Phi\colon \operatorname{Inj}(G,A) \longrightarrow \prod_{\ell\in\mathbb{P}}(G_\ell, A_\ell), \quad \phi \longmapsto (\phi|_{G_\ell})_{\ell\in\mathbb{P}}.$$

This is well-defined as monomorphisms preserve orders of group elements. More precisely, $\operatorname{ord}(g_\ell) = \ell^k \iff \operatorname{ord}(\phi(g_\ell)) = \ell^k$ for $\phi \in \operatorname{Inj}(G,A)$, $\ell \in \mathbb{P}$ and $g_\ell \in G_\ell$.

It is immediate that $\Phi \circ \Psi$ and $\Psi \circ \Phi$ are the identity, hence Φ is an isomorphism.

The factorization of $\alpha_G(A)$ is then immediate by the equations

$$\alpha_G(A) \cdot |\operatorname{Aut}(G)| = |\operatorname{Inj}(G,A)|$$

and

$$|\operatorname{Aut}(G)| = \prod_{\ell\in\mathbb{P}}|\operatorname{Aut}(G_\ell)|, \qquad |\operatorname{Inj}(G,A)| = \prod_{\ell\in\mathbb{P}}|\operatorname{Inj}(G_\ell,A_\ell)|. \qquad \square$$

Thus it is sufficient to consider finite abelian p-groups. In the following, G and A will be finite abelian p-groups, and we write $r_i(G) = \operatorname{rk}_{p^i}(G)$ throughout. As in [Lag10] we define

$$f_G(t_1,\dots,t_e) := \prod_{k=1}^{e} t_k^{r_{k+1}(G)} \prod_{j=r_{k+1}(G)}^{r_k(G)-1} (t_k - p^j). \tag{2.2}$$

Lemma 2.6. *Let $t(A) := (p^{r_1(A)},\dots,p^{r_e(A)})$ for an abelian p-group A. Then:*

(a) $|\operatorname{Inj}(G,A)| = f_G(t(A)) = \prod_{k=1}^{e} p^{r_k(A)r_{k+1}(G)} \prod_{j=0}^{\tilde{r}_k(G)-1} (p^{r_k(A)} - p^{r_{k+1}(G)+j})$,

(b) $|\operatorname{Aut}(G)| = |\operatorname{Inj}(G,G)| = f_G(t(G))$.

The formula goes back to works of Delsarte [Del48]. A proof can be found in [Lag10], Lemma A.1 and Remark A.3., where we use $\tilde{r}_k(G) = r_k(G) - r_{k+1}(G)$.

Remark 2.7. We get another formula which is useful for asymptotic considerations:

$$|\operatorname{Inj}(G,A)| = \prod_{k=1}^{e} p^{r_k(A)r_k(G)} \prod_{j=0}^{\tilde{r}_k(G)-1} \left(1 - \frac{p^{r_{k+1}(G)+j}}{p^{r_k(A)}}\right). \tag{2.3}$$

Proof. In formula (2.2), we pull out t_k from the product and make an index shift to obtain (2.3). $\square$

We apply these formulas to the norm groups whose p^k-ranks involve ceiling operations. In the following we write

$$\left\{\frac{a}{b}\right\} := \frac{a}{b} - \left\lfloor\frac{a}{b}\right\rfloor \in [0,1).$$

Definition 2.8. For a finite abelian p-group G of exponent p^e and $n \in \mathbb{N}_0$, $k \in \mathbb{N}$ we define

$$\delta(n,k) := \left\{\frac{n}{p^k}\right\} - \left\{\frac{n}{p^{k-1}}\right\} = \lfloor \frac{n}{p^{k-1}} \rfloor - \lfloor \frac{n}{p^k} \rfloor - \frac{(p-1)n}{p^k} \tag{2.4}$$

and

$$\alpha_p(G) := \sum_{k=1}^{e} \frac{p-1}{p^k} r_k(G), \tag{2.5}$$

$$\delta_G \colon \mathbb{N}_0 \longrightarrow [-\alpha_G, 0], \quad \delta_G(n) := -\alpha_p(G) + \sum_{k=1}^{e} r_k(G)\left(\delta(n-1,k)\right). \tag{2.6}$$

We show in Remark 2.9(c) that $-\alpha_G \leq \delta_G(n) \leq 0$ and thus, δ_G is well-defined.

We immediately see that $\delta(n,k)$ is p^k-periodic and therefore $\delta_G(n)$ is p^e-periodic.

Remark 2.9. Let G and H be finite abelian p-groups of exponent $\leq p^e$. Then:

(a) $\delta_G(n) = -\alpha_p(G) + \sum\limits_{k=1}^{e} \tilde{r}_k(G) \left\{\frac{n-1}{p^k}\right\}$ and $\delta_{G\times H}(n) = \delta_G(n) + \delta_H(n)$,

(b) $\alpha_p(G) = \sum\limits_{k=1}^{e} \tilde{r}_k(G) \frac{p^k-1}{p^k}$ and $\alpha_p(G \times H) = \alpha_p(G) + \alpha_p(H)$,

(c) $\delta_G(1) = -\alpha_p(G) \leq \delta_G(n) \leq 0 = \delta_G(0)$.

Proof. We use an index shift and $r_{e+1}(G) = 0$ to obtain

$$\begin{aligned}
\sum_{k=1}^{e} \tilde{r}_k(G) \frac{p^k-1}{p^k} &= \sum_{k=1}^{e} (r_k(G) - r_{k+1}(G)) \frac{p^k-1}{p^k} \\
&= \sum_{k=1}^{e} r_k(G) \left(\frac{p^k-1}{p^k} - \frac{p^{k-1}-1}{p^{k-1}} \right) \\
&= \sum_{k=1}^{e} r_k(G) \frac{p-1}{p^k} \\
&= \alpha_p(G).
\end{aligned}$$

Similarly, we get

$$\begin{aligned}
\sum_{k=1}^{e} \tilde{r}_k(G) \left\{\frac{n-1}{p^k}\right\} &= \sum_{k=1}^{e} (r_k(G) - r_{k+1}(G)) \left\{\frac{n-1}{p^k}\right\} \\
&= \sum_{k=1}^{e} r_k(G) \left(\left\{\frac{n-1}{p^k}\right\} - \left\{\frac{n-1}{p^{k-1}}\right\} \right) \\
&= \sum_{k=1}^{e} r_k(G) \delta(n-1,k) \\
&= \alpha_p(G) + \delta_G(n).
\end{aligned}$$

Combining these formulas with $\tilde{r}_k(G \times H) = \tilde{r}_k(G) + \tilde{r}_k(H)$ for $k \geq 1$ completes the proofs of (a) and (b).
Finally $-\alpha_p(G) = \delta_G(1) \leq -\alpha_p(G) + \sum_{k=1}^{e} \tilde{r}_k(G) \left\{ \frac{n-1}{p^k} \right\} = \delta_G(n) \leq 0 = \delta_G(0)$. □

Example 2.10. *Let $r \in \mathbb{N}$.*

(a) If $G = (C_p)^r$, then $\alpha_p(G) = r \cdot \frac{p-1}{p}$.

(b) If $G = C_{p^r}$ is cyclic, then $\alpha_p(G) = \sum_{k=1}^{r} \frac{p-1}{p^k} = \frac{p^r-1}{p^r}$.

Remark 2.11. Let $n \in \mathbb{N}$. Then:

$$\prod_{k=1}^{e} p^{r_k(G) r_k(X_n(G))} = |G| q^{n\alpha_p(G)} q^{\delta_G(n)}.$$

Proof. We use $q = p^f$ here. For all $k = 1, \ldots, e$ we have

$$r_k\left(X_n(G)\right) \overset{\text{La. 2.4}}{=} 1 + f\left(\lfloor \frac{n-1}{p^{k-1}} \rfloor - \lfloor \frac{n-1}{p^k} \rfloor \right) \overset{(2.4)}{=} 1 + f\frac{p-1}{p^k}(n-1) + f\delta(n-1,k). \tag{2.7}$$

We get:

$$\begin{aligned} \sum_{k=1}^{e} r_k(G) r_k\left(X_n(G)\right) &\overset{(2.7)}{=} \sum_{k=1}^{e} r_k(G) + f\sum_{k=1}^{e} r_k(G)\frac{p-1}{p^k}(n-1) + f\sum_{k=1}^{e} r_k(G)\delta(n-1,k) \\ &= \log_p(G) + fn\alpha_p(G) + f\delta_G(n). \end{aligned}$$

Using $q = p^f$ yields the required identity. □

Let G be a finite abelian p-group with exponent $\exp(G) = p^e$. Let $n = mp^e + y$ with $0 \leq y < p^e$ and $\alpha_p(G) := \sum_{k=1}^{e} \frac{p-1}{p^k} r_k(G)$.

Theorem 2.12. *Let G be a finite abelian p-group with exponent $\exp(G) = p^e$. Let $\alpha_p(G)$ and $\delta_G(n)$ as defined in (2.5) where $\delta_G(\cdot)$ is p^e-periodic. Let $F = \mathbb{F}_q((t))$ and*

$$\varepsilon(G,q,n) := \prod_{k=1}^{e} \prod_{j=0}^{\tilde{r}_k(G)-1} \left(1 - \frac{p^{r_{k+1}(G)+j-1}}{q^{(p-1)(n-1)/p^k + \delta(n-1,k)}} \right). \tag{2.8}$$

Then we have:

(a) $\mathfrak{Z}(F,G;n) = \frac{|G|}{|\mathrm{Aut}(G)|} q^{n\alpha_p(G)} q^{\delta_G(n)} \varepsilon(G,q,n)$.

(b) $\lim_{n\to\infty} \varepsilon(G,q,n) = 1$ and $\mathfrak{Z}(F,G;n) \sim \frac{|G|}{|\mathrm{Aut}(G)|} q^{n\alpha_p(G)} q^{\delta_G(n)}$.

(c) For fixed $i = 0, \dots, p^e - 1$ let $f_i(n) = n \cdot p^e + i$, i.e. $f_i(n) \equiv i \mod p^e$. Then we have

$$\mathfrak{Z}(F, G; f_i(n)) \sim c_i \frac{|G|}{|\mathrm{Aut}(G)|} q^{f_i(n)\alpha_p(G)}$$

with $c_i = q^{i\alpha_p(G)+\delta_G(i)}$ and $c_0 = 1$.

Proof.

$$\begin{aligned}
\mathfrak{Z}(F, G; n) = \alpha_G\left(X_n(G)\right) &\overset{(2.1)}{=} \frac{|\mathrm{Inj}(G, X_n(G))|}{|\mathrm{Aut}(G)|} \\
&\overset{(2.3)}{=} \frac{1}{|\mathrm{Aut}(G)|} \prod_{k=1}^{e} p^{r_k(G) r_k(X_n(G))} \prod_{j=0}^{\tilde{r}_k(G)-1} \left(1 - \frac{p^{r_{k+1}(G)+j}}{p^{r_k(X_n(G))}}\right) \\
&\overset{\text{Rem.2.11}}{=} \frac{1}{|\mathrm{Aut}(G)|} |G| q^{n\alpha_p(G)} q^{\delta_G(n)} \prod_{k=1}^{e} \prod_{j=0}^{\tilde{r}_k(G)-1} \left(1 - \frac{p^{r_{k+1}(G)+j}}{p^{r_k(X_n(G))}}\right) \\
&\overset{(2.7),(2.8)}{=} \frac{|G|}{|\mathrm{Aut}(G)|} q^{n\alpha_p(G)} q^{\delta_G(n)} \varepsilon(G, q, n).
\end{aligned}$$

Using $|\delta(n-1, k)| < 1$ we get $\lim_{n\to\infty} \varepsilon(G, q, n) = 1$ for all $k \geq 1$ which proves (b).
Finally, δ_G is p^e-periodic and Remark 2.9(c) yields $\delta_G(f_i(0)) = \delta_G(0) = 0$ and thus $c_0 = 1$. □

Example 2.13. *(a) Let $G = (C_p)^r$ be elementary abelian. Then $\alpha_p(G) = r\frac{p-1}{p}$ and*

$$\delta_G(n) = -\alpha_p(G) + r \cdot \left\{\frac{n-1}{p}\right\} = \begin{cases} 0, & p \mid n \\ r(\left\{\frac{n}{p}\right\} - 1), & p \nmid n. \end{cases}$$

Hence, if p does not divide n, we get

$$\mathfrak{Z}(F, G; n) = \frac{|G|}{|\mathrm{Aut}(G)|} q^{n\alpha_p(G)} q^{r(\left\{\frac{n}{p}\right\}-1)} \prod_{j=0}^{r-1} \left(1 - \frac{p^{j-1}}{q^{(p-1)(n-1)/p + \left\{\frac{n-1}{p}\right\}}}\right).$$

(b) Let $G = C_{p^r}$ be cyclic. Then $\alpha_p(G) = \frac{p^r-1}{p^r}$ and

$$\delta_G(n) = -\alpha_p(G) + \left\{\frac{n-1}{p^r}\right\} = \begin{cases} 0, & p^r \mid n \\ \left\{\frac{n}{p^r}\right\} - 1, & p^r \nmid n. \end{cases}$$

Hence, if p^r does not divide n, we get

$$\left(1 - \frac{p^{-1}}{q^{(p-1)(n-1)/p^r + \{(n-1)/p^r\} - \{(n-1)/p^{r-1}\}}}\right).$$

2.3 Conductor Density of Arbitrary Finite Abelian Groups

We now consider an arbitrary finite abelian group G instead of a p-group. It is well-known that G is the direct product of its abelian ℓ-Sylow-subgroups, i.e.

$$G \cong \prod_{\ell \in \mathbb{P}} G_\ell.$$

The hard part is to analyse G_p which was already done in Chapter 2.2. For the remaining part, we fix a prime number $\ell \in \mathbb{P}$ with $p \neq \ell$ and consider the asymptotic problem for the abelian ℓ-group G_ℓ.

The task is to count the number of open subgroups $U \leq F^\times$ such that $F^\times/U \cong G_\ell$. Then the extension given by U is at most tamely ramified, so the conductor exponent is ≤ 1 which implies $1 + \mathfrak{p} \leq U$. Hence we can consider G_ℓ as a quotient of $\mathbb{Z} \times \mathbb{F}_q^\times \cong \mathbb{Z} \times C_{q-1}$. If $\ell \nmid (q-1)$, then there is only the unramified G_ℓ-extension if G_ℓ is cyclic, or no G_ℓ-extension at all.

Obviously, the only possible quotients isomorphic to ℓ-groups are groups of the form $C_{\ell^a} \times C_{\ell^b}$, where $\ell^b \mid (q-1)$ and where we assume $a \geq b$. This is solved in the following remark where we consider G of this type and A as an abelian ℓ-group with ℓ-rank 2 and $\exp(A) = \exp(G)$. Note that the number of subgroups $\alpha_G(A)$ of type G only depends on the p^i-ranks $r_i(A)$ and $r_i(G)$ with $p^i \leq \exp(G)$.

Remark 2.14. Let $G = C_{\ell^a} \times C_{\ell^b}$ and $A = C_{\ell^a} \times C_{\ell^d}$ with $a \geq d \geq b$.

(a) If $a = b$ or $d = 0$, then $\alpha_G(A) = \alpha_G(G) = 1$.

(b) If $a > b$, then

$$\alpha_G(A) = \begin{cases} \ell^{d-b}, & a > d, \\ (\ell+1)\ell^{d-b-1}, & a = d. \end{cases}$$

Proof. We write $r_i(A) := \mathrm{rk}_{\ell^i}(A)$ and $r_i(G) := \mathrm{rk}_{\ell^i}(G)$ in this proof.

(a) If $a = b$ or $d = 0$, then we get $G = A$ and therefore $\alpha_G(A) = \alpha_G(G) = 1$.

(b) By (2.1) and Lemma 2.6(a) we have

$$\begin{aligned} \alpha_G(A) &= \frac{\prod_{k=1}^{a} \ell^{r_{k+1}(G) r_k(A)} \prod_{j=0}^{\tilde{r}_k(G)-1} (\ell^{r_k(A)} - \ell^{r_{k+1}(G)+j})}{\prod_{k=1}^{a} \ell^{r_{k+1}(G) r_k(G)} \prod_{j=0}^{\tilde{r}_k(G)-1} (\ell^{r_k(G)} - \ell^{r_{k+1}(G)+j})} \\ &= \frac{(\ell^{r_b(A)} - \ell)(\ell^{r_a(A)} - 1)}{(\ell^2 - \ell)(\ell - 1)} \prod_{k=1}^{a} \ell^{r_{k+1}(G)(r_k(A) - r_k(G))}. \end{aligned}$$

As $r_k(G) = r_k(A)$ for $k \leq b$ we have $\ell^{r_b(G)} - \ell = \ell^2 - \ell$. Moreover:

$$\prod_{k=1}^{a} \ell^{r_{k+1}(G)(r_k(A) - r_k(G))} = \prod_{k=b+1}^{a-1} \ell^{1 \cdot (r_k(A) - 1)} = \ell^{\min(a-1,d)-b}$$

and

$$\frac{\ell^{r_a(A)}-1}{\ell-1}=\begin{cases}\ell+1, & r_a(A)=2 \iff d=a\\ 1, & r_a(A)=1 \iff b\le d<a.\end{cases}$$

□

Note in the following theorem that $X_1(G)=\mathbb{Z}/\exp(G)\mathbb{Z}\times\mathbb{Z}/(q-1)\mathbb{Z}$. We still use the notation $G_{p'}$ for the prime to p-part of G.

Theorem 2.15. *Let G be a finite abelian group and $F=\mathbb{F}_q((t))$ with $q=p^f$.*

(a) G is realisable as a Galois group over F if and only if $\mathrm{rk}_\ell(G)\le 2$ and G_ℓ^{q-1} is cyclic for all prime numbers $\ell\nmid p$.

(b) If G is realisable, then for all $n\ge 1$ we have

$$\mathfrak{Z}(F,G;n)=\mathfrak{Z}(F,G_p;n)\cdot\prod_{\ell\mid(q-1)}\alpha_{G_\ell}(C_{|G|}\times C_{q-1})\le\frac{(q-1)q}{2}\mathfrak{Z}(F,G_p;n).$$

Proof. We use Lemma 2.5:

$$\mathfrak{Z}(F,G;n)=\alpha_G\left(X_n(G)\right)=\prod_{\ell\in\mathbb{P}}\alpha_{G_\ell}\left(X_n(G)\right)=\alpha_{G_p}\left(X_n(G)\right)\cdot\prod_{p\neq\ell\in\mathbb{P}}\alpha_{G_\ell}\left(X_1(G)\right),$$

where for the last equation we use that $\ell\neq p$ and the fact that $X_n(G)/X_1(G)$ is a p-group. If G is realisable, we get for $\ell\neq p$ that G_ℓ is a quotient of $\mathbb{Z}\times\mathbb{Z}/(q-1)\mathbb{Z}$ and therefore G_ℓ^{q-1} has to be cyclic. Note that for $\ell\nmid p(q-1)$ we get by Remark 2.14 that $\alpha_{G_\ell}\left(X_1(G)\right)=1$. It remains to show the estimate in (b). We have

$$\begin{aligned}\prod_{\ell\mid(q-1)}\alpha_{G_\ell}\left(X_1(G)\right)&\le\prod_{\ell\mid(q-1)}\ell^{\nu_\ell(q-1)-1}(\ell+1)=(q-1)\prod_{\ell\mid(q-1)}\frac{\ell+1}{\ell}\\&\le(q-1)\prod_{k=2}^{q-1}\frac{k+1}{k}=(q-1)\frac{q}{2}.\end{aligned}$$

□

Example 2.16. *(a) For $q=3$ and $G=C_2$, the bound in Theorem 2.15(b) is sharp:*

$$\alpha_{C_2}\left(X_1(G)\right)=\alpha_{C_2}(C_2\times C_2)=3=\frac{(q-1)q}{2}.$$

(b) If G is cyclic of order coprime to $p(q-1)$, then $\mathfrak{Z}(F,G;n)=1$.

2.4 Lower Bounds on Discriminant Density

The asymptotic behaviour weighted by conductor gives interesting insights to the counting problem weighted by discriminant. Let G be a finite group and

$$D(F,G;n):=|\{E/F\ :\ \mathrm{Gal}(E/F)\cong G,\mathrm{N}\left(\mathfrak{D}(E/F)\right)\le q^n\}|$$

be the counting function of local function field extensions with Galois group G and bounded discriminant. To describe the asymptotics exponent weighted by discriminant, we define for abelian p-groups G of exponent p^e

$$\beta_p(G) := \frac{\alpha_p(G)}{\rho(G)}, \qquad \text{where } \rho(G) := \sum_{k=0}^{e-1} \frac{1}{p^k} \left(|G^{p^k}| - |G^{p^{k+1}}| \right).$$

We use the local version of the conductor-discriminant theorem for abelian extensions, see Theorem 1.28.

In preparation, we need a result on characters of X_n.

Lemma 2.17. *Let G be a finite abelian group and $U \leq G$ a subgroup. Then there are $|G/U|$ characters of G with $U \leq \mathrm{Ker}(\chi)$.*

Proof. Using $|H^*| = |H|$ and $1 \to U \to G \to G/U \to 1$ implies

$$1 \to (G/U)^* \to G^* \to U^* \to 1. \qquad \square$$

The idea of the proof of Theorem 2.18 is contained in [Lag15, Ch. 2].

Theorem 2.18. *Let $F = \mathbb{F}_q((t))$, G be a finite abelian p-group and $n \in \mathbb{N}$.*

(a) Let E/F be a normal extension with Galois group G and $\mathrm{N}(\mathfrak{f}(E/F)) = q^n$. Then

$$\mathrm{N}(D(E/F)) \leq \mathrm{N}(\mathfrak{f}(E/F))^{\rho(G)} q^{|G|-1} = q^{n \cdot \rho(G)} q^{|G|-1}.$$

(b) There exists a constant $\gamma(F,G) > 0$ such that

$$D(F,G;n) \geq \gamma(F,G) \cdot q^{n\beta_p(G)}.$$

Proof. Let n be the conductor exponent and U be the norm group of $E^\times$. Using $G = F^\times/U$, we have for $k = 1, \ldots, e$:

$$M_k := \{\chi \text{ character of } G : G[p^{k-1}] \leq \mathrm{Ker}(\chi) \ \wedge G[p^k] \not\leq \mathrm{Ker}(\chi)\}.$$

By Lemma 2.4(c), we have $c(\mathrm{Ker}(\chi)) \leq c(U_n[p^{k-1}]) = \lceil n/p^{k-1} \rceil$ for all $\chi \in M_k$.
Then we have

$$|M_k| = |G/G[p^{k-1}]| - |G/G[p^k]| = |G^{p^{k-1}}| - |G^{p^k}|. \tag{2.9}$$

Moreover, $\sum_{k=1}^{e} |M_k| = |G| - 1$ and the M_k are disjoint – we only miss the trivial character which has

trivial conductor. Thus:

$$\begin{aligned}
\mathrm{N}\left(D(E/F)\right) &\overset{\text{Thm. 1.28}}{=} \prod_{\chi \text{ char. of } \mathrm{Gal}(E/F)} \mathrm{N}\left(\mathfrak{f}(\chi)\right) && = \prod_{k=0}^{e-1} \prod_{\chi \in M_k} \mathrm{N}\left(\mathfrak{f}(\chi)\right) \\
&\leq \prod_{k=1}^{e} \prod_{\chi \in M_k} q^{\lceil n/p^{k-1} \rceil} && = \prod_{k=1}^{e} q^{\lceil n/p^{k-1} \rceil |M_k|} \\
&\overset{(2.9)}{=} \prod_{k=1}^{e} q^{\lceil n/p^{k-1} \rceil (|G^{p^{k-1}}| - |G^{p^k}|)} && \leq \prod_{k=1}^{e} q^{\left(n/p^{k-1}+1\right)(|G^{p^{k-1}}| - |G^{p^k}|)} \\
&= q^{\sum_{k=0}^{e-1} p^{-k} n (|G^{p^k}| - |G^{p^{k+1}}|)} q^{|G|-1} && = q^{n \cdot \rho(G)} q^{|G|-1}.
\end{aligned}$$

Hence

$$D(F, G; n\rho(G) + |G| - 1) \geq \mathfrak{Z}(F, G; n).$$

We set $\tilde{n} := \lfloor (n - |G| + 1)/\rho(G) \rfloor$. By Theorem 2.12 there exists a constant $C > 0$ such that $\mathfrak{Z}(F, G; \tilde{n}) \geq C q^{\tilde{n}\alpha_p(G)}$. Hence in total

$$\begin{aligned}
D(F, G; n) &\geq D(F, G; \tilde{n}\rho(G) + |G| - 1) && \overset{(a)}{\geq} \mathfrak{Z}(F, G; \tilde{n}) \\
&\geq C \cdot q^{\tilde{n}\alpha_p(G)} && = C q^{\lfloor \frac{n-|G|+1}{\rho(G)} \rfloor \alpha_p(G)} \geq C q^{\frac{n-|G|+1-\rho(G)}{\rho(G)} \alpha_p(G)} \\
&= C q^{n\beta_p(G)} q^{(-|G|+1-\rho(G))\beta_p(G)} && = \tilde{C} q^{n\beta_p(G)}.
\end{aligned}$$

□

We highlight here the following theorem which gives the asymptotic exponent for abelian p-groups over local function fields:

Theorem 2.19 (Lagemann)**.** *Let G be a finite p-group and $r_i := r_i(G)$ be the p^i-rank of G. Then*

$$Z(F, G; X) \asymp X^{a_{\mathfrak{p}}(G)},$$

where

$$a_{\mathfrak{p}}(G) = \frac{(1 - p^{-1}) \sum_{i=0}^{e-1} p^i r_{e-i}}{\sum_{i=0}^{e-1} p^i (1 - p^{-r_{e-i}}) p^{r_{e-i} + \ldots + r_e}}.$$

See Satz 2.1 in [Lag10].

Using index shifts we can show that our constant $\beta_p(G)$ coincides with the asymptotic exponent

$a_{\mathfrak{p}}(G)$ from Theorem 2.19. We show this in the following computation.

$$\begin{aligned}
a_{\mathfrak{p}}(G) = \frac{(1-p^{-1})\sum_{i=0}^{e-1} p^i r_{e-i}}{\sum_{i=0}^{e-1} p^i(1-p^{-r_{e-i}})p^{r_{e-i}+\ldots+r_e}} &= \frac{p-1}{p}\frac{\sum_{i=0}^{e-1} p^i r_{e-i}}{\sum_{i=0}^{e-1} p^i(1-p^{-r_{e-i}})p^{r_{e-i}+\ldots+r_e}} \\
&= \frac{(p-1)p^e \sum_{i=0}^{e-1} \frac{1}{p^{e-i}} r_{e-i}}{p\sum_{i=0}^{e-1} p^i(1-p^{-r_{e-i}})p^{r_{e-i}+\ldots+r_e}} \\
&\overset{\text{Eq. (2.5)}}{=} \frac{p^e \alpha_p(G)}{p\sum_{i=0}^{e-1} p^i(p^{r_{e-i}}-1)p^{r_{e-i+1}+\ldots+r_e}} \\
&= \frac{\alpha_p(G)}{p^{1-e}\sum_{i=0}^{e-1} p^i(p^{r_{e-i}}-1)|G^{p^{e-i}}|} \\
&= \frac{\alpha_p(G)}{\sum_{i=0}^{e-1} p^{-e+i+1}(|G^{p^{e-i-1}}|-|G^{p^{e-i}}|)} \\
&\overset{k=e-i-1}{=} \frac{\alpha_p(G)}{\sum_{k=0}^{e-1} p^{-k}(|G^{p^k}|-|G^{p^{k+1}}|)} = \frac{\alpha_p(G)}{\rho(G)}.
\end{aligned}$$

Example 2.20.

(a) For the elementary abelian group $G = (C_p)^r$ we get the discriminant exponent

$$a_p((C_p)^r) = \frac{r(p-1)}{p}\cdot\frac{1}{p^r-1}.$$

(b) For the cyclic p-group $G = C_{p^r}$ we have

$$\begin{aligned}
\rho(G) &= \sum_{k=0}^{r-1}\frac{1}{p^k}\left(|G^{p^k}|-|G^{p^{k+1}}|\right) = \sum_{k=0}^{r-1}\frac{1}{p^k}\left(p^{r-k}-p^{r-k-1}\right) \\
&= p^r(1-p^{-1})\sum_{k=0}^{r-1}p^{-2k} = p^r(1-p^{-1})\frac{1-p^{-2r}}{1-p^{-2}} \\
&= \frac{p^r\left(1-p^{-2r}\right)}{1+p^{-1}}.
\end{aligned}$$

Hence we get the discriminant exponent

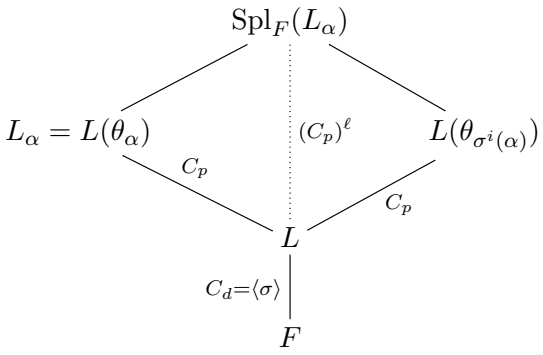
$$a_p(G) = \frac{\alpha_p(G)}{\rho_p(G)} = \frac{p^r-1}{p^r}\frac{1+p^{-1}}{p^r-p^{-r}} = \frac{(p^r-1)(p+1)}{p(p^{2r}-1)} = \frac{p+1}{p(p^r+1)}.$$

Chapter 3

On Subgroups of Affine Linear Groups $\mathrm{AGL}_1(\mathfrak{q})$

Let $F = \mathbb{F}_q((t))$ be a local function field with $\mathrm{char}(F) = p$. In this chapter we consider the Galois closure of C_p-extensions over (at most) tamely ramified cyclic C_d-extensions where $p \nmid d$.

The situation is summarised in the following field diagram, where $\mathrm{Spl}_F(L_\alpha)$ denotes the Galois closure of L_α/F.



Using the group ring $\mathbb{F}_p[C_d]$ as we will define in Definition 3.7, the Galois group is basically determined by the cyclic $\mathbb{F}_p[C_d]$-module

$$\mathbb{F}_p[C_d] \cdot \alpha = \{z \cdot \alpha \mid z \in \mathbb{F}_p[C_d]\} \quad \text{with} \quad p^\ell = \#\mathbb{F}_p[C_d] \cdot \alpha.$$

This cyclic module is a direct sum of distinct irreducible submodules corresponding to irreducible factors of $X^d - 1$ over $\mathbb{F}_p$ via the Frobenius normal form for linear operators.

The corresponding Galois group $G := \mathrm{Gal}\,(\mathrm{Spl}_F(L_\alpha)/F)$ is a subgroup of $C_p \wr C_d$ by the Theorem of Krasner and Kaloujnine, see Theorem 1.11. In particular, the Galois group is a semi-direct product of type $(C_p)^\ell \rtimes C_d$, where we want to interpret $(C_p)^\ell$ as a direct sum of finite fields of characteristic p. In the case that $(C_p)^\ell$ corresponds to an irreducible module and C_d operates faithfully, we can consider the Galois group as a subgroup of $\mathrm{AGL}_1(p^\ell) \cong \left(\mathbb{F}_{p^\ell}, +\right) \rtimes \mathbb{F}_{p^\ell}^\times$.

We will approach as follows: In the first section, we compile some basic facts on affine groups and semi-direct products. We use the classification theorem of tamely ramified extensions due to Hasse [Has69] in order to construct and enumerate C_p-extensions over an at most tamely ramified C_d-extension L/F.

For this, we use the decomposition of the group rings $\mathbb{F}_p[C_d]$ and $\mathbb{F}_q[C_d]$. This allows us to determine the $\mathbb{F}_p[C_d]$-module structure of L and later of $J(L) = L/\wp(L)$. We give a description of the occurring Galois groups. We will determine the asymptotic behaviour of the discriminant counting function with respect to $\asymp$ over pd points, and as Galois extensions. Finally, we determine the asymptotic behaviour of degree-p-extensions with Galois group which is a subgroup of $\mathrm{AGL}_1(p)$. This is the special case that requires $d \nmid (p-1)$. Overall, for a ramified C_d-extension L/F with ramification index e to exist we require $e|(q-1)$.

3.1 Affine Linear Groups and Semi-direct Products

First we recall the definition of the semi-direct product.

Definition 3.1. Let N, H be groups and $\phi\colon H \to \mathrm{Aut}(N)$ be a group homomorphism. Then the *semi-direct product* of N and H by ϕ is the group

$$N \rtimes_\phi H := (N \times H, \circ), \quad (n_1, h_1) \circ (n_2, h_2) := (n_1 \phi(h_1)(n_2), h_1 h_2).$$

For a definition of affine groups, we follow [AB95, p.101f]. Let K be a field and V be a K-vector space. We define

$$T(V) := \{T_v\colon V \to V,\ x \mapsto x + v \mid v \in V\}$$

as the set of all translations on V. Then $T(V)$ and $\mathrm{GL}(V)$ are subgroups of $\mathrm{Sym}(V)$ which have trivial intersection, since $\varphi(0) = 0$ and $T_v(0) = v$ for all $\varphi \in \mathrm{GL}(V)$ and $v \in V$. According to the rule

$$\varphi T_v \varphi^{-1} = T_{\varphi(v)} \quad \text{for all} \quad \varphi \in \mathrm{GL}(V) \quad \text{and} \quad v \in V$$

we define the *affine linear group* of V as the (inner) semi-direct product

$$\mathrm{AGL}(V) := T(V) \rtimes \mathrm{GL}(V) \leq \mathrm{Sym}(V).$$

Identifying $T(V) \cong V$ via $T_v \mapsto v$ we get

$$\mathrm{AGL}(V) \cong V \rtimes_\phi \mathrm{GL}(V), \text{ where } \phi(\varphi)(v) := \varphi(v) \text{ for all } \varphi \in \mathrm{GL}(V) \text{ and } v \in V.$$

It is common to define $\mathrm{AGL}_n(K) := \mathrm{AGL}_K(K^n)$. In the case $K = \mathbb{F}_q$ of a finite field with q elements we write

$$\mathrm{AGL}_n(q) := \mathrm{AGL}(\mathbb{F}_q^n).$$

Example 3.2. *For a prime power q, the affine group $(\mathbb{F}_q, +) \rtimes C_{q-1} = \mathrm{AGL}_1(q) \leq \mathrm{Sym}(\mathbb{F}_q)$ is a transitive primitive permutation group.*

Our main goal is to describe and enumerate C_p-extensions over tamely ramified cyclic degree d-extensions. In particular we will study subgroups of $\mathrm{AGL}_1(p^r)$ $\mathrm{AGL}_1(p^r) \cong {C_p}^r \rtimes C_{p^r-1}$.

Remark 3.3. Let C_n and C_m be cyclic of order n and m and let $\phi \in \mathrm{Hom}(C_m, \mathrm{Aut}(C_n))$, then

$$C_n \rtimes_\phi C_m = \langle \sigma, \tau \mid \sigma^n = \tau^m = 1, \sigma^\tau = \phi(\tau)(\sigma) \rangle = \langle \sigma, \tau \mid \sigma^n = \tau^m = 1, \sigma^\tau = \sigma^k \rangle,$$

where $\phi(\tau)(\sigma) = \sigma^k$ for some $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ with $\mathrm{ord}(k) \mid m$.

In [Tau55] is proven that there is a group action of $\mathrm{Aut}(H) \times \mathrm{Aut}(N)$ on $\mathrm{Hom}(H, \mathrm{Aut}(N))$ via

$$(\alpha_H, \alpha_N) \cdot \psi(h) := \psi(\alpha_H^{-1}(h))^{\alpha_N} = \alpha_N^{-1} \circ \psi(\alpha_H^{-1}(h)) \circ \alpha_N.$$

This group action can be used to decide whether two semi-direct products are isomorphic. One variant that will be sufficient for our purposes is due to Taunt from 1955 in the same paper:

Theorem 3.4 (Taunt)**.** *Let N, H be finite soluble groups with $\gcd(|N|, |H|) = 1$. Furthermore, let $\psi_i \colon H \to \mathrm{Aut}(N)$ for $i = 1, 2$ be two group homomorphisms from H into $\mathrm{Aut}(N)$. Define $G_i := N \rtimes_{\psi_i} H$ for $i = 1, 2$.*

Then $G_1 \cong G_2$ if and only if there exist automorphisms $\alpha_N \in \mathrm{Aut}(N)$ and $\alpha_H \in \mathrm{Aut}(H)$ such that

$$(h^{\alpha_H})^{\psi_2} = \left(h^{\psi_1}\right)^{\alpha_N} \qquad \text{for all } \ h \in H,$$

where $\left(h^{\psi_1}\right)^{\alpha_N} = \alpha_N^{-1} \circ \psi_1(h) \circ \alpha_N$ and $h^{\alpha_H} = \alpha_H(h)$.

See [BE99, Theorem 5.1] or [Tau55, Theorem 3.3] for a detailed proof.

We will apply this theorem in the following case:

Proposition 3.5.

(a) Let $H = \langle \sigma \rangle$ be a finite cyclic group and N be a finite group. Then we get

$$N \rtimes_{\psi_1} H \cong N \rtimes_{\psi_2} H \iff \psi_1(H) \text{ and } \psi_2(H) \text{ are conjugate in } \mathrm{Aut}(N).$$

(b) Let $n, m \in \mathbb{N}$ be such that $\mathrm{Aut}(C_n)$ is cyclic and $\gcd(n, m) = 1$. Then for all $k_1, k_2 \in (\mathbb{Z}/n\mathbb{Z})^\times$ we have for the semi-direct products $C_n \rtimes C_m$:

$$\begin{aligned} & \{\sigma, \tau \mid \sigma^n = \tau^m = 1, \ \sigma^\tau = \sigma^{k_1}\} \cong \{\sigma, \tau \mid \sigma^n = \tau^m = 1, \ \sigma^\tau = \sigma^{k_2}\} \\ \iff \quad & \mathrm{ord}(k_1) = \mathrm{ord}(k_2) \text{ in } (\mathbb{Z}/n\mathbb{Z})^\times. \end{aligned}$$

Proof. (a) Since abelian groups are soluble we can apply Theorem 3.4. Thus the two semi-direct products are isomorphic if and only if

$$\begin{aligned} & \text{there exists } \beta \in \mathrm{Aut}(H), \alpha \in \mathrm{Aut}(N) \text{ with } \quad \psi_2(\beta(h)) = \alpha^{-1} \circ \psi_1(h) \circ \alpha \quad \text{for all } h \in H \\ \iff & \psi_2(\beta(\sigma^n)) = \alpha^{-1} \circ \psi_1(\sigma^n) \circ \alpha \quad \text{for all } n \in \mathbb{N} \\ \iff & \psi_2(\beta(\sigma))^n = \left(\alpha^{-1} \circ \psi_1(\sigma) \circ \alpha\right)^n \quad \text{for all } n \in \mathbb{N} \\ \iff & \psi_2(\beta(\sigma)) = \alpha^{-1} \circ \psi_1(\sigma) \circ \alpha \\ \iff & \psi_2(H) = \alpha^{-1} \circ \psi_1(H) \circ \alpha \quad \text{for some } \alpha \in \mathrm{Aut}(N). \end{aligned}$$

(b) If $\mathrm{Aut}(N)$ is cyclic, then conjugation is trivial and thus $\psi_1(H)$ and $\psi_2(H)$ are conjugate if and only if they coincide. This shows that

$$\mathrm{Im}(\psi_1) = \mathrm{Im}(\psi_2) \iff \mathrm{ord}(\psi_1) = \mathrm{ord}(\psi_2)$$

since $\mathrm{Aut}(N)$ is cyclic. □

We will apply this proposition in the case $C_{p^r} \rtimes C_d$ for $\gcd(d,p) = 1$.

