Discriminants of totally wild extensions

Buise, Matthijs

Universiteit Leiden

Leiden University
Mathematical Institute

Discriminants of totally wild extensions

Matthijs Buise

Master's Thesis

Advisor: Prof. Hendrik W. Lenstra

April 27, 2026

Abstract

We study totally wild extensions of local fields. To such an extension, we associate a cohomological invariant derived from the discriminant of a generator. Under suitable divisibility conditions, we prove that this invariant attains all possible values.

The construction provides a tool for the study of totally wild extensions, which are in general poorly understood. Our proof uses non-standard group-theoretic methods, including a generalization of the transfer homomorphism and a notion of determinants of automorphisms of p-groups. These methods may be of independent interest.

Acknowledgements

I would like to thank my advisor, Prof. Hendrik W. Lenstra, for suggesting this topic and for the many insightful discussions we have had over the past two years. His guidance and enthusiasm have been a constant source of inspiration.

I am also grateful for the support and encouragement of my family, and especially my partner Stan, who helped me stay grounded throughout this work.

Contents

1 Introduction

Let K be a field with multiplicative group K^*. For an integer m, write $K^{*m} = \{x^m : x \in K^*\}$. Let L be a finite separable field extension of K, and for an element $\alpha \in L$ such that $K(\alpha) = L$, denote by $\Delta(\alpha)$ the discriminant of the irreducible polynomial of α over K, so that $\Delta(\alpha) \in K^*$. It is well known that one has

$$\Delta(\alpha) \cdot K^{*2} = \Delta(\beta) \cdot K^{*2} \text{ if } \alpha, \beta \in L \text{ are such that } K(\alpha) = K(\beta) = L. \tag{1.1}$$

We shall, in a special situation, prove a strikingly stronger statement.

Let p be a prime number. We now make the additional assumptions that K be *local* with residue characteristic p, and that L be *totally wild* over K; see Sections 5 and 6 for the definitions of the italicized terms.

Theorem 1.2. *With the notation and hypotheses as above, let $\alpha, \beta \in L$ be such that $K(\alpha) = K(\beta) = L$. Then we have $\Delta(\alpha) \cdot K^{*p-1} = \Delta(\beta) \cdot K^{*p-1}$.*

A proof of Theorem 1.2 is given in Section 7. For $p = 2$, the theorem is obvious, and for $p = 3$ it follows from (1.1); but for $p \geq 5$, the conclusion of the theorem is stronger than (1.1). In the situation of the theorem, there exists a non-negative integer n with $[L : K] = p^n$; in the case $n = 1$ and K has characteristic zero, a proof of the theorem is given in [7].

Theorem 1.2 shows that, for any pair p, K as above, there is a well-defined map Φ from the set $\mathcal{L}(K, p^n)$ of K-isomorphism classes of separable, totally wild field extensions L of K of degree $[L : K] = p^n$ to the group K^*/K^{*p-1}, sending the isomorphism class of $L = K(\alpha)$ to $\Delta(\alpha) \cdot K^{*p-1}$. This map may be viewed as attaching a cohomological invariant to each L, because by [10, Chapitre II, §1] the group K^*/K^{*p-1} is isomorphic to the cohomology group $\mathrm{H}^1(K, \mathbb{F}_p^*)$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Given our general lack of understanding of wild extensions, such an invariant is of interest to have.

Assume moreover that the group K^*/A^* is isomorphic as an ordered group to the additive group of integers, where A is the valuation ring associated to K. The following result shows that in this case the invariant assumes all possible values.

Theorem 1.3. *With K being as above, the map*

$$\Phi \colon \mathcal{L}(K, p^n) \to K^*/K^{*p-1}$$

just defined is surjective for every positive integer n.

A stronger version of Theorem 1.3 is given in Section 8. The conditions of Theorem 1.3 are satisfied when K is a finite extension of a field of p-adic numbers $\mathbb{Q}_p$ or a field $k((T))$ of formal Laurent series over a field of characteristic p. There are also fields where the map is not surjective; obvious examples are separably closed fields and other fields that have no non-trivial, separable, totally wild extensions. In Proposition 8.8, we construct such a local field that is not separably closed. It would be of interest to see for which perfectoid fields K, as defined in [9], the conclusion of Theorem 1.3 is valid.

One proof of the classical fact (1.1) for general finite separable field extensions $K \subseteq L$ proceeds as follows. Let M be a Galois closure of L over K, and G the Galois group of M over K. One first defines a group homomorphism $\epsilon \colon G \to \{1, -1\}$ by viewing G as a permutation group of the set X of K-embeddings $L \to M$ and letting ϵ be the sign map. Secondly, viewing $\{1, -1\}$ as a subgroup of K^* (the trivial

subgroup if K has characteristic 2) and letting $\alpha \in L$ be such that $K(\alpha) = L$, one constructs $\delta(\alpha) \in M^*$ such that $\delta(\alpha)^2 = \Delta(\alpha)$ and such that for all $\sigma \in G$ one has $\epsilon(\sigma) = \sigma(\delta(\alpha))/\delta(\alpha)$. With these two ingredients, one proves (1.1) as follows. If α, β are as in (1.1), then for all $\sigma \in G$ one has $\sigma(\delta(\alpha))/\delta(\alpha) = \epsilon(\sigma) = \sigma(\delta(\beta))/\delta(\beta)$ so $\sigma(\delta(\alpha)/\delta(\beta)) = \delta(\alpha)/\delta(\beta)$. Therefore, $\delta(\alpha)/\delta(\beta)$ is an element of K^* and $\delta(\alpha)\cdot K^* = \delta(\beta)\cdot K^*$. Upon squaring, one obtains (1.1).