3.2 Decomposition of $J(L)$ for a Tamely Ramified Extension L/F

We give a folklore classification theorem on the structure of tamely ramified extensions in local fields. Note that unramified extensions are also considered to be tamely ramified by our definition. Later, we will use this to decompose the Galois module $J(L)$ for a cyclic tamely ramified extension L/F.

Theorem 3.6 (Classification of tamely ramified extensions)**.** *Let K be a local function field with residue class field $\kappa_K = \mathbb{F}_q$ and prime element π_K. Let L/K be an at most tamely ramified extension with ramification index $e = e_{L/K}$ and inertia degree $f = f_{L/K}$. Let $\left(\mathbb{F}_{q^f}\right)^\times = \langle w \rangle$ and $g := \gcd(e, q^f - 1)$.*

(a) Then L is conjugate to exactly one field $K(w, \sqrt[e]{w^r \pi_K})$ where $0 \le r < g$.

(b) The extension L/K is a Galois extension if and only if $e \mid (q^f - 1)$ and $e \mid r(q-1)$.
Set $\pi_L := \sqrt[e]{w^r \pi_K}$ as in (a). If L/K is Galois, then $\mathrm{Gal}(L/K)$ is generated by σ_1, σ_2 with

$$\begin{aligned} \sigma_1(w) &= w, & \sigma_1(\pi_L) &= w^l \cdot \pi_L, \\ \sigma_2(w) &= w^q, & \sigma_2(\pi_L) &= w^k \cdot \pi_L, \end{aligned}$$

where $k = \frac{r(q-1)}{e}$ and $l = \frac{q^f - 1}{e}$. The Galois group has the finite presentation

$$\mathrm{Gal}(L/K) = \langle \sigma_1, \sigma_2 \mid \sigma_1^e = 1,\ \sigma_1^r = \sigma_2^f,\ \sigma_1^{\sigma_2} = \sigma_1^q \rangle.$$

(c) The extension L/K is abelian if and only if $e \mid (q-1)$.
It is moreover cyclic if and only if $e \mid (q-1)$ and $\gcd(e, f, r) = 1$. In this case we have a generator via $N := \prod_{\ell \in \mathbb{P},\ \ell \mid \gcd(e,r)} \ell$ and

$$\mathrm{Gal}(L/K) = \langle \sigma \rangle \quad \textit{with} \quad \sigma = \begin{cases} \langle \sigma_2 \rangle, & \textit{if } \gcd(e,r) = 1, \textit{ or} \\ \langle \sigma_1^N \sigma_2 \rangle, & \textit{if } \gcd(e,r) \neq 1. \end{cases}$$

In particular, the generator σ of $\mathrm{Gal}(L/K)$ has the property

$$\sigma(w) = w^q, \quad \sigma(\pi_L) = w^n \cdot \pi_L \quad \textit{with} \quad n = \begin{cases} k, & \gcd(e,r) = 1 \\ k + Nl, & \gcd(e,r) \neq 1. \end{cases}$$

Proof. (a) and (b) are proven in [Has69, Chapter 16, p. 249ff].

In (c) note that $\operatorname{ord}(\sigma_1) = e$ and

$$\operatorname{Gal}(L/K) \text{ is abelian } \iff \sigma_1 = \sigma_1^{\sigma_2} = \sigma_1^q \iff \sigma_1^{q-1} = \mathrm{id} \iff \operatorname{ord}(\sigma_1) = e \mid (q-1).$$

If $\operatorname{Gal}(L/K) = \langle \sigma_1, \sigma_2 \rangle$ is abelian, we have $\exp(\operatorname{Gal}(L/K)) = \operatorname{lcm}(\operatorname{ord}(\sigma_1),\ \operatorname{ord}(\sigma_2))$. Concerning σ_2, we use $\operatorname{ord}(\sigma_1) = e$ to get

$$\operatorname{ord}(\sigma_2) \overset{(b)}{=} f \cdot \operatorname{ord}(\sigma_1^r) = f \cdot \frac{e}{\gcd(e,r)}.$$

Thus, $\operatorname{Gal}(L/K)$ is cyclic if and only if $\operatorname{Gal}(L/K)$ is abelian and

$$\begin{aligned} d = \exp(\operatorname{Gal}(L/K)) &\iff e \cdot f = \operatorname{lcm}(\operatorname{ord}(\sigma_1), \operatorname{ord}(\sigma_2)) = \operatorname{lcm}(e,\ f\frac{e}{\gcd(e,r)}) \\ &\iff e \cdot f = \frac{e}{\gcd(e,r)} \cdot \operatorname{lcm}\left(\gcd(e,r),\ f\right) \\ &\overset{\cdot \frac{\gcd(e,r)}{e}}{\iff} \gcd(e,r) \cdot f = \operatorname{lcm}(\gcd(e,r),\ f) \iff \gcd(e,r,f) = 1. \end{aligned}$$

Now we can assume that L/K is cyclic. We have $\operatorname{ord}(\sigma_1) = e$ and $\operatorname{ord}(\sigma_2) = \frac{ef}{\gcd(e,r)}$.

Let $\ell \nmid \gcd(e,r)$. Then

$$\nu_\ell\left(\operatorname{ord}(\sigma_2)\right) = \nu_\ell\left(\frac{ef}{\gcd(e,r)}\right) = \nu_\ell(ef) \quad \text{and} \quad \nu_\ell\left(\operatorname{ord}(\sigma_1^\ell)\right) < \nu_\ell(ef),$$

hence $\nu_\ell\left(\operatorname{ord}(\sigma_1^\ell \sigma_2)\right) = \nu_\ell\left(\operatorname{ord}(\sigma_2)\right) = \nu_\ell(ef)$ has the right ℓ-order.

Let $\ell \mid \gcd(e,r)$, then $\ell \nmid f$ by $\gcd(e,r,f) = 1$. Thus $\nu_\ell\left(\operatorname{ord}(\sigma_2)\right) < \nu_\ell(ef) = \nu_\ell(e)$ and

$$\nu_\ell(\operatorname{ord}(\sigma_1\sigma_2)) = \nu_\ell(\operatorname{ord}(\tau)) = \nu_\ell(e) = \nu_\ell(ef).$$

Hence, the element $\sigma := \sigma_1^N \sigma_2$ for $N := \prod_{\substack{\ell \in \mathbb{P} \\ \ell \nmid \gcd(e,r)}} \ell$ has order ef and is a generator of the Galois group. Finally, for the last assertion we have

$$\sigma_2(w) = w^q = \sigma_1^N \sigma_2(w) \quad \text{and} \quad \sigma_2(\pi_L) = w^k \pi_L$$

and

$$\sigma_1^N \sigma_2(\pi_L) = \sigma_1^N(w^k \pi_L) = w^k \sigma_1^N(\pi_L) = w^k w^{Nl} \pi_L. \qquad \square$$

From now on we fix L/F to be a tamely ramified C_d-extension with the notations of Theorem 3.6. I.e. we will assume $d = ef$ with $p \nmid d$, $\kappa(F) \cong \mathbb{F}_q$, that $\langle w \rangle = \left(\mathbb{F}_{q^f}\right)^\times$ is a primitive $\left(q^f - 1\right)$-st root of unity and that

$$\pi = \sqrt[d]{w^r \pi_F},\ L = \mathbb{F}_{q^f}((\pi)), \quad \langle \sigma \rangle = \operatorname{Gal}(L/F) \cong C_d \ \text{ with } \ \sigma(w) = w^q,\ \sigma(\pi) \in \mathbb{F}_{q^f} \cdot \pi. \tag{3.1}$$

Denote by $\mu(d)$ the set of d-th roots of unity and by $\operatorname{Eig}_\sigma(\zeta) \leq L$ the eigenspace of σ to the eigenvalue ζ.

Definition 3.7. Let G be a finite group and K be a field.

(a) The *group ring* of G over K is defined as the K-algebra

$$K[G] := \left\{ \sum_{g\in G} a_g \cdot g \mid a_g \in K \right\} \quad \text{with } K\text{-basis } G$$

and by the multiplication rule

$$\left(\sum_{g\in G} a_g \cdot g\right) \cdot \left(\sum_{g\in G} b_g \cdot g\right) := \sum_{g,\tilde{g}\in G} a_g b_{\tilde{g}} \cdot g\tilde{g} \text{ for all } \ a_g, b_g \in K.$$

(b) Let $X^d - 1 = f_1 \cdots f_r \in \mathbb{F}_p[X]$ be the prime factorisation of $X^d - 1$. We define

$$M_{f_i} := \mathbb{F}_p[X]/(f_i) \text{ for all } \ 1 \le i \le r, \quad M_I := \bigoplus_{i\in I} M_{f_i} \text{ for all } \ I \subseteq \{1, \dots, r\}.$$

If $\eta_i \in \widehat{\mathbb{F}_p}$ is a root of f_i for all $1 \le i \le r$, we will identify $\mathbb{F}_p(\eta_i) \cong M_{f_i}$ via $\eta_i \mapsto \bar{X}$, and accordingly make the identification $M_I = \oplus_{i\in I}\mathbb{F}_p(\eta_i)$.

(c) We set $\ell(i) := \deg(f_i)$ for $1 \le i \le r$ and $\ell(I) := \sum_{i\in I} \ell(i)$ for all $I \subseteq \{1, \dots, r\}$.

We compute the $\mathbb{F}_p[C_d]$-decomposition of $J(L) = L/\wp(L)$. We proceed by considering L as $\mathbb{F}_q[C_d]$-module first. We will use the σ-invariant building blocks $V_n := \mathbb{F}_{q^f} \cdot \pi^n$ for all $n \in \mathbb{Z}$ who occur e-periodically, that is $V_{n+e} \cong V_n$. By this, we can deduce the $\mathbb{F}_p[C_d]$-module structure of L and consequently of $\wp(L)$.

We start with an example to outline the basic concepts in the specialised situation $d \mid (q-1)$ where σ is a diagonalisable operator.

Example 3.8. *Let $F = \mathbb{F}_q((t))$ be a local function field with $\mathrm{char}(F) = p \in \mathbb{P}$. Let $d \mid (q-1)$ and let $\zeta_d \in \mathbb{F}_q^\times$ be a primitive d-th root of unity.*

(a) Let $f = d, e = 1$ and $L := \mathbb{F}_{q^f}((t))$ be the unramified C_d-extension of F. By Theorem 3.6(c), there is a generator σ of $\mathrm{Gal}(L/F)$ with $\sigma(t) = t$ and $\sigma|_{\mathbb{F}_{q^f}}$ being the Frobenius automorphism. The minimal polynomial of σ is $X^d - 1$, over both F and $\mathbb{F}_q$, and $X^d - 1 = \prod_{i=0}^{d-1}(X - \zeta_d^i)$, hence σ is diagonalisable. We thus have $\eta_0, \dots, \eta_{d-1} \in \mathbb{F}_{q^f}$ so that $\sigma(\eta_i) = \zeta_d^i \cdot \eta_i$. Therefore, we obtain

$$\sigma(\eta_i t^n) = \sigma(\eta_i)\sigma(t)^n = \zeta_d^i \cdot (\eta_i t^n) \text{ for all } \ 0 \le i \le d-1, \quad n \in \mathbb{Z}.$$

And for the eigenspaces, we have

$$\mathrm{Eig}_F(\zeta_d^i) = \sum_{n\in\mathbb{Z}} \mathbb{F}_q \cdot \eta_i t^n.$$

(b) Now for a totally ramified C_d-extension with $d = e$ and $f = 1$, we have $L = F(\sqrt[d]{w^r t})$ for some $0 \leq r < e$ by Theorem 3.6. Write $\pi := \sqrt[d]{w^r t}$. Here, we have a generator σ of $\mathrm{Gal}(L/F)$ with $\sigma(\pi) = \zeta_d \cdot \pi$ and $\sigma|_{\mathbb{F}_q} = \mathrm{id}_{\mathbb{F}_q}$. We immediately get

$$\sigma(\pi^n) = \sigma(\pi)^n = (\zeta_d \pi)^n = \zeta_d^n \pi^n \text{ for all } n \in \mathbb{Z}.$$

For the eigenspaces we obtain for $0 \leq i \leq d-1$ the assertion

$$\mathrm{Eig}_F(\zeta_d^i) = \sum_{n \in \mathbb{Z}} \mathbb{F}_q \cdot \pi^{d \cdot n + i} = \sum_{n \in \mathbb{Z}} \mathbb{F}_q \cdot \pi^{e \cdot n + i}.$$

Remark 3.9. Consider the prime factorisation $X^d - 1 = f_1 \cdots f_r$ in $\mathbb{F}_p[X]$. Let d be coprime to $p \in \mathbb{P}$.

(a) We have $\mathbb{F}_q[C_d] \cong (\mathbb{F}_p[C_d])^{[\mathbb{F}_q : \mathbb{F}_p]}$ as $\mathbb{F}_p[C_d]$-modules.

(b) The group ring $\mathbb{F}_p[C_d]$ is semisimple and we get the module decomposition

$$\mathbb{F}_p[C_d] \cong \bigoplus_{i=1}^{r} \mathbb{F}_p[X]/(f_i) =: M_{f_1} \oplus \ldots \oplus M_{f_r}$$

into irreducible submodules.

(c) Let N be an $\mathbb{F}_p[C_d]$-module, then we get

$$N \cong \bigoplus_{i=1}^{r} \mathrm{Ker}(f_i(\sigma)) \quad \text{as } \mathbb{F}_p[C_d]\text{-modules.}$$

We will write $M_{f_i}(N) := \mathrm{Ker}(f_i(\sigma))$, then we get

$$N \cong \bigoplus_{i=1}^{r} M_{f_i}(N) \cong \bigoplus_{i=1}^{r} \bigoplus_{R_i} M_{f_i} \quad \text{for certain index sets } R_i.$$

Proof. For part (a) let $\omega_1, \ldots, \omega_s$ be an $\mathbb{F}_p$-basis of $\mathbb{F}_q$. Then

$$\mathbb{F}_q[C_d] = \left\{ \sum_{g \in G} b_g \cdot g \mid b_g \in \mathbb{F}_q \right\} = \left\{ \sum_{g \in G} \sum_{i=1}^{s} a_{g,i} \omega_i \cdot g \mid a_{g,i} \in \mathbb{F}_p \right\} = \sum_{i=1}^{s} \omega_i \cdot \mathbb{F}_p[C_d] \cong (\mathbb{F}_p[C_d])^s .$$

Now using $s = [\mathbb{F}_q : \mathbb{F}_p]$ yields the result.

For part (b), we use $\mathbb{F}_p[C_d] \cong \mathbb{F}_p[X]/(X^d - 1) = \mathbb{F}_p[X]/(f_1 \cdots f_r)$ and the Chinese Remainder Theorem.

The fact that $\mathrm{char}(F) \nmid \#C_d = d$ guarantees the direct decomposition in (c). The rest follows easily by linear algebra and due to the fact that the minimal polynomial of σ is $X^d - 1$ over both F and $\mathbb{F}_q$ as $X^d - 1$ is square-free. □

In the following, we consider a local function field $F = \mathbb{F}_q((t))$ with $\mathrm{char}(F) = p$ and a cyclic C_d-extension $L = \mathbb{F}_{q^f}((\sqrt[e]{w^r t}))$ with $p \nmid d$ for some (q^f-1)-st root of unity $\omega \in \mathbb{F}_{q^f}$. $\mathrm{Gal}(L/F) = \langle\sigma\rangle$ is cyclic with σ as in Theorem 3.6(c). In particular, σ has the properties $\sigma|_{\mathbb{F}_q} = \mathrm{id}$, $\sigma(\pi) \in \mathbb{F}_{q^f} \cdot \pi$ and $\sigma\,|_{\mathbb{F}_{q^f}}$ acts as the Frobenius automorphism.

We will first consider the $\mathbb{F}_q[C_d]$-module structure of L and use this to derive the $\mathbb{F}_p[C_d]$-module structure of $J(L)$.

Theorem 3.10. *Let $p \nmid d$ and L/F be a tamely ramified C_d-extension with $e := e_{L/F}$ and $f := f_{L/F}$. Let $\omega \in \mathbb{F}_{q^f}^{\times}$ be a primitive (q^f-1)-st root of unity and let $\pi := \pi_L = \sqrt[e]{\omega^r \pi_F}$ as in Theorem 3.6. Then:*

(a) The $\mathbb{F}_q$-subspace $V_n := \mathbb{F}_{q^f} \cdot \pi^n$ is σ-invariant for all $n \in \mathbb{Z}$.

(b) There is a primitive e-th root of unity $\zeta_e \in \mathbb{F}_q$ so that $\sigma|_{V_n}$ has minimal polynomial $X^f - \zeta_e^n$ for all $n \in \mathbb{Z}$. In particular, $V_{n+e} \cong V_n$ as $\mathbb{F}_q[C_d]$-modules for all $n \in \mathbb{Z}$.

(c) For all $n \in \mathbb{Z}$, the two $\mathbb{F}_q[C_d]$-modules $V_n \oplus V_{n+1} \oplus \ldots \oplus V_{n+e-1}$ and $\mathbb{F}_q[C_d]$ are isomorphic.

(d) For all $n \in \mathbb{Z}$, the two $\mathbb{F}_p[C_d]$-modules $V_n \oplus V_{n+1} \oplus \ldots \oplus V_{n+e-1}$ and $(\mathbb{F}_p[C_d])^{[\mathbb{F}_q:\mathbb{F}_p]}$ are isomorphic.

Proof. Let $n \in \mathbb{Z}$. Using $\sigma(\mathbb{F}_{q^f}) \subseteq \mathbb{F}_{q^f}$ and Theorem 3.6(c) we get

$$\sigma(\pi^n) \overset{\text{Thm. 3.6(c)}}{=} w^t \cdot \pi^n \quad \text{for a suitable } t \in \mathbb{N}.$$

Thus $\mathbb{F}_{q^f} \cdot \pi^n$ is a σ-invariant subspace for all $n \in \mathbb{Z}$ which proves (a).

For (b) we show the existence of a certain primitive e-th root of unity ζ_e so that $\left(\sigma^f - \zeta_e^n\right)(V_n) = 0$ for all $n \in \mathbb{N}$. We have

$$\sigma^f(\omega^k) = \left(\sigma^f(\omega)\right)^k \overset{\mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)\cong C_f}{=} \omega^k \text{ for all } \; k \in \mathbb{N}.$$

Furthermore, let $\sigma(\pi) = \omega^x \pi$, then we have

$$\begin{aligned}\sigma^f(\pi^n) = \left(\sigma^f(\pi)\right)^n &= \left(\omega^x \omega^{qx} \cdots \omega^{q^{f-1}x} \pi\right)^n \\ &= \left(N_{\mathbb{F}_{q^f}/\mathbb{F}_q}(\omega^x)\pi\right)^n = \left(\omega^{\frac{q^f-1}{q-1}x}\pi\right)^n \\ &= \omega^{\frac{q^f-1}{q-1}x \cdot n}\pi^n.\end{aligned}$$

Note that $x = \begin{cases} \frac{r(q-1)}{e}, & \gcd(e,r) = 1 \\ \frac{r(q-1)}{e} + N\frac{q^f-1}{e}, & \gcd(e,r) \neq 1 \end{cases}$ with N as in Theorem 3.6(c) and that

$$e \cdot \frac{q^f-1}{q-1}x = \begin{cases} r(q^f-1), & \gcd(e,r) = 1, \\ r(q^f-1) + N(q^f-1)\frac{q^f-1}{q-1}, & \gcd(e,r) \neq 1, \end{cases}$$

thus $\omega^{\frac{q^f-1}{q-1}x} =: \zeta_e$ is an e-th root of unity. It is indeed a primitive e-th root of unity, as

$$X^d - 1 = \prod_{i=0}^{e-1}(X^f - \zeta^i) \text{ for } \zeta \text{ a primitive e-th root of unity.}$$

Using $\sigma^f(\omega^k) = \omega^k$, we thus obtain $\sigma^f(\omega^k\pi^n) = \zeta_e^n\omega^k\pi^n$, hence $(\sigma^f - \zeta_e^n)(V_n) = 0$.

Part (c) follows by part (b), the identity $X^d - 1 = \prod_{i=0}^{e-1}(X^f - \zeta_e^i)$ and Remark 3.9(b), which also holds true for $\mathbb{F}_q[C_d]$.

Part (d) is a direct consequence of part (c) and Remark 3.9(b). □

We can use Theorem 3.10 to decompose $J(L)$ in components where we can read off the Galois group and the discriminant. Naturally, $J(L)$ is an $\mathbb{F}_p[C_d]$-module via $\sigma\left(\alpha + \wp(L)\right) := \sigma(\alpha) + \wp(L)$. We want to work with a system of representatives $R_L(\pi_L, \omega_0)$ again. Therefore, we have to choose π_L and ω_0 carefully so that choosing a representatives defines an $\mathbb{F}_p[C_d]$-module isomorphism.

Concerning the $\mathbb{F}_p[C_d]$-module structure on $L/\wp(L)$ we study for $z < 0,\ z \in \mathbb{Z}$ the $\mathbb{F}_p[C_d]$-modules

$$W_z := \sum_{\substack{i=ep\cdot z \\ p\nmid i}}^{ep\cdot(z+1)-1} V_i. \tag{3.2}$$

and fix an element

$$\omega_0 \in \mathbb{F}_q^\times \ : \ \omega_0 \notin \wp(\mathbb{F}_{q^f}). \tag{3.3}$$

Such an element ω_0 exists since $\mathbb{F}_q \subseteq \wp(\mathbb{F}_{q^f})$ implied that the unique C_p-extension of $\mathbb{F}_q$ was contained in $\mathbb{F}_{q^f}$, which is impossible by degrees.

The submodules W_z and $\mathbb{F}_p\omega_0 \cong \mathbb{F}_{q^f}/\wp\left(\mathbb{F}_{q^f}\right)$ determine the $\mathbb{F}_p[C_d]$-structure of $R_L(\pi, \omega_0)$. Note that we have the periodicity $W_z \cong W_{z+k}$ as $\mathbb{F}_p[C_d]$-modules for all $k < 0$ due to $V_{i+kpe} \cong V_i$ for all $i \in \mathbb{Z}$.

Proposition 3.11. *Let π as in (3.1) and $\omega_0 \in \mathbb{F}_q^\times \setminus \wp(\mathbb{F}_{q^f})$ as in (3.3). Then we have an $\mathbb{F}_p[C_d]$-module isomorphism*

$$R_L(\pi, \omega_0) = \mathbb{F}_p\omega_0 \oplus \bigoplus_{z<0} W_z \xrightarrow{\sim} J(L), \quad x \longmapsto x + \wp(L). \tag{3.4}$$

Proof. $R_L(\pi, \omega_0)$ is an $\mathbb{F}_p[C_d]$-module as $\sigma(\mathbb{F}_{q^f}\pi^i) = \mathbb{F}_{q^f}\pi^i$ and $\sigma(\omega_0) = \omega_0$ by definition.

We have already shown in Chapter 1 that the map is bijective and $\mathbb{F}_p$-linear, see Lemma 1.20.

Note that $\sigma \circ \wp(x) = \wp \circ \sigma(x)$ and $\sigma(\wp(L)) = \wp(L)$, thus $\sigma(w + \wp(L)) = \sigma(w) + \wp(L)$ for all $w \in \bigoplus_{z<0} W_z$. For $\eta \in \mathbb{F}_{q^f}$, we have

$$\sigma(\eta + \wp(L)) = \sigma(\eta) + \wp(L) = \eta^q + \wp(L) = \eta + \wp(L),$$

where for the last equality we write $q = p^s$ and use the telescopic sum

$$\eta^q - \eta = \eta^{p^s} - \eta = \sum_{i=0}^{s-1} \left(\eta^{p^{i+1}} - \eta^{p^i}\right) = \wp(\sum_{i=0}^{s-1} \eta^{p^i})$$

for the last equality. Thus, $\mathbb{F}_{q^f} + \wp(L)$ is fixed under σ, and so is ω_0. Hence, the map commutes with σ and is an $\mathbb{F}_p[C_d]$-module isomorphism. □

From now on we will write $R_L := R_L(\pi, \omega_0)$ for this specific π and ω_0. Using the $\mathbb{F}_p[C_d]$-module-isomorphism $R_L \cong J(L)$, we can now both control the Galois group and discriminant of Artin-Schreier extensions of L.

$$J(L) = \bigoplus_{i=1}^{r} M_{f_i}\left(J(L)\right) = \mathbb{F}_p\omega_0 \oplus \bigoplus_{n=1}^{\infty} W_{-n} \cong \mathbb{F}_p \oplus \bigoplus_{\substack{i=1 \\ p\nmid i}}^{\infty} V_{-i},$$

where $M_{f_i}\left(J(L)\right) = \mathrm{Ker}(f_i(\overline{\sigma}))$ and $\omega \in \mathbb{F}_{q^f} \setminus \wp(\mathbb{F}_{q^f})$.

Lemma 3.12. *We use the assumptions of* (3.1) *and* $R_L := R_L(\pi, \omega_0)$ *as in Proposition 3.11.*

(a) For all $n \in \mathbb{Z}_{<0}$ *we have*

$$W_n \cong (\mathbb{F}_p[C_d])^{(p-1)\cdot[\mathbb{F}_q:\mathbb{F}_p]}.$$

(b) Let $1 \le i \le r$. *Assume* $f_1 = X - 1$ *and define* $M_{f_i}(R_L) := \mathrm{Ker}(f_i(\sigma)) \cap R_L$ *and* $\ell(i) := \deg(f_i)$. *Then there are* $j_1(i), \ldots, j_{d_i}(i) \in \{0, \ldots, e-1\}$ *and* $\eta_{n,i,1}, \ldots, \eta_{n,i,\ell(i)} \in \mathbb{F}_{q^f}^{\times}$ *so that*

$$M_{f_1}(R_L) = \{\lambda_0\omega_0 + \sum_{\substack{\nu \le n \le -1 \\ p\nmid n}} \sum_{k=1}^{\ell(i)} a_{n,k}\eta_{n,i,k}\pi^{en} \mid \lambda_0 \in \mathbb{F}_p,\ a_{n,k} \in \mathbb{F}_q,\ \nu \in \mathbb{Z}\}$$

and in the case $i \ge 2$ *we have*

$$M_{f_i}(R_L) = \{ \sum_{\substack{\nu \le n \le -1 \\ p\nmid (en + j_k(i))}} \sum_{k=1}^{\ell(i)} a_{n,k}\eta_{n,i,k}\pi^{en+j_k(i)} \mid a_{n,k} \in \mathbb{F}_q,\ \nu \in \mathbb{Z}\}.$$

Proof. By the periodicity of σ in Theorem 3.10(b) it is sufficient to prove the statement for $n = -1$. We have when considering as $\mathbb{F}_q[C_d]$-modules

$$W_{-1} = \bigoplus_{\substack{i=1 \\ p\nmid i}}^{ep} V_{-i} \overset{\text{Thm. 3.10}(b)}{\cong} \bigoplus_{j=1}^{p-1} \bigoplus_{i=0}^{e-1} V_{-i} \overset{\text{Thm. 3.10}(d)}{\cong} (\mathbb{F}_p[C_d])^{(p-1)[\mathbb{F}_q:\mathbb{F}_p]}.$$

For part (b) we take suitable $\mathbb{F}_p$-bases of V_{-i} for $p \nmid i$. □

With the notations of (3.1), consider the factorisation $X^d - 1 = f_1 \cdots f_r$ in $\mathbb{F}_p[X]$ and set

$$M_{f_i}(R_L) := \mathrm{Ker}(f_i(\sigma)) \cap R_L \tag{3.5}$$

with $R_L := R_L(\pi, \omega_0)$ as defined in Lemma 1.20(b). Let $\alpha \in R_L$. We want to consider the Galois group of $L(\theta_\alpha)$ over F.

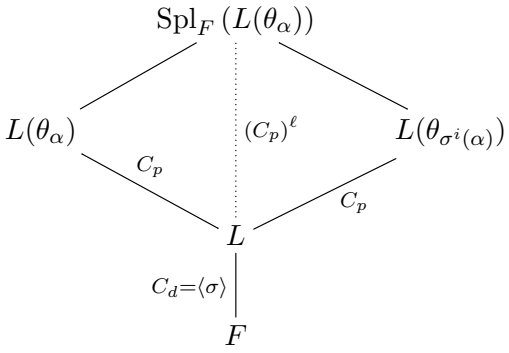


Figure 3.1: Field diagram

Theorem 3.13. *Let $X^d - 1 = f_1 \cdots f_r \in \mathbb{F}_p[X]$ be the prime factorisation over the prime field $\mathbb{F}_p$. Let $1 \le i \le r$ and let η_i be a root of f_i in an algebraic closure of $\mathbb{F}_p$. Let $0 \ne \alpha \in J(L)$ and write*

$$\alpha = \alpha_1 + \ldots + \alpha_r \in M_{f_1}(R_L) \oplus \ldots \oplus M_{f_r}(R_L) = R_L.$$

Moreover, let $I := \{1 \le i \le r \mid \alpha_i \ne 0\}$. Then:

(a) The degree of the splitting field of $L(\theta_\alpha)$ is $[\mathrm{Spl}_F(L(\theta_\alpha)) : L] = p^{\sum_{i\in I} \deg(f_i)}$ and

$$\mathrm{Gal}\left(\mathrm{Spl}_F(L(\theta_\alpha))/F\right) \cong \left(\bigoplus_{i\in I} (\mathbb{F}_p(\eta_i), +)\right) \rtimes_\phi C_d$$

via the homomorphism $\phi = \phi_1 + \ldots + \phi_{|I|} \colon C_d \to \mathrm{Aut}\left(\bigoplus_{i\in I} \mathbb{F}_p(\eta_i)\right)$ with $\phi_i(k)(x) = \eta_i^k x$ for $x \in \mathbb{F}_p(\eta_i)$ and $k \in \mathbb{Z}/d\mathbb{Z} \cong C_d$ and $1 \le i \le |I|$.

(b) The extension $L(\theta_\alpha)/F$ is Galois if and only if $\sum_{i\in I} \deg(f_i) = 1$, i.e. α is a σ-eigenvector for an eigenvalue in $\mathbb{F}_p^\times$.

(c) Let $\ell(i) := \deg(f_i)$ and

$$m_i := \nu_L(\alpha_i) = \nu_i \cdot e + j_i < 0 \quad \text{for all } i \in I$$

and let $\tau\colon \{1,\dots,|I|\} \to I$ *be a bijection such that* $|m_{\tau(1)}| \le |m_{\tau(2)}| \le \ldots \le |m_{\tau(|I|)}|$ *. Then we get the discriminant exponents*

$$\operatorname{disc}(\operatorname{Spl}_F(L(\theta_\alpha))/L) = \sum_{i=1}^{|I|}(p^{\ell(\tau(i))}-1)(|\nu_L(\alpha_i)|+1)p^{\ell(\tau(i-1))+\ldots+\ell(\tau(1))}, \tag{3.6}$$

$$\operatorname{disc}(\operatorname{Spl}_F(L(\theta_\alpha))/F) = p^{\ell(I)}f(e-1) + \sum_{i=1}^{|I|}(p^{\ell(\tau(i))}-1)\left(d|\nu_{\tau(i)}| + d - j_{\tau(i)}f\right). \tag{3.7}$$

Proof. Consider first the case $I=\{i\}$ and $\alpha=\alpha_i \in M_{f_i}(L)$. By assumption we have $\alpha_i \neq 0$. Let $\theta_{\sigma^j(\alpha_i)}$ be a root of $X^p - X - \sigma^j(\alpha_i)$, let $\ell(i) = \deg(f_i)$ and $\Delta := \langle \sigma^j(\alpha_i) + \wp(L) \ : \ 1 \le j \le \ell(i)\rangle_{\mathbb{F}_p}$. Note that we have an $\mathbb{F}_p$-basis $\alpha_i+\wp(L), \sigma(\alpha_i)+\wp(L), \cdots, \sigma^{\ell(i)-1}(\alpha_i)+\wp(L)$ of Δ with $f_i(\sigma)(\alpha_i+\wp(L)) = 0$ as $\alpha_i \in M_{f_i}(L)$. Then

$$\operatorname{Spl}_F(L(\theta_{\alpha_i})) = L\left(\wp^{-1}(\Delta)\right) = L\left(\theta_{\alpha_i}, \theta_{\sigma(\alpha_i)}, \ldots, \theta_{\sigma^{\ell(i)-1}(\alpha_i)}\right).$$

Through the identifications

$$\mathbb{F}_p(\eta_i) \cong \mathbb{F}_p[X]/(f_i) \xrightarrow{\sim} \Delta \quad \text{via} \quad \eta_i \longmapsto \overline{X} \longmapsto \sigma(\alpha_i)$$

we get $\operatorname{Gal}\left(L(\wp^{-1}(\Delta))/L\right) \cong \mathbb{F}_p(\eta_i)$ by Theorem 1.7.

Furthermore, $\operatorname{Gal}(\operatorname{Spl}_F(L(\theta_{\alpha_i}))/L)$ is a normal subgroup of $\operatorname{Gal}(\operatorname{Spl}_F(L_{\alpha_i})/F)$, since its fixed field L is Galois over F. With $\gcd(p,d)=1$ and the Theorem of Zassenhaus (see [Hup67, Hauptsatz I.18.1]) we have that $\operatorname{Gal}(\operatorname{Spl}_F(L(\theta_{\alpha_i}))/F)$ is a semi-direct product which concludes (a) for $|I|=1$.

If $|I|>1$, we use $\bigoplus_{i\in I}\langle\alpha_i\rangle_{\mathbb{F}_p[C_d]} \cong \bigoplus_{i\in I} M_{f_i}$ yielding the degree and the description of the Galois group via restriction to $\langle\alpha_i\rangle$.

For (b) we use that $L(\theta_{\alpha_i})/F$ is Galois if and only if $\dim_{\mathbb{F}_p}(\Delta)=1$, i.e. $\ell(i) = [\mathbb{F}_p(\eta_i):\mathbb{F}_p] = 1$, hence if and only if $\eta_i \in \mathbb{F}_p$.

Now for (c). From the Theorem 3.13 we get

$$\operatorname{Spl}_F(L(\theta_\alpha)) \overset{(a)}{=} L\left(\theta_{\sum\limits_{i\in I}\lambda_i\cdot\alpha_i} \mid \lambda_i \in \mathbb{F}_p(\eta_i)\setminus\{0\}\right).$$

Clearly $\nu_L(\lambda\cdot\alpha) = \nu_L(\alpha)$ and $\lambda\cdot\alpha \in R_L$ for all $\lambda \in \mathbb{F}_p(\eta_i)^\times \subseteq \mathbb{F}_{q^f}^\times$. Using that $\nu_L(\alpha) < 0$ is not divisible by p, the Conductor-Discriminant Formula in Theorem 1.28 yields

$$\begin{aligned}\operatorname{disc}(\operatorname{Spl}_F(L(\theta_\alpha))/L) &= \sum_{0\neq(\lambda_1,\ldots,\lambda_{|I|})\in\mathbb{F}_p(\eta_1)\times\ldots\times\mathbb{F}_p(\eta_{|I|})} \operatorname{cond}\left(L(\theta_{\sum\limits_{i\in I}\lambda_i\cdot\alpha_i})/L\right)\\ &= \sum_{0\neq(\lambda_1,\ldots,\lambda_{|I|})\in\mathbb{F}_p(\eta_1)\times\ldots\times\mathbb{F}_p(\eta_{|I|})} \left(|\nu_L(\sum_{i\in I}\lambda_i\cdot\alpha_i)|+1\right).\end{aligned}$$

In this case we have $\nu_L(\sum_{i\in I}\lambda_i\cdot\alpha_i)=\nu_L(\alpha_m)$, where $m=\max\{i\in I\mid \lambda_{\tau(i)}\neq 0\}$. Thus we have

$$\begin{aligned}\operatorname{disc}(\operatorname{Spl}_F(L(\theta_\alpha))/L)&=\sum_{i=1}^{|I|}|\mathbb{F}_p(\eta_{\tau(i)})^\times|\sum_{(\lambda_1,\dots,\lambda_{i-1})\in\mathbb{F}_p(\eta_{\tau(1)})\times\dots\times\mathbb{F}_p(\eta_{\tau(i-1)})}\left(|\nu_L(\alpha_{\tau(i)})|+1\right)\\&=\sum_{i=1}^{|I|}(p^{\ell(\tau(i))}-1)\cdot p^{\ell(\tau(1))+\dots+\ell(\tau(i-1))}\left(|\nu_L(\alpha_{\tau(i)}|+1\right).\end{aligned}$$

For the second formula we use the tower formula

$$\begin{aligned}\operatorname{disc}(\operatorname{Spl}_F(L(\theta_\alpha))/F)&=p^{\ell(I)}\operatorname{disc}(L/F)+f_{L/F}\operatorname{disc}(\operatorname{Spl}_F(L(\theta_\alpha))/L)\\&=p^{\ell(I)}f(e-1)+f\operatorname{disc}(\operatorname{Spl}_F(L(\theta_\alpha))/L).\end{aligned}\tag{3.8}$$

We substitute (3.8) in (3.6) and rewrite $\nu_L(\alpha_i)=\nu_i e+j_i$ to obtain

$$\begin{aligned}\operatorname{disc}(\operatorname{Spl}_F(L(\theta_\alpha))/F)&\overset{(3.8)}{=}p^{\ell(I)}f(e-1)+f\operatorname{disc}(\operatorname{Spl}_F(L(\theta_\alpha))/L)\\&\overset{(3.6)}{=}p^{\ell(I)}f(e-1)+f\sum_{i=1}^{|I|}(p^{\ell(\tau(i))}-1)\cdot p^{\ell(\tau(1))+\dots+\ell(\tau(i-1))}\left(|\nu_L(\alpha_{\tau(i)}|+1\right)\\&=p^{\ell(I)}f(e-1)+f\sum_{i=1}^{|I|}(p^{\ell(\tau(i))}-1)\cdot p^{\ell(\tau(1))+\dots+\ell(\tau(i-1))}(\nu_i e+j_i+1)\\&=p^{\ell(I)}f(e-1)+\sum_{i=1}^{|I|}(p^{\ell(\tau(i))}-1)\cdot p^{\ell(\tau(1))+\dots+\ell(\tau(i-1))}(d\nu_i+fj_i+d).\end{aligned}$$

□

3.2.1 Enumeration over pd points

According to the occurring Galois groups in Theorem 3.13 we define:

Definition 3.14. Let $d=ef$ with $p\nmid d$ and L/F be a C_d-extension with $e_{L/F}=e$ and $f_{L/F}=f$. Let $X^d-1=f_1\cdots f_r$ be the prime factorisation in $\mathbb{F}_p[X]$ with $f_1=(X-1)$.

Let moreover $I\subseteq\{1,\dots,r\}$ with $I\neq\emptyset$.

(a) We define

$$M_I(R_L):=\bigoplus_{i\in I}M_{f_i}(R_L)\quad\text{and}\quad\widetilde{M}_I(R_L):=\left\{y\in M_I(R_L)\mid\langle y\rangle_{\mathbb{F}_p[C_d]}\cong M_I\right\}$$

where $M_{f_i}(R_L)$ is defined in (3.5). Note that $M_{\{i\}}(R_L)=M_{f_i}(R_L)$.

(b) We define

$$G_p(d,I) := \left(\bigoplus_{i\in I} \mathbb{F}_p(\eta_i)\right) \rtimes_\phi C_d \quad \text{via} \quad \phi(k)(\sum_{i\in I} m_i) = \sum_{i\in I} \eta_i^k m_i.$$

We furthermore define $G_p(d,i) := G_p(d,\{i\})$ and we set

$$G_p(d) := (\mathbb{F}_p(\zeta_d),+) \rtimes C_d, \quad \text{where } C_d \text{ acts via multiplication by } \zeta_d.$$

(c) For $x \in \mathbb{R}_{\geq 0}$ we set

$$\begin{aligned} Y_I(L;x) &:= \#\{\alpha \in M_I(R_L) \ : \ \alpha = 0 \vee |\nu_L(\alpha)| \leq x\} \quad \text{and} \\ \widetilde{Y}_I(L;x) &:= \#\{\alpha \in \widetilde{M}_I(R_L) \ : \ |\nu_L(\alpha)| \leq x\}; \\ Z_L(F,I;x) &:= \#\{\alpha \in M_I(R_L) \ : \ \mathrm{disc}(L(\theta_\alpha)/F) \leq x\} \quad \text{and} \\ \widetilde{Z}_L(F,I;x) &:= \#\{\alpha \in \widetilde{M}_I(R_L) \ : \ \mathrm{disc}(L(\theta_\alpha)/F) \leq x\}. \end{aligned}$$

Note that $M_I(R_L)$ and $\widetilde{M}_I(R_L)$ depend on a choice of π and ω_0, while the four counting functions $Y_I(L,x)$ et cetera are independent of these choices.