Our proof of Theorem 1.2 follows the same lines, but with two changes. First, the group homomorphism $\epsilon\colon G \to \{1, -1\}$ is replaced by a homomorphism $\epsilon_X\colon G \to \mathbb{F}_p^*$; as we shall see in Section 5, there is a natural embedding $\mathbb{F}_p^* \subseteq K^*$. Second, the condition $\delta(\alpha)^2 = \Delta(\alpha)$ is replaced by $\delta(\alpha)^{p-1} = (-1)^{n(p+1)/2}\cdot\Delta(\alpha)$; here $[L : K] = p^n$, and p is assumed odd.

The construction of the map ϵ_X and our proof of the relation $\epsilon(\sigma) = \sigma(\delta(\alpha))/\delta(\alpha)$ make use of some group-theoretic tools that are not entirely standard. As a byproduct of these, we obtain the following determinant formula.

Let k be a field, let m be a non-negative integer, and write k^m for the standard m-dimensional k-vector space. Define the *leading coefficient* function $\mathrm{lc}\colon k^m \to k$ by

$$\mathrm{lc}((x_i)_{i=0}^{m-1}) = \begin{cases} 0 & \text{if all } x_i \text{ equal } 0, \\ x_j & \text{if } j = \min\{i : x_i \neq 0\}. \end{cases}$$

Let $\mathcal{L}$ be a finite set of one-dimensional subspaces of k^m, and put $X = \bigcup_{l\in\mathcal{L}} l$. Let G be the group of k-linear automorphisms generated by all k-linear automorphisms σ with $(\sigma - 1)k^m \in \mathcal{L}$ that permute $\mathcal{L}$. For example, if k is finite, and $\mathcal{L}$ is the set of all one-dimensional subspaces of k^m, then G is the full general linear group $\mathrm{GL}(m, k)$, see [6, Chapter XIII §9, Theorem 9.1].

Theorem 1.4. *With the notation above, let $\sigma \in G$. Then the determinant of σ is given by*

$$\det\sigma = \prod_{x\in\mathrm{lc}^{-1}(1)\cap X} \mathrm{lc}(\sigma x).$$

A proof of Theorem 1.4 is given in Section 3. This theorem generalizes the results of Cartier [2, §8 and 9], where G is a group generated by reflections of a real vector space.

In Section 2 we discuss a transfer map introduced by Cartier [2], and we characterize it by a universal property. As an application, we develop in Section 3 a notion of determinants of automorphisms of p-groups, and we prove Theorem 1.4. In Section 4, we construct the map ϵ_X mentioned above. Section 5 assembles a few facts on local fields, and Section 6 is devoted to generalities on totally wild extensions. The construction of $\delta(\alpha)$ and our proof of Theorem 1.2 are in Section 7. Section 8 addresses Theorem 1.3.

There is a second proof of (1.1), which proceeds by considering the determinant of the K-bilinear form $L \times L \to K$ sending (x, y) to the trace of xy. It would be of interest to have a similar "multilinear" proof of Theorem 1.2, possibly more enlightening than the proof contained in the present paper.

The permutation group of a set X is denoted by $\mathrm{Sym}(X)$, and the identity map of X by id_X. For any group G, we write G° for the set of elements of G that are different from the identity element. For any ring R, we denote by R^* the group of invertible elements of R.

2 The transfer

If d is a non-negative integer, and X, Y are sets, then a map $f\colon X \to Y$ is said to be a *cover of degree* d if for every $y \in Y$ one has $\#f^{-1}y = d$.

Let F be a group. By an *F-set* we mean a set X equipped with a group homomorphism $\psi\colon F \to \mathrm{Sym}(X)$, which we call the *action* of F on X. For $\gamma \in F$, and $x \in X$, we shall write $\gamma \cdot x$ or simply γx for $\psi(\gamma)(x)$. An *F-map* between F-sets X and Y is a map $\phi\colon X \to Y$ such that for all $\gamma \in F$, $x \in X$ one has $\phi(\gamma \cdot x) = \gamma \cdot \phi(x)$. The F-sets together with the F-maps form a category. For an F-set X, its group of automorphisms in this category is denoted by $\mathrm{Aut}_F(X)$. Two elements $x, y \in X$ are said to be *equivalent* under F if there exists $\gamma \in F$ such that $\gamma x = y$. This is indeed an equivalence relation, and we write X/F for the set of equivalence classes; its elements are called the *orbits* of X under F, and for $x \in X$ we write Fx for the orbit containing x. The *stabilizer* of $x \in X$ is the subgroup F_x of F consisting of elements that map x to itself. The action is called *transitive* if there is exactly one orbit. The action is called *free* if for all $\gamma \in F^\circ$ and all $x \in X$, one has $\gamma x \neq x$.

For the remainder of this section, we fix an *abelian* group F. We write it multiplicatively and denote its identity element by 1. In this case there is, for each F-set X, a group homomorphism $F \to \mathrm{Aut}_F(X)$ sending $\gamma \in F$ to the map $x \mapsto \gamma x$.

We write $\mathcal{X}_F$ or simply $\mathcal{X}$ for the class of all F-sets X that are *free* with X/F *finite*. For example, one has $F \in \mathcal{X}$, where F acts on itself by multiplication; in this case the map $F \to \mathrm{Aut}_F(F)$ just defined is an isomorphism.

For a group G, we write $\mathcal{T}(G)$ for the class of all systems of group homomorphisms $u = (u_X\colon \mathrm{Aut}_F(X) \to G)_{X \in \mathcal{X}}$ that have the following two properties:

(a) if $X \in \mathcal{X}$ is the disjoint union of two subsets Y, Z that are stable under the action of F, and $\rho \in \mathrm{Aut}_F(X)$ restricts to $\sigma \in \mathrm{Aut}_F(Y)$ on Y and to $\tau \in \mathrm{Aut}_F(Z)$ on Z, then one has

$$u_X(\rho) = u_Y(\sigma) \cdot u_Z(\tau) \text{ in } G;$$

(b) for $d \in \mathbb{Z}_{>0}$, $X, Y \in \mathcal{X}$, $\rho \in \mathrm{Aut}_F(X)$ and $\sigma \in \mathrm{Aut}_F(Y)$, if $\phi\colon X \to Y$ is an F-map that is a cover of degree d and satisfies $\phi \circ \rho = \sigma \circ \phi$, then

$$u_X(\rho) = u_Y(\sigma)^d \text{ in } G.$$

For any homomorphism $v\colon G \to H$ of groups and any $u = (u_X)_{X \in \mathcal{X}} \in \mathcal{T}(G)$ one defines $v \circ u = (v \circ u_X)_{X \in \mathcal{X}}$, which is an element of $\mathcal{T}(H)$. An element $u \in \mathcal{T}(G)$ is called *universal* if for every group H the map $\mathrm{Hom}(G, H) \to \mathcal{T}(H)$, $v \mapsto v \circ u$, is bijective.

One readily shows that a pair consisting of a group G and a universal element $u \in \mathcal{T}(G)$ is *unique up to unique isomorphism* if it exists; that is, if (G', u') is another such pair, then there is a unique group isomorphism $v\colon G \to G'$ with $u' = v \circ u$. There are also general arguments to prove the existence of such a pair, but instead we give an explicit description.

Let $X \in \mathcal{X}_F$. By a *section* of X we mean a subset S of X that intersects each orbit of X in exactly one element. To any two sections S and S' of X, we associate an element $d(S, S')$ of F, which may be interpreted as an asymmetric "distance" between S and S'. For each $s \in S$, there exists an element γ_s of F such that $s \in \gamma_s S'$, which is unique because X is free. Let $d(S, S') = \prod_{s \in S} \gamma_s$. The map d is multiplicative in the sense that for a third section S'', one has $d(S, S'') = d(S, S')d(S', S'')$. Any F-automorphism ρ of X transforms sections into sections, and we have $d(\rho S, \rho S') = d(S, S')$.

Proposition 2.1. *Let F be an abelian group. Then there exists a unique element $\mathrm{t} = (\mathrm{t}_X)_{X\in\mathcal{X}} \in \mathcal{T}(F)$ with the property that the map $\mathrm{t}_F\colon \mathrm{Aut}_F(F) \to F$ is the inverse of the isomorphism $F \to \mathrm{Aut}_F(F)$ given by the multiplication in F. Moreover, t is universal.*

Furthermore, let $X \in \mathcal{X}$, let $\rho \in \mathrm{Aut}_F(X)$ and let $S \subseteq X$ be a section. For each $s \in S$, let $\gamma_s \in F$ be the unique element such that $\rho(s) \in \gamma_s S$. Then

$$\mathrm{t}_X(\rho) = \prod_{s\in S} \gamma_s.$$

Proof. Let X be an element of $\mathcal{X}$. Define $\mathrm{t}_X\colon \mathrm{Aut}_F(X) \to F$ as the map $\rho \mapsto d(\rho S, S)$ for some section S of X. Using the properties of d above, one readily checks that t_X is independent of the choice of the section S, and that t_X is a homomorphism of groups. This map has the desired properties that $\mathrm{t}_F(\gamma) = d(\gamma S, S) = \gamma$ for every $\gamma \in F$ and $\mathrm{t}_X(\rho) = \prod_{s\in S} \gamma_s$, where $\rho(s) \in \gamma_s S$. Moreover, t has properties (a) and (b), so $\mathrm{t} \in \mathcal{T}(F)$. We prove uniqueness. One may write any automorphism ρ of a free F-set X as the composition of an automorphism σ that permutes a given section S and an automorphism τ that maps each orbit to itself. Property (a) implies

$$\mathrm{t}_X(\tau) = \prod_{s\in S} \tau|_{Fs},$$

and one has $\mathrm{t}_X(\sigma) = d(\sigma S, S) = d(S, S) = 1$. By the homomorphism property of t_X, we conclude that t is completely determined by its value on F. Hence t is unique with the given property.

To show that t is universal, we prove that the map $\mathrm{Hom}(F, H) \to \mathcal{T}(H)$ sending v to $v\circ\mathrm{t}$ is injective and surjective. Injectivity is easily checked: for $v, w \in \mathrm{Hom}(F, H)$, whenever $v \circ \mathrm{t} = w \circ \mathrm{t}$, one has $v \circ \mathrm{t}_F = w \circ \mathrm{t}_F$. The map t_F is an isomorphism, so v is equal to w.

Surjectivity requires a little more work. Let H be a group and let $u \in \mathcal{T}(H)$. Let $v\colon F \to H$ be the homomorphism of groups defined by $\gamma \mapsto u_F(\psi(\gamma))$, where ψ is the action of F on itself via multiplication. Let $X \in \mathcal{X}$ and $\rho \in \mathrm{Aut}_F(X)$. As before, write ρ as the composition of an automorphism σ that permutes a given section S and an automorphism τ that maps each orbit to itself. Property (a) implies that $u_X(\tau)$ is equal to $v(\mathrm{t}_X(\tau))$. The F-map $\phi\colon X \to F$ sending every element of S to the identity element is a cover of degree $\#X/F$ satisfying $\phi \circ \sigma = \mathrm{id}_F \circ \phi$. Property (b) yields $u_X(\sigma) = u_F(\mathrm{id}_F)^{\#X/F} = 1$. So we also have $u_X(\sigma) = v(\mathrm{t}_X(\sigma))$. By the homomorphism properties of u_X, t_X, and v, we obtain $u_X = v \circ \mathrm{t}_X$. Hence the map $\mathrm{Hom}(F, H) \to \mathcal{T}(H)$ is surjective. This shows that t is universal. □

The definition of t is due to Cartier [2]. We show that the classical transfer is a special case. Let G be a group and $H \subseteq G$ a subgroup of finite index. Write $[H, H]$ for the commutator subgroup of H, and set $F = H/[H, H]$. The abelian group F acts on $X = G/[H, H]$ by right multiplication; under this action we have $X \in \mathcal{X}_F$. Let S be a subset of G that intersects each coset of H in exactly one element. Let S' be the section $\{s[H, H] : s \in S\}$ of $G/[H, H]$ under $H/[H, H]$. The group G acts on X by left multiplication, and for each $g \in G$, this action is an $H/[H, H]$-automorphism of X, yielding a group homomorphism $\phi\colon G \to \mathrm{Aut}_F(X)$. The classical transfer homomorphism $G \to H/[H, H]$ is defined by $g \mapsto \prod_{s\in S'} \gamma_s$, where $gs \in \gamma_s S'$. This coincides with the map $\mathrm{t}_X \circ \phi$.