Remark 3.15. (a) We have a $1:1$-correspondence $\{I \subseteq \{1,\dots,r\}\} \leftrightarrow \{g(X) \in \mathbb{F}_p[X] \ : \ g(X) \mid X^d - 1\}$ by setting $g_I := \prod_{i\in I} f_i$ with $\ell(g_I) = \deg(g)$. Similarly, we can identify M_{g_I} with $\mathbb{F}_p[X]/(g(X))$ as $\mathbb{F}_p[C_d]$-modules and we could have equivalently defined the group via

$$G_p\left(d, g(X)\right) := G_p(d, g_I).$$

(b) The elements in $\widetilde{M}_I(R_L)$ correspond to g_I-cyclic module generators in R_L, where R_L is our standard representative system of $J(L)$.

Then $\widetilde{Y}_I(L,x)$ is the number of these g_I-cyclic generators up to a valuation bound, while $\widetilde{Z}_L(F,I;x)$ counts all Artin-Schreier extensions generated by $M_I(R_L)$ whose discriminant over F is bounded by x.

Remark 3.16. Let $p \nmid d$ and ζ_d be a primitive d-th root of unity. Let $0 \leq i \leq d-1$.

(a) If a root η_i of f_i is a primitive d-th root of unity, then $G_p(d,i)$ is isomorphic to a subgroup of $\mathrm{AGL}_1(q_i)$ for $q_i = |\mathbb{F}_p(\eta_i)|$.

(b) We have $G_p(p^\ell - 1) = \mathrm{AGL}_1(p^\ell) \cong C_p^\ell \rtimes C_{p^\ell - 1}$ and $G_2(3) = A_4$.

Proof. (a) Let $u \in \mathbb{F}_q^\times$ be a generator of the unit group $\mathbb{F}_q^\times$. Then we have $\eta_i = u^k$ for some $k \in \mathbb{N}$. By definition, η_i acts on $\mathbb{F}_q$ by multiplication. Now, $C_d \cong \langle \eta_i \rangle$ as η_i is a primitive d-th root of unity by assumption which defines the semi-direct product and shows the claim.

(b) Note that here $\zeta_{p^\ell-1}$ is a primitive $(p^\ell-1)$-st root of unity and that $[\mathbb{F}_p(\zeta_{p^\ell-1}):\mathbb{F}_p]=\ell$. The fact that $G_p(d)$ is isomorphic to $\mathrm{AGL}_1(p^\ell)$ is obvious by part (a).

The case $G_2(3)$ is a specialisation with $p=2$ and $\ell=2$. Then $G_2(3)\cong \mathrm{AGL}_1(4)\cong A_4$. □

We want to prove the following: Consider $M_I \rtimes C_d \leq S_{pd}$. Then we have

$$Z(F, M_I \rtimes C_d; X) \asymp X^{\frac{\ell(I)}{pd}}.$$

We will prove a $\sim$-estimate for $Z_L(F,I;a_n)$ for a certain arithmetic progression a_n and therefore prove a $\asymp$-estimate for this function.

Theorem 3.17. *Let $x\in\mathbb{R}_{\geq 0}$ and $\emptyset\neq I\subseteq\{1,\dots,r\}$. Let $d_0:=pf(e-1)$ and*

$$d(n):=pf(e-1)+(p-1)f(ep\cdot n+1) \text{ for all } n\in\mathbb{N}.$$

(a) We have $Y_I(L;x)=\prod_{i\in I} Y_{\{i\}}(L;x)$ and $Z_L(F,I;x)=\prod_{i\in I} Z_L(F,\{i\};x)$.

(b) We have $Y_I(L;ep\cdot n)=Z_L(F,I;d(n))=q^{n\cdot(p-1)\ell(I)}p^{\delta(I)}$ for all $n\in\mathbb{N}$, where $\delta(I)=\begin{cases}1, & 1\in I\\ 0, & 1\notin I.\end{cases}$

(c) We have $\widetilde{Z}_L(F,I;d(n))\sim p^{\delta(I)}q^{n\cdot(p-1)\ell(I)}$ and

$$Z_L(F,I;x)\asymp q^{x\frac{\ell(I)}{pd}}, \qquad \widetilde{Z}_L(F,I;x)\asymp q^{x\frac{\ell(I)}{pd}}.$$

Proof. (a) Let $\alpha=\sum_{i\in I}\alpha_i\in M_I(R_L)$, then we claim that we have

$$|\nu_L(\alpha)|=\max\{|\nu_L(\alpha_i)| : i\in I\}.$$

Set $l:=\ell(I)$. Let $i_1,\dots,i_l\in I$ be the indices such that $|\nu_L(\alpha_{i_j})|=N$ is maximal. Write $\alpha_{i_j}=\sum_{k=-N}^{0}\lambda_{j_k}\pi^k$ for certain $\lambda_{j_k}\in\mathbb{F}_q$ where $\lambda_{j_{-N}}\neq 0$. Using the direct sum in Lemma 3.12(c) the leading coefficients $\lambda_{1_{-N}},\dots,\lambda_{l_{-N}}$ are $\mathbb{F}_p$-linearly independent, thus $\sum_{i\in I}\lambda_{i_{-N}}\pi^N\neq 0$ and

$$|\nu_L(\alpha)|=N=\max\{|\nu_L(\alpha_i)| : i\in I\}.$$

Thus,

$$\begin{aligned} Y_I(L,x) &= \#\{\alpha=\sum_{i\in I}\alpha_i\in M_I(R_L) \ : |\nu_L(\alpha)|\leq x\}\\ &= \prod_{i\in I}\#\{\alpha_i\in M_{\{i\}}(R_L) \ : \ |\nu_L(\alpha_i)|\leq x\}=\prod_{i\in I}Y_{\{i\}}(L;x). \end{aligned} \tag{3.9}$$

For the statement on $Z_L(F, I; x)$ we let $\alpha = \sum_{i\in I} \alpha_i \in Y_I(L)$. If $\nu_L(\alpha) < 0$ then we have

$$\begin{aligned}\operatorname{disc}(L(\theta_\alpha)/L) &= (p-1)(|\nu_L(\alpha)|+1)\\ &= (p-1)f_{L/F}(|\nu_L(\sum_{i\in I}\alpha_i)|+1)\\ &= (p-1)f\left(\max\{|\nu_L(\alpha_i)| \ : \ i\in I\}+1\right)\\ &= \max\{\operatorname{disc}\left(L(\alpha_i)/L\right) \ : \ i\in I\}\end{aligned}$$

and by the discriminant tower formula, we get $\operatorname{disc}(L(\theta_\alpha)/F) = \max\{\operatorname{disc}\left(L(\theta_{\alpha_i})/F\right) \ : \ i\in I\}$. If $\alpha = 0$ or $\nu_L(\alpha)$, we similarly have

$$\operatorname{disc}(L(\theta_\alpha)/F) = \begin{cases}\operatorname{disc}(L/F) = \max\{\operatorname{disc}\left(L(\alpha_i)/F\right) \ : \ i\in I\}, & \alpha = 0\\ p\cdot\operatorname{disc}(L/F) = \max\{\operatorname{disc}\left(L(\alpha_i)/F\right) \ : \ i\in I\}, & \alpha\neq 0, \nu_L(\alpha) = 0.\end{cases}$$

Hence $\alpha \in Z_L(F, I; x) \iff \alpha_i \in Z_L(F, \{i\}, x)$ for all $i \in I$.

(b) By (a) it is sufficient to consider $Y_{\{i\}}(L; x)$ and $Z_L(F, \{i\}, d(n))$ for $1 \le i \le r$. We first show that $Y_{\{i\}}(L; x)$ gives the desired formula. By Lemma 3.12 we have

$$M_{\{i\}}(R_L) \cong \begin{cases}\mathbb{F}_p \oplus \bigoplus\limits_{n<0} \mathbb{F}_p^{[\mathbb{F}_q:\mathbb{F}_p]} \cong \mathbb{F}_p \oplus \bigoplus\limits_{n<0} \mathbb{F}_q, & i = 1\\ \bigoplus\limits_{n<0} \mathbb{F}_p^{[\mathbb{F}_q:\mathbb{F}_p]\ell(i)} \cong \bigoplus\limits_{n<0} \mathbb{F}_q^{\ell(i)}, & i \neq 1\end{cases}$$

and we obtain accordingly

$$Y_{\{i\}}(L; ep\cdot n) = \left\{\begin{array}{ll} pq^{(p-1)\cdot n}, & i = 1\\ q^{(p-1)\ell(i)\cdot n}, & i\neq 1\end{array}\right\} = p^{\delta(I)}q^{(p-1)\ell(i)\cdot n}. \tag{3.10}$$

It is left to show the equality $Y_{\{i\}}(L; ep\cdot n) = Z_L(F, \{i\}; d(n))$. Therefore, for any $y \in Y_i(L)$ we use the discriminant formula

$$\operatorname{disc}(L(\theta_y)/F) = pf(e-1) + (p-1)f\left(|\nu_L(y)|+1\right).$$

Set $|\nu_L(y)| =: N$, then we have

$$Y_{\{i\}}(L; N) = Z_L\left(F, \{i\}; pf(e-1) + (p-1)f(N+1)\right), \tag{3.11}$$

and using $N = ep\cdot n$ yields

$$pf(e-1) + (p-1)f(ep\cdot n + 1) = d(n).$$

Hence we finally obtain $Y_{\{i\}}(L; ep\cdot n) \overset{(3.11)}{=} Z_L\left(F, \{i\}; d(n)\right) \overset{(3.10)}{=} q^{(p-1)\ell(i)\cdot n}p^{\delta(I)}$.

(c) We prove the $\sim$-statement for $I = \{i\}$ first.

For $n \in \mathbb{N}$ we have

$$\widetilde{Z}_L(F, I; d(n)) = Z_L(F, I; d(n)) - 1 \overset{(b)}{=} q^{(p-1)\ell(i)n} p^{\delta(\{i\})} - 1 \sim q^{(p-1)\ell(i)n} p^{\delta(\{i\})} \quad \text{for } n \to \infty.$$

This shows the statement for a singleton $I = \{i\}$. For arbitrary $I \subseteq \{1, \dots, r\}$ we use

$$\widetilde{Z}_L(F, I; d(n)) = \prod_{i \in I} \widetilde{Z}_L(F, \{i\}; d(n)) \sim \prod_{i \in I} q^{(p-1)\ell(i)n} p^{\delta(\{i\})} = q^{(p-1)\ell(I)\cdot n} p^{\delta(I)},$$

where the identity $p^{\delta(I)} = \prod_{i \in I} p^{\delta(\{i\})}$ is immediate from the definitions. This proves the $\sim$-statement.

For the second part, we consider $x \geq d_0$ and we furthermore consider $n_x \in \mathbb{N}$ so that $d(n_x) \leq x \leq d(n_x + 1)$ holds. Obviously, $Z_L(F, I; x)$ is a monotonously increasing function in x and we get

$$\begin{aligned} q^{-\frac{\ell(I)}{pd}} \cdot q^{\frac{x\ell(i)}{pd}} &\leq q^{n_x(p-1)\ell(I)} \overset{(b)}{=} Z_L\left(F, I; d(n_x)\right) \leq Z_L(F, I; x) \\ &\leq Z_L\left(F, I; d(n_x + 1)\right) \overset{(b)}{\leq} pq^{(n_x+1)(p-1)\ell(I)} \leq pq^{\frac{\ell(I)}{pd}} \cdot q^{x\frac{\ell(I)}{pd}}, \end{aligned}$$

hence $Z_L(F, I; x) \asymp q^{x\frac{\ell(I)}{pd}}$. For the final statement, we use the simple estimate

$$\begin{aligned} Z_L(F, I; x) \geq \widetilde{Z}_L(F, I; x) &= \prod_{i \in I} \left(Z_L(F, \{i\}; x) - 1\right) \\ &\geq \prod_{i \in I} \frac{q-1}{q} Z_L(F, \{i\}; x) = \left(\frac{q-1}{q}\right)^{|I|} Z_L(F, I; x). \end{aligned}$$ □

We can combine this to prove an estimate on the asymptotics of $G_p(d, I)$-extensions over pd points and for the corresponding splitting fields.

Theorem 3.18. *Let F be a function field with $\operatorname{char}(F) = p$, let $d \in \mathbb{N}$ be coprime to p. Let $X^d - 1 = \prod_{i=1}^{r} f_i \in \mathbb{F}_p[X]$ be its prime factorisation and let $\emptyset \neq I \subseteq \{1, \dots, r\}$.*

(a) Consider $G_p(d, I) \leq S_{pd}$ as a transitive permutation group over pd points. Then we have

$$Z_{pd}\left(F, G_p(d, I); X\right) \asymp X^{\frac{\ell(I)}{pd}}.$$

(b) Let $|I| = 1$ and consider $G_p(d, I) \cong \mathbb{F}_p^{\ell(I)} \rtimes C_d \leq S_{p^{\ell(I)}d}$ as a transitive permutation group over $p^{\ell(I)}d$ points, i.e. as Galois extensions. Then we have

$$Z_{p^{\ell(I)}d}(F, G_p(d, I); X) \asymp X^{\frac{(p-1)\ell(I)}{pd\left(p^{\ell(I)}-1\right)}}.$$

Proof. (a) It is clear that

$$Z_{pd}(F, G_p(d,I); X) = \sum_{\substack{L/F \\ \mathrm{Gal}(L/F)\cong C_d}} \#\{\mathrm{Spl}_F(L(\theta_y)) \mid y \in \widetilde{M}_I(R_L), \\ \mathrm{disc}(L(\theta_y)/F) \le \log_q(X)\}. \tag{3.12}$$

Let L/F be a C_d-extension. The $G_p(d,I)$-extensions containing L are parametrised by $\widetilde{Y}_I(L)$. Note that for every $\alpha \in \widetilde{Y}_I(L)$ there exist

$$\psi(I) := \prod_{i\in I}(p^{\ell(i)} - 1)$$

many elements $\beta \in \widetilde{Y}_I(L)$ defining the same splitting field and thus defining isomorphic fields. The analogous number is the same for $\widetilde{Z}_L(F, I; n)$. Hence we get

$$Z_{pd}(F, G_p(d,I); X) \overset{(3.12)}{=} \sum_{\substack{L/F \\ \mathrm{Gal}(L/F)\cong C_d}} \frac{1}{\psi(I)} \widetilde{Z}_L\left(F, I; \log_q(X)\right).$$

There are only finitely many degree-d-extensions of F as $p \nmid d$, hence this is a finite sum and thus $Z_L(F, I; X) \asymp q^{\log_q(X)\frac{\ell(I)}{pd}} = X^{\frac{\ell(I)}{pd}}$. It follows that

$$\widetilde{Z}(F, G_p(d,I); X) \asymp \sum_{\text{finite}} X^{\frac{\ell(I)}{pd}} \asymp X^{\frac{\ell(I)}{pd}}.$$

(b) By the assumption $|I| = 1$ we have $I = \{i\}$ for some $i \in \{1, \dots, r\}$.
Let $y \in M_{\{i\}}(R_L)$ and $M_y = \mathrm{Spl}_F(L(\theta_y))$. Then we have

$$\begin{aligned}\mathrm{disc}(M_y/F) &= [M_y : L] \cdot \mathrm{disc}(L/F) + f_{L/F}\,\mathrm{disc}(M_y/L) \\ &\overset{(3.6)}{=} p^{\ell(i)} f(e-1) + f(p^{\ell(i)} - 1)\left(|\nu_L(y)| + 1\right).\end{aligned}$$

Hence setting $\widetilde{d}(n) := p^{\ell(i)} f(e-1) + f(p^{\ell(i)} - 1)(ep \cdot n + 1)$ for $n \in \mathbb{N}$, we get

$$\{y \in M_{\{i\}}(R_L) \mid \mathrm{disc}(M_y/F) \le \widetilde{d}(n)\} = Y_{\{i\}}(L; ep \cdot n) \overset{3.17(b)}{=} p^{\delta(i)} q^{(p-1)\ell(i)\cdot n}.$$

Hence using the monotony of the counting function, applying $\log_q$ and using (3.12), we obtain

$$Z(F, G_p(d, \{i\}); X) \asymp X^{\frac{(p-1)\ell(i)}{f(p^{\ell(i)}-1)pe}} = X^{\frac{(p-1)\ell(i)}{pd(p^{\ell(i)}-1)}}.$$ □

Remark 3.19. The statement of Theorem 3.18 is also true for general $I \subseteq \{1, \dots, r\}$. We can adapt the same proof and need to address some technical obstacles. We use the discriminant formula in

Theorem 3.13(c). Moreover, for any bijection $\tau\colon \{1,\dots,|I|\} \to I$, we consider all $(m_i)_{i\in I}$ following an ordering of valuation given by τ, that is

$$|\nu_L(m_{\tau(1)})| \le |\nu_L(m_{\tau(2)})| \le \ldots \le |\nu_L(m_{\tau(|I|)})|.$$

For the i-th component m_i, we get the discriminant weight

$$q^{(|\nu_L(m_i)|+1)\cdot f\cdot\left(p^{\ell(\tau(i))}-1\right)\cdot p^{\ell(\tau(1)+\ell(\tau(2))+\ldots+\ell(\tau(i-1))}}.$$

The number of m_i is given by

$$\widetilde{Y}_L(\{\tau(i)\}; m_i) \asymp q^{\frac{(p-1)\ell(\tau(i))}{pe)}m_i}.$$

One can show that the concerning asymptotics exponent is then

$$\begin{aligned}
&\prod_{i=1}^{r} q^{\frac{p-1}{pe}\cdot\frac{\ell(\tau(i))}{f\cdot\left(p^{\ell(\tau(1))+\ldots+\ell(\tau(i))}-p^{\ell(\tau(1))+\ldots+\ell(\tau(i))}\right)}} \\
=&q^{\frac{p-1}{pe}\cdot\frac{\ell(\tau(1))+\ell(\tau(2))+\ldots+\ell(\tau(|I|))}{f\left(p^{\ell(\tau(1))+\ldots+\ell(\tau(|I|))}-1\right)}} \\
=&q^{\frac{p-1}{pe}\cdot\frac{\ell(I)}{f\left(p^{\ell(I)}-1\right)}} = q^{\frac{p-1}{pd}\cdot\frac{\ell(I)}{\left(p^{\ell(I)}-1\right)}}
\end{aligned} \tag{3.13}$$

independently of the chosen bijection τ.

Example 3.20. *(a) We consider the group A_4 and write $A_4(12) \le S_{12}$ respectively $A_4(6) \le S_6$ as transitive permutation groups over 12 points and 6 points, respectively. Let F be a local function field with $\mathrm{char}(F) = 2$ and $X^3 - 1 = (X-1)\cdot f_2 \in \mathbb{F}_2[X]$ with $f_2 = X^2 + X + 1$. We then have that $G_2(3,\{2\}) \cong A_4$. By Theorem 3.18 we have for counting degree-12-extensions*

$$Z(F, A_4(12); X) = Z_{12}(F, G_2(3,\{2\}); X) \asymp X^{\frac{(p-1)\ell(2)}{pd(p^{\ell(2)}-1)}} = X^{\frac{1}{9}}.$$

Considering $A_4(6) \le S_6$ as transitive permutation group over $pd = 6$ points, we get

$$Z(F, A_4(6); X) = Z_6(F, G_2(3,\{2\}), X) \asymp X^{\frac{\ell(2)}{6}} = X^{\frac{1}{3}}.$$

(b) We consider the group $C_2^3 \rtimes C_7 \le S_{56}$ as transitive permutation group over 56 points. Let again F be a local function field with $\mathrm{char}(F) = 2$. We find the decomposition into irreducible factors

$$X^7 - 1 = (X-1)(X^3 + X + 1)(X^3 + X^2 + 1) \in \mathbb{F}_2[X].$$

The index sets $I = \{2\}$ or $I = \{3\}$ lead to the group $C_2^3 \rtimes C_7$ with our methods. We then have

$$Z(F, C_2^3 \rtimes C_7; X) \asymp X^{\frac{(p-1)\ell(2)}{pd(p^{\ell(2)}-1)}} = X^{\frac{3}{2\cdot 7\cdot 7}} = X^{\frac{3}{98}}.$$

(c) Let $p \in \mathbb{P}$ be any prime and $d \in \mathbb{N}$ coprime to p. Let F be a local function field with $\mathrm{char}(F) = p$. For the wreath product $C_p \wr C_d \le S_{dp^d}$, we consider $I = \{1,\dots,r\}$ with $\ell(I) = \deg(X^d - 1) = d$ and obtain

$$Z(F, C_p \wr C_d; X) \asymp X^{\frac{\ell(I)}{pd(p^{\ell(I)}-1)}} = X^{\frac{d}{pd(p^d-1)}} = X^{\frac{1}{p(p^d-1)}}.$$

3.2.2 Subgroups of $\mathrm{AGL}_1(p)$

In this section we will always assume $d \mid (p-1)$ and $\zeta_d \in \mathbb{F}_p^\times$ to be a primitive d-th root of unity. Then

$$X^d - 1 = \prod_{i=1}^{d} (X - \zeta_d^i) \in \mathbb{F}_p[X]$$

splits and thus σ is a diagonalisable F-linear map. We can identify f_i with a d-th root of unity ζ_d^i and we can regard a subset $I \subseteq \{1, \dots, d\}$ as a set of d-th roots of unity. Then M_i corresponds to the eigenspace of σ of the eigenvalue ζ_d^i. For the corresponding eigenvalue ζ_d^i we have the Galois group $G_p(d,i) \cong C_p \rtimes C_d$ where we consider $C_p \cong (\mathbb{F}_p, +)$ and C_d is acting by multiplication with ζ_d^i.

In this case it is obvious that the fixed field of $1 \times C_d$ defines a degree-p-extension.

Theorem 3.21. *Let $G = C_p \rtimes C_d \leq \mathrm{AGL}_1(p)$ where $1 \neq d \mid (p-1)$. Let L/F be a C_d-extension with $\mathrm{Gal}(L/F) = \langle \sigma \rangle$. Let $\alpha \in R_L$ so that $\sigma(\alpha) = \zeta \cdot \alpha$ for some primitive d-th root of unity $\zeta \in \mathbb{F}_p^\times$. Let $K_\alpha = \mathrm{Fix}(1 \times C_d)$ be a degree-p-subfield.*

(a) We have

$$\mathrm{disc}(K_\alpha/F) = \frac{p-1}{d} \mathrm{disc}(L/F) + \frac{f_{L/F}}{d} \mathrm{disc}(L(\theta_\alpha)/L).$$

(b) Consider $G \cong G_p \leq S_p$ with $|G_p| = p \cdot d$ as transitive permutation group over p points. Then we have

$$Z(F, G_p; X) \asymp X^{\frac{1}{p}}.$$

Proof. Part (a) is Corollary 6(2) in [FK03].

For part (b) we start with a bound on $\mathrm{disc}(L(\theta_\alpha)/F)$ so that $\mathrm{disc}(K_\alpha/F) \leq X$. We have

$$\begin{aligned}
\mathrm{disc}(K_\alpha/F) \leq X &\overset{(a)}{\iff} \frac{p-1}{d} \mathrm{disc}(L/F) + \frac{f_{L/F}}{d} \mathrm{disc}\left(L(\theta_\alpha)/L\right) \leq X \\
&\iff \frac{1}{e_{L/F}} \mathrm{disc}\left(L(\theta_\alpha)/L\right) \leq X - \frac{p-1}{d} f_{L/F}(e_{L/F} - 1) \\
&\iff \mathrm{disc}\left(L(\theta_\alpha)/L\right) \leq e_{L/F} X - (p-1)(e_{L/F} - 1) \\
&\iff (p-1)(|\nu_L(\alpha)| + 1) \leq e_{L/F} X - (p-1)(e_{L/F} - 1) \\
&\iff |\nu_L(\alpha)| \leq \frac{e_{L/F}}{p-1} \cdot X - e_{L/F}. \qquad (3.14)
\end{aligned}$$

There might be different i leading to the same Galois group. Let $I := \{i \in \{1, \dots, d\} \mid G_p(d,i) \cong G\}$.

There are precisely $(p-1)$ elements in $Y_{\{i\}}(L)$ defining the same field, hence this way, we get

$$\begin{aligned} Z(F, G_p; X) &\overset{(3.14)}{=} \sum_{\substack{L/F \\ \mathrm{Gal}(L/F)\cong C_d}} \sum_{i\in I} \frac{1}{p-1} Y_{\{i\}}\left(L, \frac{e_{L/F}}{p-1}X - e_{L/F}\right) \\ &\overset{(3.10)}{\asymp} \sum_{\substack{L/F \\ \mathrm{Gal}(L/F)\cong C_d}} \sum_{i\in I} X^{\frac{(p-1)\ell(i)}{p\cdot e_{L/F}}\cdot\left(\frac{e_{L/F}}{p-1}X - e_{L/F}\right)} \asymp X^{\frac{1}{p}}. \end{aligned}$$ □

3.2.3 Number of C_d-Extensions with Fixed Ramification Index

Definition 3.22. Let $\alpha_H(G) := \#\{U \leq G \mid U \cong H\}$ be the number of subgroups of G isomorphic to H.

Remark 3.23. Let $d \in \mathbb{N}$ such that $d \mid (q-1)$. Then there are exactly

$$d \prod_{\ell\in\mathbb{P},\ \ell \mid d} \frac{\ell+1}{\ell}$$

non-isomorphic C_d-extensions of $\mathbb{F}_q((t))$.

Proof. This is proven in Remark 2.14(b), see [KM20], for $\ell \in \mathbb{P}$. The general case follows by the multiplicativity shown in Lemma 2.5. □

Remark 3.24. Let $d = ef$ with $e, f \in \mathbb{N}$ such that $e \mid (q-1)$ and $\gcd(d, q) = 1$. Then there are precisely

$$e \prod_{\substack{\ell\in\mathbb{P} \\ \ell\mid\gcd(f,e)}} \frac{\ell-1}{\ell}$$

C_d-extensions of $\mathbb{F}_q((t))$ with ramification index e and inertia degree f, where φ is the Euler totient function.

Proof. By Theorem 3.6(a) and (c), all C_d-extensions with $e_{L/F} = e$ and $f_{L/F} = f$ are parametrised by some

$$1 \leq r \leq \gcd(e, q^f - 1) \text{ with } \gcd(e, f, r) = 1, \quad \text{where} \quad \gcd(e, q^f - 1) \overset{e\mid(q-1)}{=} e.$$

Hence, for the parameter r we have the conditions $1 \leq r \leq e, \quad \gcd(e, f, r) = 1$. With

$$\varphi\left(\gcd(e, f)\right) = \#\left\{1 \leq r \leq \gcd(e, f) \mid \gcd(r, \gcd(e, f)) = 1\right\}$$

and using $e = \frac{e}{\gcd(e,f)} \cdot \gcd(e,f)$, we get precisely

$$\frac{e}{\gcd(e,f)} \cdot \varphi\left(\gcd(e,f)\right) = \frac{e}{\gcd(e,f)} \cdot \gcd(e,f) \cdot \prod_{\substack{\ell \in \mathbb{P} \\ \ell \mid \gcd(e,f)}} \frac{\ell - 1}{\ell} = e \cdot \prod_{\substack{\ell \in \mathbb{P} \\ \ell \mid \gcd(e,f)}} \frac{\ell - 1}{\ell}$$

choices for r. □

Example 3.25.

(a) In the unramified case $e = 1$ the formula gives exactly 1 extension as expected.

(b) In the totally ramified case $e = d$ the formula gives e extensions as expected from Theorem 3.6.

Chapter 4

On Constructing Subgroups of $C_p \wr C_p$

In this chapter we will thoroughly study the Galois group $\mathrm{Gal}(L/F)$ of a tower of two C_p-extensions $L/E/F$ with $\mathrm{Gal}(L/E) \cong C_p \cong \mathrm{Gal}(E/F)$. This corresponds precisely to $\mathrm{Gal}(L/F) \leq C_p \wr C_p$ by Theorem 1.11. The field extensions can be described as the Galois closure of C_p-extensions $L/E/F$, similar to the situation in Chapter 3 and Section 3.1. The possible Galois groups in this case are well-known (e.g. [Sch14, Section 3]). Write $G := \mathrm{Gal}(L/F)$. If $\#G = p^{p+1}$, then $G \cong C_p \wr C_p$ is isomorphic to the wreath product. If $\#G = p^{r+1} < p^{p+1}$, then G is isomorphic to one of the two non-isomorphic groups $H(p,r)$ or $\widetilde{H}(p,r)$ which we will call *generalised Heisenberg group* and *twisted Heisenberg group*, respectively (see Definition 4.1). Both groups are solutions of a group extension

$$1 \to (C_p)^r \to G \to C_p \to 1$$

where $\exp(H(p,r)) = p$ and $\exp\left(\widetilde{H}(p,r)\right) = p^2$. Hence the knowledge of $\#G$ and the exponent $\exp(G)$ are sufficient to determine G up to isomorphism.

The main goal is to prove Theorem C and Theorem D from the introduction.

In order to achieve this, we firstly describe the groups. We will distinguish $H_{p^2}(p,r) \leq S_{p^2}$ and $\widetilde{H}_{p^2}(p,r) \leq S_{p^2}$ which correspond to non-Galois degree p^2-extensions, from $H_{p^{r+1}}(p,r) \leq S_{p^{r+1}}$ and $\widetilde{H}_{p^{r+1}}(p,r) \leq S_{p^{r+1}}$, respectively, which correspond to Galois extensions over the ground field F, i.e. for the Galois closure of L/F. This can be done by the module theoretic approach outlined in Schultz [Sch14] which gives us a nice way to determine the Galois group. Writing $[\alpha] := \alpha + \wp(E)$ for any $\alpha \in E \setminus \wp(E)$, we will associate a length function given as minimal i such that $(\sigma - 1)^i([\alpha])$ is zero, and a (restricted) function $\varepsilon_{E/F}$ which is basically determined by the value $(\sigma - 1)(\mathrm{Tr}_{E/F}(\alpha))$. This will give us a description of $J(E)$ as a $\mathrm{Gal}(E/F)$-module. See Section 4.2 for the details.

We give representative systems of $E/\wp(E)$ that describe $H(p,r)$-extensions respectively $\widetilde{H}(p,r)$-extensions. This will use the fact that $E = F(\theta_a)$ for some $a \in R_F$ and that there is a generator σ of $\mathrm{Gal}(E/F)$ so that $\sigma(\theta_a) = \theta_a + 1$. This makes it very convenient with the power basis $1, \theta_a, \ldots, \theta_a^{p-1}$ since it is easy to describe the involved automorphisms, the trace map etc.

In Section 4.3 we provide two systems of representatives which parametrise the $H(p,r)$-extensions.

Let $E = F(\theta_a)$ be a C_p-extension. Then one system of representatives

$$M_{a,r} = \{f_0 + f_1\theta_a + \dots f_{r-1}\theta_a^{r-1} \mid f_i \in R_{V_a}\},$$

where R_{V_a} is defined as in Remark 1.22, has the advantage of having a very simple description and makes it easy to read off the Galois group by Schultz' theory. We will prove the following decomposition:

Theorem. *Let $0 \neq a \in R_F$ and $E = F(\theta_a)$. Then we have:*

(a) $J(E) = \langle \gamma_E \rangle \bigoplus_{i=1}^{p-1} (M_{a,i} + \wp(E))$.

(b) For every normal $H(p,r)$-extension L/F containing E, there is an $\alpha \in M_{a,r}$ such that

$$L = E\left(\wp^{-1}(\langle \alpha \rangle_G)\right).$$

(c) For $\alpha \in M_a$ with $\operatorname{len}([\alpha]) = r$ we have $\operatorname{Gal}\left(E\left(\wp^{-1}(\langle \alpha \rangle_G)\right)/F\right) \cong \begin{cases} \widetilde{H}(p,r), & f_{p-1} \in R_F \setminus R_{V_a}, \\ H(p,r), & f_{p-1} \in R_{V_a}. \end{cases}$

The representative system $M_{a,r}$ has the flaw of not consisting of reduced elements if E/F is ramified. In order to control the discriminant of the occurring extensions in the ramified case, we develop a reduced system of representatives $\Omega_{E,r}$, which basically gives a reduced element in the class $f_0 + \wp(E)$ for $f_0 \in F$. There is a slight twist, however, as the elements in $\Omega_{E,r}$ define $H(p,i)$-extensions for $i \leq r$ only as will be proven in Theorem 4.47. The technical definition of $\Omega_{E,r}$ and further details can be found in Section 4.3.1.

For the counting problem by discriminant, we determine the minimal discriminant for the corresponding embedding problem for the permutation groups for the groups $H_{p^2}(p,r)$, $\widetilde{H}_{p^2}(p,r)$ and $\widetilde{H}_{p^{r+1}}(p,r)$. The formulas are outlined in Subsection 4.2.2 for the minimal Heisenberg extensions and for the minimal twisted Heisenberg extensions in (4.64) over p^2 points and in Theorem 4.65 over p^{r+1} points where we use the notations of Defintion i. As a second ingredient, it is crucial to determine the number of representatives up to a valuation bound.

Using the system of representatives $\Omega_{E,r}$ this way, we prove the discriminant density of $H_{p^2}(p,r)$ in Section 4.4, hence prove Theorem C from the introduction:

Theorem C. *For $1 \leq r \leq p-1$ we have*

$$Z\left(F, H_{p^2}(p,r); x\right) \asymp x^{a_p\left(H_{p^2}(p,r)\right)},$$

where $a_p\left(H_{p^2}(p,r)\right) = \begin{cases} \frac{r+1}{p(p+r)}, & r^2 < p \\ \frac{r}{p^2}, & r^2 > p. \end{cases}$

We approach by counting the extensions defined by $\Omega_{E,r}$ up to a discriminant bound X over all C_p-extensions E/F. The corresponding asymptotics exponents for all extensions with Galois group $H_{p^2}(p,i)$ for $1 \leq i \leq r$ are strictly increasing in r, and so we can deduce the asymptotics exponents for all $H_{p^2}(p,r)$-extensions.

The discriminant density of $\widetilde{H}_{p^2}(p,r)$-extensions can be proven analogously, where a simple variation of the representative system $\Omega_{E,r}$ does the trick which will be done in Section 4.5. Every $\widetilde{H}(p,r)$-extension arises as a C_{p^2}-twist of a certain $H(p,r)$-extension. Therefore, we give an explicit element $\gamma_E \in E$ such that $E(\theta_{\gamma_E})/F$ is a minimal C_{p^2}-extensions containing E. Then the representative system

$$\widetilde{\Omega}_{E,r} = \{\lambda\gamma_E + \alpha \mid \alpha \in M_{a,r},\ \lambda \in \mathbb{F}_p^\times\}$$

plays the role of $\Omega_{E,r}$ for $\widetilde{H}(p,r)$-extensions. We use the analogous method to the case of $H_{p^2}(p,r)$ to prove Theorem D from the introduction:

Theorem D. *For $1 \leq r \leq p-1$ we have*

$$Z\left(F, \widetilde{H}_{p^2}(p,r); x\right) \asymp x^{a_p\left(\widetilde{H}_{p^2}(p,r)\right)},$$

where $a_p\left(\widetilde{H}_{p^2}(p,r)\right) = \begin{cases} \frac{pr-r^2+r+1}{p(p^2-pr+p+r)}, & r^2 < p \\ \frac{r}{p^2}, & r^2 > p. \end{cases}$

Finally, we will consider Galois twisted Heisenberg extensions in Section 4.6, i.e. the transitive permutation groups $\widetilde{H}_{p^{r+1}}(p,r)$ for $1 \leq r \leq p-1$. We deduce the minimal solution of the embedding problem $1 \to (C_p)^r \to \widetilde{H}_{p^{r+1}}(p,r) \to C_p \to 1$ and deduce a lower bound on the asymptotics of $\widetilde{H}_{p^{r+1}}(p,r)$-extensions in Theorem 4.67.

Concerning the lower bound on $a_p\left(\widetilde{H}_{p^{r+1}}(p,r)\right)$, we construct a minimal solution for the embedding problem, see Theorem 4.65, and count the number of extensions having minimal discriminant. We will construct a minimal solution in the terms of the description of γ_E with respect to the power basis. All the other (minimal) solutions can be described by the elements in $\Omega_{E,r}$ up to an easily deduced valuation bound.

We conjecture the lower bound attained this way to be sharp.

4.1 Heisenberg Groups and Arithmetic of C_p-Extensions

4.1.1 Generalised and Twisted Heisenberg Groups

Let $p \in \mathbb{P}$ and $1 \leq r \leq p-1$. Up to isomorphism, there exist two groups satisfying a group extension

$$1 \longrightarrow (C_p)^r \longrightarrow G \longrightarrow C_p \longrightarrow 1 \quad \text{where} \quad (C_p)^r \text{ is a cyclic } \mathbb{F}_p[C_p]\text{-module.}$$

For more details, see [Wat94, Section 3] and [Sch14, Section 3]. The construction of the groups is taken from Definition 3.1 and 3.6 in [Sch14]. Here, we write $[g,h] := ghg^{-1}h^{-1}$ for the commutator of two group elements.

Definition 4.1. Let $p \in \mathbb{P}$ and $1 \leq r \leq p-1$. Then we define the *generalised Heisenberg group* as

$$H(p,r) := \langle \alpha_1, \ldots, \alpha_r; \tau \mid \alpha_i^p = 1, \tau^p = 1, [\alpha_i, \alpha_j] = 1, [\tau, \alpha_j] = \alpha_{j-1}, [\tau, \alpha_1] = 1 \\ \text{for } \ 1 \leq i \leq r, \ 2 \leq j \leq r \rangle.$$

We define the *twisted Heisenberg group* as

$$\widetilde{H}(p,r) := \langle \alpha_1, \ldots, \alpha_r; \tau \mid \alpha_i^p = 1, \tau^p = \alpha_1, [\alpha_i, \alpha_j] = 1, [\tau, \alpha_j] = \alpha_{j-1}, [\tau, \alpha_1] = 1 \\ \text{for } 1 \leq i \leq r, \ 2 \leq j \leq r \rangle.$$

We moreover set $H(p,p) := \widetilde{H}(p,p) := C_p \wr C_p$.

Note that $\widetilde{H}(p,r)$ coincides with Schultz' definition of $(C_p)^r \bullet_r C_p$ given in Definition 3.6 of [Sch14] and we have $H(p,r) \cong (C_p)^r \rtimes C_p$.

Remark 4.2. Let $p \in \mathbb{P}$ and $1 \leq r \leq p-1$.

(a) The group $H(p,r)$ has order p^{r+1} and exponent p. The group $\widetilde{H}(p,r)$ has order p^{r+1} and exponent p^2. In particular, we have $H(p,1) \cong C_p \times C_p$ and $\widetilde{H}(p,1) \cong C_{p^2}$.

(b) Let $r > 1$ and $G = H(p,r)$ or $\widetilde{H}(p,r)$. Its commutator subgroup is $[G,G] = \langle \alpha_i \mid 1 \leq i \leq r-1 \rangle$ and the center is $C(G) = \langle \alpha_1 \rangle \cong C_p$.

(c) We have the following interpretation in mind: For the normal subgroup $M := \langle \alpha_1, \ldots, \alpha_r \rangle \leq G$, its quotient group $\langle \tau \rangle / \langle \tau^p \rangle \cong C_p$ acts on M via

$$\bar{\tau} \cdot m := \tau \cdot m \cdot \tau^{-1} \text{ for all } \ m \in M.$$

Indeed, this is a well-defined C_p-action on M as $\tau^p \in C(G)$ acts trivial on M. This way, M defines an $\mathbb{F}_p[C_p]$-module, where $M = \langle \alpha_r \rangle_{\mathbb{F}_p[C_p]} \cong \mathbb{F}_p[G]/(\sigma - 1)^r$ is a cyclic C_p-module of rank r.

Example 4.3. *Let $p \in \mathbb{P}$.*

(a) As we have seen in Remark 4.2 we have $H(p,1) \cong C_p \times C_p$ and $\widetilde{H}(p,1) \cong C_{p^2}$.

(b) Let now $p \neq 2$ and let H be the classical Heisenberg group of upper-triangular 3×3-matrices whose diagonal is 1, i.e.

$$H := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{F}_p \right\} \leq \mathrm{GL}_3(\mathbb{F}_p).$$

This group is defined by the relations $H := \langle u, v, w \mid u^p = v^p = w^p = 1, \ uv = vu, uw = wu, wv = vwu \rangle$. By manipulating the last defining relation, it is easy to see that $H(p,2) \cong H$ is isomorphic to the classical Heisenberg group. This is a non-abelian group with p^3 elements and exponent p.

There is no group with these properties for $p = 2$ as groups of exponent 2 are abelian, and so does the corresponding matrix group. Note that $H(2,2) := D_4$ is non-abelian of exponent 4.

We have the group extensions

$$1 \longrightarrow (C_p)^r \xrightarrow{\iota} G \xrightarrow{\varphi} C_p = \langle \sigma \rangle \longrightarrow 1 \tag{4.1}$$

via $\iota(\lambda_1, \ldots, \lambda_r) := \alpha_1^{\lambda_1} \cdots \alpha_r^{\lambda_r}$ and $\varphi(\alpha_i) = 1$ for $1 \leq i \leq r$ and $\varphi(\tau) = \sigma$.

For $p = r$ we have $H(p,p) \cong \widetilde{H}(p,p) \cong C_p \wr C_p$ and the wreath product $C_p \wr C_p$ is the only group satisfying this embedding problem up to isomorphism. We will not distinguish between the two.

We call a field extension K/F a *(twisted) Heisenberg extension* if $\mathrm{Gal}(K/F) \cong H(p,r)$ or $\mathrm{Gal}(K/F) \cong \widetilde{H}(p,r)$ for some $1 \leq r \leq p$, respectively.

4.1.2 Traces in Towers of Artin-Schreier-Extensions

At first we thoroughly study C_p-extensions E/F and the corresponding Galois module $J(E)$.

In the following we fix

$$E = F(\theta_a) \text{ for } a \in R_F \quad \text{and} \quad \mathrm{Gal}(E/F) = \langle \sigma \rangle \text{ with } \sigma(\theta_a) = \theta_a + 1 \tag{4.2}$$

and the power basis $\mathscr{B} = \left(1, \theta_a, \ldots, \theta_a^{p-1}\right)$.

Lemma 4.4.

(a) Let $E = F(\theta_a)$ be an Artin-Schreier C_p-extension and $f_0, \ldots, f_{p-1} \in F$. Then we get

$$\mathrm{Tr}_{E/F}\left(\sum_{i=0}^{p-1} f_i \theta_a^i\right) = -f_{p-1}.$$

(b) Let $L = F(\theta_1, \ldots, \theta_r)$ be an Artin-Schreier tower as in Definition 1.10 with $[L:F] = p^r$. Then

$$\mathrm{Tr}_{L/F}\left(\sum_{(e_1,\ldots,e_r)\in\{0,\ldots,p-1\}^r} f_{(e_1,\ldots,e_r)} \theta_1^{e_1} \cdots \theta_r^{e_r}\right) = (-1)^r f_{(p-1,\ldots,p-1)}.$$

Proof. (Idea of proof is taken from [Alb34].)

Let $\mathscr{B} = (1, \theta_a, \ldots, \theta_a^{p-1})$ be the power basis of $F(\theta_a)/F$.

For $0 \leq i, j \leq p-1$ we have

$$\theta_a^{i+j} = \begin{cases} \theta_a^{i+j}, & i+j < p \\ (a+\theta_a)\theta_a^{i+j-p} = a\theta_a^{i+j-p} + \theta_a^{i+j-p+1}, & i+j \geq p. \end{cases} \tag{4.3}$$

Let $M = M_{\mathscr{B},\mathscr{B}}(\varphi_{\theta_a})$ be the representation matrix of θ_a, given by $\varphi_{\theta_a}\colon E \to E, x \mapsto x \cdot \theta_a$. The (k,j)-coefficient of the matrices M^i with $0 \leq i \leq p-1$ is given by

$$\theta_a^{i+j-1} = \sum_{k=1}^{p} \left(M^i\right)_{k,j} \cdot \theta_a^{k-1}, \quad 1 \leq k, j \leq p-1.$$

Thus we obtain as matrix coefficients

$$(M^i)_{k,j} \overset{(4.3)}{=} \begin{cases} 1, & i+j-1 = k-1 \text{ or } (i+j \geq p \text{ and } i+j-1-p+1 = k-1), \\ a & i+j-1-p = k-1, \\ 0, & \text{else.} \end{cases}$$
$$= \begin{cases} 1, & i+j = k \text{ or } i+j-p+1 = k, \\ a & i+j-p = k, \\ 0, & \text{else.} \end{cases}$$

For the diagonal entries we get $\left(M^i\right)_{k,k} = 1$ if and only if $i = 0$ or $i = p-1$ and $k \geq 1$. We cannot have $(M^i)_{k,k} = a$ as this implied $i = p$ which is absurd. Hence

$$\mathrm{Tr}_{E/F}(\theta_a^i) = \mathrm{Tr}(M^i) = \begin{cases} \sum_{k=0}^{p-1} 1 = p = 0, & i = 0 \\ \sum_{k=1}^{p-1} 1 = p-1 = -1, & i = p-1, \\ 0, & 1 \leq i \leq p-2. \end{cases}$$

Thus by linearity we get $\mathrm{Tr}_{E/F}\left(\sum_{k=0}^{p-1} f_i \theta_a^i\right) = \sum_{k=0}^{p-1} f_i \cdot \mathrm{Tr}_{E/F}(\theta_a^k) = f_{p-1} \cdot (-1) = -f_{p-1}$.

For (b) let $r > 1$ and $L_{r-1} := F(\theta_1, \ldots, \theta_{r-1})$. Write

$$\gamma = \sum_{(e_1,\ldots,e_r) \in \{0,\ldots,p-1\}^r} f_{(e_1,\ldots,e_r)} \theta_1^{e_1} \cdots \theta_r^{e_r}.$$

By the trace formula in towers we get

$$\begin{aligned} \mathrm{Tr}_{L/F}(\gamma) &= \mathrm{Tr}_{L_{r-1}/F}\left(\mathrm{Tr}_{L/L_{r-1}}(\gamma)\right) \\ &\underset{\text{Linearity of Tr}}{\overset{r=1}{=}} \mathrm{Tr}_{L_{r-1}/F}\left(\sum_{(e_1,\ldots,e_{r-1})} -f_{(e_1,\ldots,e_{r-1},p-1)} \theta_1^{e_1} \cdots \theta_{r-1}^{e_{r-1}}\right) \\ &\overset{\text{Ind.}}{=} (-1)^r f_{(p-1,\ldots,p-1)}. \end{aligned}$$

□

Lemma 4.5. *Let $E = F(\theta_a)$ for $a \in R_F$. Then for all $f_0, \ldots, f_{p-1} \in F$ we get*

$$\nu_E\left(\sum_{i=0}^{p-1} f_i \theta_a^i\right) = \min\left\{\nu_E(f_i \theta_a^i) \mid 0 \leq i \leq p-1\right\}. \tag{4.4}$$

Proof. For the case $f_0 = f_1 = \ldots = f_{p-1} = 0$ the statement is obvious.

If E/F is totally ramified, then $\nu_F(a) = \nu_E(\theta_a) < 0$ and $p \nmid \nu_F(a)$. Thus for all $0 \leq i \neq j \leq p-1$ with $f_i \neq 0$ or $f_j \neq 0$ we have

$$\nu_E(f_i \theta_a^i) = p\nu_F(f_i) + i\nu_F(a) \not\equiv \nu_F(f_j) + j\nu_F(a) = \nu_E(f_j \theta_a^j) \mod p,$$

and the claim follows by the ultra-metric triangle inequality.

Now let E/F be unramified. Then $1, \theta_a, \ldots, \theta_a^{p-1}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^p}$ and t is a prime element of E. For $f_i \neq 0$, write $f_i = \sum_{k=\nu_i}^{\infty} f_{i,k} t^k$ with $f_{i,k} \in \mathbb{F}_q$, $f_{i,\nu_i} \neq 0$ and $\nu_i = \nu_F(f_i) \in \mathbb{Z}$. Set $\nu_i = \infty$ if $f_i = 0$. Let $n := \min\{\nu_0, \ldots, \nu_{p-1}\}$, then

$$\begin{aligned}\sum_{i=0}^{p-1} f_i \theta_a^i &= \sum_{i=0}^{p-1} \sum_{k=\nu_i}^{\infty} f_{i,k} t^k \theta_a^i \\ &= \sum_{i=0}^{p-1} \left(f_{i,n} \theta_a^i\right) t^n + \sum_{k=n+1}^{\infty} \left(f_{0,k} + f_{1,k}\theta_a + \ldots + f_{p-1,k}\theta_a^{p-1}\right) t^k.\end{aligned}$$

By $\mathbb{F}_q$-linear independence of $\theta_a^0, \ldots, \theta_a^{p-1}$ we have $\sum_{i=0}^{p-1} f_{i,n}\theta_a^i \neq 0$ and thus

$$n = \nu_E\left(\sum_{i=0}^{p-1} f_i \theta_a^i\right) = \min\left\{\nu_E(f_i\theta_a^i) \mid 0 \leq i \leq p-1\right\}. \qquad \square$$

Lemma 4.6. *Let E, a and σ as in Remark 4.2 and $\mathscr{B} = (1, \theta_a, \ldots, \theta_a^{p-1})$ be the power basis of E/F. Then:*

(a) The representation matrix of σ, corresponding to $\mathscr{B}$, is the upper-triangular Pascal matrix

$$M_{\mathscr{B}}(\sigma) = \left(\binom{j-1}{i-1}\right)_{\substack{i=1,\ldots,p \\ j=i,\ldots,p}} \in \mathrm{GL}_p(\mathbb{F}_p).$$

Its inverse is the alternating Pascal matrix $M_{\mathscr{B}}(\sigma^{-1}) = \left((-1)^{i+j}\binom{j-1}{i-1}\right)_{\substack{i=1,\ldots,p \\ j=i,\ldots,p}}$.

(b) We have $\mathrm{Ker}(\sigma - 1) = F$ and the image $\mathrm{Im}(\sigma - 1) = \mathrm{Span}_F(1, \theta_a, \ldots, \theta_a^{p-2})$.

(c) We have $\nu_E\left((\sigma-1)(\theta_a^i)\right) = (i-1)\nu_E(\theta_a)$ for $1 \leq i \leq p-1$. Moreover, for all $\beta \in E$ we have

$$\nu_E\left((\sigma-1)(\beta)\right) \geq \nu_E(\beta) - \nu_E(\theta_a).$$

Proof. For (a) note that $\sigma(\theta_a) = \theta_a + 1$, hence

$$\sigma(\theta_a^i) = \sigma(\theta_a)^i = (\theta_a + 1)^i = \sum_{k=0}^{i} \binom{i}{k} \theta_a^k \tag{4.5}$$

showing the result on the coefficients of the representation matrix. The coefficients of the inverse matrix can be found in [Yat14, Theorem 2.9].

For part (b), let $\alpha = \sum_{i=0}^{p-1} f_i \theta_a^i$ for $f_i \in F$. Then we have

$$(\sigma-1)(\alpha) \overset{(4.5)}{=} \sum_{i=0}^{p-1} f_i \cdot \left(\sum_{k=0}^{i-1} \binom{i}{k} \theta_a^k \right) = \sum_{i=0}^{p-2} \left(\sum_{k=i+1}^{p-1} f_k \binom{k}{i} \right) \theta_a^i.$$

This expression is 0 if and only if $0 = f_{p-1} = f_{p-2} = \ldots = f_1$, hence $\mathrm{Ker}(\sigma-1) = F$.

By (4.5) we have $\mathrm{Im}(\sigma-1) \subseteq \mathrm{Span}_F(1, \theta_a, \ldots, \theta_a^{p-2})$ and thus $\mathrm{Im}(\sigma-1) = \mathrm{Span}_F(1, \theta_a, \ldots, \theta_a^{p-2})$ as both F-vector spaces have dimension $p-1$.

For (c) note that for $f_i \in F$ and $1 \le i \le p-1$ we have

$$\begin{aligned} \nu_E((\sigma-1)(f_i\theta_a^i)) &= \nu_E\left(f_i \left(\sum_{k=0}^{i} \binom{i}{k} \theta_a^k - \theta_a^i \right) \right) = \nu_E\left(f_i \sum_{k=0}^{i-1} \binom{i}{k} \theta_a^k \right) \\ &= \nu_E(f_i i \theta_a^{i-1}) = \nu_E(f_i \theta_a^i) - \nu_E(\theta_a), \end{aligned} \tag{4.6}$$

thus by the ultra-metric triangle-inequality

$$\begin{aligned} \nu_E\left((\sigma-1)(\alpha)\right) = \nu_E\left((\sigma-1)(\sum_{i=0}^{p-1} f_i \theta_a^i) \right) &\ge \min\left\{ \nu_E((\sigma-1)(f_i\theta_a^i)) \mid 1 \le i \le p-1 \right\} \\ &= \min\left\{ \nu_E(f_i\theta_a^i) - \nu_E(\theta_a) \mid 1 \le i \le p-1 \right\} \\ &\overset{\text{Lemma } 4.5}{=} \nu_E(\alpha) - \nu_E(\theta_a). \end{aligned}$$

Inserting $f_i = 1$ in (4.6) yields the statement on $\nu_E\left(\sigma-1)(\theta_a^i)\right)$. □

Lemma 4.7. *(a) The F-linear map*

$$\Psi\colon \mathrm{Span}_F(\theta_a, \ldots, \theta_a^{p-1}) \longrightarrow \mathrm{Span}_F(1, \theta_a, \ldots, \theta_a^{p-2}), \quad x \mapsto (\sigma-1)(x)$$

is an isomorphism.

(b) For all $0 \le i \le p-2$ there exist $\mu_{1,i+1}, \ldots, \mu_{i,i+1} \in \mathbb{F}_p$ such that

$$\Psi^{-1}(\theta_a^i) = \frac{1}{i+1}\theta_a^{i+1} + \sum_{k=1}^{i} \mu_{k,i+1}\theta_a^k. \tag{4.7}$$

(c) For all $\beta \in \mathrm{Span}_F(1, \theta_a, \ldots, \theta_a^{p-2})$ we have $\nu_E\left(\Psi^{-1}(\beta)\right) = \nu_E(\beta) + \nu_F(a)$.

Proof. Part (a) follows by Lemma 4.6(b).

For part (b), we consider the F-bases $\mathscr{B} = (\theta_a, \ldots, \theta_a^{p-1}) = (b_1, \ldots, b_{p-1})$ and $\mathscr{C} = (1, \theta_a, \ldots, \theta_a^{p-2}) = (c_1, \ldots, c_{p-1})$ and the representation matrix of Ψ. We get by (4.5) that

$$M := \mathcal{M}_{\mathscr{C},\mathscr{B}}(\Psi) = \left(\binom{i}{k-1} \right)_{\substack{1 \le i \le p-1 \\ 1 \le k \le i}}.$$

In particular, the matrix $\mathcal{M}_{\mathscr{C},\mathscr{B}}(\Psi) \in \mathrm{GL}_{p-1}(\mathbb{F}_p)$ is an upper triangular matrix with diagonal entries $M_{ii} = \binom{i}{i-1} = i$. We get

$$\widetilde{M} := \mathcal{M}_{\mathscr{C},\mathscr{B}}(\Psi^{-1}) = \mathcal{M}_{\mathscr{B},\mathscr{C}}(\Psi)^{-1} \in \mathrm{GL}_{p-1}(\mathbb{F}_p)$$

with diagonal entries $\widetilde{M}_{ii} = \frac{1}{i}$. Writing $c_i = \theta_a^{i-1}$ and $b_i = \theta_a^i$ for the base vectors, we have

$$\Psi^{-1}(\theta_a^i) = \Psi^{-1}(c_{i+1}) = \sum_{k=1}^{i+1} \widetilde{M}_{k,i+1} \cdot b_k = \sum_{k=1}^{i} \widetilde{M}_{k,i+1}\theta_a^k + \frac{1}{i+1}\theta_a^{i+1}.$$

The claim in (b) follows with $\mu_{k,i+1} = \widetilde{M}_{k,i+1}$.

We prove part (c) first for $f_i\theta_a^i$ and $f_i \in F$. Let $0 \le i \le p-2$ and $f_i \in F$. Then by (a),

$$\nu_E\left(\Psi^{-1}(f_i\theta_a^i)\right) = \nu_E\left(\frac{1}{i+1}f_i\theta_a^{i+1} + \sum_{k=1}^{i}\mu_{k,i+1}f_i\theta_a^k\right) = \nu_E(\frac{1}{i+1}f_i\theta_a^{i+1}) = \nu_E(f_i\theta_a^i) + \nu_E(\theta_a). \quad (4.8)$$

Now let $\beta = \sum_{i=0}^{p-2} f_i\theta_a^i$. By the triangle inequality and (4.8) we have

$$\nu_E(\Psi^{-1}(\beta)) \ge \nu_E(\beta) + \nu_F(a). \quad (4.9)$$

To establish equality, let $z := \max\left\{0 \le i \le p-2 \ : \ \nu_E(\beta) = \nu_E(f_i\theta_a^i)\right\}$. Then necessarily,

$$\nu_F(f_z) < \nu_F(f_{z+1}), \ldots, \nu_F(f_z) < \nu_F(f_{p-1}). \quad (4.10)$$

$$\begin{aligned}
\Psi^{-1}(\beta) = \sum_{i=0}^{p-2}\Psi^{-1}(f_i\theta_a^i) &\overset{(a)}{=} \sum_{i=0}^{p-2}\left(\frac{1}{i+1}f_i\theta_a^{i+1} + \sum_{k=1}^{i}\mu_{k,i+1}f_i\theta_a^k\right)\\
&= \sum_{k=1}^{p-1}\left(\frac{1}{k}f_{k-1}\theta_a^k + \sum_{j=k+1}^{p-1}\mu_{k,j}f_{j-1}\theta_a^k\right)\\
&= \sum_{k=1}^{p-1}\left(\frac{1}{k}f_{k-1} + \mu_{k,k+1}f_k + \ldots + \mu_{k,p-1}f_{p-2}\right)\theta_a^k\\
&\overset{\text{La. 4.5}}{=} \min\left\{\nu_F\left(\left(\frac{1}{k}f_{k-1} + \mu_{k,k+1}f_k + \ldots + \mu_{k,p-1}f_{p-2}\right)\theta_a^k\right) \mid 1 \le k \le p-1\right\}. \quad (4.11)
\end{aligned}$$

For the value $k = z$ we obtain

$$\nu_E(\left(\frac{1}{z+1}f_z + \mu_{z+1,z+2}f_{z+1} + \ldots + \mu_{z+1,p-1}f_{p-2}\right)\theta_a^{z+1}) \overset{(4.10)}{=} \nu_E(f_z\theta_a^{z+1}) = \nu_E(\beta) + \nu_F(a)$$

and by (4.9) we have $\nu_E\left(\Psi^{-1}(\beta)\right) \ge \nu_E(\beta) + \nu_F(a)$. This proves the equality by (4.11). □

4.2 Galois Module Theory

We follow Schultz et al. [Sch14] who study embedding problems

$$1 \to (C_p)^r \to \tilde{G} \to C_{p^n} \to 1$$

in both $\mathrm{char}(E) = p$ and $\mathrm{char}(E) \neq p$. We will only consider the case $n = 1$.

Definition 4.8. Let E/F be a C_p-extension and $G = \langle\sigma\rangle = \mathrm{Gal}(E/F)$. For a G-module M we define

$$\mathrm{len}(M) := \min\{l \in \mathbb{N} \mid (\sigma - 1)^l(M) = 0\}$$

as the length of M. For a field element $\beta \in E$ we set $[\beta] = \beta + \wp(E) \in J(E)$ and $\mathrm{len}([\beta]) := \mathrm{len}(\langle[\beta]\rangle_G)$, where $\langle[\beta]\rangle_G$ is the G-submodule of $J(E)$ generated by $[\beta]$. We define the trace map

$$\mathrm{Tr}_{E/F} \colon J(E) \to J(F), \quad [\beta] \mapsto [\mathrm{Tr}_{E/F}(\beta)].$$

Remark 4.9. Let $[\alpha], [\beta] \in J(E) = E/\wp(E)$. Then we have

$$\mathrm{len}([\alpha + \beta]) \leq \max\{\mathrm{len}([\alpha]), \mathrm{len}([\beta])\}. \tag{4.12}$$

Moreover, we have

$$\mathrm{len}([\alpha]) \neq \mathrm{len}([\beta]) \Longrightarrow \mathrm{len}([\alpha + \beta]) = \max\{\mathrm{len}([\alpha]), \mathrm{len}([\beta])\}. \tag{4.13}$$

Proof. We have $(\sigma - 1)^i([\alpha + \beta]) = (\sigma - 1)^i([\alpha]) + (\sigma - 1)^i([\beta])$ for $i \in \mathbb{N}$. With the choice $i := \max\{\mathrm{len}([\alpha]), \mathrm{len}([\beta])\}$ we get

$$[0] + [0] = (\sigma - 1)^i([\alpha]) + (\sigma - 1)^i([\beta]) = (\sigma - 1)^i([\alpha + \beta]),$$

thus $\mathrm{len}([\alpha + \beta]) \leq \max(\mathrm{len}([\alpha]), \mathrm{len}([\beta]))$.

Now let $\mathrm{len}([\alpha]) \neq \mathrm{len}([\beta])$. We may assume $\mathrm{len}([\alpha]) > \mathrm{len}([\beta])$. Setting $i := \mathrm{len}([\alpha]) - 1$, we get

$$(\sigma - 1)^i([\alpha + \beta]) = (\sigma - 1)^i([\alpha]) + (\sigma - 1)^i([\beta]) = \underbrace{(\sigma - 1)^i([\alpha])}_{\neq [0]} + [0] \neq [0],$$

hence $\mathrm{len}([\alpha + \beta]) > i = \mathrm{len}([\alpha]) - 1 = \max(\mathrm{len}([\alpha]), \mathrm{len}([\beta])) - 1$. By (4.12) we thus have $\mathrm{len}([\alpha + \beta]) = \max(\mathrm{len}([\alpha]), \mathrm{len}([\beta]))$. □

Recall $\nu_{J(E)}([\alpha]) = \max_{x \in E}(\nu_E(\alpha + \wp(x))) = \max_{\beta \in [\alpha]}(\nu_E(\beta))$.

Lemma 4.10. *Let $E = F(\theta_a)$ for $a \in R_F$ with $G := \mathrm{Gal}(E/F) \cong C_p$. Let $\beta \in E$, and $l := \mathrm{len}([\beta])$. Then:*

(a) We get $\mathrm{len}([\beta]) = \min\{n \in \mathbb{N} \mid (\sigma - 1)^n(\beta) \in \wp(E)\}$.

(b) *The system* $\left([(\sigma-1)^i(\beta)]\right)_{i=0,\dots,l-1}$ *forms an* $\mathbb{F}_p$*-basis of* $\langle[\beta]\rangle_G$.
In particular, we have $\operatorname{len}([\beta]) = \dim_{\mathbb{F}_p}(\langle[\beta]\rangle_G)$.

(c) *For all* $(\lambda_0,\dots,\lambda_{l-1}) \in \mathbb{F}_p^l$ *we have*

$$\nu_{J(E)}\left(\left[\sum_{i=0}^{l-1}\lambda_i(\sigma-1)^i(\beta)\right]\right) = \nu_{J(E)}\left([(\sigma-1)^z(\beta)]\right),$$

where $z := \min\{0 \le i \le l-1 \mid \lambda_i \neq 0\}$.

(d) *In particular, for the field discriminant of the degree* p^l*-extension we get*

$$\operatorname{disc}(E(\langle[\beta]\rangle_G)/E) = \sum_{i=0}^{l-1} p^i \operatorname{disc}_{J(E)}((\sigma-1)^{l-i-1}(\beta)).$$

Proof. The maps $\wp$ and σ commute, thus $(\sigma-1)(\wp(x)) = \wp((\sigma-1)(x))$ for all $x \in E$ and $[(\sigma-1)(\beta)] = (\sigma-1)([\beta])$.

This shows (b) and (a) via $(\sigma-1)^i([\beta]) = [0] \iff (\sigma-1)^i(\beta) \in \wp(E)$.

(c) Choose $\beta_i \in [(\sigma-1)^i(\beta)]$ such that $\nu_{J(E)}([(\sigma-1)^i(\beta)]) = \nu_E(\beta_i)$ for $0 \le i \le \operatorname{len}([\beta])$ and let $z := \min\{0 \le i \le l-1 \mid \lambda_i \neq 0\}$

If E/F is totally ramified, then Lemma 4.6(c) immediately proves that

$$\nu_E(\beta_0) < \nu_E(\beta_1) < \ldots < \nu_E(\beta_{\operatorname{len}([\beta])-1})$$

are pairwise different and the result follows by the ultrametric triangle-inequality.

Let E/F be unramified now. Again, we have

$$\nu_E(\beta_0) \le \nu_E(\beta_1) \ldots \le \nu_E(\beta_{\operatorname{len}([\beta])-1}).$$

Write $\beta_i = \sum_{k=0}^{p-1} g_{i,k}\theta_a^k$ for $g_{i,k} \in F$, and set

$$\rho(i) := \max\left(0 \le k \le p-1 \mid \nu_E(\beta_i) = \nu_E(g_{i,k}\theta_a^k)\right) \qquad \text{for } 0 \le i \le \operatorname{len}([\beta])-1.$$

Note that we have $p \nmid \nu_E(\beta_i)$ or $\nu_E(\beta_i) = 0$ and $\beta_i \notin \wp(E)$ for $0 \le i \le \operatorname{len}([\beta])-1$. By assumption and (4.6) we have $\nu_F(g_{i,\rho(z)}) > \nu_F(g_{z,\rho(z)})$ for all $i > z$. Hence with Lemma 4.5 we get

$$\begin{aligned}\nu_E(\sum_{i=0}^{l-1}\lambda_i\beta_i) \overset{0=\lambda_{z-1}=\ldots=\lambda_0}{=} \nu_E(\sum_{i=z}^{l-1}\lambda_i\beta_i) &= \nu_E(\sum_{i=0}^{\operatorname{len}([\beta])-1}\lambda_i\sum_{k=0}^{p-1}g_{i,k}\theta_a^k)\\ &= \nu_E(\sum_{i=0}^{}\lambda_i g_{i,\rho(i)}\theta_a^{\rho(i)}) \overset{\text{La. 4.5}}{=} \nu_E(\beta_z).\end{aligned}$$

As $p \nmid \nu_E(\beta_z)$ or $\beta_z \notin \wp(E)$ and $\nu_E(\beta_z) = 0$, we have

$$\nu_E(\beta_z) = \nu_{J(E)}([\beta_z]) = \nu_{J(E)}\left(\left[\sum_{i=0}^{l-1} \beta_i\right]\right).$$

(d) $(\beta_i)_{i=0,\dots,l-1} := ([(\sigma-1)^i(\beta)])_{i=0,\dots,l-1}$ forms an $\mathbb{F}_p$-basis of $\langle[\beta]\rangle$ by (b). The discriminant formula for elementary abelian p-extensions implies

$$\begin{aligned}
\operatorname{disc}(E(\wp^{-1}(\langle[\beta]\rangle))/E) &= \sum_{(\lambda_0,\dots,\lambda_{l-1})\in\mathbb{F}_p^l\setminus 0} \operatorname{cond}(E(\wp^{-1}(\sum_{i=0}^{l-1}\lambda_i\beta_i))/E) \\
&= \sum_{(\lambda_0,\dots,\lambda_{l-1})\in\mathbb{F}_p^l\setminus 0} (\operatorname{cond}_{J(E)}(\sum_{i=0}^{l-1}\lambda_i\beta_i)) \\
&\overset{(c)}{=} \sum_{i=0}^{l-1}(p^{l-i}-p^{l-i-1})\operatorname{cond}_{J(E)}(\beta_i) \\
&= \sum_{i=0}^{l-1} p^{l-1-i}\operatorname{disc}_{J(E)}(\beta_i) = \sum_{i=0}^{l-1} p^i \operatorname{disc}_{J(E)}(\beta_{l-1-i}).
\end{aligned}$$

Inserting $\beta_i = [(\sigma-1)^i(\beta)]$ proves (d). □

Corollary 4.11. *Let $\alpha, \beta \in E$ such that $\langle\alpha\rangle_G = \langle\beta\rangle_G$. Then $\nu_{J(E)}([\alpha]) = \nu_{J(E)}([\beta])$.*

Proof. Let $l = \operatorname{len}([\alpha])$. Using the F-basis $\left((\sigma-1)^i(\alpha)\right)_{0\le i\le l-1}$ we get

$$[\beta] = \sum_{i=0}^{l-1}\lambda_i[(\sigma-1)^i(\alpha)] \quad \text{for some } \lambda_i \in \mathbb{F}_p.$$

Suppose $\lambda_0 = 0$, then $\operatorname{len}([\beta]) = \operatorname{len}\left(\left[\sum_{i=1}^{l-1}\lambda_i[(\sigma-1)^i(\alpha)]\right]\right) < l$ and $\langle\alpha\rangle_G \neq \langle\beta\rangle_G$.

Thus $\lambda_0 \neq 0$ and by Lemma 4.10(c) we have $\nu_{J(E)}([\alpha]) = \nu_{J(E)}([\beta])$. □

Following [Sch14] we suggest the following definition.

Definition 4.12. Let $E = F(\theta_a)$ for $a \in R_F$.

(a) Let $\mathscr{B}$ be an $\mathbb{F}_p$-basis of $J(F)$ such that $[a] \in \mathscr{B}$. Consider the corresponding dual basis $(\lambda_v)_{v\in\mathscr{B}}$. Then we define a map

$$\varepsilon_{E/F}\colon J(E) \longmapsto \mathbb{F}_p, \qquad [\beta] \longmapsto \lambda_{[a]}([\operatorname{Tr}_{E/F}(\beta)]).$$

(b) For $1 \leq r \leq p-1$ we set

$$J_r(E) := \{[\beta] \in J(E) \ : \ \operatorname{len}([\beta]) \leq r, \quad \varepsilon_{E/F}([\beta]) = 0\}$$

and

$$\widetilde{J}_r(E) := \{[\beta] \in J(E) \ : \ \operatorname{len}([\beta]) \leq r, \quad \varepsilon_{E/F}([\beta]) \neq 0\}$$

Moreover, we set $J_p(E) := \{[\beta] \in J(E) \ : \ \operatorname{len}([\beta]) \leq p\} = J(E)$.

(c) For $1 \leq r, s \leq p$, $s \neq p$ and $x \in \mathbb{R}_{\geq 0}$ we set

$$J_r(E,x) := \left\{[\beta] \in J_r(E) \ : \ |\nu_{J(E)}([\beta])| \leq x\right\},$$
$$\widetilde{J}_s(E,x) := \left\{[\beta] \in \widetilde{J}_s(E) \ : \ |\nu_{J(E)}([\beta])| \leq x\right\}.$$

Schultz uses in his paper [Sch14, Section 4.1] actually a different definition from our definition of $\varepsilon_{E/F}$ and defines it in greater generality. For now, let K/F be a cyclic C_{p^n}-extension with $\langle\sigma\rangle = \operatorname{Gal}(K/F)$. Let $(\sigma-1)\colon J(K) \to J(K), [\beta] \mapsto [\sigma(\beta)-\beta]$ be the corresponding endomorphism on $J(K)$. Then Schultz defines the function

$$e\colon \operatorname{Ker}((\sigma-1)^{p^n-1}) \to \mathbb{F}_p, \quad [\beta] \mapsto [(\sigma-1)(\theta_{\operatorname{Tr}_{K/F}(\beta)})].$$

In the case $n=1$, this definition indeed coincides with $\varepsilon_{K/F}$ on $\operatorname{Ker}(\sigma-1)^{p-1}$ as we show next. This way, we can apply all results from [Sch14] on the function e on our function $\varepsilon_{E/F}$.

Remark 4.13. Let $n = 1$ and E/F be a C_p-extension, then $e([\beta]) = \varepsilon_{E/F}([\beta])$ for all $[\beta] \in \operatorname{Ker}((\sigma-1)^{p-1})$.

Proof. Let $\beta = \sum_{i=0}^{p-1} f_i \theta_a^i$ with $f_i \in F$ and $(\sigma-1)^{p-1}([\beta]) = 0$. This means that $f_{p-1} \in \wp(E) \cap F = \mathbb{F}_p \cdot a + \wp(F)$, hence

$$f_{p-1} = \mu a + \wp(f) = -\operatorname{Tr}_{E/F}(\beta) \quad \text{for some} \quad \mu \in \mathbb{F}_p, \ f \in F. \tag{4.14}$$

Thus we get

$$(\sigma-1)\left([\theta_{\operatorname{Tr}_{E/F}(\beta)}]\right) = [(\sigma-1)(-\mu\theta_a - f)] = -\mu = \lambda_{[a]}([-\mu a + \wp(f)]) = \varepsilon_{E/F}([\beta]). \qquad \square$$

The purpose of the $\varepsilon_{E/F}$-function is to predict the group exponent of the Galois group defined by a cyclic module. More precisely, let K/F be an C_{p^n}-extension. Let $[\beta] \in J(K)$ with $\operatorname{len}([\beta]) = r < p^n$ and write $L := K(\wp^{-1}(\langle\beta\rangle))$. For any $\hat{\sigma} \in \operatorname{Gal}(L/F)$ such that $\hat{\sigma}|_E = \sigma$, Schultz proves the equivalence

$$\hat{\sigma}^{p^n} = \mathrm{id} \iff \hat{\sigma}^p(\theta_\beta) = \theta_\beta \iff (\hat{\sigma}-1)(\theta_{\operatorname{Tr}_{E/F}(\beta)}) = 0. \tag{4.15}$$

If $\operatorname{len}([\beta]) < p^n$, then $\operatorname{Tr}_{K/F}(\beta) \in \wp(K) \cap F$ and thus, $\hat{\sigma}$ acts the same as σ on $\theta_{\operatorname{Tr}_{K/F}(\beta)} \in K$. Thus $\varepsilon_{E/F}([\beta])$ is indeed independent of any choice of $\hat{\sigma}$.

Conclusively, considering the embedding problem $1 \to (C_p)^r \to G \to C_{p^n} \to 1$ with $r < p^n$, we get $\exp(G) = p^n$ if and only if $\varepsilon_{E/F}([\beta]) = 0$. In our case $n = 1$, this enables us to distinguish $H(p,r)$ and $\widetilde{H}(p,r)$. Embedding theoretically, this means that all pre-images of σ in G have the same order.

This is not true in the case $r = p^n$, where $\varepsilon_{E/F}$ is not base-independent. It depends on a choice of either a basis of $J(E)$ or a choice of a continuation $\hat{\sigma}$, or a choice on a pre-image of σ in the group extension. On the other hand, both groups are isomorphic, hence the length is sufficient as an invariant.

Finally, in the case $n = 1$ and $r = p$, it is worth pointing out that the trace describes the underlying $C_p \times C_p$-extension, as

$$\mathrm{Span}_{\mathbb{F}_p}\left(a, \mathrm{Tr}_{E/F}(\beta)\right) + \wp(F) = \wp(L) \cap F \quad \text{is of rank 2 modulo } \wp(F).$$

Remark 4.14.

(a) Note that $\mathrm{Tr}_{E/F}(\wp(\alpha)) = \wp\left(\mathrm{Tr}_{E/F}(\alpha)\right)$ for all $\alpha \in E$, thus $\varepsilon_{E/F}$ is a well-defined $\mathbb{F}_p$-linear map. However, the definition of $\varepsilon_{E/F}$ depends on the chosen basis $\mathscr{B}$ of $J(E)$.

(b) Let $f_0, \ldots, f_{p-1} \in F$. Using Lemma 4.4(a) we have

$$\varepsilon_{E/F}\left(\left[\sum_{i=0}^{p-1} f_i \theta_a^i\right]\right) = \lambda_{[a]}([\mathrm{Tr}_{E/F}(\sum_{i=0}^{p-1} f_i \theta_a^i)]) = \lambda_{(a)}\left([-f_{p-1}]\right) \quad \text{for all} \quad f_i \in F. \tag{4.16}$$

Therefore we get

$$\varepsilon_{E/F}\left(\left[\sum_{i=0}^{p-2} f_i \theta_a^i + \wp(f_{p-1})\theta_a^{p-1}\right]\right) = 0 \qquad \text{for all} \quad f_i \in F. \tag{4.17}$$

If we write $[f_{p-1}] = \mu_{[a]} \cdot [a] + \sum_{[b] \in \mathscr{B} \setminus \{[a]\}} \mu_{[b]} \cdot [b]$ as its unique $\mathbb{F}_p$-linear combination of $\mathscr{B}$, then we obtain

$$\varepsilon_{E/F}([f_{p-1}\theta_a^{p-1}]) = \lambda_{[a]}([-f_{p-1}]) = -\mu[a].$$

4.2.1 Description of (Twisted) Heisenberg Extensions

Theorem 4.15. *Let $[\alpha] \in J(E)$ and $r := \mathrm{len}([\alpha])$.*

(a) If $r < p$, then $E(\wp^{-1}(\langle\alpha\rangle_G))$ is an $H(p,r)$- or an $\tilde{H}(p,r)$-extension. Moreover, it is a twisted Heisenberg extension if and only if $\varepsilon_{E/F}([\alpha]) \neq 0$.

(b) If $r = p$ then $E(\wp^{-1}(\langle\alpha\rangle_G))$ is a $C_p \wr C_p$-extension.

A proof is given in [Sch14, Prop. 4.2]. The major step is (4.15) combined with Lemma 4.10(b).

Theorem 4.16. *Let $a \in R_F$ with $E = F(\theta_a)$ and $1 \le r \le p-1$.*

(a) For any $\alpha \in E$ with $\nu_E(\alpha) > r\nu_F(a)$ we get $\operatorname{len}([\alpha]) \le r$.

(b) Let $\alpha = f_0 + f_1\theta_a + \ldots + f_r\theta_a^r \in E$ with $f_i \in F$. Then

$$\operatorname{len}([\alpha]) = r+1 \iff f_r \notin \wp(E) \cap F.$$

Proof. (a) If E/F is unramified, then the assertion $\nu_E(\alpha) > r\nu_F(a)$ implies that $\nu_E(\alpha) > 0$. Therefore $\alpha \in \wp(E)$ and $\operatorname{len}([\alpha]) = 0 \le r$.

Now assume E/F to be totally ramified. Then by Lemma 4.6(c) we have

$$\nu_E\left((\sigma-1)^r(\alpha)\right) \ge \nu_E(\alpha) - r\nu_F(a) > 0,$$

thus $(\sigma-1)^r(\alpha) \in \wp(E)$ and $\operatorname{len}([\alpha]) \le r$ which shows (a).