Remark. When $\#F = 2$, we may identify F with the group $\{1, -1\}$, where 1 is the identity element. With this identification, the sign map and the transfer coincide

on $\mathrm{Aut}_F(X)$ for any $X \in \mathcal{X}_F$. Indeed, let $\rho \in \mathrm{Aut}_F(X)$ and let S be a section of X. Write $\rho = \sigma \circ \tau$, where σ permutes S and τ maps every orbit to itself. Since σ acts in the same way on S and on $-S = \{-1 \cdot s : s \in S\}$, it is an even permutation of X, so $\epsilon(\sigma) = 1 = \mathrm{t}_X(\sigma)$. For τ, each orbit $\{s, -s\}$ is either fixed pointwise (contributing nothing to the sign and $\gamma_s = 1$ to t_X) or swapped (contributing a transposition and $\gamma_s = -1$), so $\epsilon(\tau) = \mathrm{t}_X(\tau)$. Since both the sign map and t_X are group homomorphisms, they coincide.

In the final result of this section, we consider groups V whose underlying sets are equipped with an F-set structure. We assume that $F1 = \{1\}$ and that V° belongs to $\mathcal{X}_F$. Let U, V, and W be groups equipped with such F-set structures. Let $\phi\colon U \to V$ and $\psi\colon V \to W$ be maps that are simultaneously group homomorphisms and F-maps, and that fit in a short exact sequence of groups

$$0 \to U \xrightarrow{\phi} V \xrightarrow{\psi} W \to 0.$$

Proposition 2.2. *The situation being as above, suppose that ρ, σ, τ are group automorphisms of U, V, W respectively that are simultaneously F-maps and satisfy $\phi \circ \rho = \sigma \circ \phi$ and $\psi \circ \sigma = \tau \circ \psi$. Then one has*

$$\mathrm{t}_{V^\circ}(\sigma|_{V^\circ}) = \mathrm{t}_{U^\circ}(\rho|_{U^\circ}) \cdot \mathrm{t}_{W^\circ}(\tau|_{W^\circ}).$$

Proof. The case in which U or W is the trivial group is immediate. Assume that U and W are non-trivial. Then W° contains an F-orbit isomorphic to F, and the inverse image of such an orbit under ψ is the disjoint union of $\#U$ orbits under F. Hence U is finite, and since F acts freely on the finite non-empty set U°, the group F is finite as well, with $\#F$ dividing $\#U^\circ$. It follows that one has $\#U \equiv 1 \bmod \#F$.

The set V° is equal to the disjoint union of $\phi(U^\circ)$ and $V \backslash \phi(U)$, so by property (a) we have

$$\mathrm{t}_{V^\circ}(\sigma|_{V^\circ}) = \mathrm{t}_{\phi(U^\circ)}(\sigma|_{\phi(U^\circ)}) \cdot \mathrm{t}_{V\backslash\phi(U)}(\sigma|_{V\backslash\phi(U)}).$$

Since ϕ restricts to a cover $U^\circ \to \phi(U^\circ)$ of degree 1 and ψ to a cover $V \backslash \phi(U) \to W^\circ$ of degree $\#U$, property (b) now implies

$$\mathrm{t}_{\phi(U^\circ)}(\sigma|_{\phi(U^\circ)}) = \mathrm{t}_{U^\circ}(\rho|_{U^\circ}),\ \mathrm{t}_{V\backslash\phi(U)}(\sigma|_{V\backslash\phi(U)}) = \mathrm{t}_{W^\circ}(\tau|_{W^\circ})^{\#U} = \mathrm{t}_{W^\circ}(\tau|_{W^\circ}).$$

The proposition follows. □

3 Determinants

The first part of this section is dedicated to our proof of Theorem 1.4.

Proof of Theorem 1.4. The situation being as in Theorem 1.4, the set $X^\circ = X \setminus \{0\}$ is an element of $\mathcal{X}_{k^*}$ as defined in the previous section, and the elements of G restrict to k^*-automorphisms of X°. The set $\mathrm{lc}^{-1}(1) \cap X$ forms a section of X° under k^*, so by Proposition 2.1, the element $\prod_{x \in \mathrm{lc}^{-1}(1)\cap X} \mathrm{lc}(\sigma x)$ of k^* is exactly $\mathrm{t}_{X^\circ}(\sigma|_{X^\circ})$, the transfer of σ as it acts on X°. By definition, the k-linear automorphisms σ with $(\sigma - 1)k^m \in \mathcal{L}$ that permute $\mathcal{L}$ generate G; both det and t_{X° are group homomorphisms, so it suffices to show that $\det \sigma = \mathrm{t}_{X^\circ}(\sigma|_{X^\circ})$ for those σ.