(b) For $f \in F$ we have

$$(\sigma-1)(f\theta_a^i) = f \cdot \left((\theta_a+1)^i - \theta_a^i\right) = f \cdot \sum_{i=0}^{j-1} \binom{i}{j} \theta_a^j$$

hence

$$(\sigma-1)^r(f_0 + f_1\theta_a + \ldots + f_r\theta_a^r) = \lambda f_r \quad \text{for } \lambda = r! \in \mathbb{F}_p^\times.$$

Thus $(\sigma-1)^{r+1}(\alpha) = 0$ and $\operatorname{len}([\alpha]) \le r+1$. Moreover

$$[(\sigma-1)^r(\alpha)] = [\lambda f_r] = 0 \overset{\text{La. 1.5(b)}}{\iff} [f_r] = 0 \iff f_r \in \wp(E).$$

Thus $\operatorname{len}(\alpha) = r+1 \iff f_r \notin \wp(E)$. □

Example 4.17. *Let $1 \le r \le p-1$ and $f_0, \ldots, f_r \in F$. In the case $f_r \in \wp(E) \cap F$ every length $\operatorname{len}\left(\left[\sum_{i=0}^{r} f_i\theta_a^i\right]\right) \in \{0, \ldots, r\}$ is possible: For this, choose $g_r \in R_F$ and $f_r = \wp(g_r)$. We get*

$$\wp(g_r\theta_a^r) = \underbrace{\wp(g_r)}_{=f_r}\theta_a^r + \sum_{i=0}^{r-1} \binom{r}{i} g_r^p a^{r-i}\theta_a^i =: f_r\theta_a^r + h_{r-1}\theta_a^{r-1} + \ldots + h_0 \in \wp(E) \tag{4.18}$$

and this element has length 0.

For length $r-1$ take for instance $\beta := \Psi^{-(r-1)}(\wp(g)\theta_a)$, then $\operatorname{len}([\beta]) = r-1$.

Note furthermore that $h_i \notin \wp(E) \cap F$ for all $0 \le i \le r-2$. Thus $\operatorname{len}\left(\left[\sum_{k=0}^{i} h_i\theta_a^i\right]\right) = i$, hence

$$\operatorname{len}\left(\left[f_r\theta_a^r + h_{r-1}\theta_a^{r-1} + \ldots + h_{i+1}\theta_a^{i+1}\right]\right) = \operatorname{len}\left(\left[\wp(g_r\theta_a^r) - \sum_{k=0}^{i} h_i\theta_a^i\right]\right) \overset{\text{La. 4.9}}{=} \max(0, i) = i.$$

Lemma 4.18. *Let $E = F(\theta_a)$ for $a \in R_F$ be a totally ramified C_p-extension. Define $\gamma_E := \Psi^{-1}(\wp(\theta_a^{p-1}))$.*

(a) Write $\gamma_E = \sum_{i=1}^{p-1} f_i \theta_a^i$ for $f_i \in F$. Then

$$f_i = (-1)^{i-1} \cdot \frac{1}{i} \cdot a^{p-i} + h_i, \quad \text{where } h_i \in F \text{ with } \nu_F(h_i) > \nu_F(a^{p-i}).$$

(b) We have $\operatorname{len}([\gamma_E]) = 1$ and $\varepsilon_{E/F}([\gamma_E]) = -1$. In particular, $E(\theta_{\gamma_E})/F$ is a C_{p^2}-extension.

Proof. (a) We have

$$\begin{aligned}\wp(\theta_a^{p-1}) &= (\theta_a^p)^{p-1} - \theta_a^{p-1} = (\theta_a + a)^{p-1} - \theta_a^{p-1} = -\theta_a^{p-1} + \sum_{i=0}^{p-1} \binom{p-1}{i} a^{p-1-i}\theta_a^i \\ &= \sum_{i=0}^{p-2} \binom{p-1}{i} a^{p-1-i}\theta_a^i = \sum_{i=0}^{p-2} (-1)^i a^{p-1-i}\theta_a^i. \end{aligned} \tag{4.19}$$

Thus there is a pre-image of $\wp(\theta_a^{p-1})$ under the isomorphism Ψ by Lemma 4.7. Again by Lemma 4.7

$$\gamma_E \overset{(4.11)}{=} \sum_{i=1}^{p-1} \left((-1)^{i-1} \frac{1}{i} a^{p-i}\theta_a^i + \sum_{k=i}^{p-2} (-1)^k \mu_{i,k} a^{p-(k+1)}\theta_a^i \right). \tag{4.20}$$

Using $\nu_F(a) < 0$ we get $\nu_F(a^{p-k}) > \nu_F(a^{p-i})$ for all $i < k$ which proves the description of γ_E.

(b) By the calculation in (a) we have $f_{p-1} = -a$ and thus

$$\varepsilon_{E/F}([\gamma_E]) = \lambda_{[a]}([\operatorname{Tr}_{E/F}(\gamma_E)]) \overset{(4.17)}{=} \lambda_{[a]}([-a]) = -1.$$

Note that $\gamma_E \notin \wp(E)$ as $\nu_E(\gamma_E) < 0$ and $p \nmid \nu_E(\gamma_E)$. Then Theorem 4.15 shows that $E(\theta_{\gamma_E})/F$ is indeed a C_{p^2}-extension. □

Corollary 4.19. *Let $E = F(\theta_a)$ for $a \in R_F$ and $2 \le r \le p-1$. Then $[\beta] \in J(E)$ defines a $\widetilde{H}(p,r)$-extension if and only if $[\beta] = [\alpha] + \lambda[\gamma_E]$, where $\lambda \in \mathbb{F}_p^\times$ and $[\alpha]$ defines a $H(p,r)$-extension.*

Proof. By Theorem 4.15 we have $\operatorname{len}([\beta]) = r$ and $\varepsilon_{E/F}([\beta]) = \lambda = \lambda \cdot \varepsilon_{E/F}([\gamma_E])$ for some $\lambda \in \mathbb{F}_p^\times$. Set $[\alpha] := [\beta - \lambda\gamma_E]$, then we get

$$\varepsilon_{E/F}([\beta - \lambda\gamma_E]) = \varepsilon_{E/F}([\beta]) - \lambda\varepsilon_{E/F}([\gamma_E]) = \lambda - \lambda = 0.$$

Moreover $\operatorname{len}([\alpha]) = \operatorname{len}([\beta - \lambda\gamma_E]) \overset{\text{Rem. 4.9}}{=} r$ as $\operatorname{len}([\beta]) = r \neq 1 = \operatorname{len}([\lambda\gamma_E])$. Thus $[\alpha]$ defines a $H(p,r)$-extension by Theorem 4.15. □

In the case $r = 1$ we easily get a similar result by the reasoning: $[\beta] \in J(E)$ defines a C_{p^2}-extension if and only if $[\beta] = [\alpha] + \lambda[\gamma_E]$, where $\lambda \in \mathbb{F}_p^\times$ and $[\alpha] = [0]$ or $[\alpha]$ defines a $C_p \times C_p$-extension.

The only difference is that we cannot establish equality for the length, and the length of $[\alpha]$ can be 0.

In Schultz [CMS16] we find the following nice decomposition for fields of characteristic p. We need the $n = 1$ situation.

Theorem 4.20. *Let Z/F be a C_{p^n}-extension. Then there exists $\gamma \in J(Z)$ and $\Delta \subseteq J(Z)$ such that*

$$J(Z) = \langle\gamma\rangle \oplus \bigoplus_{\alpha\in\Delta} \langle\alpha\rangle_G \qquad \text{and}$$

- $\operatorname{len}([\gamma]) = 1$, $\varepsilon_{Z/F}([\gamma]) \neq 0$,
- $\langle\alpha\rangle_G \cong \mathbb{F}_p[C_{p^n}]$ *for all* $\alpha \in \Delta$.

A proof is given in [CMS16, Prop. 6.2].

In the case $n = 1$ we can take $\gamma = \gamma_E$ with γ_E defined in Lemma 4.18.

4.2.2 Minimal Heisenberg Extensions

Corollary 4.21. *Let $a \in R_F$ so that $E = F(\theta_a)/F$ is totally ramified and let $1 \leq r \leq p$.*

(a) If $\omega_0 \in \mathbb{F}_q \setminus \wp(\mathbb{F}_q)$ then $L_r(a) := E(\theta_{\omega_0\theta_a^{r-1}})$ defines an $H_{p^2}(p, r)$-extension of degree p^2 over F containing E of minimal discriminant.

(b) The corresponding discriminants over p^2 points are $\operatorname{disc}(L_1(a)/F) = p \operatorname{disc}(E/F)$ for $r = 1$ and

$$\operatorname{disc}(L_r(a)/F) = (p + r - 1)\operatorname{disc}(E/F) - (p - 1)(r - 2) \qquad \text{for } 2 \leq r \leq p.$$

Proof. We have $\operatorname{len}\left(\left[\omega_0\theta_a^{r-1}\right]\right) = r$ by Theorem 4.16(b) thus the corresponding extension has Galois group $H(p, r)$ or $\widetilde{H}(p, r)$. If $r = p$, we have $H(p, p) = \widetilde{H}(p, p)$ and $L_r(a)$ defines a $H(p, p)$-extension. For $r < p$ we immediately get $\varepsilon_{E/F}([\omega_0\theta_a^{r-1}]) = 0$ by (4.17). Thus the corresponding extension has Galois group $H(p, r)$ by Theorem 4.15(a).

For minimality, let $\beta \in R_E$ be any element with $\nu_E(\beta) > \nu_E\left(\theta_{\omega_0\theta_a^{r-1}}\right) = (r - 1)\nu_F(a)$, then $\operatorname{len}([\beta]) \leq (r - 1)$ by Theorem 4.16(a) and thus $E(\theta_\beta)/F$ does not define a $H(p, r)$-extension. Thus no extension of E/F of smaller discriminant is an $H(p, r)$-extension which proves the minimality.

For the discriminant we consider $r = 1$ first. Then $\nu_E\left(\omega_0\theta_a^0\right) = \nu_E(\omega_0) = 0$ and

$$\operatorname{disc}(L_1(a)/F) = pda + 0 = pd_a.$$

For $r \geq 2$, the tower formula yields

$$\begin{aligned}\operatorname{disc}(L_r(a)/F) &= p\operatorname{disc}(E/F) + (p-1)\left(|\nu_E(\omega_0\theta_a^{r-1})| + 1\right)\\ &= p\operatorname{disc}(E/F) + (p-1)\left((r-1)|\nu_E(\omega_0\theta_a)| + 1\right)\\ &= p\operatorname{disc}(E/F) + (r-1)(p-1)\left(|\nu_E(\theta_a)| + 1\right) - (p-1)(r-2)\\ &= (p+(r-1))\operatorname{disc}(E/F) - (p-1)(r-2).\end{aligned}$$

□

Remark 4.22. We also have

$$\operatorname{disc}(L_r(a)/F) = (p+r-1)(p-1)|\nu_F(a)| + (p-1)(p+1) \tag{4.21}$$

since

$$\begin{aligned}\operatorname{disc}(L_r(a)/F) &= (p+r-1)\operatorname{disc}(E/F) - (p-1)(r-2)\\ &= (p+r-1)(p-1)(|\nu_F(a)|+1) - (p-1)(r-2)\\ &= (p+r-1)(p-1)|\nu_F(a)| + (p-1)(p+1).\end{aligned}$$

Lemma 4.23. *Let $a \in R_F$ with $\nu_F(a) = 0$ so that $E = F(\theta_a)/F$ is unramified and let $1 \leq r \leq p$. Then $L_r(a) := E(\theta_{t^{-1}\theta_a^{r-1}})$ defines a minimal $H(p,r)$-extension over p^2 points, with discriminant*

$$\operatorname{disc}(L_r(a)/F) = 2p(p-1).$$

Proof. The discriminant is given by the formula

$$\operatorname{disc}(L_r(a)/F) = pd_a + f_{E/F}(p-1)(|\nu_E(t^{-1}\theta_a^{r-1})|+1) = 0 + p\cdot(p-1)\cdot 2.$$

Note that $\operatorname{Gal}(L_r(a)/F) \cong H(p,r)$ by Theorem 4.16(b) as $t^{-1} \notin \wp(E)\cap F$. Moreover, it is a minimal Heisenberg extension as any extension with smaller discriminant is unramified and therefore defines an abelian extension. □

4.2.3 Minimal Twisted Heisenberg Extensions

Let $E = F(\theta_a)$ for some $a \in R_F$. Recall Lemma 4.18 and the element

$$\gamma_E = \Psi^{-1}(\wp(\theta_a^{p-1}))$$

and write $\gamma_E = \sum_{i=1}^{p-1} f_i\theta_a^i$ as its representation with respect to the power basis $1, \theta_a, \ldots, \theta_a^{p-1}$.

For $1 \leq r \leq p-1$ we can decompose

$$\gamma_E = \underbrace{\sum_{i=1}^{r-1} f_i\theta_a^i}_{:=\delta_{E,r}} + \underbrace{\sum_{i=r}^{p-1} f_i\theta_a^i}_{:=\gamma_{E,r}} = \delta_{E,r} + \gamma_{E,r}, \tag{4.22}$$

where we are mainly interested in the element $\gamma_{E,r}$.

Lemma 4.24. *Let $E = F(\theta_a)$ for some $a \in R_F$ with $G = \mathrm{Gal}(E/F)$ and $1 \le r \le p-1$.*

(a) We have $\mathrm{len}\,([\gamma_{E,r}]) = r$.

(b) The element $\gamma_{E,r}$ generates a $\widetilde{H}(p,r)$-extension, that is $\mathrm{Gal}(E(\langle[\gamma_{E,r}]\rangle_G)/F) \cong \widetilde{H}_{p^{r+1}}(p,r)$.

(c) If $\nu_F(a) < 0$ we have $\nu_E(\gamma_{E,r}) = (p(p-r)+r)\,\nu_F(a)$.

Proof. (a) For the coefficients we have

$$\nu_F(f_r) = \nu_F(a^{p-r}) \quad \text{for } 1 \le r \le p-1, \qquad \nu_E(\gamma_E) = (p^2-1)\nu_F(a). \tag{4.23}$$

If $r < p-1$ we have $p - r > 1$ and we obtain $f_{r-1} \notin \wp(E) \cap F$. Then we have

$$\mathrm{len}\,([\delta_{E,r}]) \overset{\text{Thm. } 4.16}{=} (r-1)+1 = r,$$

thus we have $\mathrm{len}\,([\gamma_{E,r}]) = r$ as well by (4.13).

(b) We have

$$-1 = \varepsilon_{E/F}([\gamma_E]) = \varepsilon_{E/F}([\delta_{E,r}]) + \varepsilon_{E/F}([\gamma_{E,r}]) = 0 + \varepsilon_{E/F}([\gamma_{E,r}]).$$

Using part (a) and Theorem 4.15, the element $\gamma_{E,r}$ defines a $\widetilde{H}(p,r)$-extension.

(c) Using Lemma 4.18 we have

$$\nu_E(\gamma_{E,r}) = \nu_E\left(\sum_{i=r}^{p-1} \frac{(-1)^{i-1}}{i} a^{p-i}\theta_a^i \; + h_i\theta_a^i\right) \quad \text{with } h_i \in F \text{ and } \nu_F(h_i) > \nu_F(a^{p-i}),$$

thus

$$\nu_E(\gamma_{E,r}) = \min\{\nu_E(a^{p-i}\theta_a^i) \;:\; r \le i \le p-1\} = \nu_E(a^{p-r}\theta_a^r) = (p(p-r)+r)\,\nu_F(a). \qquad \square$$

We will show later in Theorem 4.60 that $\gamma_{E,r}$ defines a minimal twisted Heisenberg extension. Our proof requires to know all possible discriminants for Heisenberg extensions first. We illustrate the notations and ideas with an example here.

Example 4.25. *Let us consider $p = 3$ and $F = \mathbb{F}_3((t))$. Let $E = F(\theta_a)$ for some $a \in R_F$ with $\nu_F(a) < 0$. Using our standard generator $\sigma \in \mathrm{Gal}(E/F)$ with $\sigma(\theta_a) = \theta_a + 1$ and the isomorphism $\Psi = \sigma - 1$ from Lemma 4.7 with the F-bases $\mathscr{B} = (\theta_a, \theta_a^2)$ and $\mathscr{C} = (1, \theta_a)$. We have*

$$M_{\mathscr{B},\mathscr{C}}(\Psi) = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} = \big(M_{\mathscr{B},\mathscr{C}}(\Psi)\big)^{-1} \in \mathrm{GL}_2(\mathbb{F}_3). \tag{4.24}$$

Now $\wp(\theta_a^2) = (a+\theta_a)^2 - \theta_a^2 = 2a\theta_a + a^2$ and

$$\gamma_E = \Psi^{-1}\left(\wp(\theta_a^2)\right) \overset{(4.24)}{=} 2a(\theta_a + 2\theta_a^2) + a^2\theta_a = a\theta_a^2 + (a^2 - a)\theta_a.$$

Note $\gamma_{E,1} = \gamma_E$ and $\gamma_{E,2} = a\theta_a^2$.

- *A minimal C_9-extension over E is given by $Z = E(\theta_{\gamma_E})$ with*
$$\operatorname{disc}(Z/E) = (p-1)\left(|\nu_E((a^2-a)\theta_a)|+1\right) = 2\cdot(7|\nu_F(a)|+1) = 14|\nu_F(a)|+2.$$

- *A minimal $\widetilde{H}_9\,(3,2)$-extension over E is given by $E(\theta_{\gamma_{E,2}})$.*
First of all, $\gamma_{E,2} = (a^2-a)\theta_a$ corresponds to a module of length 2, as
$$(a^2-a)\theta_a \notin \wp(E) \quad \text{and} \quad (\sigma-1)((a^2-a)\theta_a) = a^2-a \notin \wp(E).$$
Secondly, $\varepsilon_{E/F}\left([(a^2-a)\theta_a]\right) = 0$ by Remark 4.14(b), hence combining these two facts, the element $\gamma_{E,2}$ defines a $\widetilde{H}_9(3,2)$-extension by Theorem 4.15.
To show the minimality, take $\beta = f_0 + f_1\theta_a + f_2\theta_a^2 \in E$ with $f_i \in F$ such that $E(\theta_\beta)$ defines a $\widetilde{H}(p,2)$-extension. Then $\operatorname{len}([\beta]) = 2$ which implies $f_2 \in \wp(E)\cap F$. Moreover, by $\varepsilon_{E/F}([\beta]) = \lambda_{[a]}([-f_2]) \neq 0$, we get $f_2 \notin \wp(F)$. Hence $f_2 = \wp(f) \pm a$ for some $f \in F$, and thus $\nu_F(f_2) = \nu_F(\wp(f)\pm a) \leq \nu_F(a)$. Thus
$$\operatorname{disc}\left(E(\theta_\beta)/E\right) = 2\cdot(|\nu_E(\beta)|+1) \geq 2\cdot(|\nu_E(a\theta_a^2)|+1) = 2\cdot(|\nu_E(\gamma_{E,2})|+1) = \operatorname{disc}(E(\theta_{\gamma_{E,2}})/E).$$
This shows that the minimal twisted Heisenberg extension has smaller discriminant than the minimal cyclic C_{p^2}-extension, considered over p^2 points.

- *To construct the wreath product $C_3 \wr C_3$ as a Galois group, we can take the Galois closure of $E\left(\wp^{-1}\left(\theta_a^2\right)\right)$. As $\wp(\mathbb{F}_3) = 0$ and $1 \notin \wp(\mathbb{F}_3)$, we have $\operatorname{len}\left(\left[1\cdot\theta_a^2\right]\right) = 3$.*

This example works in principal analogously in the case $p > 3$ where it is just more difficult to explicitly describe the element γ_E.

4.3 Heisenberg Modules and Systems of Representatives

Our next goal is to enumerate Heisenberg $H_{p^2}(p,r)$-extensions of degree p^2 containing a fixed C_p-extension $E = F(\theta_a)$ for some $a \in R_F$. For this purpose we will construct new systems of representatives of $J(E)$. The main emphasis lies on expressing the representatives in terms of the power basis $1, \theta_a, \ldots, \theta_a^{p-1}$ rather than in terms of powers of a prime element (opposed to $R_E(\pi)$ defined in Chapter 1). This is done to easily read off properties of the Galois group from the defined extensions $E(\theta_\alpha)$ for a representative α.

We will use these systems to describe the set of all module generators for modules of length $\leq r$ with $\varepsilon_{E/F}$-value 0.

Remark 4.26. For $a \in R_F$ recall the $\mathbb{F}_p$-vector spaces $V_a = \wp(F(\theta_a)) \cap F$ and R_{V_a} we defined in Remark 1.22.
$$V_a = \wp(F) \oplus \mathbb{F}_p \cdot a.$$
Let $R_{V_a} \leq R_F$ be a suitable subspace of codimension 1 such that $R_F = R_{V_a} \oplus \mathbb{F}_p \cdot a$. Then R_{V_a} is a reduced complement of F/V_a with $R_{V_a} \subseteq R_F$.

Note that $x \in R_{V_a} \cap V_a \iff x = 0$ and $x \in R_F \cap \wp(F) \iff x = 0$.

Definition 4.27. Let $a \in R_F$ and $1 \leq r \leq p$. We define

$$M_a := \{f_0 + f_1\theta_a + \ldots + f_{p-1}\theta_a^{p-1} \ : \ f_i \in R_{V_a},\ f_{p-1} \in R_F\} \qquad \text{and}$$
$$M_{a,r} := \{f_0 + f_1\theta_a + \ldots + f_{r-1}\theta_a^{r-1} \in M_a \ : \ 0 \neq f_{r-1} \in R_{V_a}\}.$$

We give an overview on useful direct sum decompositions for a given $a \in R_F$ where some will be proven in this subsection:

$$E = \wp(E) \oplus R_E = \wp(E) \oplus M_a, \qquad \wp(E) \cap F = \wp(F) \oplus \mathbb{F}_p \cdot a =: V_a,$$
$$F = \wp(F) \oplus R_F = \wp(F) \oplus \mathbb{F}_p \cdot a \oplus R_{V_a}$$

Lemma 4.28. *Let $1 \leq r \leq p$, $E := F(\theta_a)$ and $\alpha \in M_{a,r}$. Let $L := E\left(\wp^{-1}(\langle\alpha\rangle_G)\right)$ be the extension defined by α. Then* $\mathrm{Gal}(L/F) \cong H(p,r)$.

Proof. Let $\alpha = \sum_{i=0}^{r-1} f_i\theta_a^i$ with $f_i \in R_{V_a}$ and $f_{r-1} \neq 0$. Then $\mathrm{len}([\alpha]) = r$ by Theorem 4.16(b).

If $r < p$, then $f_{p-1} = 0$ and thus $\mathrm{Tr}_{E/F}(\alpha) \overset{\text{La. } 4.4}{=} 0$. This shows $\varepsilon_{E/F}([\alpha]) = 0$ by Remark 4.14(b). Thus $\mathrm{Gal}(L/F) \cong H(p,r)$. For $p = r$ the Galois group is the wreath product $C_p \wr C_p \cong H(p,p)$. □

Remark 4.29. Define $W_a := \bigoplus_{i=1}^{p} M_{a,i}$. Then $M_a \neq W_a$, more specifically,

$$f_0 + f_1\theta_a + \ldots + f_{p-1}\theta_a^{p-1} \in M_a \setminus W_a \iff f_{p-1} \in R_F \setminus R_{V_a}. \tag{4.25}$$

Lemma 4.30. *Let $a \in R_F$, $E := F(\theta_a)$ and $W_a := \bigoplus_{i=1}^{p} M_{a,i}$.*

(a) We have $\dim_{\mathbb{F}_p}(M_a/W_a) = 1$.

(b) If $\mathrm{Gal}(E(\theta_\gamma)/F) \cong C_{p^2}$ *generates a cyclic extension for some $\gamma \in M_a$, then $\mathbb{F}_p \cdot \gamma \oplus W_a = M_a$.*

Proof. Consider the projection

$$\mathrm{pr}\colon M_a \longrightarrow F, \qquad f_0 + f_1\theta_a + \ldots + f_{p-1}\theta_a^{p-1} \longmapsto f_{p-1}. \tag{4.26}$$

Then $u \in W_a$ if and only if $\mathrm{pr}(u) \in R_{V_a}$. Consequently, there exists $v \in V$ with $\mathrm{pr}(v) \notin R_{V_a}$. Now $R_{V_a} \leq R_F$ has codimension 1, hence $\mathrm{pr}(\mathbb{F}_p \cdot v + W) = R_F$. Consequently, $\mathbb{F}_p \cdot v \oplus W_a = M_a$ and $V = \mathbb{F}_p \cdot v$ which proves (a).

Let $\gamma \in M_a$ generate a C_{p^2}-extension. Then we have

$$\mathrm{Tr}_{E/F}(\gamma) \overset{\text{La. } 4.4}{=} -\mathrm{pr}(\gamma) \notin \wp(F),$$

hence $\mathbb{F}_p \cdot \gamma \cap W_a = 0$ and $\mathbb{F}_p \cdot \gamma \oplus W_a \overset{(a)}{=} M_a$ by part (a). □

Lemma 4.31. *Let $a \in R_F$ and $E := F(\theta_a)$. Then $E = \wp(E) \oplus M_a$.*

Proof. We first analyse $\wp(E)$. For $f \in F$ and $i \in \{1, \dots, p-1\}$ we get

$$\wp(f\theta_a^i) \overset{\theta_a^p = \theta_a + a}{=} f^p(\theta_a + a)^i - f\theta_a^i = \sum_{k=0}^{i-1} \binom{i}{k} f^p a^{i-k} \theta_a^k + \wp(f)\theta_a^i, \tag{4.27}$$

where $\wp(f) = 0 \iff f \in \mathbb{F}_p$. Hence if $x_0, \dots, x_r \in F$ with $x_r \neq 0$ then

$$\wp(x_0 + \ldots + x_r\theta_a^r) \overset{(4.27)}{=} \wp(x_r)\theta_a^r + (r \cdot a x_r^p + \wp(x_{r-1}))\theta_a^{r-1} + \sum_{i=0}^{r-2} y_i\theta_a^i =: \sum_{i=0}^{r} y_i\theta_a^i,$$

where the $y_i \in F$ are defined by the last equality. We get

$$\begin{aligned} x_r \notin \mathbb{F}_p &\Longrightarrow 0 \neq \wp(x_r) =: y_r \in \wp(F) \subseteq V_a, \quad \text{or} \\ 0 \neq x_r \in \mathbb{F}_p &\Longrightarrow y_r = 0 \quad \text{and} \quad 0 \neq y_{r-1} = \underbrace{r x_r^p}_{\in \mathbb{F}_p} a + \wp(x_{r-1}) \in \wp(F) \oplus \mathbb{F}_p \cdot a = V_a. \end{aligned} \tag{4.28}$$

Conclusively, if $\alpha \in E$ and $\wp(\alpha) = \sum_{i=0}^{s} y_i\theta_a^i$ for certain $y_i \in F$ with $y_s \neq 0$ then (4.28) implies

$$\begin{cases} y_s \in \wp(F), & s = p-1 \\ y_s \in V_a, & s < p-1. \end{cases}$$

As the three systems $M_{a,r}$, R_F, and R_{V_a} are additively closed satisfying $R_{V_a} \cap V_a = 0$ and $R_F \cap \wp(F) = 0$ this immediately shows

$$\wp(E) \cap M_a = 0.$$

We are left to prove

$$x \in E \Longrightarrow \exists\, \gamma \in M_a \text{ such that } x + \wp(E) = \gamma + \wp(E).$$

For $0 < r < p-1$ let $x_r \in F$ and $x = x_r\theta_a^r$. We show that

$$\exists \gamma \in M_a, \quad y_0, \dots, y_{r-1} \in F, \ \beta \in E \quad : \quad x = \gamma + \sum_{i=0}^{r-1} y_i\theta_a^i + \wp(\beta). \tag{4.29}$$

By $V_a \oplus R_{V_a} = F$ we get

$$\forall f \in F \ \exists\, f_0 \in F, \mu \in \mathbb{F}_p \quad : \quad f - \wp(f_0) + \mu a \in V_a. \tag{4.30}$$

Thus there exist $f_0 \in F$ and $\mu \in \mathbb{F}_p$ such that

$$x_r - \wp(f_0) - \mu a \in R_{V_a}. \qquad \text{Set } f := \wp(f_0) + \mu a. \tag{4.31}$$

Then $(x_r - f)\theta_a^r \in M_a$ by definition of M_a and we get

$$\wp(f_0\theta_a^r) \overset{(4.27)}{=} \wp(f_0)\theta_a^r + \sum_{k=0}^{r-1} \binom{r}{k} f_0^p a^{r-k}\theta_a^k,$$
$$\wp(\frac{\mu}{r+1}\theta_a^{r+1}) \overset{(4.27)}{=} 0 + \mu a\theta_a^r + \sum_{k=0}^{r-1} \binom{r+1}{k} \frac{\mu}{r+1} a^{r+1-k}\theta_a^k$$

and

$$\begin{aligned} x = x_r\theta_a^r &= ((x_r - f) + f)\,\theta_a^r \\ &\overset{(4.31)}{=} (x_r - f)\theta_a^r + (\wp(f_0) + \mu a)\theta_a^r \\ &= (x_r - f)\theta_a^r + \wp(f_0\theta_a^r + \frac{\mu}{r+1}\theta_a^{r+1}) \\ &\quad + \sum_{k=0}^{r-1} \left(\binom{r}{k} f^p a^{r-k} + \binom{r+1}{k} \frac{\mu}{r+1} a^{r+1-k} \right) \theta_a^k \\ &= (x_r - f)\theta_a^r + \wp(\beta) + \sum_{i=0}^{r-1} y_i\theta_a^i, \end{aligned}$$

which proves (4.29) for $r \leq p-2$. For $r = p-1$ we can use the same proof as for $0 < r < p-1$ only with $\mu = 0$, $f = \wp(f_0) \in \wp(F)$ and $f - x_{p-1} \in R_F$.

For arbitrary $\alpha = \sum_{i=0}^{p-1} f_i\theta_a^i \in E$, $f_i \in F$, we can apply (4.29) on $f_{p-1}\theta_a^{p-1}$, then $\tilde{f}_{p-2}\theta_a^{p-2}$ etc. and lastly apply (4.30) which shows that $\alpha \equiv \gamma \mod \wp(E)$ for some $\gamma \in M_a$. □

Corollary 4.32. *Let $E = F(\theta_a)$ for $a \in R_F$ and let $\gamma_E = \Psi^{-1}(\wp(\theta_a^{p-1}))$ as in Lemma 4.18. Let $J(W_a) = \{[\beta] \;\; \beta \in W_a\}$. Then we have*

$$J(E) = \langle [\gamma_E] \rangle \oplus J(W_a).$$

Proof. The class $[\gamma_E]$ defines a C_{p^2}-extension by Lemma 4.18. Now combine Lemma 4.30 and Theorem 4.20. □

In total, we obtain a nice description of all Heisenberg extensions.

Corollary 4.33. *Let $1 \leq r \leq p-1$ and $\alpha = \sum_{i=0}^{p-1} f_i\theta_a^i \in M_a$ with $f_i \in F$. Then:*

(a) For every normal $H(p,r)$-extension L/F containing E, there is an $\alpha \in M_{a,r}$ such that

$$L = E\left(\wp^{-1}(\langle\alpha\rangle_G)\right).$$

(b) For $\alpha \in M_a$ with $\operatorname{len}([\alpha]) = r$ we have $\operatorname{Gal}\left(E\left(\wp^{-1}(\langle\alpha\rangle_G)\right)/F\right) \cong \begin{cases} \widetilde{H}(p,r), & f_{p-1} \in R_F \setminus R_{V_a}, \\ H(p,r), & f_{p-1} \in R_{V_a}. \end{cases}$

Proof. For part (a), consider $U := \wp(L)/\wp(E) \leq J(E)$. It is a cyclic $\operatorname{Gal}(E/F)$-module, i.e. $U = \langle[\beta]\rangle$ for some $\beta \in E$. By Lemma 4.31 we have $\beta = \alpha + \wp(h)$ for some $\alpha \in M_a$ and $h \in E$. By the condition $\operatorname{len}([\beta]) = r = \operatorname{len}([\alpha])$ we have $\alpha \in M_{a,r}$, so $U = \langle[\alpha]\rangle$ and $L = E(\wp^{-1}(E\left(\wp^{-1}(\langle\alpha\rangle_G)\right)))$.

For proving part (b), note that the condition $f_{p-1} \in R_F \setminus R_{V_a}$ implies

$$f_{p-1} = \mu a + \wp(b) \quad \text{for some} \quad \mu \in \mathbb{F}_p^\times,\ b \in F.$$

Thus

$$\varepsilon_{E/F}([\alpha]) = \lambda_{[a]}([-f_{p-1}]) = \lambda_{[a]}(-[\mu a + b]) = -\mu \neq 0,$$

and $E(\theta_\alpha)/F$ is a twisted Heisenberg extension by Theorem 4.16. □

4.3.1 Reduced Representative System in the Ramified Case

Let $\alpha \in E$. Recall the valuation-type function

$$\nu_{J(E)} \colon J(E) \to \mathbb{Z}, \quad \nu_{J(E)}([\alpha]) = \max_{\beta \in E} \left(\nu_E(\alpha + \wp(\beta))\right).$$

We call an element $\alpha \in E$ *reduced* if $\nu_E(\alpha) = \nu_{J(E)}([\alpha])$.

For α to be reduced it is necessary that $\nu_E(\alpha) \leq 0$ and it is sufficient that $p \nmid \nu_E(\alpha)$ if $\nu_E(\alpha) < 0$ or that $\nu_E(\alpha) = 0$ and the leading coefficient is not in $\wp(\mathbb{F}_q)$.

A reduced element $\widetilde{\alpha} \in E$ with $\alpha - \widetilde{\alpha} \in \wp(E)$ is called a *reduction* of α in E.

If E/F is totally ramified, then $\nu_E(f) = p \cdot \nu_F(f)$ for every $f \in F$ and thus, any element $f_0 \in F$ with $\nu_F(f_0) < 0$ is not reduced in E. Hence we need to find a reduction of f_0 to turn M_a into a reduced system of representatives. Note that the elements of the form $\sum_{i=1}^{r} f_i \theta_a^i$ are reduced in E.

Notation 4.34. Let $E = F(\theta_a)$ for $a \in R_F$ be a C_p-extension and $(1, \theta_a, \ldots, \theta_a^{p-1})$ be the power basis of E. For $0 \leq i \leq p-1$ we denote

$$\pi_i \colon E \longrightarrow F, \quad \sum_{k=0}^{p-1} f_k \theta_a^k \longmapsto f_i \theta_a^i$$

as the i-th projection. Obviously, π_i is F-linear.

We start with an easy observation from (4.27).

Definition 4.35. Let $E = F(\theta_a)$ for some $0 \neq a \in R_F$. Let $1 \leq r \leq i$ and $f \in F$. We define

$$\beta_{r,i}(f) := \sum_{k=r}^{i} \pi_k\left(\wp(f \cdot \theta_a^i)\right).$$

Lemma 4.36. *Let $E = F(\theta_a)$ for $0 \neq a \in R_F$, $f \in F$ and $1 \leq i \leq p-1$.*

(a) $\pi_0(\wp(f\theta_a^i)) = f^p a^i$.
In particular, we have $-f^p a^i \equiv \beta_{1,i}(f) \mod \wp(E)$.

(b) $\pi_i(\wp(f\theta_a^i)) = \wp(f)\theta_a^i$.

(c) For $1 \leq r \leq i$ *we have* $\pi_r(\wp(f\theta_a^i)) = \binom{i}{r} f^p a^{i-r}\theta_a^r$.

Proof. We have

$$\wp(f\theta_a^i) = f^p(a+\theta_a)^i - f\theta_a^i = f^p a^i + \sum_{k=1}^{i-1} \binom{i}{k} f^p a^{i-k}\theta_a^k + \wp(f)\theta_a^i. \tag{4.32}$$

This shows by definition (a), (b) and (c) except for the second choice of (a).
By re-arranging the terms, we get

$$\wp(f\theta_a^i) - f^p a^i = \sum_{k=1}^{i-1} \binom{i}{k} f^p a^{i-k}\theta_a^k + \wp(f)\theta_a^i = \beta_{1,i}(f).$$

Hence $-f^p a^i \equiv \beta_{1,i}(f) \mod \wp(E)$. □

Definition 4.37. For $a \in R_F$ and $z \in \mathbb{Z}$ we define $w_z(a) := \lfloor \frac{z|\nu_F(a)|}{p} \rfloor$ and

$$R_a^{(z)} := t^{w_z(a)} \cdot \mathbb{F}_q[t^{-1}].$$

Note that $R_a^{(z)}$ is the $\mathbb{F}_q$-vector space with basis $\big(t^i \,:\, i \leq w_z(a)\big)$. The elements $f \in R_a^{(z)}$ can be thought of as shifted polynomial expressions $f = \sum_{i \leq w_z(a)} f_i t^i$ so that every term $0 \neq f_i t^i$ satisfies

$$\nu_F(f_i t^{pi} a^z) \leq 0 \iff f_i t^i \in R_a^{(z)} \iff i \leq w_z(a). \tag{4.33}$$

The integer $w_z(a) \in \mathbb{Z}$ is maximal with the property $\nu_F(t^{p\cdot n} a^z) \leq 0$. Note that $\nu_E(t^n \theta_a^z) = \nu_F(t^{pn} a^z)$ if $\nu_F(a) < 0$.

Lemma 4.38. *Let $a \in R_F$ with $\nu_F(a) < 0$. Let $f \in F$ and $1 \leq r \leq i \leq p-1$. Then:*

(a) If $i = r$ we have $\beta_{r,r}(f) = \wp(f)\theta_a^r$ and $\nu_E(\beta_{r,r}(f)) = \nu_E(f^p\theta_a^r)$ if $\nu_F(f) < 0$.

(b) In the case $i > r$ or $\nu_F(f) \neq 0$ we have

$$\nu_E(\beta_{r,i}(f)) = \begin{cases} \nu_E(f^p a^{i-r}\theta_a^r) = p^2\nu_F(f) + (p(i-r)+r)\nu_F(a) & \nu_F(f^p a^{i-r}) \leq 0 \\ \nu_E(f\theta_a^i) = \nu_F(f^p a^i), & \nu_F(f^p a^{i-r}) > 0. \end{cases}$$

Moreover, $\nu_E(\beta_{r,i}(f)) < r\nu_F(a) \iff \nu_F(f^p a^i) < 0$.

(c) We have $\nu_E(\beta_{r,i}(f)) \leq r\nu_F(a) \iff \nu_F(f^p a^{i-r}) \leq 0 \iff \nu_F(f) \leq w_{i-r}(a)$.