Let σ be a k-linear automorphism with $(\sigma - 1)k^m \in \mathcal{L}$ that permutes $\mathcal{L}$. Then X° is the disjoint union of the sets $Y_{[l]} = \bigcup_{l' \in [l]} l'^\circ$ where $[l]$ is the orbit of l under

the action of σ. The sets $Y_{[l]}$ are stable under the action of k^*, and σ restricts on each $Y_{[l]}$ to a k^*-automorphism. Property (a) yields

$$\mathrm{t}_{X^\circ}(\sigma|_{X^\circ}) = \prod_{[l]} \mathrm{t}_{Y_{[l]}}(\sigma|_{Y_{[l]}}).$$

Clearly σ sends $(\sigma-1)k^m$ to itself, so $Y_{[(\sigma-1)k^m]} = ((\sigma-1)k^m)^\circ$. Write W for the vector space $k^m/(\sigma-1)k^m$, then the natural short exact sequence

$$0 \to (\sigma-1)k^m \to k^m \to W \to 0$$

induces a k-linear automorphism σ' on W; we have $\sigma' = \mathrm{id}_W$. Hence

$$\det(\sigma) = \det(\sigma') \cdot \det(\sigma|_{(\sigma-1)k^m}) = \det(\sigma|_{(\sigma-1)k^m}).$$

For $l \in \mathcal{L}$ unequal to $(\sigma-1)k^m$, the natural projection $\pi\colon k^m \to W$ sends $Y_{[l]}$ to a single subspace of W of dimension one; the orbit $[l]$ is finite, because σ permutes $\mathcal{L}$, which is finite, so, π restricts on $Y_{[l]}$ to a cover of degree $\#[l]$. Property (b) yields

$$\mathrm{t}_{X^\circ}(\sigma|_{X^\circ}) = \mathrm{t}_{((\sigma-1)k^m)^\circ}(\sigma|_{((\sigma-1)k^m)^\circ}) \cdot \prod_{[l]\neq\{(\sigma-1)k^m\}} \mathrm{t}_{\pi(Y_{[l]})}(\sigma'|_{\pi(Y_{[l]})})^{\#[l]}.$$

Because $\sigma' = \mathrm{id}_W$, for every $l \in \mathcal{L}$ unequal to $(\sigma-1)k^m$, one has $\mathrm{t}_{\pi(Y_{[l]})}(\sigma'|_{\pi(Y_{[l]})}) = 1$. Thus,

$$\mathrm{t}_{X^\circ}(\sigma|_{X^\circ}) = \mathrm{t}_{((\sigma-1)k^m)^\circ}(\sigma|_{((\sigma-1)k^m)^\circ}).$$

Since σ is a k-linear automorphism of $(\sigma-1)k^m$, which has dimension one, there exists $\lambda \in k^*$ such that for all $v \in (\sigma-1)k^m$, we have $\sigma(v) = \lambda v$; it is immediate that $\mathrm{t}_{((\sigma-1)k^m)^\circ}(\sigma|_{((\sigma-1)k^m)^\circ}) = \lambda$ and $\det(\sigma|_{(\sigma-1)k^m}) = \lambda$. Thus,

$$\det(\sigma) = \mathrm{t}_{X^\circ}(\sigma|_{X^\circ}) = \prod_{x\in \mathrm{lc}^{-1}(1)\cap X} \mathrm{lc}(\sigma x).$$

Theorem 1.4 follows. □

Throughout the rest of this section, we fix a prime number p. By a *p-group* we mean a finite group whose order is of the form p^m, with $m \in \mathbb{Z}_{\geq 0}$. We write $\mathcal{P}$ for the class of all p-groups and for $V \in \mathcal{P}$ we denote by $\mathrm{Aut}(V)$ the group of all group automorphisms of V. For example, the additive group $\mathbb{Z}/p\mathbb{Z}$ belongs to $\mathcal{P}$, and the map $\mathbb{F}_p^* \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ sending c to $x \mapsto cx$ is an isomorphism of groups. The following lemma endows any p-group with an $\mathbb{F}_p^*$-set structure as in Proposition 2.2.

Lemma 3.1. *There exists a unique collection of actions $(\phi_V\colon \mathbb{F}_p^* \to \mathrm{Sym}(V))_{V\in\mathcal{P}}$ with $\phi_V(\gamma)(1) = 1$ such that every homomorphism between p-groups is an $\mathbb{F}_p^*$-map, and the action on $\mathbb{Z}/p\mathbb{Z}$ is defined by the group isomorphism $\mathbb{F}_p^* \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \subseteq \mathrm{Sym}(\mathbb{Z}/p\mathbb{Z})$ defined above. Moreover, for $V \in \mathcal{P}$, under this action V° is an element of $\mathcal{X}_{\mathbb{F}_p^*}$.*

Proof. We first consider the cyclic group $\mathbb{Z}/p^m\mathbb{Z}$ for a positive integer m. We seek an action $\mathbb{F}_p^* \to \mathrm{Sym}(\mathbb{Z}/p^m\mathbb{Z})$ such that every homomorphism is an $\mathbb{F}_p^*$-map. In particular, this applies to endomorphisms of $\mathbb{Z}/p^m\mathbb{Z}$ of the form $v \mapsto v^k$ for $k \in \mathbb{Z}$. Thus, for all $v \in V$, $k \in \mathbb{Z}$ and $\gamma \in \mathbb{F}_p^*$, the action ϕ_V that is to be defined must

satisfy $\phi_V(\gamma)(v^k) = \phi_V(\gamma)(v)^k$. Together with the requirement $\phi_V(\gamma)(1) = 1$, it follows that each $\phi_V(\gamma)$ must be an automorphism of V.

The group of automorphisms of $\mathbb{Z}/p^m\mathbb{Z}$ is $\mathrm{Aut}(\mathbb{Z}/p^m\mathbb{Z}) = (\mathbb{Z}/p^m\mathbb{Z})^*$, which has order $(p-1)p^{m-1}$. There is a short exact sequence defined by $a \bmod p^m \mapsto a \bmod p$:

$$0 \to 1 + (p\mathbb{Z}/p^m\mathbb{Z}) \to (\mathbb{Z}/p^m\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^* \to 0.$$

Since p^{m-1} and $p-1$ are coprime, there is a unique homomorphism of groups $\mathbb{F}_p^* \to (\mathbb{Z}/p^m\mathbb{Z})^*$ such that the composition with $a \bmod p^m \mapsto a \bmod p$ is the group isomorphism defined above. Define $\phi_{\mathbb{Z}/p^m\mathbb{Z}}$ to be this map. It follows that the natural projection $f : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^{m-1}\mathbb{Z}$ is an $\mathbb{F}_p^*$-map.