Proof. Now to prove (a), if $i = r$ we simply have

$$\nu_E\left(\beta_{r,r}(f)\right) = \nu_E\left(\wp(f)\theta_a^r\right) = \nu_E\left(f^p\theta_a^r - f\theta_a^r\right)$$

and $\nu_E(f^p\theta_a^r) \not\equiv \nu_E(f\theta_a) \mod p$. Thus we get the claim in (a).
In case of (b) we have $i > r$. We first show

$$\nu_E\left(\gamma_{r,i}(\theta_a)\right) = \nu_E(a^{i-r}\theta_a^r) = (p(i-r)+r)\nu_F(a). \tag{4.34}$$

Since $\nu_E(a) = p\nu_E(\theta_a) = p\nu_F(a) < 0$ we have

$$\nu_E\left(\frac{\theta_a}{a}\right) = \nu_F(a) - p\nu_F(a) = -(p-1)\nu_F(a) > 0. \tag{4.35}$$

Thus for all $1 \leq r < k \leq i$ we get

$$\nu_E(a^{i-k}\theta_a^k) = \nu_E(a^{i-r}\theta_a^r) + (k-r)\nu_E\left(\frac{\theta_a}{a}\right) \overset{(4.35)}{>} \nu_E(a^{i-r}\theta_a^r).$$

Thus we can prove equation (4.34) using

$$\nu_E(\gamma_{i,r}(\theta_a)) = \nu_E(a^{i-r}\theta_a^r) = (p(i-r)+r)\nu_F(a).$$

Then

$$\nu_E(f^p a^{i-r}\theta_a^r) \not\equiv \nu_E(f\theta_a^i) \mod p \tag{4.36}$$

and using $\beta_{r,i}(f) = f^p\gamma i, r - f\theta_a^i$ we get

$$\nu_E(\beta_{r,i}(f)) = \nu_E\left(f^p\gamma_{r,i}(\theta_a) - f\theta_a^i\right) \underset{(4.36)}{\overset{(a)}{=}} \min\left\{\nu_E(f^p a^{i-r}\theta_a^r),\ \nu_E(f\theta_a^i)\right\}.$$

The condition for the minimum is

$$\begin{aligned}
\nu_E(\beta_{r,i}(f)) = \nu_E(f\theta_a^i) &\overset{(4.36)}{\iff} \nu_E(f\theta_a^i) < \nu_E(f^p a^{i-r}\theta_a^r) \\
&\overset{(a)}{\iff} p\nu_F(f) + i\nu_F(a) < p^2\nu_F(f) + (pi-(p-1)r)\nu_F(a) \\
&\iff 0 < (p^2-p)\nu_F(f) + (p-1)(i-r)\nu_F(a) \\
&\overset{\cdot\frac{1}{p-1}}{\iff} 0 < p\nu_F(f) + (i-r)\nu_F(a) \\
&\iff 0 < \nu_F(f^p a^{i-r}),
\end{aligned}$$

proving (b) and (c) by using $\nu_F(f^p a^{i-r}) < 0 \iff \nu_F(f) \leq w_{i-r}(a)$. □

Remark 4.39. For the only missing case $i = r$ and $\nu_F(f) = 0$ we write $f = \sum_{k=0}^{\infty} f_k t^k$ so that

$$\nu_E(\beta_{r,r}(f)) = \nu_E(\wp(f)\theta_a^r) = \begin{cases} \nu_E(\theta_a^r) = r\nu_F(a), & \wp(f_0) \neq 0 \\ \nu_E((f - f_0)\theta_a^r) = p\nu_F(f - f_0) + r\nu_F(a), & \wp(f_0) = 0. \end{cases}$$

Combining Lemma 4.38 and Proposition 4.31 we obtain a generating system for all $H(p, j)$-extensions with $j \leq r$ containing $E = F(\theta_a)$ as follows:

$$\{f_1\theta_a^1 + \ldots + f_{r-1}\theta_a^{r-1} + \beta_{\theta_a,i}(g_i) \mid f_j \in R_{V_a};\ g_i \in F \text{ for } 1 \leq i \leq p-1\}.$$

Our next task is to find a minimal generating system. We will fix one element $\omega_0 \in \mathbb{F}_q \setminus \wp(\mathbb{F}_q)$.

Lemma 4.40. *Let $a \in R_F$ with $\nu_F(a) < 0$.*

(a) For any $f \in F$ there exist a $\beta \in F$ and uniquely determined $\lambda_0 \in \mathbb{F}_p$, $g_1 \in R_a^{(1)}, \ldots, g_{p-1} \in R_a^{(p-1)}$ such that

$$f = \wp(\beta) + \lambda_0\omega_0 + \sum_{i=1}^{p-1} g_i^p a^i.$$

(b) For all $f \in R_{V_a}$ there exist $\lambda \in \mathbb{F}_p$ and $g_i \in R_a^{(i)}$ for $1 \leq i \leq p$ such that

$$f \equiv \lambda_0\omega_0 + \sum_{i=1}^{p-1} \beta_i(g_i) \mod \wp(E)$$

is a reduction of f in E, where $\beta_i(g_i)$ is defined in (4.32).

Proof. We first use induction on $|\nu_F(f)|$ for the existence part.

Let $\nu_F(f) \geq 0$ and $f = \sum_{i=0}^{\infty} f_i t^i$. Then $\nu_E(f - f_0) > 0$ and thus $f - f_0 = \wp(\tilde{\beta}) \in \wp(F)$. Moreover, we have $f_0 = h_0 + \wp(\beta_0)$ for some $h_0 \in R_F$ with h_0 a constant and $\beta_0 \in F$, thus $h_0 = \lambda_0\omega_0$ for a uniquely determined $\lambda_0 \in \mathbb{F}_p$ so that

$$f = \lambda_0\omega_0 + \wp(\beta_0 + \tilde{\beta}).$$

Now let $n = \nu_F(f) < 0$, then $f = \lambda t^n + \tilde{f}$ for uniquely determined $\lambda \in \mathbb{F}_q^\times$ and $\tilde{f} \in F$ where $\nu_F(\tilde{f}) > n$.

Assume first that $p \mid n$, that is $n = pk$ for some $k \in \mathbb{Z}$. Then there exists a unique $\mu \in \mathbb{F}_q^\times$ such that $\mu^p = \lambda$, thus

$$\wp(-\mu t^k) = -\mu t^k + \lambda t^n$$

and $\nu_F(f + \wp(-\mu t^k)) > \nu_F(f)$. Now we can apply induction to $f + \wp(-\mu t^k)$ and we are done.

Otherwise $p \nmid n$. As $p \nmid \nu_F(a)$ there exists an $1 \leq j \leq p-1$ such that

$$n \equiv j\nu_F(a) \mod p, \quad n = pk + j\nu_F(a),$$

Hence $\nu_F(\lambda t^n) = \nu_F(t^{pk}a^j)$ and there exists a uniquely determined $\mu \in \mathbb{F}_q^\times$ such that

$$\nu_F(\lambda t^n - \mu^p t^{pk} a^j) > \nu_F(\lambda t^n).$$

Thus we can use induction on $(f - (\mu t^k)^p \cdot a^j)$ and have proven the existence in (a).

The uniqueness of $g_1, \ldots, g_{p-1}$ follows by

$$g_i \in R_a^{(i)} \text{ and } g_i^p a^i \in \wp(F) \iff g_i = 0.$$

Consequently, β is unique up to $\ker(\wp) = \mathbb{F}_p$.

For (b) we combine part (a) and (4.32): By (a) there exist $\lambda_0 \in \mathbb{F}_p$ and $g_i \in R_a^{(i)}$, $\beta \in F$ such that

$$f \overset{(a)}{=} \wp(\beta) + \lambda_0\omega_0 + \sum_{i=1}^{p-1} g_i^p a^i$$

leading to

$$\begin{aligned} f &\overset{\text{Eq. (4.32)}}{=} \wp(\beta) + \lambda_0\omega_0 + \sum_{i=1}^{p-1} \big(\wp(g_i\theta_a^i) - \beta_i(g_i)\big) \\ &\overset{(-1)^p=-1}{=} \wp(\beta) + \lambda_0\omega_0 + \sum_{i=1}^{p-1} \big(\wp(g_i\theta_a^i) + \beta_i(-g_i)\big) \\ &= \wp(\beta + g_1\theta_a + \ldots + g_{p-1}\theta_a^{p-1}) + \lambda_0\omega_0 + \sum_{i=1}^{p-1} \beta_i(-g_i). \end{aligned}$$

Finally, we have $-g_i \in R_a^{(i)}$ for all $1 \leq i \leq p-1$. □

Example 4.41. *Let $F = \mathbb{F}_2((t))$ and $a := t^{-7} \in R_F$. Let $E = F(\theta_a)$.*

- *We have $w_1(a) = 3$, as we have*

  $$\nu_F(t^{2i}a) = \nu_F(t^{2i-7}) = 2i - 7 < 0 \iff i \leq 3.$$

  We then have $R_1^{(a)} = \left\{ \sum_{i=\nu}^{3} b_i t^i \mid b_i \in \mathbb{F}_2,\ \nu \leq 3 \right\}$.

- *Choosing the basis $\mathscr{B} = \left(1 \cdot t^0, t^{-2i+1}\right)_{i\in\mathbb{N}}$ we get*

  $$R_{V_a} = \left\{\lambda_0 + b_{-1}t^{-1} + b_{-3}t^{-3} + b_{-5}t^{-5} + b_{-9}t^{-9} + \ldots b_{-(2n+1)}t^{-2n-1} \mid b_i \in \mathbb{F}_2,\ 3 \neq n \in \mathbb{N}_0\right\}.$$

  We have $M_{a,1} = \{f_0 + f_1\theta_a \mid f_i \in R_{V_a}\}$.

- *Let $0 \neq \beta = f_0 + f_1\theta_a$ for $f_0, f_1 \in R_F$. Then we have*

$$\mathrm{Gal}(E(\theta_\beta)/F) \cong \begin{cases} C_2 \times C_2, & f_1 = 0 \\ C_4, & f_1 = a \\ D_4, & \text{else.} \end{cases}$$

  In the special case $p = 2$ we have $\mathbb{F}_2^\times = \{1\}$ and $\gamma_E = a\theta_a$ has a very simple shape.

- *For $b \in F$ we have $\beta_{1,1}(b) = \wp(b) \cdot \theta_a$.*

4.3.2 Enumeration of some Systems of Representatives

Now we construct a system of representatives of $J_r(E)$ in order to analyse the asymptotics of Heisenberg extensions of degree p^2. For this, we combine the system of representatives M_a with the description of $f_0 \in F$ from Lemma 4.40.

For $1 \leq r \leq j \leq p-1$ and $g_j \in F$ recall $\beta_{r,j}(g_j) := \wp(g_j)\theta_a^j + \sum_{i=r}^{j-1} g_j^p \binom{j}{i} a^{j-i}\theta_a^i$.

Let π_E be a uniformiser of E and recall

$$R_E = \{\mu_0\omega_0 + \sum_{\substack{i=\nu \\ p\nmid i}}^{-1} \lambda_i \pi_E \mid \mu_0 \in \mathbb{F}_p,\ \lambda_i \in \mathbb{F}_q,\ \nu \leq 0\}.$$

Definition 4.42. Let $a \in R_F$ with $\nu_F(a) < 0$ and $E = F(\theta_a)$.

(a) We define for $1 \leq r \leq p-1$:

$$N_r(E) := \{\alpha \in R_E \ :\ \nu_E(\alpha) > r\nu_E(\theta_a)\} = \{\alpha \in R_E \ :\ |\nu_E(\alpha)| < r|\nu_E(\theta_a)|\},$$

$$\Omega_{E,r} := \{\alpha_0 + \sum_{i=1}^{r-1} f_i\theta_a^i + \wp(f_r)\theta_a^r + \sum_{i=r+1}^{p-1} \beta_{r,i}(f_i) \ :\ \alpha_0 \in N_r(E),\ f_i \in R_a^{(i-r)}\}.$$

(b) For $r = p$ we set $\Omega_{E,p} := R_E$.
(c) For $x \in \mathbb{R}_{\geq 0}$ and $1 \leq r \leq p$ we define $\Omega_{E,r}(x) := \{\alpha \in \Omega_{E,r} \ :\ |\nu_E(\alpha)| \leq x\}$.

The purpose of $\Omega_{E,r}$ is to describe all module generators of length $\leq r$ with $\varepsilon_{E/F}(\alpha) = 0$. The key difference to the representative system M_a is that we decompose f_0 according to

$$f_0 = \lambda_0\omega_0 + \sum_{i=1}^{p-1} f_i^p a^i \equiv \lambda_0\omega_0 + \sum_{i=1}^{p-1} \beta_{1,i}(f_i) \mod \wp(E).$$

In particular, now the valuations for $f_1, \ldots, f_{r-1}$ can be divisible by p which was excluded in M_a. Moreover, $\beta_{r,j}(g_j)$ have to be considered. And finally, we use a technical distinction between terms with valuation $> r\nu_E(\theta_a)$ and with valuation $\leq r\nu_E(\theta_a)$. We use this to simplify $\nu_E(\beta_{r,i}(f_i))$, while on the other hand the elements in $N_r(E)$ are easy to count.

Example 4.43. *We continue Example 4.41 with* $F = \mathbb{F}_2((t))$ *and* $a = t^{-7}$. *Let* $E = F(\theta_a)$ *and* $r = 1$. *We choose the prime element* $\pi := t^4\theta_a$ *of* E.

- *We have* $N_1(E) = \{\alpha \in R_E \ : \ \nu_E(\alpha) > \nu_E(\theta_a) = -7\} = \{b_0 + b_{-1}\pi^{-1} + b_{-3}\pi^{-3} + b_{-5}\pi^{-5} \mid b_i \in \mathbb{F}_2\}$.
- *We have* $R_a^{(1)} = \{\sum_{i=\nu}^{3} b_i t^i \ : \ \nu \leq 3, \ b_i \in \mathbb{F}_2\}$ *and* $R_a^{(0)} = \left\{\sum_{i=\nu}^{0} b_i t^i \mid \nu \leq 0, \ b_i \in \mathbb{F}_2\right\}$.
- *We have* $\Omega_{E,1} = \left\{\alpha_0 + \wp(f_1)\theta_a \ : \ \alpha_0 \in N_1(E), \ f_1 \in R_a^{(0)}\right\}$.

Note that $\Omega_{E,1} \setminus \{0\}$ *only corresponds to* $C_2 \times C_2$*-extensions.*

Lemma 4.44. *For* $a \in R_F$ *with* $\nu_F(a) < 0$ *and* $1 \leq r \leq p-1$ *we have the direct sum decomposition*

$$\Omega_{E,r} = N_r(E) \oplus \bigoplus_{i=1}^{r-1} R_a^{(i-r)} \cdot \theta_a^i \oplus \bigoplus_{j=r}^{p-1} \beta_{r,j}(R_a^{(j-r)}). \tag{4.37}$$

More precisely, we have

(i) $\nu_E(\beta) \leq r\nu_F(a)$ *for all* $\beta \in \Omega_{E,r} \setminus N_r(E)$.

(ii) For $A := \nu_F(a)$ *we have*

$$\nu_E(f_i\theta_a^i) \equiv iA \mod p \quad \text{for all} \quad 1 \leq i \leq r-1 \text{ and } f_i \in R_a^{(i-r)}$$
$$\nu_E\left(\beta_{r,j}(f_j)\right) \equiv rA + p(j-r)A \mod p^2 \quad \text{for all} \quad r \leq j \leq p-1 \text{ and } f_j \in R_a^{(j-r)}.$$

In particular, their valuations are pairwise different or both ∞.

Proof. By assumption E/F is totally ramified and thus $\nu_E(f) = p\nu_F(f)$ for all $f \in F$. For all $f_i \in R_a^{(i-r)}$ we get

$$\nu_E(f_i\theta_a^i) = p\nu_F(f_i) + i\nu_E(\theta) = p\nu_F(f_i) + iA \equiv iA \mod p \tag{4.38}$$

and

$$\nu_E(f_i\theta_a^i) = \nu_F(f_i^p a^i) = \nu_F(f_i^p a^{i-r}) + r\nu_F(a) \overset{(4.33)}{\leq} 0 + r\nu_F(a),$$

where the final inequality is valid by the definition of $R_a^{(i-r)}$. Moreover, by Lemma 4.38(a) and (c) we have

$$\nu_E(\beta_{r,j}(f_j)) = p^2\nu_F(f_j) + (p(j-r) + r)\,\nu_F(a) \equiv p(j-r)A + rA \mod p^2 \tag{4.39}$$

and $f_j \in R_a^{(j-r)}$ implies $p\nu_F(f_j^p a^{j-r}) \leq 0$ and thus $\nu_E\left(\beta_{r,j}(f_j)\right) \leq r\nu_F(a)$. This concludes (i).

Part (ii) follows by combining (4.38) and (4.39), as the resulting valuations are pairwise incongruent modulo p^2: Note that $p(j-r)A + rA \equiv rA \mod p$, thus for all $1 \le i \le p-1$ and all $f_i \in R_a^{(j-r)}$ we have

$$\nu_E\left(\sum_{i=1}^{r-1} f_i\theta_a^i + \sum_{j=r}^{p-1} \beta_{r,j}(f_j)\right) = \min\left\{\nu_E(f_1\theta_a), \dots, \nu_E(f_{r-1}\theta_a^{r-1}), \nu_E(\beta_{r,r}(f_r)), \dots, \nu_E(\beta_{r,p-1}(g_{p-1}))\right\}.$$

Combining this with (i), the sum in (4.37) is direct. □

Lemma 4.45. *Let $a \in R_F$ with $\nu_F(a) < 0$, let π be a prime element of $E = F(\theta_a)$ and $1 \le r \le i \le p-1$.*

(a) For $r < i$ let $\rho_{i-r} \in \{-(p-1), \dots, -1, 0\}$ with $\rho_{i-r} \equiv (i-r)\nu_F(a) \mod p$. Then there exists a valuation-preserving bijection

$$\beta_{r,i}(R_a^{(i-r)}) \xrightarrow{\sim} \mathbb{F}_q[\pi^{-p^2}] \cdot \pi^{p\rho_{i-r} + r\nu_F(a)}.$$

For $r = i$ we have a valuation-preserving bijection

$$\beta_{r,r}(R_a^{(0)}) \xrightarrow{\sim} \wp(\mathbb{F}_q)\pi^{r\nu_F(a)} \oplus \bigoplus_{\substack{k < r\nu_F(a) \\ k \equiv r\nu_F(a) \mod p^2}} \mathbb{F}_q \cdot \pi^k.$$

(b) For $x \in \mathbb{R}_{\ge 0}$ set $\beta_{r,i}(R_a^{(i-r)}, x) := \#\{\alpha \in \beta_{r,i}(R_a^{(i-r)}) \ : \ |\nu_E(\alpha)| \le x\}$. Then for $r < i$ we have

$$\beta_{r,i}(R_a^{(i-r)}, x) = q^{\#\{-|x| \le k \le r\nu_F(a) \ : \ k \equiv r\nu_F(a) + p\rho_{i-r} \mod p^2\}}$$

and $r = i$ we have

$$\beta_{r,r}(R_a^{(0)}, x) = \frac{1}{p} q^{\#\{-|x| \le k \le r\nu_F(a) \ : \ k \equiv r\nu_F(a) \mod p^2\}}.$$

Proof. For $g \in R_a^{(i-r)}$ we will implicitly write

$$g = \sum_{k \le w_{i-r}(a)} g_k t^k, \quad \text{with} \quad g_k \in \mathbb{F}_q.$$

We show that we have valuation-preserving bijections

$$\begin{aligned} \beta_{r,i}(R_a^{(i-r)}) \xrightarrow{\Psi_1} \{g^p \ : \ g \in R_a^{(i-r)}\} \cdot a^{i-r}\theta_a^r \xrightarrow{\Psi_2} \mathbb{F}_q[\pi^{-p^2}] \cdot \pi^{\rho_{i-r} + r\nu_F(a)}, \\ \beta_{r,i}(g) \longmapsto g^p \cdot a^{i-r}\theta_a^r \longmapsto \sum_{k \le w_{i-r}(a)} g_k \pi^{p^2 k + p(i-r)\nu_F(a) + r\nu_F(a)}. \end{aligned}$$

We start with the injectivity of Ψ_1. For $g, h \in R_a^{(i-r)}$ we have

$$\Psi_1(\beta_{r,i}(g)) = \Psi_1(\beta_{r,i}(h)) \overset{\text{La. 4.36}}{\underset{r<i}{\Longrightarrow}} g^p a^{i-r}\theta_a^r = h^p a^{i-r}\theta_a^r \Longrightarrow g = h$$

as p-powering is injective, thus Ψ_1 is injective. Moreover,

$$\nu_E\left(\beta_{r,i}(g)\right) \overset{\text{La. 4.38}}{=} \nu_E(g^p a^{i-r}\theta_a^r) = \nu_E\left(\Psi_1(\beta_{r,i}(g))\right),$$

and similarly, Ψ_1 is surjective.

For Ψ_2 we write

$$g = \sum_{k \le w_{i-r}(a)} g_k t^{pk} = \sum_{\tilde{k} \le 0} g_{\tilde{k}+w_{i-r}(a)} t^{p\tilde{k}+pw_{i-r}(a)}. \tag{4.40}$$

Moreover

$$\nu_F(t^{pk}a^{i-r}) < 0 \iff k \le w_{i-r}(a), \qquad \nu_F(t^{pw_{i-r}(a)}a^{i-r}) = \rho_{i-r}(a), \tag{4.41}$$

where the first equivalence is true by (4.33), and $\nu_F(t^{pw_{i-r}(a)}a^{i-r})$ is the minimal integer ≤ 0 congruent to $\nu_F(a^{i-r})$ modulo p, which shows the second equation. Thus we obtain

$$\nu_E(t^{p\tilde{k}+pw_{i-r}(a)}a^{i-r}\theta_a^r) \overset{(4.41)}{=} p^2\tilde{k} + p\rho_{i-r}(a) + r\nu_F(a). \tag{4.42}$$

This shows that Ψ_2 is valuation-preserving. Finally, Ψ_2 is indeed bijective as p-powering is injective on F and it defines an isomorphism on $\mathbb{F}_q$.

For the case $i = r$ we use

$$\beta_{r,r}(g_0) = \wp(g_0)\theta_a^r \quad \text{for} \quad g_0 \in \mathbb{F}_q$$

and the results follow analogously to the proven case of $r < i$.

For part (b), we consider for $r \le i \le p-1$ the exponents

$$e_{r,i}(x) := \#\{r|\nu_F(a)| \le k \le x \ : \ k \in \mathbb{Z},\ k \equiv r\nu_F(a) + \rho_{i-r} \mod p^2\},$$

with $\rho_{r,r} := 0$. By the bijections established in (a) we have

$$\#\beta_{r,i}(R_a^{(i-r)}, x) = \begin{cases} q^{e_{r,i}(x)}, & r < i \\ \frac{1}{p}q^{e_{r,r}(x)}, & r = i. \end{cases}$$

□

Lemma 4.46. *Let $a \in R_F$ with $\nu_F(a) < 0$, let $E = F(\theta_a)$ and $1 \le r \le p$. Then we get:*

(a) $\#N_r(E) = \Gamma_q(r(p-1)|\nu_F(a)|) = pq^{\lceil \frac{r(p-1)|\nu_F(a)|}{p} \rceil}$.

(b) Let $x \in \mathbb{R}_{\ge 0}$, then

$$\#\Omega_{E,r}(x) = \begin{cases} \Gamma_q(\lfloor x \rfloor) = pq^{\lceil \frac{p-1}{p} \cdot \lfloor x \rfloor \rceil}, & x < r|\nu_F(a)| \\ q^{\frac{p-1}{p^2} r \cdot (x - r|\nu(a)|)} \cdot q^{\frac{p-1}{p} r \cdot |\nu_F(a)|} \cdot \varepsilon_r(a,x), & x \ge r|\nu_F(a)| \end{cases}$$

where $\varepsilon_r(a,x) \in [q^{-(p-1)r}, q^{(p-1)r}]$.

Proof. Recall Definition 4.42. For $x < r|\nu_F(a)|$ we have

$$\beta \in \Omega_{E,r} \setminus N_r(E) \overset{(4.37)}{\Longrightarrow} \nu_E(\beta) \leq r\nu_F(a) \Longrightarrow \beta \notin \Omega_{E,r}(x),$$

thus $\Omega_{E,r}(x) \subseteq N_r(E)$ in this case. We get

$$\begin{aligned}\Omega_{E,r}(x) &= \#\{\alpha \in \Omega_{E,r} \ : \ |\nu_E(\alpha)| \leq x < r|\nu_F(a)|\} \\ &= \#\{\alpha \in N_r(E) \ : \ |\nu_E(\alpha)| \leq x\} \\ &= \#\{\alpha \in R_E \ : \ |\nu_E(\alpha)| \leq x\} \overset{(1.5)}{=} pq^{\lceil \frac{\lfloor x \rfloor (p-1)}{p} \rceil},\end{aligned}$$

which proves the equality in the first case of (b) and proves (a) with the choice $x = r|\nu_F(a)| - 1$.

Now assume $x \geq r|\nu_F(a)|$. Write $E^{(x)} := \{\alpha \in E \ : \ |\nu_E(\alpha)| \leq x\}$. Then the decomposition (4.37) yields

$$\Omega_{E,r}(x) = |N_r(E)| \cdot \prod_{i=1}^{r-1} |R_a^{(i-r)} \cdot \theta_a^i \cap E^{(x)}| \cdot \prod_{i=r} |\beta_{r,i}\left(R_a^{(i-r)}\right) \cap E^{(x)}|. \tag{4.43}$$

We have computed $|N_r(E)|$ in (a), moreover for $1 \leq i \leq r-1$ we simply have

$$|R_a^{(i-r)} \cdot \theta_a^i \cap E^{(x)}| = q^{\#\{-x \leq pk + i\nu_F(a) \leq r\nu_F(a) \ | \ k \in \mathbb{Z}\}}, \tag{4.44}$$

and using $\beta_{r,i}\left(R_a^{(i-r)}\right) \cap E^{(x)} = \beta_{r,i}(R_a^{(i-r)}, x)$ we get

$$|\beta_{r,i}\left(R_a^{(i-r)}\right) \cap E^{(x)}| \overset{\text{La. 4.45}}{=} \begin{cases} \frac{1}{p} q^{\#\{-x \leq k \leq r\nu_F(a) \ : \ k \equiv r \cdot \nu_F(a) \mod p^2\}}, & r = i, \\ q^{\#\{-x \leq k \leq r\nu_F(a) \ : \ k \equiv (p(i-r)+r) \cdot \nu_F(a) \mod p^2\}}, & r < i. \end{cases} \tag{4.45}$$

Thus by counting

$$\begin{aligned}e_r(x) := \#\{r|\nu_F(a)| \leq n \leq x \ : \ & n \equiv \nu_F(a), \ldots, (r-1)\nu_F(a) \mod p \\ & \vee\, n \equiv r\nu_F(a), (r+p)\nu_F(a), \ldots, (r+(p-1-r)p)\nu_F(a) \mod p^2\},\end{aligned}$$

we get

$$\frac{1}{p} q^{e_r}(x) \overset{(4.44)}{\underset{(4.45)}{=}} |R_a^{(i-r)} \cdot \theta_a^i \cap E^{(x)}| \cdot \prod_{i=r} |\beta_{r,i}\left(R_a^{(i-r)}\right) \cap E^{(x)}|.$$

Note that $e_r(x)$ corresponds to $p(r-1) + (p-r) = (p-1)r$ congruence classes modulo p^2. Thus $e_r(\cdot)$ is a monotonously increasing function with

$$e_r(p^2N + r|\nu_F(a)|) = (p-1)r \cdot N \quad \text{for all} \quad N \in \mathbb{N}. \tag{4.46}$$

For all $z, Z \in \mathbb{Z}$ we get

$$\#\{Z + p^2N \leq k \leq Z + p^2N + y \ : \ k \equiv z \mod p^2\} = \#\{Z \leq k \leq Z + y \ : \ k \equiv z \mod p^2\}. \tag{4.47}$$

Thus, for $x \in \mathbb{R}_{>0}$ and $x = r|\nu_F(a)| + p^2N + y$ with $0 \leq y < p^2$ we get

$$\begin{aligned} e_r(x) &= e_r(r|\nu_F(a)| + p^2N + y) \overset{(4.47)}{=} e_r(r|\nu_F(a)| + p^2N) + e_r(r|\nu_F(a)| + y) \\ &= (p-1)rN + e_r(r|\nu_F(a)| + y) \\ &= \frac{r \cdot (p-1)}{p^2}x + \underbrace{e_r(r|\nu_F(a)| + y) - \frac{r(p-1)}{p^2} \cdot y}_{} \\ &=: \frac{r \cdot (p-1)}{p^2}x + \epsilon_r(y). \end{aligned} \tag{4.48}$$

Using (4.46), we have $0 \leq e_r(r|\nu_F(a)| + y) \overset{y<p^2}{\leq} (p-1)r$ and $-(p-1)r \leq -r\frac{p-1}{p^2}r \leq 0$, thus

$$-(p-1)r \leq \epsilon_r(y) = e_r(r|\nu_F(a)| + y) - \frac{r(p-1)}{p^2} \cdot y \leq (p-1)r. \tag{4.49}$$

Lastly, to analyse the auxiliary function ϵ_r we have

$$q^{\lceil \frac{(p-1)r|\nu_F(a)|}{p} \rceil} = q^{\frac{(p-1)r|\nu_F(a)|}{p}} \cdot \epsilon_r(a) \text{ for some } \epsilon_r(a) \in [1, q] \tag{4.50}$$

by Lemma 1.33. Setting $\epsilon_r(a, x) := \epsilon_r(a)q^{\epsilon_r(y)}$ we get

$$q^{-(p-1)r} \leq \epsilon_r(a, x) \leq q^{1+(p-1)r}.$$

Altogether we get

$$\begin{aligned} \#\Omega_{E,r}(x) &\overset{(4.43)}{=} q^{\lceil \frac{(p-1)r|\nu_F(a)|}{p} \rceil} q^{e_r(x)} \\ &\overset{(4.48)}{=} q^{\lceil \frac{(p-1)r|\nu_F(a)|}{p} \rceil} \cdot q^{\frac{(p-1)r(x-r|\nu_F(a)|)}{p^2}} q^{\epsilon_r(y)} \\ &\overset{(4.50)}{=} q^{\frac{(p-1)}{p^2} \cdot r(x-r|\nu_F(a)|)} q^{\frac{p-1}{p}r \cdot |\nu_F(a)|} \epsilon_r(a, x). \end{aligned}$$

□

Theorem 4.47. *Let E/F be a ramified C_p-extension and $1 \leq r \leq p$. Then $\Omega_{E,r}$ is a representative system of $J_r(E)$ of all classes $[\alpha] \in J(E)$ with $\operatorname{len}([\alpha]) \leq r$ and $\varepsilon_{E/F}([\alpha]) = 0$.*

Proof. For $r = p$ this is obvious by the definitions of $J_p(E) = J(E)$ and $\Omega_{E,p} = R_E$ and by Lemma 1.20(b).

Now let $1 \leq r \leq p-1$. We will show the following:

(i) $\varepsilon_{E/F}([\alpha]) = 0$ for all $\alpha \in \Omega_{E,r}$.

(ii) $\operatorname{len}([\alpha]) \leq r$ for all $\alpha \in \Omega_{E,r}$.

(iii) For all $1 \leq i \leq r$ and $\alpha \in M_{a,i}$ there exists a $\tilde{\alpha} \in \Omega_{E,r}$ such that $\alpha \equiv \tilde{\alpha} \mod \wp(E)$.

(iv) For two elements $x \neq y \in \Omega_{E,r}$ we have $x \not\equiv y \mod \wp(E)$.

For (i) write $\alpha = \alpha_0 + \sum_{i=1}^{r-1} f_i\theta_a^i + \sum_{j=r}^{p-1} \beta_{r,j}(f_j)$ with $\nu_E(\alpha_0) > r\nu_F(a)$ and $f_i \in R_a^{(i-r)}$. Then

$$\begin{aligned}\varepsilon_{E/F}([\alpha]) &= \varepsilon_{E/F}([\alpha_0]) + \varepsilon_{E/F}([\sum_{i=1}^{r-1} f_i\theta_a^i]) + \sum_{i=r}^{p-1} \varepsilon_{E/F}([\beta_{r,i}(f_i)]) \\ &\overset{\text{Rem. 4.14(b)}}{=} \varepsilon_{E/F}([\alpha_0]) + 0 + \varepsilon_{E/F}\left([\wp(f_{p-1})\theta_a^{p-1}]\right) \\ &\overset{\text{Rem. 4.14(b)}}{=} \varepsilon_{E/F}([\alpha_0]) + 0 + 0.\end{aligned}$$

Write $\alpha_0 = \sum_{i=0}^{p-1} h_i\theta_a^i \in N_r(E)$ for suitable $h_i \in F$. We have

$$|\nu_E(\alpha_0)| \overset{\text{by def.}}{\leq} (r-1)|\nu_E(\theta_a)| \leq (p-1)|\nu_E(\theta_a)| = \nu_E(\theta_a^{p-1}).$$

Thus $\nu_F(h_i) \geq 0 > \nu_F(a)$ and

$$\varepsilon_{E/F}([\alpha_0]) \overset{\text{Rem. 4.14(b)}}{=} \lambda_{[a]}([-h_{p-1}]) = 0.$$

This shows $\varepsilon_{E/F}([\alpha]) = 0$ and thus (i).

Now to prove (ii). For all $\alpha \in N_r(E)$ we have $\operatorname{len}([\alpha]) \leq r$ by Theorem 4.16. For all $f_0, \ldots, f_{r-1} \in F$ we have shown in Corollary 4.33 that

$$\operatorname{len}\left(\left[f_0 + f_1\theta_a + \ldots + f_{r-1}\theta_a^{r-1}\right]\right) \leq r. \tag{4.51}$$

Furthermore, for all $g \in F$ and $r \leq j \leq p-1$ we have

$$\beta_{r,j}(g) \overset{(4.32)}{=} \sum_{k=0}^{r-1} g^p a^{j-k} \binom{j}{k} \theta_a^k,$$

hence $\operatorname{len}([\beta_{r,j}(g)]) \leq r$ by (4.51). Thus $\operatorname{len}([x+y]) \leq \max(\operatorname{len}([x]), \operatorname{len}([y]))$ completes (ii).

For (iii) let $\alpha = f_0 + f_1\theta_a + \ldots + f_{i-1}\theta_a^{i-1} \in M_{a,i}$ for certain $f_j \in R_{V_a}$. Let $f_j = \sum_{k\in\mathbb{Z}} f_{j,k}t^k$ with $f_{j,k} \in \mathbb{F}_q$. Then we write

$$f_j := x_j + y_j \quad \text{with} \quad x_j = \sum_{k \leq w_{j-r}(a)} f_{j,k}t^k \in R_a^{(j-r)} \quad \text{and} \quad y_j := f_j - x_j.$$

By (4.51) we have $\nu_E(y_j\theta_a^j) = p\nu_F(y_j) + j\nu_F(a) \geq r\nu_F(a)$. Thus $y_i\theta_a^i \in N_r(E) \subseteq \Omega_{E,r}$ and $x_i\theta_a^i \in \Omega_{E,r}$ per definition. For the constant term we decompose

$$f_0 = \lambda_0\omega_0 + \sum_{j=1}^{p-1} g_j^p a^j \quad \text{with } g_j \in F$$

which implies by Lemma 4.40

$$f_0 \equiv \lambda_0\omega_0 + \sum_{j=1}^{p-1} \beta_{1,j}(g_j) \mod \wp(E).$$

For $j \geq r$ we write

$$\beta_{1,j}(g_j) := \underbrace{\sum_{i=1}^{r-1} h_{ji}\theta_a^i}_{:=\delta_{r,j}(g_j)} + \underbrace{\sum_{i=r}^{j} h_{ji}\theta_a^i}_{:=\beta_{r,j}(g_j)}.$$

By what we have already shown in (ii) we know there exist $\alpha_i \in \Omega_{E,r}$ such that $\delta_{r,j}(g_j) \equiv \alpha_j \mod \wp(E)$ for $r \leq j \leq p-1$ and $\beta_{1,i}(g_i) \equiv \alpha_i \mod \wp(E)$ for $1 \leq i \leq r-1$. Finally note for $\beta_{r,j}(g_j)$ that

$$\nu_E(\beta_{r,j}(g_j)) > r\nu_E(\theta_a) \iff \nu_F(g_j^p a^j) > r\nu_F(a).$$

Thus there is some $\beta_j \in \Omega_{E,r}$ such that $\beta_{r,j}(g_j) \equiv \beta_j \in \Omega_{E,r}$ we have shown (iii).

Lastly, for (iv) note that $\Omega_{E,r}$ is additively closed, thus the claim is true if $\Omega_{E,r} \cap \wp(E) = \{0\}$. This fact holds true as $\alpha \in \Omega_{E,r}$ implies either $\nu_E(\alpha) > r\nu_F(a)$ and thus $\alpha \in R_E$ by definition, or $\nu_E(\alpha) \leq r\nu_F(a)$ is non-divisible by p. This shows (iv). □

Remark 4.48. Here, we briefly consider the missing case $r = p$. Let E/F be an arbitrary C_p-extension. Then $\Omega_{E,p} = R_E$ is a representative system of $J(E)$, hence corresponds to all C_p-extensions K/E. Let $x \in \mathbb{R}_{>0}$. In Lemma 1.34 we have already computed

$$\#\Omega_{E,p}(x) = \Gamma_q(x) \overset{\text{La. } 1.34}{=} p \cdot q^{T_p(x)} = pq^{\lfloor \frac{p-1}{p}|x| \rfloor}.$$

Lemma 4.49. *Let $1 \leq r \leq p$ and $\alpha \in M_{a,r}$. Then there are precisely $p^r - p^{r-1}$ elements in $M_{a,r}$ defining the same G-module.*

Proof. Let $\alpha \in E$ such that $\langle [\alpha] \rangle_G$ is an $\mathbb{F}_p$-space of length r. Then $N_\alpha := \mathrm{Ker}(\sigma - 1)^{r-1} \cap \langle [\alpha] \rangle_G$ is a subspace of $\langle [\alpha] \rangle_G$ of codimension 1. Thus the $p^r - p^{r-1}$ elements of $\langle [\alpha] \rangle_G \setminus N_\alpha$ are precisely the G-module generators of $\langle [\alpha] \rangle_G$. Finally, every generator has precisely one representative in $M_{a,r}$. □

Example 4.50. *Let $a \in R_F$ and $E = F(\theta_a)$ be an Artin-Schreier extension.*

(a) Let $p > 2$. Then $E(\theta_{a\theta_a})/F$ is a $C_p \times C_p$-extension since $\mathrm{Tr}_{E/F}(a\theta_a) \overset{4.4}{=} 0$ and $(\sigma - 1)(a\theta_a) = a \in \wp(E)$.

(b) However, if $p = 2$ we get $(\sigma - 1)(a\theta_a) = a \in \wp(E)$ and

$$(\sigma - 1)(\theta_{\mathrm{Tr}_{E/F}(a\theta_a)}) = (\sigma - 1)(\theta_a) = 1,$$

hence $E(\theta_{a\theta_a})/F$ is a cyclic C_{p^2}-extension.

4.4 Counting Heisenberg Extensions over p^2 Points

In this section we consider $H_{p^2}(p,r) \leq S_{p^2}$ as a permutation group over p^2 points and we will count non-Galois extensions, i.e. field extensions L/F with $[L:F]=p^2$ and $\mathrm{Gal}(L/F) \cong H_{p^2}(p,r)$, and $\widetilde{H}_{p^2}(p,r) \leq S_{p^2}$ analogously. We will analyse the corresponding counting functions for $x \in \mathbb{R}_{\geq 0}$:

$$Z\left(F, H_{p^2}(p,r); x\right) := \#\left\{L/F \ : \ \mathrm{Gal}(L/F) \cong H_{p^2}(p,r), [L:F]=p^2, \mathrm{disc}(L/F) \leq x\right\},$$
$$Z\left(F, \widetilde{H}_{p^2}(p,r); x\right) := \#\left\{L/F \ : \ \mathrm{Gal}(L/F) \cong \widetilde{H}_{p^2}(p,r), [L:F]=p^2, \mathrm{disc}(L/F) \leq x\right\}.$$

We start by counting all wanted fields containing a given cyclic E/F.

Proposition 4.51. *Let $1 \leq r \leq p$. For a fixed C_p-extension E/F and $x \in \mathbb{R}_{\geq 0}$ we write*
$Z_E(r,x) := \#\{L \in Z(F, H_{p^2}(p,r); x) \mid E \leq L\}$ *and*
$\widetilde{Z}_E(r,x) := \#\{L \in Z(F, \widetilde{H}_{p^2}(p,r); x) \ : \ E \leq L\}$. *Then*

$$Z_E(r,x) \asymp \tilde{Z}_E(r,x) \asymp q^{x\frac{r}{p^2}}.$$

Proof. Firstly, let E/F be unramified. For any $\alpha = \sum_{i=0}^{p-1} f_i \theta_a^i \in E$ which is reduced and which defines a $H_{p^2}(p,r)$-extension, we have that $E(\theta_\alpha)/E$ is ramified and thus

$$\mathrm{disc}(E(\theta_\alpha)/F) = 0 + p(p-1)(|\nu_E(\alpha)|+1) = p(p-1)(\max\{|\nu_F(f_i)| \ : \ 1 \leq i \leq p-1\}+1).$$

For $1 \leq r \leq p-1$, every $H_{p^2}(p,r)$-extension L/F containing E is generated by some $\alpha \in M_{a,r}$.
In the case $r=p$, every such extension L/F is generated by some $\beta = \alpha + \lambda\gamma_E$ with $\alpha \in M_{a,p}$ and $\lambda \in \mathbb{F}_p$. Then the cyclic generator γ_E defines an unramified extension with $\nu_E(\gamma_E)=0$. Thus,

$$\nu_E(\alpha + \lambda\gamma_E) = \nu_E(\alpha) \quad \text{for all } \ \lambda \in \mathbb{F}_p \text{ and } \alpha \in M_a \setminus \{0\}.$$

For any element $\alpha = f_0 + \ldots + f_{r-1}\theta_a^{r-1} \in M_{a,r}$ we have $f_i \in R_F$ with constant coefficient $f_i(0)=0$ for all i.