Let $V \in \mathcal{P}$ and $v \in V$, then v has order p^m for some $m \in \mathbb{Z}_{\geq 0}$. The inclusion $\mathbb{Z}/p^m\mathbb{Z} \to V$ where $n \mapsto v^n$ must be an $\mathbb{F}_p^*$-map, so we must define $\phi_V(\gamma)(v^n) = v^{\phi_{\mathbb{Z}/p^m\mathbb{Z}}(\gamma)(n)}$. This uniquely determines ϕ_V.

One easily verifies that every homomorphism of p-groups is an $\mathbb{F}_p^*$-map under ϕ and that the action is free. The Lemma follows. □

Remark. One readily checks that the action of ϕ on additively written $\mathbb{F}_p$-vector spaces is exactly scalar multiplication. When using multiplicative notation it is, for lack of a better word, scalar exponentiation. In what follows, we will write v^γ for $\phi_V(\gamma)(v)$ for multiplicatively written p-groups V.

If G is a group, then we write $\mathcal{D}(G)$ for the class of all systems of group homomorphisms $e = (e_V \colon \mathrm{Aut}(V) \to G)_{V \in \mathcal{P}}$ that have the following property: if

$$0 \to U \xrightarrow{\phi} V \xrightarrow{\psi} W \to 0$$

is a short exact sequence of groups in $\mathcal{P}$, and ρ, σ, τ are group automorphisms of U, V, W respectively that satisfy $\phi \circ \rho = \sigma \circ \phi$ and $\psi \circ \sigma = \tau \circ \psi$, then one has

$$e_V(\sigma) = e_U(\rho) \cdot e_W(\tau) \text{ in } G. \tag{3.2}$$

For any homomorphism $v \colon G \to H$ of groups and any $e = (e_V)_{V \in \mathcal{P}} \in \mathcal{D}(G)$ one defines $v \circ e = (v \circ e_V)_{V \in \mathcal{P}}$, which is an element of $\mathcal{D}(H)$. If G is a group, then an element $e \in \mathcal{D}(G)$ is called *universal* if for all groups H the map $\mathrm{Hom}(G, H) \to \mathcal{D}(H)$, $v \mapsto v \circ e$, is bijective. One readily shows that a pair consisting of a group G and a universal element $e \in \mathcal{D}(G)$ is uniquely unique if it exists; that is, if (G', e') is another such pair, then there is a unique isomorphism of groups $v \colon G \to G'$ with $e' = v \circ e$. Again, there are general arguments to prove the existence of such a pair, but we give an explicit description instead.

Proposition 3.3. *There is a unique element* $\det = (\det_V)_{V \in \mathcal{P}} \in \mathcal{D}(\mathbb{F}_p^*)$ *with the property that* $\det_{\mathbb{Z}/p\mathbb{Z}} \colon \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \to \mathbb{F}_p^*$ *is the inverse of the isomorphism* $\mathbb{F}_p^* \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ *sending* γ *to* $x \mapsto \gamma x$. *This element* $\det$ *is universal. Moreover, for* $V \in \mathcal{P}$, *an automorphism* ρ *of* V, *a section* S *of* V° *under* $\mathbb{F}_p^*$, *and* $\gamma_s \in \mathbb{F}_p^*$ *such that* $\rho(s) \in S^{\gamma_s}$, *we have the formula*

$$\det_V(\rho) = \mathrm{t}_{V^\circ}(\rho|_{V^\circ}) = \prod_{s \in S} \gamma_s. \tag{3.4}$$

Before we prove Proposition 3.3, we treat a lemma, which states that an element of $\mathcal{D}(G)$ is completely determined by its value on $\mathbb{Z}/p\mathbb{Z}$.

Lemma 3.5. *Let* G *be a group, and let* $d, e \in \mathcal{D}(G)$ *be such that* $d_{\mathbb{Z}/p\mathbb{Z}} = e_{\mathbb{Z}/p\mathbb{Z}}$. *Then one has* $d = e$.

Proof. We argue by induction on the order of the p-group V. If $\#V = p$, then $V \cong \mathbb{Z}/p\mathbb{Z}$; The base case $\#V = p$ holds. Now let V be a p-group of order greater than p. Let $\sigma \in \mathrm{Aut}(V)$.

First suppose that V is elementary abelian. Then V is an $\mathbb{F}_p$-vector space. We may reduce to the case that $\dim_{\mathbb{F}_p}(\sigma - 1)V = 1$, because e and d are systems of group homomorphisms and the group of k-linear automorphisms of V is generated by those automorphisms [6, Chapter XIII §9, Theorem 9.1]. Immediately, we see that σ restricts to a group automorphism on $(\sigma - 1)V$ and induces one on the cokernel $W = V/(\sigma - 1)V$. By (3.2) applied to the short exact sequence

$$0 \to (\sigma - 1)V \to V \to W \to 0$$

and the induction hypothesis, we obtain $e_V(\sigma) = d_V(\sigma)$.

Next suppose that V is not elementary abelian. Then the subgroup

$$\{v \in \mathrm{Z}(V) : v^p = 1\},$$

where $\mathrm{Z}(V)$ is the center of V, is non-trivial, proper and characteristic in V, and hence invariant under σ. Thus there exists a non-trivial proper subgroup $U \subset V$ that is invariant under σ. We obtain a short exact sequence

$$1 \to U \to V \to V/U \to 1$$

of non-trivial p-groups, together with compatible automorphisms $\rho = \sigma|_U$ on U and τ on V/U in the sense of (3.2). By (3.2) we therefore have

$$e_V(\sigma) = e_U(\rho)\, e_{V/U}(\tau), \qquad d_V(\sigma) = d_U(\rho)\, d_{V/U}(\tau).$$

The induction hypothesis gives $e_V(\sigma) = d_V(\sigma)$, which proves the Lemma. □