Thus $\mathrm{disc}(E(\theta_\alpha)/F) \leq x \iff |\nu_F(f_i)| \leq \frac{x}{p(p-1)} - 1$ for all $0 \leq i \leq r-1$. As $\left(p^r - p^{r-1}\right)$ elements α generate the same module. We thus get for $c_p = p$ and $c_r = 1$ for $r < p$ that

$$\begin{aligned}
Z_E(r,x) &= \frac{c_r}{p^r - p^{r-1}} \#\{\alpha \in M_{a,r} \ : \ |\nu_E(\alpha)| \leq \frac{x}{p(p-1)} - 1\} \\
&= \frac{c_r}{p^r - p^{r-1}} q^{r \cdot T_p\left(\frac{x}{p(p-1)}-1\right)} \\
&\overset{\text{La. 1.33}}{=} \frac{c_r}{p^r - p^{r-1}} q^{r\left(\frac{p-1}{p}\left(\frac{x}{p(p-1)}-1\right)+\epsilon_p(x/p(p-1)-1)\right)} \\
&= c_r q^{r\frac{x}{p^2}} \cdot \frac{\epsilon_0(x)}{p^r - p^{r-1}} q^{-r\frac{p-1}{p}},
\end{aligned}$$

where

$$0 < \epsilon_0(x) = q^{-r+\epsilon_p(x/p(p-1)-1)} \overset{\text{La. } 1.33}{\leq} q^{r+\frac{p-1}{p}}$$

is a bounded error term for all $x \geq 0$. This proves $Z_E(r,x) \asymp q^{x\cdot\frac{r}{p^2}}$ when E/F is the unramified C_p-extension.

Consider now E/F to be totally ramified, that is $d_a = \operatorname{disc}(E/F) > 0$ and assume $x > (p+r)d_a$. Any $H_{p^2}(p,r)$-extension containing E is generated by some $\alpha \in \Omega_{E,r} \setminus \Omega_{E,r-1}$ and we have

$$\begin{aligned} \operatorname{disc}(E(\theta_\alpha)/F) = pd_a + (p-1)(|\nu_E(\alpha)|+1) \leq x \\ \iff |\nu_E(\alpha)| + 1 \leq \frac{x-pd_a}{p-1} \\ \iff |\nu_E(\alpha)| \leq \frac{x-pd_a}{p-1} - 1. \end{aligned} \tag{4.52}$$

For each module generator of length r there exist $p^r - p^{r-1}$ generators of the same module, and we obtain for the numbers of fields

$$Z_E(r,x) \overset{\substack{\text{Thm. } 4.47\\ (4.52)}}{=} \frac{1}{p^r - p^{r-1}} \left(\#\Omega_{E,r}\left(\frac{x-pd_a}{p-1} - 1\right) - \#\Omega_{E,r-1}\left(\frac{x-pd_a}{p-1} - 1\right)\right).$$

Writing $x_0 := \frac{x-pd_a}{p-1} - 1 - r|\nu_F(a)|$ and $\widetilde{x_0} := \frac{x-pd_a}{p-1} - 1 - (r-1)|\nu_F(a)|$ we have

$$\begin{aligned} \left(p^r - p^{r-1}\right) \#Z_E(r,x) =& \#\Omega_{E,r}(x_0 + r|\nu_F(a)|)) - \#\Omega_{E,r-1}(\widetilde{x}_0 + (r-1)|\nu_F(a)|) \\ \overset{\text{La. } 4.46}{=}& pq^{\frac{r(p-1)}{p^2}x_0} \cdot q^{r\frac{(p-1)}{p}|\nu_F(a)|} \cdot \epsilon_r(a,x) - pq^{\frac{(r-1)(p-1)\widetilde{x_0}}{p^2}} \cdot q^{(r-1)\frac{(p-1)|\nu(a)|}{p}} \cdot \epsilon_{r-1}(a,x) \\ =& pq^{\frac{r(p-1)}{p^2(p-1)}x - \frac{prd_a + r^2(p-1)|\nu_F(a)|}{p^2}} \cdot q^{r\frac{(p-1)|\nu_F(a)|}{p}} \cdot q^{-\frac{r(p-1)}{p^2}} \epsilon_r(a,x) \\ & - pq^{\frac{(r-1)(p-1)x}{p^2(p-1)} - \frac{p(r-1)d_a + (r-1)^2(p-1)^2|\nu_F(a)|}{p^2(p-1)}} \cdot q^{(r-1)\frac{(p-1)|\nu_F(a)|}{p}} \cdot \epsilon_{r-1}(a,x) \\ \overset{d_a=(p-1)(|\nu_F(a)|+1)}{=}& q^{\frac{r}{p^2}x} q^{-\frac{r^2(p-1)|\nu_F(a)|}{p^2}} \cdot pq^{-\frac{r(p-1)}{p^2}} \epsilon_r(a,x) \\ & - q^{\frac{r-1}{p^2}x} q^{-\frac{(r-1)^2(p-1)|\nu_F(a)|}{p^2}} \cdot pq^{-\frac{(r-1)(p-1)}{p^2}} \epsilon_{r-1}(a,x) \\ =& q^{\frac{r\cdot x}{p^2}} \cdot c_1(a,x) - q^{\frac{(r-1)x}{p^2}} \cdot c_2(a,x) \asymp q^{\frac{r}{p^2}x}, \end{aligned}$$

where $c_1(a,x), c_2(a,x) > 0$ are constants depending only on r, $\nu_F(a)$, $\{x\}$ and the residues of $\lfloor x \rfloor$ and $\nu_F(a)$ modulo p. Clearly, $c_1(a,x) > 0$ and $c_2(a,x) > 0$ are bounded in x for fixed r, p and a. This shows $Z_E(r,x) \asymp q^{r\frac{x}{p^2}}$.

Finally, we have $\tilde{Z}_E(r,x) = (p-1)Z_E(r,x)$ for $x \gg 0$ as we will show in Theorem 4.60(c). This then shows

$$\widetilde{Z}_E(r,x) = (p-1)Z_E(r,x) \asymp q^{x\cdot\frac{r}{p^2}}. \qquad \square$$

Definition 4.52. For $1 \leq r \leq p$ we define

$$a_p\left(H_{p^2}(p,r)\right) := \max\left(\frac{r+1}{p(p+r)}, \frac{r}{p^2}\right).$$

It is easy to check

$$a_p\left(H_{p^2}(p,r)\right) = \begin{cases} \frac{r+1}{p(p+r)}, & r^2 < p, \\ \frac{r}{p^2}, & r^2 > p. \end{cases}$$

Remark 4.53. By elementary calculations we get

$$a_p(H_{p^2}(p,r)) = \frac{r}{p^2} \iff r^2 > p, \tag{4.53}$$

$$\text{as indeed} \quad \frac{r}{p^2} \geq \frac{r+1}{p(p+r)} \iff r(p^2+pr) \geq (r+1)p^2 \iff pr^2 \geq p^2 \iff r^2 \geq p.$$

Here, $\frac{r}{p^2}$ is the exponent attained in Proposition 4.51 by fixing one C_p-extension E/F. In the following we will show that $a_p(H_{p^2}(p,r))$ is the local asymptotic exponent.

We start with a lemma and use the notations

$$\nu_F(R_F) := \{\nu(f) \ : \ f \in R_F\} \quad \text{and} \quad |\nu_F(R_F)| := \{|\nu_F(f)| \ : \ f \in R_F\}.$$

Lemma 4.54. *Let $q > 1$, $p \in \mathbb{P}$ and $c \in \mathbb{R}$. Then we have*

$$\sum_{\substack{n \in |\nu_F(R_F)| \\ 0<n\leq X}} q^{c\cdot n} = \sum_{\substack{0<n\leq X \\ n \nmid p}} q^{c\cdot n} \asymp \begin{cases} 1, & c < 0 \\ q^{cX}, & c > 0 \\ X, & c = 0. \end{cases}$$

Proof. The first equality is clear by the definition of R_F.
For $c = 0$, write $X = pN + r + \epsilon \in \mathbb{R}_{>0}$ with $N \in \mathbb{N}$, $0 \leq r \leq p-1$ and $\varepsilon \in [0,1)$. Then we just have

$$\sum_{\substack{0<n\leq X \\ p \nmid n}} 1 = (p-1)N + r \asymp X.$$

For $c < 0$, the geometric series is a converging majorant.

For $c > 0$, we set $\delta\colon \mathbb{N}_0 \to \mathbb{C}, \delta(x) := \begin{cases} 0, & x \in p \cdot \mathbb{N}_0 \\ 1, & \text{else.} \end{cases}$
Then δ is periodic with period p. We can apply Lemma 1.41 with $D := p$ and $\alpha(z) := -c$. Note that $\Delta(\delta, \alpha, s) = \sum_{j=0}^{p-1} \delta(j) q^{cj} = \sum_{j=1}^{p-1} q^{cj} = \frac{q^{cp}-q^c}{q-1}$. Then

$$\sum_{\substack{0 \le n \le x \\ p \nmid n}} q^{cn} = \sum_{0 \le n \le \lfloor x \rfloor} \delta(n) q^{cn} = \frac{1 - q^{-\alpha(s)p\lfloor \frac{x}{p} \rfloor}}{1 - q^{-\alpha(s)p}} \Delta(\delta, \alpha, s) \asymp q^{-\alpha(s)p\frac{x}{p}} = q^{-(-c)x} = q^{cx}. \qquad \square$$

For technical purposes, we introduce the constant

$$\Lambda_r(a) := (p+r)d_a - (r-1)(p-1) = (p-1)(p+r)|\nu_F(a)| + (p+1)(p-1), \tag{4.54}$$

which arises as the maximal discriminant exponent for fields generated by $N_r(F(\theta_a))$. We will use this to handle the different cases arising out of Lemma 4.46.

Recall $J_r(E)$ and $J_r(E, x)$ as defined in Definition 4.12.

Theorem 4.55. *Let $1 \le r \le p$. Then we have*

$$Z(F, H_{p^2}(p,r); x) \asymp x^{a_p(H_{p^2}(p,r))}, \quad \text{where} \quad a_p\left(H_{p^2}(p,r)\right) = \begin{cases} \frac{r+1}{p(p+r)}, & r^2 < p, \\ \frac{r}{p^2}, & r^2 > p. \end{cases}$$

I.e. there exist constants $C_1, C_2 > 0$ such that for all $x \ge 0$ holds

$$C_1 x^{a_p(H_{p^2}(p,r))} \le Z(F, H_{p^2}(p,r); x) \le C_2 x^{a_p(H_{p^2}(p,r))}.$$

Proof. Throughout this proof we will write $T_p(x) := \lfloor x \rfloor - \lfloor \frac{x}{p} \rfloor$.

Let $E_a := F(\theta_a)$ for $0 \ne a \in R_F$. Let

$$d_a := \operatorname{disc}(E_a/F) \quad \text{and} \quad x_a := \max\left(\frac{x - pd_a}{p-1} - 1, 0\right). \tag{4.55}$$

As in (4.52) we obtain by the tower-discriminant formula

$$\begin{aligned} Z(F, H_{p^2}(p,r); x) &= \sum_{a \in R_F} \frac{1}{p^r - p^{r-1}} \left(J_r\left(F(\theta_a), x_a\right) - J_{r-1}\left(F(\theta_a), x_a\right)\right) \\ &\overset{\text{Thm. 4.47}}{=} \sum_{a \in R_F} \frac{1}{p^r - p^{r-1}} \left(\#\Omega_{F(\theta_a),r}(x_a) - \#\Omega_{F(\theta_a),r-1}\left(x_a\right)\right). \end{aligned}$$

We approach by finite induction on r to prove

$$\sum_{E/F} J_r(E, x_a) \asymp q^{a_p(H_{p^2}(p,r)) \cdot x} \quad \text{and} \quad J_{r-1}(E, x_a) = o(J_r(E, x_a)).$$

Case $r = 1$: Then we have $H_{p^2}(p,1) \cong C_p \times C_p$ and

$$a_p(C_p \times C_p) = \frac{2}{p(p+1)} = \frac{r+1}{p(p+r)}$$

by results of Lagemann, see Example 2.20 and Theorem 2.19.

Case $2 \leq r \leq p$: Recall x_a from (4.55). Using $\Lambda_r(a) = (p+r)d_a - (r-1)(p-1)$ as defined in (4.54) we have

$$U_r(x) := \sum_{\substack{a \in R_F \\ \Lambda_r(a) > x}} \#\Omega_{E_a,r}(x_a), \qquad W_r(x) = \sum_{\substack{a \in R_F \\ \Lambda_r(a) \leq x}} \#\Omega_{E_a,r}(x_a)\,. \tag{4.56}$$

With these notations, we get the decomposition

$$\sum_{a \in R_F} J_r(E_a, x_a) = \sum_{a \in R_F} \#\Omega_{E_a,r}(x_a) =: U_r(x) + W_r(x). \tag{4.57}$$

The sum $U_r(x)$ counts all fields E_a/F with large discriminant such that $\Omega_{E_a,r}(x) \subseteq N_r(E_a)$, i.e. we only consider small module generators. This gives an easier counting formula.

Whereas $W_r(x)$ corresponds to fields E_a/F with small discriminant such that

$$\Omega_{E_a,r}(x) \not\subseteq N_r(E_a).$$

We treat the two cases separately.

Concerning the bound for $U_r(x)$ we have $\#\Omega_{E_a,r}(x) = 0 \iff pd_a > x$ and thus require

$$\begin{aligned} pd_a \leq x < \Lambda_r(a) &\iff p(p-1)(|\nu_F(a)|+1) \leq x < (p-1)(p+r)|\nu_F(a)| + (p-1)(r-1) \\ &\iff \frac{x}{(p-1)p} - 1 \ \geq |\nu_F(a)| > \frac{x-(p-1)(r-1)}{(p-1)(p+r)}. \end{aligned} \tag{4.58}$$

By $\Omega_{E_a,r}(x_a) = R_E(x_a)$ we have the simple formula

$$\#\Omega_{E_a,r}(x_a) \overset{\text{La. } 4.46}{=} \Gamma_q(x_a) = pq^{T_p(x_a)} \overset{\text{La. } 1.33}{=} pq^{\frac{p-1}{p}x_a}\epsilon(x, \nu_F(a)), \tag{4.59}$$

where $\epsilon(x, \nu_F(a)) := \epsilon_p(x_a) \in [1, q]$ only depends on x and $|\nu_F(a)|$. We will also write $\epsilon(x, |\nu_F(a)|) :=$

$\epsilon(x, \nu_F(a))$. Thus we have

$$\begin{aligned}
U_r(x) &= \sum_{\substack{a\in R_F\\ pd_a\le x<\Lambda_r(a)}} \#\Omega_{E_a,r}(x_a) \overset{\substack{(4.59)\\(4.54)}}{=} \sum_{\substack{a\in R_F\\ pd_a<x\le(p+r)d_a-(r-1)(p-1)}} pq^{T_p(x_a)}\\
&\overset{(4.58)}{=} \sum_{\substack{a\in R_F\\ \frac{x-(p-1)(r-1)}{(p-1)(p+r)}\le|\nu_F(a)|\le\frac{x}{(p-1)p}-1}} pq^{T_p(x_a)}\\
&= \sum_{\substack{a\in R_F\\ \frac{x-(p-1)(r-1)}{(p-1)(p+r)}\le|\nu_F(a)|\le\frac{x}{(p-1)p}-1}} pq^{T_p(\frac{x-(p-1)p(|\nu_F(a)|+1)}{p-1})}\\
&\overset{\text{La. 1.33}}{=} \sum_{\substack{A\in\nu_F(R_F)\\ \frac{x-(p-1)(r-1)}{(p-1)(p+r)}\le|A|\le\frac{x}{(p-1)p}-1}} \gamma_q(|A|)\cdot pq^{\frac{1}{p}(x-(p-1)p(|A|+1)))}\epsilon(x,A)\\
&\overset{\text{La. 1.33}}{=} \sum_{\substack{A\in\nu_F(R_F)\\ \frac{x}{(p-1)(p+r)}\le|A|\le\frac{x}{(p-1)p}}} p(q-1)q^{\frac{p-1}{p}|A|}pq^{\frac{x}{p}-(p-1)|A|}q^{\epsilon_p(|A|)}\epsilon(x,A)q^{-1}\\
&= \sum_{\substack{A\in\nu_F(R_F)\\ \frac{x}{(p-1)(p+r)}\le|A|\le\frac{x}{(p-1)p}}} q^{\frac{x}{p}-1}q^{-\frac{(p-1)^2}{p}|A|}q^{\epsilon_p(|A|)}\epsilon(x,A)q^{-1}\\
&= q^{\frac{x}{p}}q^{-\frac{(p-1)^2}{p}\frac{x}{(p-1)(p+r)}}\sum_{\substack{A=0\\ p\nmid A}}^{\frac{r\cdot x}{(p-1)p(p+r)}-1} q^{-\frac{(p-1)^2}{p}A}q^{\epsilon_p(A)}\epsilon(x,A)q^{-1}\cdot q^{\left\{\frac{x}{(p-1)(p+r)}\right\}}\\
&\asymp q^{x\frac{r+1}{p(p+r)}}, \qquad (4.60)
\end{aligned}$$

as indeed for the exponent

$$\frac{x}{p}-\frac{(p-1)^2x}{p(p-1)(p+r)}=\frac{x(p+r-(p-1))}{p(p+r)}=\frac{x(r+1)}{p(p+r)},$$

and the finite sum running over A is bounded by a constant via

$$q^{-1}\le\sum_{\substack{A=0\\ p\nmid A}}^{\frac{r\cdot x}{(p-1)p(p+r)}-1} q^{-\frac{(p-1)^2}{p}A}q^{\epsilon_p(A)}\epsilon(x,A)q^{-1}q^{\left\{\frac{x}{(p-1)(p+r)}\right\}}\le\sum_{A=0}^{\infty}q^{-\frac{(p-1)^2}{p}A}q^3=\frac{q^3}{1-q^{-\frac{(p-1)^2}{p}}}<\infty.$$

Secondly, we have

$$\begin{aligned}
W_r(x) &= \sum_{\substack{a\in R_F\\ \Lambda_r(a)\le x}} \#\Omega_{E_a,r}\left(x_a\right) = \sum_{\substack{a\in R_F\\ \Lambda_r(a)\le x}} \#\Omega_{E_a,r}\left(\frac{x-p(p-1)(|\nu_F(a)|+1)}{p-1}\right)\\
&\overset{(4.58)}{=} \sum_{\substack{A\in\nu_F(R_F)\\ |A|\le\frac{x-(r-1)(p-1)}{(p-1)(p+r)}}} \gamma_q(|A|)\#\Omega_{E_a,r}\left(\frac{x-p(p-1)(|A|+1)}{p-1}\right)\\
&\overset{\substack{\text{La. 4.46}\\ \text{La. 1.33}}}{=} \sum_{\substack{A\in\nu_F(R_F)\\ |A|\le\frac{x}{(p-1)(p+r)}}} p(q-1)q^{\frac{p-1}{p}(|A|-1)}q^{r\cdot\frac{p-1}{p}|A|}q^{\left(\frac{x-p(p-1)(|A|+1)}{p-1}-r\cdot|A|\right)\frac{r(p-1)}{p^2}}\epsilon_p(A)\epsilon_r(A,x_A)\\
&\asymp \sum_{\substack{A\in\nu_F(R_F)\\ |A|\le\frac{x}{(p-1)(p+r)}}} q^{\frac{r}{p^2}x}q^{(r+1)\frac{p-1}{p}|A|}q^{-\frac{r(p+r)(p-1)}{p^2}|A|}\\
&= \sum_{\substack{A\in\nu_F(R_F)\\ |A|\le\frac{x}{(p-1)(p+r)}}} q^{\frac{r}{p^2}x}q^{\frac{|A|(p-1)}{p^2}\left((r+1)p-pr-r^2\right)}\\
&= q^{\frac{r}{p^2}x}\sum_{\substack{A\in\nu_F(R_F)\\ |A|\le\frac{x}{(p-1)(p+r)}}} q^{|A|\frac{(p-1)}{p^2}(p-r^2)}.
\end{aligned}\tag{4.61}$$

With the values

$$X=\lambda(x):=\frac{x}{(p-1)(p+r)}\quad\text{and}\quad c:=\frac{(p-1)(p-r^2)}{p^2}$$

we can apply Lemma 4.54 and obtain

$$q^{\frac{r}{p^2}x}\sum_{\substack{A\in\nu_F(R_F)\\ |A|\le\frac{x}{(p-1)(p+r)}}} q^{|A|\frac{(p-1)}{p^2}(p-r^2)} = q^{\frac{r}{p^2}x}\sum_{\substack{A\in\nu_F(R_F)\\ |A|\le\lambda(x)}} q^{|A|\cdot c}\asymp\begin{cases} q^{\frac{r}{p^2}x}, & c<0\\ q^{\frac{r}{p^2}x}\cdot q^{c\cdot\lambda(x)}, & c\ge 0.\end{cases}\tag{4.62}$$

We have $c\ge 0 \iff (p-r^2)\ge 0$. In this case we get

$$q^{\frac{r}{p^2}x}\cdot q^{c\cdot\lambda(x)} = q^{\frac{r}{p^2}x}\cdot q^{\frac{(p-1)(p-r^2)}{p^2(p+r)(p-1)}x} = q^{\frac{pr+p}{p^2(p+r)}x} = q^{\frac{r+1}{p(p+r)}x}.$$

If $p-r^2<0$ then

$$\sum_{\substack{A\in\nu_F(R_F)\\ |A|\le\frac{x}{(p-1)(p+r)}}} q^{|A|\frac{(p-1)}{p^2}(p-r^2)} = \mathcal{O}(1)\quad\text{and}\quad W_r(x)\asymp q^{\frac{r}{p^2}x}.$$

Note that $p-r^2<0$ if and only if $\frac{r}{p^2}\ge\frac{r+1}{p(p+r)}$. Hence we have

$$W_r(x)\asymp q^{a_p\left(H_{p^2}(p,r)\right)}.$$

Together with (4.60) in (4.57) we obtain

$$\sum_{i=1}^{r} Z(F, H_{p^2}(p,i); x) \asymp q^{a_p\left(H_{p^2}(p,r)\right)}.$$

Having completed the induction, we see that

$$\sum_{i=1}^{r-1} Z(F, H_{p^2}(p,i); x) \asymp q^{a_p\left(H_{p^2}(p,r-1)\right)}$$

is of strictly smaller order as

$$\frac{r+1}{p(p+r)} > \frac{r}{p(p+r-1)} \iff (r+1)(p+r-1) > r(p+r) \iff p-1>0$$

and $\frac{r}{p^2} > \frac{r-1}{p^2}$ and $\frac{r}{p^2} > \frac{r}{p(p+r-1)}$. This finally proves that $Z(F, H_{p^2}(p,r); x) \asymp q^{a_p\left(H_{p^2}(p,r)\right)}$. □

Remark 4.56. The proof gives some more insights and an interpretation of the constants.

(i) The sum $W_r(x)$ counting the fields E/F with small enough discriminant is always in the main term of the asymptotics.

(ii) If $r^2 > p$ then the $H_{p^2}(p,r)$-asymptotics over F is dominated by the asymptotical growth of the $H_{p^2}(p,r)$-extensions over one fixed C_p-extension, see Proposition 4.51.

The same statement holds true in the case of the twisted Heisenberg groups $\tilde{H}_{p^2}(p,r)$ which will be addressed in the next subsection.

(iii) Counting only the minimal Heisenberg extensions over each field E, we obtain the asymptotical growth $x^{\frac{r}{p(p+r-1)}}$ which is in the error term of the respective counting function.

(iv) The exponent $\frac{r+1}{p(p+r)}$ arises by counting the $H_{p^2}(p,r)$-extensions over all C_p-extensions E/F satisfying $\operatorname{disc}(K/F) \leq (p+r)\operatorname{disc}(E/F)$. This has asymptotical growth $x^{\frac{r+1}{p(p+r)}}$.

In the case of $r^2 < p$ this is dominant for the asymptotics, otherwise this subfamily is in the error term of the asymptotics.

Example 4.57. *(a) For $r=1$ we get $H(p,1) \cong C_p \times C_p$ and*

$$a_p(H_{p^2}(p,1)) = \frac{r+1}{p(p+r)} = \frac{2}{p(p+1)},$$

which coincides with the asymptotic exponent found in Lagemann [Lag10].

(b) For $r=p$ we get the wreath product. Here we have the exponent

$$a_p(H_{p^2}(p,p)) = \frac{r}{p^2} = \frac{1}{p} = a_p(C_p).$$

Furthermore, for E/F a fixed C_p-extension, it is obvious that $J_p(E)$ corresponds to all C_p-extensions over E and hence, $a_p\left(H_{p^2}(p,p)\right)$ corresponds to the asymptotics exponent of the C_p-extensions over E. Thus $a_p(C_p) = a_p\left(H_{p^2}(p,p)\right) = \frac{1}{p}$.

4.5 Counting Twisted Heisenberg Extensions over p^2 Points

Recall the definition of the finite p-group $\widetilde{H}(p,r)$ in Definiton 4.1 for $1 \leq r < p$. We exclude the case $r = p$ here as $H(p,p) \cong \widetilde{H}(p,p)$.

In the following, we count all twisted Heisenberg group extensions $\widetilde{H}_{p^2}(p,r) \leq S_{p^2}$ over p^2 points with respect to the discriminant. More precisely, for a given discriminant bound $X \geq 0$ we consider the set

$$\left\{ L/F \ : \ [L:F] = p^2, \ \mathrm{Gal}(L/F) \cong \widetilde{H}(p,r), \ \ \mathrm{D}(L/F) \leq X \right\}.$$

We can approach analogously as for $H_{p^2}(p,r)$.

Fix $a \in R_F$ and $E = F(\theta_a)$ as well as $1 \leq r \leq p-1$. We recall

$$\gamma_E := \Psi^{-1}(\wp(\theta_a^{p-1})) = \sum_{i=1}^{p-1} f_i \theta_a^i \in \mathrm{Span}_F(\theta_a, \ldots, \theta_a^{p-1})$$

as defined in Lemma 4.18 and (4.20).

Definition 4.58. Let $1 \leq r \leq p-1$. Let $E = F(\theta_a)$ for $a \in R_F$. We set

$$\widetilde{\Omega}_{E,r} := \{\alpha + \lambda \cdot \gamma_E \ : \ \alpha \in \Omega_{E,r}, \ \lambda \in \mathbb{F}_p^\times\}$$
$$\text{and } \widetilde{\Omega}_{E,r}(x) := \{\beta \in \widetilde{\Omega}_{E,r} \ : \ |\nu_E(\beta)| \leq x\} \text{ for } x \in \mathbb{R}_{\geq 0}.$$

Using (4.22) and translation by $\delta_{E,r} \in \Omega_{E,r}$ we also get

$$\widetilde{\Omega}_{E,r} = \{\alpha + \lambda \cdot \gamma_{E,r} \ : \ \alpha \in \Omega_{E,r}, \ \lambda \in \mathbb{F}_p^\times\}. \tag{4.63}$$

Remark 4.59. Let $E = F(\theta_a)$ for some $a \in R_F$ and $1 \leq r \leq p-1$.

(a) Let $\beta \in \widetilde{\Omega}_{E,r}$ with $\mathrm{len}([\beta]) = s \leq r$, then $E(\theta_\beta)$ defines a $\widetilde{H}(p,s)$-extension. [1]

(b) If $E(\theta_\beta)$ for $\beta \in E$ defines a $\widetilde{H}(p,r)$-extension, then there exists $\tilde{\beta} \in \widetilde{\Omega}_{E,r}$ such that $\tilde{\beta} \equiv \beta \mod \wp(E)$.

Proof.

(a) Let $\alpha \in \Omega_{E,r}$ and $\lambda \in \mathbb{F}_p^\times$ such that $\beta = \alpha + \lambda\gamma_E$. We have $\mathrm{len}([\gamma_E]) = 1$ and $\mathrm{len}([\alpha]) \leq r$ by Theorem 4.47 for all $\alpha \in \Omega_{E,r}$ which shows the inequality $\mathrm{len}([\beta]) \leq r$ by Remark 4.9. Moreover,

$$\varepsilon_{E/F}([\beta]) = \varepsilon_{E/F}([\alpha + \lambda\gamma_E]) = \varepsilon_{E/F}([\alpha]) + \lambda\varepsilon_{E/F}([\gamma_E]) = 0 - \lambda \neq 0,$$

hence $E(\theta_\beta)$ defines a twisted Heisenberg extension. Then $\mathrm{len}([\beta]) = s \leq r$ and $\varepsilon_{E/F}(\beta) \neq 0$, i.e. $E(\theta_\beta)$ defines a $\widetilde{H}(p,s)$-extension by Theorem 4.15.

[1] Analogously to $\Omega_{E,r}$ corresponding to generators of $H(p,i)$-extensions with $i \leq r$.

(b) We have $J(E) = \langle [\gamma_E] \rangle \oplus J(W_a)$ by Corollary 4.32 and $\varepsilon_{E/F}([\beta]) \neq 0$. As $J(W_a) \leq \mathrm{Ker}(\varepsilon_{E/F})$ we have $[\beta] = \lambda[\gamma_E] + [w]$ for some $w \in W_a$ and $0 \neq \lambda \in \mathbb{F}_p^\times$. The assumption on the Galois group implies $\mathrm{len}([\beta]) = r$, thus $\mathrm{len}([w]) \leq r$ which shows $w \in M_{a,r}$ and $\beta = \lambda\gamma_E + w + \wp(x)$ for some $x \in E$ which proves (b). □

Theorem 4.60. *Let $E = F(\theta_a)$ for $a \in R_F$ and $1 \leq r \leq p-1$.*

(a) For all $\alpha \in \Omega_{E,r}$ and $\lambda \in \mathbb{F}_p^\times$ we have

$$\nu_E(\alpha + \lambda\gamma_{E,r}) = \min\{\nu_E(\alpha), \nu_E(\gamma_{E,r})\} \quad \text{and} \quad \nu_E(\alpha) \neq \nu_E(\gamma_{E,r}).$$

(b) $E(\theta_{\gamma_{E,r}})$ is a minimal $\widetilde{H}_{p^2}(p,r)$-extension containing E with discriminant

$$\begin{aligned} \widetilde{\Lambda}_r(a) &:= \mathrm{disc}(E(\theta_{\gamma_{E,r}})/F) \\ &= (p-1)\,(p(p-r+1)+r) \cdot |\nu_F(a)| + (p-1)(p+1). \end{aligned} \tag{4.64}$$

(c) For $x \in \mathbb{R}_{\geq 0}$ and $\widetilde{\Lambda}_r(a)$ as defined in (b), we have

$$\#\widetilde{\Omega}_{E,r}(x) = \begin{cases} 0, & x < \widetilde{\Lambda}_r(a), \\ (p-1) \cdot \#\Omega_{E,r}(x), & \text{else.} \end{cases}$$

Proof. (a) We have $\nu_E(\gamma_{E,r}) = (p(p-r)+r)\,\nu_F(a)$ by Lemma 4.24 and we get

$$\nu_{J(E)}([\gamma_{E,r}]) = \nu_E(\gamma_{E,r}) = \nu_E(a^{p-r}\theta_a^r) = (p^2 - pr + r)\nu_F(a) \equiv (-pr+r)\nu_F(a) \mod p^2. \tag{4.65}$$

We have to show for (a) that the value $\nu_E(\gamma_{E,r})$ is not equal to $\nu_E(\alpha)$ for all $\alpha \in \Omega_{E,r}$. Consider any $\alpha \in \Omega_{E,r}$. Then there are $x \in R_F$ with $|\nu_F(x)| > r|\nu_F(a)|$ and $g_i \in R_a^{(i)}$ so that

$$\alpha \overset{\text{Def. } 4.42}{=} x + \sum_{i=1}^{r-1} g_i\theta_a^i + \sum_{i=r}^{p-1} \beta_{r,i}(g_i), \quad |\nu_E(x)| \leq r|\nu_F(a)| \quad \text{and} \quad g_i \in R_a^{(i)}.$$

Firstly, $\nu_E(x) \geq r\nu_F(a) > (pr-r)\nu_F(a)$, thus $\nu_E(x) \neq \nu_E(\gamma_{E,r})$. Moreover, $\nu_E(\gamma_{E,r})$ is incongruent to $\nu_E\left(\sum_{i=1}^{r-1} g_i\theta_a^i + \sum_{i=r}^{p-1} \beta_{r,i}(g_i)\right)$ modulo p^2, since

$$\nu_E(g_i\theta_a^i) \overset{\nu_F(a)\neq 0}{\equiv} i\nu_F(a) \not\equiv r\nu_F(a) \mod p \quad \text{for all} \quad 1 \leq i \leq r-1$$

and $g \in R_a^{(i-r)}$ implies

$$\nu_E(\beta_{r,i}(g)) \overset{4.38}{\underset{4.39}{\equiv}} \begin{cases} (p(i-r)+r)\,\nu_F(a) \mod p^2, & r < i, \\ r\nu_F(a) \mod p^2, & r = i \end{cases} \quad \text{for all} \quad r \leq i \leq p-1.$$

Thus $\nu_E(\gamma_{E,r}) \neq \nu_E(\beta_{r,i}(g_i))$ as $r \geq 1$ and $\nu_E(\gamma_{E,r}) \neq \nu_E(g_i\theta_a^i)$ for $1 \leq i \leq r-1$ which concludes $\nu_E(\gamma_{E,r}) \neq \nu_E(\alpha)$.

(b) In Subsection 4.2.3 we have already shown that $E(\theta_{\gamma_{E,r}})$ defines a $\widetilde{H}_{p^2}(p,r)$-extension.

It is a minimal extension by (a) and the fact that every $\widetilde{H}(p,r)$-extension is given by $\beta = \alpha + \lambda \cdot \gamma_{E,r}$ for some $\alpha \in \Omega_{E,r}$ and $\lambda \in \mathbb{F}_p^\times$. For its discriminant we have by the tower formula

$$\begin{aligned}\operatorname{disc}(E(\theta_{\gamma_{E,r}})/F) &= p\operatorname{disc}(E/F) + f_{E/F}\operatorname{disc}(E(\theta_{\gamma_{E,r}})/E)\\ &= p\operatorname{disc}(E/F) + (p-1)\left(|\nu_E(\gamma_{E,r})|+1\right)\\ &\overset{(4.65)}{=} (p-1)p(|\nu_F(a)|+1) + (p-1)(p(p-r)+r)|\nu_F(a)| + (p-1)\\ &= |\nu_F(a)|(p-1)(p(p-r+1)+r) + (p-1)(p+1).\end{aligned}$$

(c) This follows by (b) and $|\mathbb{F}_p^\times| = p-1$. □

Theorem 4.61. *For $1 \le r \le p-1$ we have*

$$Z(F, \widetilde{H}_{p^2}(p,r); x) \asymp x^{a_p(\widetilde{H}_{p^2}(p,r))},$$

where $a_p(\widetilde{H}_{p^2}(p,r)) = \begin{cases} \frac{pr-r^2+r+1}{p(p^2-pr+p+r)}, & r^2 < p \\ \frac{r}{p^2}, & r^2 > p. \end{cases}$

Proof. We follow the proof of Theorem 4.55. Let $\widetilde{\Lambda}_r(a)$ as defined in (4.64). This formula directly implies $\widetilde{\Lambda}_{r-1}(a) \ge \widetilde{\Lambda}_r(a)$ for all $1 \le r \le p-1$. Thus we obtain

$$\#\widetilde{\Omega}_{E_a,r}(x) = 0 \Longrightarrow \#\widetilde{\Omega}_{E_a,i}(x) = 0 \ \forall\ i \le r \quad \text{for all } \ x < \widetilde{\Lambda}_r(a),$$

so that we only need to consider the sum of type $W_r(x)$ as seen in (4.56). For $\beta \in \widetilde{\Omega}_{E,r}$ we have

$$\operatorname{disc}(E(\theta_\beta)/F) \le x \iff |\nu_E(\beta)| \le \frac{x - pd_a}{p-1} - 1 \tag{4.66}$$

as in (4.58). We therefore obtain the expression

$$\begin{aligned}\widetilde{W}_r(x) &:= \sum_{\substack{a\in R_F\\ \widetilde{\Lambda}_r(a)\le x}} \#\widetilde{\Omega}_{E,r}\left(\frac{x-pd_a}{(p-1)} - 1\right) \overset{(4.66)}{=} \sum_{\substack{a\in R_F\\ |\nu_F(a)|\le \frac{x-(p-1)(p+1)}{p(p-r+1)+r}-1}} \#\widetilde{\Omega}_{E,r}\left(\frac{x-pd_a}{(p-1)} - 1\right)\\ &\overset{\text{Thm. 4.60(c)}}{=} (p-1) \sum_{\substack{a\in R_F\\ |\nu_F(a)|\le \frac{x-(p-1)(p+1)}{p(p-r+1)+r}-1}} \#\Omega_{E,r}\left(\frac{x-pd_a}{(p-1)} - 1\right).\end{aligned}$$

We set $\lambda(x) := \frac{x}{(p-1)(p(p-r+1)+r)} - 1$ and $c := \frac{(p-1)(p-r^2)}{p^2}$. Then analogously to (4.61) and (4.62) the above sum $\widetilde{W}_r(x)$ can be estimated via

$$\widetilde{W}_r(x) \asymp q^{\frac{r}{p^2}x} \sum_{\substack{A\in\nu_F(R_F)\\ |A|\le\lambda(x)}} q^{\frac{(p-r^2)(p-1)}{p^2}|A|} \asymp \begin{cases} q^{\frac{r}{p^2}x}, & r^2 \ge p, \\ q^{\frac{r}{p^2}x} q^{\frac{(p-r^2)(p-1)}{p^2}\lambda(x)}, & p < r^2. \end{cases}$$

We lastly calculate the exponent in the case $p < r^2$:

$$\begin{aligned}
&\frac{r}{p^2}x + \frac{(p-1)(p-r^2)}{p^2}\lambda(x)\\
=&\frac{r}{p^2}x + \frac{(p-1)(p-r^2)}{p^2}\frac{x}{(p-1)(p(p-r+1)+r)} - \frac{(p-1)(p-r^2)}{p^2(p-1)(p(p-r+1)+r)}\\
=&\frac{r(p^2-pr+p+r)+(p-r^2)}{p^2(p^2-pr+p+r)}\cdot x + O(1)\\
=&\frac{p^2r-pr^2+pr+p}{p^2(p^2-pr+p+r)}\cdot x + O(1)\\
=&\frac{pr-r^2+r+1}{p(p^2-pr+p+r)}\cdot x + O(1),
\end{aligned}$$

which shows $\widetilde{W_r}(x) \asymp x^{a_p(\widetilde{H}_{p^2}(p,r))}$. By elementary calculations it can be shown that $a_p(\widetilde{H}_{p^2}(p,r))$ is strictly monotonously increasing. Thus we can conclude analogously to the Heisenberg group case that

$$\widetilde{W_r}(x) \asymp x^{a_p(\widetilde{H}_{p^2}(p,r))} \asymp Z(F, \widetilde{H}_{p^2}(p,r); x). \qquad \square$$

Example 4.62. *For $r = 1$ we have $\widetilde{H}_{p^2}(p,1) = C_{p^2}$. Then clearly $p > r^2 = 1$ and indeed we have*

$$a_p\left(\widetilde{H}_{p^2}(p,1)\right) = \frac{p+1}{p(p^2+1)}.$$

This coincides with Lagemann's constant $a_p(C_{p^2})$ from Example 2.20(b).