Proof of Proposition 3.3. By Proposition 2.1, there exists a universal element $\mathrm{t} \in \mathcal{T}(\mathbb{F}_p^*)$ with the property that $\mathrm{t}_{\mathbb{Z}/p\mathbb{Z}} \colon \mathrm{Aut}_{\mathbb{F}_p^*}(\mathbb{Z}/p\mathbb{Z}) \to \mathbb{F}_p^*$ is the inverse of the isomorphism $\mathbb{F}_p^* \to \mathrm{Aut}_{\mathbb{F}_p^*}(\mathbb{Z}/p\mathbb{Z})$. Recall that every group homomorphism respects the $\mathbb{F}_p^*$-action on p-groups, so a group automorphism of V restricts to an $\mathbb{F}_p^*$-automorphism of V°. Define det to be the system of group homomorphisms $(\mathrm{t}_V \colon \mathrm{Aut}(V) \to \mathbb{F}_p^*)_{V \in \mathcal{P}}$ obtained by composing with the restrictions. By Proposition 2.2, this system is an element of $\mathcal{D}(\mathbb{F}_p^*)$. The homomorphism $\mathrm{t}_{\mathbb{Z}/p\mathbb{Z}}|_{\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})}$ is exactly the inverse of the multiplication action. This establishes the existence of an element det of $\mathcal{D}(\mathbb{F}_p^*)$ that satisfies the formula (3.4).

Uniqueness of the element det follows from Lemma 3.5. It remains to be shown that det is universal. Let H be any group. We show that the map $\mathrm{Hom}(\mathbb{F}_p^*, H) \to \mathcal{D}(H)$ sending $v \colon \mathbb{F}_p^* \to H$ to $v \circ \det$ is injective and surjective. Suppose $v, w \colon \mathbb{F}_p^* \to H$ are homomorphisms such that $v \circ \det = w \circ \det$. Then, in particular, $v \circ \det_{\mathbb{Z}/p\mathbb{Z}} = w \circ \det_{\mathbb{Z}/p\mathbb{Z}}$. Since $\det_{\mathbb{Z}/p\mathbb{Z}}$ is an isomorphism, one has $v = w$. Hence the map is injective.

Let $e = (e_V)_{V \in \mathcal{P}}$ be an element of $\mathcal{D}(H)$. Let $v \colon \mathbb{F}_p^* \to H$ be the homomorphism $\gamma \mapsto e_{\mathbb{Z}/p\mathbb{Z}}(\gamma\cdot)$ where we write $\gamma\cdot$ for the multiplication by γ. Now $e_{\mathbb{Z}/p\mathbb{Z}}$ is equal to $v \circ \det_{\mathbb{Z}/p\mathbb{Z}}$, so by Lemma 3.5, we have $e = v \circ \det$. This completes the proof. □

Theorem 1.4 applied to finite-dimensional vector spaces over finite prime fields shows that the maps $\det_V$ generalize the usual determinant. Therefore we shall refer to the maps $\det_V$ as *determinants*.

4 The epsilon maps

Let p be a prime number. Let G be a finite group equipped with a normal p-subgroup V. Let $\mathcal{S}_G$ be the class of G-sets on which the induced action by V is transitive.

Proposition 4.1. *There is a unique system of group homomorphisms $\epsilon = (\epsilon_X \colon G \to \mathbb{F}_p^*)_{X \in \mathcal{S}_G}$ with the property that for all $X \in \mathcal{S}_G$, $x \in X$ and σ in the stabilizer G_x of x, one has*

$$\epsilon_X(\sigma) = \frac{\det_V(\sigma_*)}{\det_{V_x}(\sigma_*)}$$

where σ_* denotes the action of σ on the relevant group by conjugation.

A proof of Proposition 4.1 is given after the following lemma.

Lemma 4.2. *Let F be a finite group of order coprime to p. Let $X \in \mathcal{S}_G$ and $x \in X$. Then the map $\mathrm{Hom}(G, F) \to \mathrm{Hom}(G_x, F)$ that sends a homomorphism $G \to F$ to its restriction to G_x is bijective.*

Proof. The subgroup V_x is normal in G_x, as it is the kernel of the map $G_x \to G/V$. Because V and V_x are p-groups and F is of order coprime to p, the natural maps $\mathrm{Hom}(G/V, F) \to \mathrm{Hom}(G, F)$, $\bar{\rho}$ to $g \mapsto \bar{\rho}(gV)$ and $\mathrm{Hom}(G_x/V_x, F) \to \mathrm{Hom}(G_x, F)$, $\bar{\tau}$ to $h \mapsto \bar{\tau}(hV_x)$ are bijective. Since V acts transitively, the inclusion induces a bijection $V/V_x \to G/G_x$. The homomorphism $G_x/V_x \to G/V$ defined by $\sigma V_x \mapsto \sigma V$ is therefore an isomorphism, which induces a bijection $\mathrm{Hom}(G/V, F) \to \mathrm{Hom}(G_x/V_x, F)$ Composing these three bijections between Hom-sets yields a bijection

$$\mathrm{Hom}(G, F) \to \mathrm{Hom}(G_x, F).$$

For $v \in \mathrm{Hom}(G, F)$ and $\sigma \in G_x$, the image of v under this bijection sends σ to $v(\sigma)$. This proves Lemma 4.2. □

Proof of Proposition 4.1. Let $X \in \mathcal{S}_G$ and $x \in X$, then the map $G_x \to \mathbb{F}_p^*$ defined by $\sigma \mapsto \frac{\det_V(\sigma_*)}{\det_{V_x}(\sigma_*)}$ is easily verified to be a group homomorphism. By Lemma 4.2, there is a unique group homomorphism $\epsilon_X \colon G \to \mathbb{F}_p^*$ that restricts to the given map. Let $y \in X$ and let $v \in V$ with $vx = y$, which is possible because V acts transitively on X. For $\sigma \in G_y$, the element $\sigma' = v^{-1}\sigma v$ of G stabilizes x. Since the image of ϵ_X is abelian, we have $\epsilon_X(\sigma) = \epsilon_X(v)\epsilon_X(\sigma')\epsilon_X(v^{-1}) = \epsilon_X(\sigma')$. Moreover, conjugation by v defines an isomorphism $v_* \colon V_x \to V_y$ and $v_* \colon V \to V$, and $v_* \circ \sigma'_* = \sigma_* \circ v_*$. The formula (3.2) yields

$$\epsilon_X(\sigma) = \epsilon_X(\sigma') = \frac{\det_V(\sigma'_*)}{\det_{V_x}(\sigma'_*)} = \frac{\det_V(\sigma_*)}{\det_{V_y}(\sigma_*)}.$$

Hence ϵ_X does not depend on x. This proves Proposition 4.1. □

We finish this section with some properties of ϵ.