4.6 Lower Bound on the Asymptotics of Galois Twisted Heisenberg Groups

Let E/F be a C_p-extension and $G := \mathrm{Gal}(E/F)$. We have seen in Section 4.1 that every $\widetilde{H}(p,r)$-extension containing E can be generated by some module element $[\beta] \in J(E)$ with $\mathrm{len}([\beta]) = r$ and $\varepsilon_{E/F}([\beta]) \neq 0$. Due to Remark 4.59, the element $[\beta]$ is given by some

$$\beta = \alpha + \lambda\gamma_{E,r} \qquad \text{for some} \qquad \lambda \in \mathbb{F}_p^\times,\ \alpha \in \Omega_{E,r}.$$

Since $\varepsilon_{E/F}([\alpha]) = 0$, we always have $\varepsilon_{E/F}([\alpha + \lambda\gamma_{E,r}]) \neq 0$, while its length might be less than r.

Next we consider the discriminant of such an extension over p^{r+1} points and consider the minimal $\widetilde{H}_{p^{r+1}}(p,r)$-extensions containing E.

Lemma 4.63. *Let $1 \leq r \leq p-1$. Let $E = F(\theta_a)$ for $a \in R_F$ be ramified with Galois group $G = \mathrm{Gal}(E/F)$ and let*

$$\widetilde{\mathrm{disc}}_r(E) := \min\{\mathrm{disc}(E\left(\wp^{-1}(\langle\omega_0\theta_a^{r-1} + \gamma_{E,i}\rangle_G\right)/F) \ :\ i = 1,\dots,r\}. \tag{4.67}$$

Then $\widetilde{\mathrm{disc}}_r(E)$ is the minimal discriminant for a twisted Heisenberg $\widetilde{H}_{p^{r+1}}(p,r)$-extension containing E.

Proof. By (4.63) and Theorem 4.60, it is clear that $E\left(\wp^{-1}(\langle\omega_0\theta_a^{r-1}+\gamma_{E,i}\rangle_G)\right)$ defines a $\widetilde{H}_{p^{r+1}}(p,r)$-extension for all $1\le i\le r$.

Recall the definition for $\gamma_E=\sum_{i=1}^{p-1} f_i\theta_a^i$ and the equality $\nu_F(f_i)=\nu_F(a^{p-i})$ from Lemma 4.18. Let M/F be any $\widetilde{H}_{p^{r+1}}(p,r)$-extension containing E. Then $M=E\left(\wp^{-1}(\langle\beta\rangle_G)\right)$ for some $\beta\in E$. For the discriminant we have

$$\operatorname{disc}(E\left(\wp^{-1}(\langle\beta\rangle_G)\right)/E)\overset{\text{La. 4.10(d)}}{=}\sum_{i=0}^{r-1}p^{r-1-i}(p-1)\left(|\nu_{J(E)}\left(\left[(\sigma-1)^i(\beta)\right]\right)|+1\right). \tag{4.68}$$

Considering the relative discriminant exponent over E and using Theorem 4.60(b), we get

$$(p-1)\left(|\nu_{J(E)}\left([\beta]\right)|+1\right)=\operatorname{disc}(E(\theta_\beta)/E)\ge\operatorname{disc}(E(\theta_{\gamma_{E,r}})/E)=(p-1)\left(|\nu_E(\gamma_{E,r})|+1\right),$$

hence $\nu_{J(E)}\left([\beta]\right)\le\nu_E(\gamma_{E,r})=\nu_E(f_r\theta_a^r)$ and consequently, there exists a minimal $1\le i\le r$ such that $\nu_{J(E)}\left([\beta]\right)\le\nu_E(f_i\theta_a^i)$.

With this choice of i, we get

$$\nu_{J(E)}\left([\beta]\right)\le\nu_E(f_i\theta_a^i)=\nu_{J(E)}\left(\left[\gamma_{E,i}+\omega_0\theta_a^{r-1}\right]\right)$$

and

$$\nu_{J(E)}\left(\left[(\sigma-1)^k(\beta)\right]\right)\le\nu_E(f_i\theta_a^{i-k})\text{ for }1\le k\le i-1.$$

Furthermore, we have $\nu_{J(E)}\left(\left[(\sigma-1)^k(\beta)\right]\right)\le\nu_E(\theta_a^{r-1-k})$ due to Lemma 4.16(b) and the fact that $\operatorname{len}\left([\beta]\right)=r$. Since $\nu_E(\theta_a^{r-1-k})=\nu_{J(E)}\left(\left[(\sigma-1)^k\left(\gamma_{E,i}+\omega_0\theta_a^{r-1}\right)\right]\right)$ for $i\le k\le r-1$ we get for $0\le k\le r-1$

$$\nu_{J(E)}\left(\left[(\sigma-1)^k\beta\right]\right)\le\nu_{J(E)}\left(\left[(\sigma-1)^k(\gamma_{E,i}+\omega_0\theta_a^{r-1})\right]\right),$$

thus equation (4.68) guarantees $\operatorname{disc}(E\left(\wp^{-1}(\langle\beta\rangle_G)\right)/E)\ge\operatorname{disc}(E\left(\wp^{-1}(\langle\gamma_{E,i}+\omega_0\theta_a^{r-1}\rangle_G)\right)/E)$. □

Conclusively, in comparing the finitely many discriminants of these explicit fields, we can compute the minimal discriminant of the embedding problem

$$1\longrightarrow(C_p)^r\xrightarrow{\iota}\widetilde{H}_{p^{r+1}}(p,r)\xrightarrow{\varphi}C_p\longrightarrow 1$$

as defined in (4.1). We give those fields a name first. We define

$$L_{i,r}(a):=E\left(\wp^{-1}(\langle\omega_0\theta_a^{r-1}+\gamma_{E,i}\rangle_G)\right)\quad\text{for}\quad 1\le i\le r$$

and we show that the minimal value is attained when $i=r$ and compute the discriminant exponents over E and F.

Definition 4.64. For $1\le i\le r\le p-1$ and $j\in\mathbb{Z}$ we define

(i) $\eta_p(j):=\sum_{k=1}^{j}kp^k$ for $j\in\mathbb{Z}$,

(ii) $\widetilde{d}_{i,r} := (p-1)\left(\eta_p(r-i-1) + p^{r-i+1}\frac{(p-i)(p^i-1)}{p-1} + p^{r-i-1}\eta_p(i)\right)$ and $d_{i,r} := \widetilde{d}_{i,r} + (p-1)p^r$,

(iii) the discriminant exponents $\widetilde{D}_{i,r}(a) := \operatorname{disc}(L_{i,r}(a)/E)$ and $D_{i,r}(a) := \operatorname{disc}(L_{i,r}(a)/F)$.

With these notations at hand we can show that the discriminant exponent is basically $d_{i,r} \cdot |\nu_F(a)|$ and that the minimal discriminant is attained by $D_{r,r}(a)$.

Theorem 4.65. *Let $E = F(\theta_a)$ for $a \in R_F$ with $\nu_F(a) < 0$, i.e. E/F is totally ramified, and $1 \le i \le r \le p-1$. Let $G := \operatorname{Gal}(E/F)$.*

(a) We have $\widetilde{D}_{i,r}(a) = \widetilde{d}_{i,r} \cdot |\nu_F(a)| + (p^r - p)$ and $D_{i,r}(a) = (p^r + \widetilde{d}_{i,r}) \cdot |\nu_F(a)| + (p^{r+1} - p)$.

(b) For all $2 \le i \le r$ we have $\widetilde{D}_{i,r}(a) \le \widetilde{D}_{i-1,r}(a)$.

In particular, $\widetilde{\operatorname{disc}}_r(E) = D_{r,r}(a) = \operatorname{disc}(E\left(\wp^{-1}(\langle\gamma_{E,r}\rangle_G)\right)/F)$ is the minimal twisted Heisenberg discriminant for the embedding problem (4.1).

Proof. (a) With $\widetilde{D}_{i,r}(a) = \operatorname{disc}(L_{i,r}(a)/E)$ and

$$\begin{aligned} L_{i,r}(a) &= E\left(\wp^{-1}(\langle\omega_0\theta_a^{r-1} + \gamma_{E,i}\rangle_G)\right) \\ &= E(\wp^{-1}\left(\omega_0\theta_a^{r-1} + \gamma_{E,i}\right), \dots, \wp^{-1}\left((\sigma-1)^{r-1}(\omega_0\theta_a^{r-1} + \gamma_{E,i})\right)) \\ &\overset{\operatorname{len}([\gamma_{E,i}])=i}{=} E\Big(\wp^{-1}\left(\omega_0\theta_a^{r-1} + \gamma_{E,i}\right), \dots, \wp^{-1}\left((\sigma-1)^{i-1}(\omega_0\theta_a^{r-1} + \gamma_{E,i})\right), \\ &\qquad \wp^{-1}\left((\sigma-1)^{i}(\omega_0\theta_a^{r-1})\right), \dots, \wp^{-1}\left((\sigma-1)^{r-1}(\omega_0\theta_a^{r-1})\right)\Big) \end{aligned}$$

we have

$$\widetilde{D}_{i,r}(a) \overset{\text{La. 4.10(d)}}{=} \sum_{k=0}^{r-1} p^{r-1-k}(p-1)\left(|\nu_{J(E)}\left(\left[(\sigma-1)^k(\omega_0\theta_a^{r-1} + \gamma_{E,i})\right]\right)| + 1\right).$$

Note that $\omega_0 \in R_E$ is reduced and $\nu_E\left((\sigma-1)(f\theta_a^j)\right) = \nu_E(f\theta_a^{j-1})$ is reduced for all $f \in F$ with $\nu_F(f) \le 0$ and $2 \le j \le p-1$, hence we get

$$\begin{aligned} \nu_{J(E)}\left(\left[(\sigma-1)^j(\omega_0\theta_a^{r-1} + \gamma_{E,i})\right]\right) &= \nu_E\left((\sigma-1)^j(\gamma_{E,i})\right) \\ &= \nu_E\left(a^{p-i}\theta_a^{i-j}\right) \text{ for all } 0 \le j \le i-1 \end{aligned} \tag{4.69}$$

and

$$\begin{aligned} \nu_{J(E)}\left(\left[(\sigma-1)^j(\omega_0\theta_a^{r-1} + \gamma_{E,i})\right]\right) &= \nu_E\left((\sigma-1)^j(\omega_0\theta_a^{r-1})\right) \\ &= \nu_E(\omega_0\theta_a^{r-1-j}) \text{ for all } i \le j \le r-1. \end{aligned} \tag{4.70}$$

Conclusively, we get

$$\begin{aligned}
\widetilde{D}_{i,r}(a) &= p^0 \operatorname{disc}([\omega_0]) + p \operatorname{disc}([\omega_0\theta_a]) + \ldots + p^{r-i-1} \operatorname{disc}([\omega_0\theta_a^{r-i-1}]) \\
&\quad + p^{r-i} \operatorname{disc}([a^{p-i}\theta_a]) + \ldots + p^{r-1} \operatorname{disc}([a^{p-i}\theta_a^i]) \\
&\overset{(4.69)}{\underset{(4.70)}{=}} \sum_{k=1}^{r-i-1} p^k(p-1)\left(|\nu_E(\theta_a^k)|+1\right) \\
&\quad + \sum_{k=1}^{i} p^{r-i+k-1}(p-1)\left(|\nu_E(a^{p-i}\theta_a^k)|+1\right) \\
&= \sum_{k=1}^{r-i-1} p^k(p-1)\left(k|\nu_F(a)|+1\right) \\
&\quad + p^{r-i-1}\sum_{k=1}^{i} p^k(p-1)\left(1+(p(p-i)+k)\,|\nu_F(a)|\right) \\
&= (p-1)|\nu_F(a)|\left(\sum_{k=1}^{r-i-1} p^k k + p^{r-i-1}\sum_{k=1}^{i} p^k\left(p(p-i)+k\right)\right) + \underbrace{(p-1)\sum_{j=1}^{r-1} p^j}_{\widetilde{c}_r} \qquad (4.71) \\
&\overset{\text{Def. i(i)}}{=} (p-1)\left(\eta_p(r-i-1) + p^{r-i-1}p(p-i)\sum_{k=1}^{i} p^k + p^{r-i-1}\eta_p(i)\right)|\nu_F(a)| + \widetilde{c}_r \\
&= (p-1)\left(\eta_p(r-i-1) + p^{r-i+1}(p-i)\sum_{k=0}^{i-1} p^k + p^{r-i-1}\eta_p(i)\right)|\nu_F(a)| + \widetilde{c}_r \\
&= (p-1)\left(\eta_p(r-i-1) + p^{r-i+1}\frac{(p-i)(p^i-1)}{p-1} + p^{r-i-1}\eta_p(i)\right)|\nu_F(a)| + \widetilde{c}_r.
\end{aligned}$$

Finally, $\widetilde{c}_r = (p-1)\sum\limits_{j=1}^{r-1} p^j = p^r - p$ concludes the formula for $\widetilde{D}_{i,r}(a)$ in (a). The assertion on $D_{i,r}(a)$ is now clear from the discriminant tower formula.

(b) Next we need to compare the values of $\widetilde{D}_{i,r}(a)$ and $\widetilde{D}_{i-1,r}(a)$. Using the formulas in (a), we get

$$\begin{aligned}
&\frac{\widetilde{D}_{i,r}(a) - \widetilde{D}_{i-1,r}(a)}{(p-1)|\nu_F(a)|} \\
&\overset{(4.71)}{=} \sum_{k=1}^{r-i-1} p^k k - \sum_{k=1}^{r-i} p^k k + \sum_{k=1}^{i} p^{r-i+k-1}(p(p-i)+k) - \sum_{k=1}^{i-1} p^{r-i+k}(p(p-i+1)+k) \\
&= -p^{r-i}(r-i) + p^{r-i}(p^2 - pi + 1) + \sum_{k=2}^{i} p^{r-i+k-1}(p(p-i)+k) \\
&\qquad - \sum_{k=1}^{i-1} p^{r-i+k}(p(p-i+1)+k) \\
&= -p^{r-i}(r-i) + p^{r-i}(p^2 - pi + 1) + \sum_{k=1}^{i-1} p^{r-i+k}(p(p-i)+k+1) \\
&\qquad - \sum_{k=1}^{i-1} p^{r-i+k}(p(p-i+1)+k) \\
&= p^{r-i}\left(p^2 - pi + 1 - (r-i)\right) + p^{r-i}\sum_{k=1}^{i-1} p^k \left(p(p-i) - p(p-i+1) + k + 1 - k\right) \\
&= p^{r-i}\left(p^2 - pi + 1 - (r-i)\right) + p^{r-i}\sum_{k=1}^{i-1} p^k \left(-p+1\right) \\
&= p^{r-i}\left(p^2 - (p-1)i - r + 1\right) - (p-1)p^{r-i+1}\frac{p^{i-1}-1}{p-1} \\
&= p^{r-i}\left(p^2 - ip + i - r + 1 - p^i + p\right)
\end{aligned}$$

For $i \geq 2$ and using $i \leq r$ we have

$$p^2 - ip + \underbrace{i - r}_{\leq 0} + 1 - p^i + p \leq -p^i + p^2 - ip + p + 1 \leq -p^i + p^2 - (p-1) < -p^2 + p^2 = 0.$$

This shows $\widetilde{D}_{r,i}(a) - \widetilde{D}_{r-i-1}(a) < 0$ and concludes the proof for all $i \geq 2$. □

Example 4.66. *Let $1 \leq r \leq p-1$. Then we have*

$$\widetilde{d}_{r,r} = (p-1)\left(p \cdot \frac{(p-r)(p^r-1)}{p-1} + p^{-1}\eta_p(r)\right), \tag{4.72}$$

and

$$d_{r,r} = (p-1)\left(p^r + p \cdot \frac{(p-r)(p^r-1)}{p-1} + p^{-1}\eta_p(r)\right). \tag{4.73}$$

For the minimal discriminant we thus have $D_{r,r}(a) = d_{r,r} \cdot |\nu_F(a)| + (p^{r+1} - p)$.

For $r = 1$, *we simply have* $\eta_p(1) = p$ *and* $d_{1,1} = (p-1)\,(p + p(p-1) + 1) = (p-1)(p^2+1)$.

For $r = 2$, *we get*

$$\begin{aligned} d_{2,2} &= (p-1)\left(p^2 + p\frac{(p-2)(p^2-1)}{p-1} + p^{-1}(p+2p^2)\right) = (p-1)\left(p^2 + p(p-2)(p+1) + 1 + 2p\right) \\ &= (p-1)(p^3+1) = p^4 - p^3 + p - 1. \end{aligned}$$

We can use the minimal discriminants to effectively obtain a lower bound on the asymptotics exponent. For this purpose, we define for every C_p-extension E/F the set of minimal $\widetilde{H}_{p^{r+1}}(p,r)$-extensions given by

$$\widetilde{\mathcal{F}}_r(E) := \{E\left(\wp^{-1}\left(\langle\gamma_{E,r} + \beta\rangle_{\mathrm{Gal}(E/F)}\right)\right) \;:\; \beta \in \Omega_{E,r},\ |\nu_E(\beta)| < |\nu_E(\gamma_{E,r})|\},$$

and consider

$$\widetilde{\mathcal{F}}_r := \bigcup_{\substack{E/F \\ \mathrm{Gal}(E/F)\cong C_p}} \widetilde{\mathcal{F}}_r(E).$$

Consider the corresponding counting function

$$Z_{\min}(F, r; X) := \#\{L \in \widetilde{\mathcal{F}}_r \;:\; \mathrm{D}(L/F) \le X\}.$$

Note that this is obviously a lower bound for the discriminant counting function $Z(F, \widetilde{H}_{p^{r+1}}(p,r), X)$.

Theorem 4.67. *Let* $1 \le r \le p-1$ *and let* $\widetilde{\Phi}_r(s) := \sum_{L \in \widetilde{\mathcal{F}}_r} q^{-\operatorname{disc}(L/F)s}$. *Then* $\widetilde{\Phi}_r(s)$ *has a pole at* $s = \frac{(p-1)(1+r(p-r+1))}{p \cdot d_{r,r}}$ *and is convergent for* $\mathrm{Re}(s) > \frac{(p-1)(1+r(p-r+1))}{p \cdot d_{r,r}}$, *where* $d_{r,r}$ *is as in* (4.73). *In particular, we get for the asymptotics exponent*

$$a_p(\widetilde{H}_{p^{r+1}}(p,r)) \ge \frac{(p-1)\,(1 + r(p-r+1))}{p \cdot d_{r,r}}.$$

Proof. For the generating series of the minimal $\widetilde{H}_{p^{r+1}}(p,r)$-extensions, we obtain

$$\begin{aligned} \widetilde{\Phi}_r(s) &= \sum_{L \in \widetilde{\mathcal{F}}_r} q^{-\operatorname{disc}(L/F)s} = \frac{1}{p-1} \sum_{\substack{a \in R_F \\ L \in \widetilde{\mathcal{F}}_r(F(\theta_a))}} q^{-\operatorname{disc}(L/F)s} \\ &= \frac{1}{p-1} \sum_{\nu_F(a) \in \nu_F(R_F)} \gamma_q(|\nu_F(a)|) \cdot \#\widetilde{\Omega}_{F(\theta_a),r}\left(|\nu_E(\gamma_{E,r})|\right) \cdot q^{-d_{r,r}(a)\cdot s}. \end{aligned}$$

Let $a \in R_F$ with $\nu_F(a) < 0$ and $E_a := E(\theta_a)$. Using Theorem 4.65 the extension

$$L_{r,r}(a) = E_a\left(\wp^{-1}(\langle\gamma_{E_a,r}\rangle_{\mathrm{Gal}(E_a/F)})\right)$$

is a minimal $\widetilde{H}_{p^{r+1}}(p,r)$-extension containing E_a. Moreover, for every reduced element $\beta \in E_a$ with $\mathrm{len}([\beta]) \leq r$ and $|\nu_E(\beta)| < |\nu_{E_a}(\gamma_{E_a,r})|$ we obtain a $\widetilde{H}_{p^{r+1}}(p,r)$-extension

$$L_\beta := E_a\left(\wp^{-1}\left(\langle \gamma_{E,r} + \beta\rangle_{\mathrm{Gal}(E_a/F)}\right)\right).$$

Using $\nu_E\left((\sigma-1)^j(\beta)\right) \geq \nu_E(\beta) - j\nu_E(\theta_a)$ by Lemma 4.6 and (4.69), we easily get

$$|\nu_E\left((\sigma-1)^j(\gamma_{E,r}+\beta)\right)| = |\nu_E\left((\sigma-1)^j(\gamma_{E,r})\right)| \text{ for all } \ 0 \leq j \leq r-1,$$

thus $\mathrm{disc}(L_\beta/E) = \mathrm{disc}(L_{r,r}(a)/E)$. We have

$$\lambda_r := |\nu_E(\gamma_{E_a,r})| = (p(p-r)+r)|\nu_F(a)| \geq r|\nu_F(a)|,$$

hence

$$\begin{aligned}
\#\Omega_{E_a,r}(\lambda_r) &\overset{\text{La. 4.46}}{=} q^{\frac{p-1}{p}r|\nu_F(a)|} q^{\frac{p-1}{p^2}r(\lambda_r - r|\nu_F(a)|)} \varepsilon_{a,r}(\lambda_r) \\
&= q^{\frac{p-1}{p}r|\nu_F(a)|} q^{\frac{p-1}{p^2}r(p(p-r)|\nu_F(a)|)} \varepsilon_{a,r}(\lambda_r) \\
&= q^{\frac{(p-1)r(p-r+1)}{p}|\nu_F(a)|} \varepsilon_{a,r}(\lambda_r). \qquad (4.74)
\end{aligned}$$

Thus for the generating series counting the minimal $\widetilde{H}_{p^{r+1}}(p,r)$-extensions for each C_p-extension E_a/F, we obtain

$$\begin{aligned}
\widetilde{\Phi}_r(s) &= \frac{1}{p-1} \sum_{\nu_F(a)\in\nu_F(R_F)} \gamma_q(|\nu_F(a)|) \cdot \#\widetilde{\Omega}_{F(\theta_a),r}\left(|\nu_E(\gamma_{E,r})|\right) \cdot q^{-(d_{r,r}|\nu_F(a)|+\widetilde{c}_r)\cdot s} \\
&\overset{(4.74)}{=} \frac{1}{p-1} \sum_{\nu_F(a)\in\nu_F(R_F)} pq^{\frac{p-1}{p}|\nu_F(a)|} \cdot q^{\frac{(p-1)r(p-r+1)}{p}|\nu_F(a)|} \cdot q^{-d_{r,r}|\nu_F(a)|s} \cdot q^{-\widetilde{c}_r s} \varepsilon_{a,r}(\lambda_r) \\
&= \frac{1}{p-1} \sum_{A\in\nu_F(R_F)} q^{|\nu_F(a)|\left(\frac{(p-1)(1+r(p-r+1))}{p}|\nu_F(a)| - d_{r,r}\cdot s\right)} \cdot p\varepsilon_{a,r}(\lambda_r) q^{-\widetilde{c}_r s} \\
&:= \frac{1}{p-1} \sum_{A\in\nu_F(R_F)} q^{|\nu_F(a)|\left(\frac{(p-1)(1+r(p-r+1))}{p}|\nu_F(a)| - d_{r,r}\cdot s\right)} \cdot C(A,r,s),
\end{aligned}$$

where $0 \neq |C(A,r,s)|$ is bounded for all $A \in \mathbb{Z}$ and $s \in \mathbb{C}$. Moreover, $C(A,r,s) > 0$ for all $s \in \mathbb{R}$. Thus Lemma 4.54 yields the convergence of $\widetilde{\Phi}(s)$ for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > \frac{(p-1)(1+r(p-r+1))}{p\cdot d_{r,r}}$, and it is unbounded for $s = \frac{(p-1)(1+r(p-r+1))}{p\cdot d_{r,r}}$. Thus by the Tauberian Theorem 1.38, we obtain

$$Z_{\min}(F,r;X) = \sum_{\substack{L\in\widetilde{\mathcal{F}}_r \\ \mathrm{D}(L/F)\leq X}} 1 \asymp X^{\frac{(p-1)(1+r(p-r+1))}{p\cdot d_{r,r}}},$$

and hence we obtain the lower bound on the asymptotics exponent. □

Remark 4.68. (a) We conjecture that the bound $\frac{(p-1)(1+r(p-r+1))}{p\cdot d_{r,r}}$ given in Theorem 4.67 is sharp.

(b) To make this bound slightly more explicit, we have

$$\begin{aligned}\frac{(p-1)\,(1+r(p-r+1))}{p\cdot d_{r,r}} &= \frac{(p-1)\,(1+r(p-r+1))}{p\cdot(p-1)\left(p^r+p(p-r)\frac{p^r-1}{p-1}+p^{-1}\eta_p(r)\right)}\\ &= \frac{1+r(p-r+1)}{p^{r+1}+p^2(p-r)\frac{p^r-1}{p-1}+\eta_p(r)}\\ &= \frac{1+r(p-r+1)}{p^{r+1}+p^2(p-r)\frac{p^r-1}{p-1}+\sum\limits_{k=1}^{r}kp^k}.\end{aligned}$$

(c) One could use the formula

$$\eta_p(r)=\sum_{k=1}^{r}kp^k=p\frac{p^r(rp-r-1)+1}{(p-1)^2}=p\cdot\frac{r\cdot p^r-p^{r-1}-\ldots-p-1}{p-1}$$

which, however, only results in a minor simplification.

Example 4.69. *(a) For $r=1$ the lower bound of Theorem 4.67 is*

$$\frac{(p-1)(1+p)}{pd_{r,r}}=\frac{(p-1)(p+1)}{(p-1)p(p^2+1)}=\frac{p+1}{p(p^2+1)}.$$

This coincides with the asymptotics exponent in [Lag10, Satz 2.1] using $r_1=r_2=1$, see Theorem 2.19

(b) For $r=2$, the lower bound is

$$\frac{1+2(p-1)}{p^3+p^2(p-2)(p+1)+(1+2p)}=\frac{2p-1}{p^4-2p^2+2p+1}.$$

Bibliography

[AB95] Jonathan L. Alperin and Rowen B. Bell. Groups and representations, 1995. 22, 66

[Alb34] Abraham Albert. Cyclic fields of degree p^n over F of characteristic p. *Bull. Amer. Math. Soc.*, 40(8):625–631, 1934. 91

[BE99] Hans Ulrich Besche and Bettina Eick. Construction of finite groups. *J. Symbolic Comput.*, 27(4):387–404, 1999. 67

[CMS16] Sunil Chebolu, Ján Mináč, and Andrew Schultz. Galois p-groups and Galois modules. *Rocky Mountain J. Math.*, 46(5):1405–1446, 2016. 103

[Del48] S. Delsarte. Fonctions de Möbius sur les groupes abeliens finis. *Ann. of Math. (2)*, 49:600–609, 1948. 55

[EV05] Jordan Ellenberg and Akshay Venkatesh. Counting extensions of function fields with bounded discriminant and specified Galois group. In *Geometric Methods in Algebra and Number Theory*, volume 235 of *Progress in Mathematics*, pages 151–168. Birkhäuser, 2005. 9, 36

[FK03] Claus Fieker and Jürgen Klüners. Minimal discriminants for fields with small Frobenius groups as Galois groups. *J. Number Theory*, 99(2):318–337, 2003. 84

[FV02] Ivan Fesenko and Sergei Vostokov. *Local fields and their extensions*, volume 121 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, second edition, 2002. With a foreword by I. R. Shafarevich. 52

[Gei03] Katharina Geißler. *Berechnung von Galoisgruppen über Zahl- und Funktionenkörpern*. Doctoral thesis, Technische Universität Berlin, Fakultät II - Mathematik und Naturwissenschaften, Berlin, 2003. 22

[Has69] Helmut Hasse. *Zahlentheorie*. Dritte berichtigte Auflage. Akademie-Verlag, Berlin, 1969. 52, 53, 66, 69

[Hup67] Bertram Huppert. *Endliche Gruppen. I.* Die Grundlehren der mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin-New York, 1967. 76

[Iwa86] Kenkichi Iwasawa. *Local class field theory*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1986. Oxford Mathematical Monographs. 17, 29

[JLY02] Christian Jensen, Arne Ledet, and Noriko Yui. *Generic polynomials*, volume 45 of *Mathematical Sciences Research Institute Publications*. Cambridge University Press, Cambridge, 2002. Constructive aspects of the inverse Galois problem. 42

[KM20] Jürgen Klüners and Raphael Müller. The conductor density of local function fields with abelian Galois group. *J. Number Theory*, 212:311–322, 2020. 51, 85

[Lag10] Thorsten Lagemann. *Asymptotik wild verzweigter abelscher Funktionenkörper*. Dissertationsschrift, Technische Universität Berlin, 2010. Logos–Verlag, ISBN 978-3-8325-2710-5. 9, 10, 51, 55, 62, 130, 141

[Lag12] Thorsten Lagemann. Distribution of Artin-Schreier extensions. *J. Number Theory*, 132(9):1867–1887, 2012. 36

[Lag15] Thorsten Lagemann. Distribution of Artin-Schreier-Witt extensions. *J. Number Theory*, 148:288–310, 2015. 61

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002. 20

[Led05] Arne Ledet. *Brauer type embedding problems*, volume 21 of *Fields Institute Monographs*. American Mathematical Society, Providence, RI, 2005. 46, 48

[Mal02] Gunter Malle. On the distribution of Galois groups. *J. Number Theory*, 92(2):315–329, 2002. 9, 10

[Mal04] Gunter Malle. On the distribution of Galois groups. II. *Experiment. Math.*, 13(2):129–135, 2004. 9, 10

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer-Verlag, Berlin, 1992. 18, 20

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323. Springer-Verlag, Berlin, second edition, 2008. 40, 41, 44, 48

[RZ00] Luis Ribes and Pavel Zalesskii. *Profinite groups*, volume 40. Springer-Verlag, Berlin, 2000. 40

[Sch14] Andrew Schultz. Parameterizing solutions to any Galois embedding problem over $\mathbb{Z}/p^n\mathbb{Z}$ with elementary p-abelian kernel. *Journal of Algebra*, 411:50 – 91, 2014. 87, 89, 90, 96, 98, 99, 100

[Ser79] Jean-Pierre Serre. *Local fields*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. 16, 27, 28

[Sna94] Victor P. Snaith. *Explicit Brauer induction*, volume 40 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994. With applications to algebra and number theory. 28

[Tau55] Derek Taunt. Remarks on the isomorphism problem in theories of construction of finite groups. *Proc. Cambridge Philos. Soc.*, 51:16–24, 1955. 67

[VS06] Gabriel Daniel Villa Salvador. *Topics in the theory of algebraic function fields*. Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 2006. 19, 24, 25

[Wat94] William C. Waterhouse. The normal closures of certain Kummer extensions. *Canad. Math. Bull.*, 37(1):133–139, 1994. 89

[Wit35] Ernst Witt. Der Existenzsatz für abelsche Funktionenkörper. *J. Reine Angew. Math.*, 173:43–51, 1935. 48

[Wit36] Ernst Witt. Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f. *J. Reine Angew. Math.*, 174:237–245, 1936. 12, 46, 48

[Wri89] David Wright. Distribution of discriminants of abelian extensions. *Proc. London Math. Soc.*, 58:17–50, 1989. 9

[Yat14] Lindsay Yates. Linear algebra of pascal matrices, 2014. https://www.gcsu.edu/sites/files/page-assets/node-808/attachments/yates.pdf. 93

Notation Index

General Notations

$\mathbb{P}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	Set of prime numbers, rational numbers, real numbers, complex numbers	
$\oplus$	Direct sum	
$[K : F]$	Degree of a field extension	
$\mathbb{Z}_p$	Field of p-adic numbers	
$\mathbb{F}_q$	Finite field with q elements	
$K[[t]]$	Power series ring in t over K	Page 15
$K((t))$	Laurent series field over K	Page 15
ν_F	normalised exponential valuation of a local field F	Page 15
$\mathcal{O}_F$, $\mathfrak{p}_F$, U_F	Valuation ring / maximal ideal / unit group of F	Page 15
κ_F	Residue Field of a local field F	Page 15
$\hat{F}$	Separable algebraic closure of F	Page 16
$e_{K/F}$, $f_{K/F}$	Ramification index, inertia degree of K/F	Page 16
$\mathrm{cond}(K/F)$	Conductor exponent of K/F	Page 17
$\mathfrak{f}(K/F)$	Conductor of K/F	Page 17
$\mathrm{Spl}_F(K)$	Splitting field resp. normal closure of K/F	Page 18
$\mathrm{disc}(K/F)$	Discriminant exponent of K/F	Page 17
$\mathfrak{D}(K/F)$	Discriminant ideal of K/F	Page 17
$\mathrm{D}(K/F)$	Discriminant of K/F	Page 17
$\mathrm{Diff}(K/F)$	Different of K/F	Page 17
$\wp(\alpha) = \alpha^p - \alpha$	Artin-Schreier operator	Page 18
θ_a	Element in $\wp^{-1}(a)$, a root of $x^p - x - a$	Page 19
$J(F) = F/\wp(F)$	Cokernel of $\wp$	Page 19
$\mathrm{Span}_K((v_i)_{i\in I})$	K-Vector space generated by the system of vectors $(v_i)_{i\in I} \leq V$	Page 20
$\nu_{J(K)}(\alpha)$	$= \max\{\nu_K(x) \mid x \in \alpha\}$, $\nu_{J(K)}(0) = \infty$ reduced valuation of α in K	Page 23
$\mathrm{cond}([a])$	Conductor exponent $\mathrm{disc}(F(\theta_a)/F)$ for $a \in F \setminus \wp(F)$	Page 24
$\mathrm{disc}([a])$	Discriminant exponent $\mathrm{disc}(F(\theta_a)/F)$ for $a \in F \setminus \wp(F)$	Page 24
$R_F(\pi, \omega) = R_F$	$\mathbb{F}_p\omega \bigoplus_{\substack{n<0 \\ p\nmid n}} \mathbb{F}_q \cdot \pi^n$ Reduced complement of $\wp(F)$ in F: $R_F \oplus \wp(F) = F$	Page 25
$T_p(x) = \lvert x\rvert - \lfloor \frac{\lvert x\rvert}{p} \rfloor$	The number of integers $1 \leq n \leq \lvert x\rvert$ not divisible by p	Page 32
$\Gamma_q(x)$	$pq^{T_p(x)}$	Page 32
$\gamma_q(x)$	$\Gamma_q(x) - \Gamma_q(x-1)$	Page 32
$\mathfrak{f}(\chi)$	Conductor of a character	Page 29
G^*	Dual group of G	Page 30
$\mathrm{Tr}_{K/F}$	Trace map	Page 17
$f \sim g$	Asymptotic equivalence, meaning: $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$	Page 31
$f = O(g)$	$0 \leq \limsup_{x\to\infty} \frac{f(x)}{g(x)} < \infty$	Page 31
$f \asymp g$	$f = O(g)$ and $f = o(g)$	Page 31
$Z(F, G; X)$	Counting function w.r.t. discriminant	Page 32
$\mathrm{Aut}(G)$	Automorphism group of G	

Notations from Chapter 2

$\mathfrak{Z}(F,G;n)$	Counting function w.r.t. conductor	Page 51
U_n	$=\langle 1+\mathfrak{p}\rangle/\langle 1+\mathfrak{p}^n\rangle$	Page 52
$r_i(H)$	p^i-rank of H	Page 53
$\tilde{r}_i(H)$	$=r_i(H)-r_{i+1}(H)$ number of p^i-blocks of H	Page 53
$\exp(H)$	Exponent of the group H	Page 57
$H[p^i]$	p^i-torsion of H	Page 52
$\alpha_G(A)$	Number of subgroups $U\leq A$ which are isomorphic to G	Page 54
$\{x\}$	$=x-\lfloor x\rfloor$ for $x\in\mathbb{R}$	Page 55
$\alpha_p(G)$	$=\sum_{k=1}^{e}\frac{p-1}{p^k}r_k(G)$: Conductor exponent for an abelian p-group	Page 56

Notations from Chapter 3

$G\wr H$	Wreath product of G and H	Page 22
$N\rtimes_\phi H$	Semi-direct product of N and H by some homomorph. $\phi\in\mathrm{Hom}(H,\mathrm{Aut}(N))$	Page 66
$\mathrm{AGL}(V)$	Affine group of a K-vector space V	Page 66
$\mathrm{AGL}_n(q)$	$\cong(\mathbb{F}_q)^n\rtimes\mathrm{GL}_n(\mathbb{F}_q)$ Affine group of $\mathbb{A}^n(\mathbb{F}_q)$	Page 66
$\mathrm{Eig}_F(\zeta)$	F-eigenspace of σ to the eigenvalue ζ	Page 70
$K[G]$	Group ring of G with coefficients in K	Page 70

Notations from Chapter 4

$H(p,r)$	Generalised Heisenberg group	Page 90
$\widetilde{H}(p,r)$	Twisted Heisenberg Group	Page 90
$\mathrm{len}\,([\gamma])$	$=\mathrm{len}(\langle\gamma\rangle_G)$ for $\gamma\in J(K)$	Page 96
$\varepsilon_{E/F}$	Special $\mathbb{F}_p$-linear map $\varepsilon_{E/F}\colon J(E)\to\mathbb{F}_p$	Page 98
$J_r(E)$	$=\left\{[\beta]\in J(E):\mathrm{len}\,([\beta])\leq r,\quad \varepsilon_{E/F}([\beta])=0\right\}$ for $1\leq r\leq p-1$	Page 99
$J_p(E)$	$=J(E)$	Page 99
$J_r(E,x)$	$=\left\{[\beta]\in J_r(E)\ :\ \nu_{J(E)}\,([\beta])\leq x\right\}$	Page 99
γ_E	Special cyclic C_{p^2}-generator	Page 102
$\gamma_{E,r}$	Generator of a minimal $\widetilde{H}(p,r)$-extension	Page 104
$M_{a,r}$	representative system for $H(p,r)$-extensions	
	$=\{f_0+f_1\theta_a+\ldots+f_{r-1}\theta_a^{r-1}\mid f_i\in R_{V_a}$ for $0\leq i\leq p-2,\ f_{p-1}\in R_F, f_{r-1}\neq 0\}$	Page 107
π_i	i-th projection w.r.t. power basis	Page 110

$\beta_{r,j}(g)$	$= \wp(g)\theta_a^j + g^p \cdot \sum_{k=r+1}^{j-1} a^{j-k}\theta_a^k \binom{j}{k}$	Page 110
$w_z(a)$	$= \lfloor \frac{z\lvert\nu_F(a)\rvert}{p} \rfloor$ for $a \in R_F$ and $z \in \mathbb{Z}$	Page 111
$R_a^{(z)}$	$= t^{\lfloor \frac{z\cdot\lvert\nu_F(a)\rvert}{p} \rfloor} \cdot \mathbb{F}_q[t^{-1}]$	Page 111
$N_r(E)$	$= \{\alpha \in R_E \mid \nu_E(\alpha) > r \cdot \nu_E(\theta_a)\}$	Page 115
$\Omega_{E,r}$	Special representative system of $Y_r(E)$	
	$= N_r(E) \bigoplus_{i=1}^{r-1} R_a^{(i-r)} \cdot \theta_a^i \bigoplus_{j=r}^{p-1} \beta_{r,j} \left(R_a^{(j-r)}\right)$	Page 115
$\widetilde{\Omega}_{E,r}$	Set of twisted Heisenberg generators of length $\leq r$	Page 131
$\Omega_{E,r}(X)$	Set of $\alpha \in \Omega_{E,r}$ with $\lvert\nu_E(\alpha)\rvert \leq X$	Page 131