Proposition 4.3. *Let $X \in \mathcal{S}_G$ and let $\phi \colon G \to \mathrm{Sym}(X)$ be the action of G on X. Let f be a surjective group homomorphism with domain G and let $\psi \colon f(G) \to \mathrm{Sym}(X)$ be such that $\phi = \psi \circ f$. Then for all $\sigma \in G$,*

$$\epsilon_X(\sigma) = \epsilon'_X(f(\sigma)),$$

where ϵ'_X is the group homomorphism associated to the action ψ of $f(G)$ on X and the subgroup $f(V)$ of $f(G)$ by Proposition 4.1.

Proof. By Lemma 4.2, it suffices to prove the statement for elements $\sigma \in G_x$, for some $x \in X$. So let $x \in X$ and $\sigma \in G_x$. Then by definition, $\epsilon_X(\sigma) = \frac{\det_V(\sigma_*)}{\det_{V_x}(\sigma_*)}$. Apply (3.2) to the short exact sequence defined by $f|_V$ and $f|_{V_x}$, then we obtain

$$\frac{\det_V(\sigma_*)}{\det_{V_x}(\sigma_*)} = \frac{\det_{\ker(f)\cap V}(\sigma_*)\det_{f(V)}(f\sigma_*)}{\det_{\ker(f)\cap V_x}(f\sigma_*)\det_{f(V_x)}(\sigma_*)}.$$

Any element of $\ker(f)$ acts trivially on X. In particular, all elements of $\ker(f)\cap V$ stabilize x, so $\ker(f)\cap V = \ker(f)\cap V_x$, and hence, $\det_{\ker(f)\cap V_x}(f\sigma_*)$ is equal to $\det_{\ker(f)\cap V}(f\sigma_*)$, and the proposition follows. □

5 Local fields

A local ring A with maximal ideal $\mathfrak{p}$ is called *Henselian* if for every polynomial $f \in A[X]$ with leading coefficient 1 and every $a \in A$ with $f(a) \in \mathfrak{p}$, $f'(a) \notin \mathfrak{p}$, where f' denotes the derivative of f, there exists $b \in a + \mathfrak{p}$ with $f(b) = 0$, see [1, Chapter III, Section 4]. One easily verifies that such an element b is necessarily unique.

Let K be a field. A *valuation ring* of K is a subring A of K with the property that for every $x \in K$ with $x \notin A$ one has $x^{-1} \in A$. Each valuation ring of K is a local ring [4, Corollary 6.4].

In the present paper, a *local field* is a field K equipped with a *Henselian* valuation ring A of K. It is well known that a valuation ring A of K is Henselian if and only if for every algebraic field extension L of K, the integral closure B of A in L is local [4, Chapter III, Corollary 13.5 and 16.6]. If that is the case, then B is automatically itself a Henselian valuation ring of L, and it is the only valuation ring of L that intersects K in A, by [4, Chapter III, 13.6 and 13.5]. Traditional examples of local fields include the field $\mathbb{Q}_p$ of p-adic numbers together with the ring $\mathbb{Z}_p$ of p-adic integers, the fields $k((T))$ of Laurent series over a field k with the ring $k[[T]]$, and their finite extensions. Our much broader notion, including arbitrary algebraic extensions of traditional local fields, reflects the generality in which our results are valid.

Let K be a field and let A be a valuation ring of K. We denote by $\mathfrak{p}$ the maximal ideal of A. The field $A/\mathfrak{p}$ is called the *residue field*, and its characteristic p is called the *residue characteristic* of K. A *fractional ideal* of A in K is an A-submodule of K generated by a single non-zero element. The abelian group $\mathcal{I}_K$ of fractional ideals under multiplication is linearly ordered by inclusion, so $\mathcal{I}_K$ is torsion-free. The groups $\mathcal{I}_K$ and K^*/A^* are isomorphic via $aA \mapsto aA^*$. For an algebraic extension L of K with a valuation ring B satisfying $B \cap K = A$, there is a natural embedding of ordered abelian groups $\mathcal{I}_K \to \mathcal{I}_L$ defined by $aA \mapsto aB$; using this embedding we will identify $\mathcal{I}_K$ with a subgroup of $\mathcal{I}_L$.

The group homomorphism $A^* \to (A/\mathfrak{p})^*$ induced by the natural map $A \to A/\mathfrak{p}$ is surjective, and its kernel is $1+\mathfrak{p}$. Thus $1+\mathfrak{p}$ is a subgroup of K^*. We are especially interested in the group $K^*/(1+\mathfrak{p})$. Clearly, there is an exact sequence

$$1 \to (A/\mathfrak{p})^* \to K^*/(1+\mathfrak{p}) \to \mathcal{I}_K \to 1. \tag{5.1}$$

The elements of $K^*/(1+\mathfrak{p})$ that map to a given element $\mathfrak{a} \in \mathcal{I}_K$ are precisely the cosets $b\cdot(1+\mathfrak{p})$ with $b \in \mathfrak{a}$ and $b \notin \mathfrak{a}\mathfrak{p}$; since such a coset $b\cdot(1+\mathfrak{p})$ coincides with the additive coset $b+\mathfrak{a}\mathfrak{p}$ of K, this yields an equality of sets

$$K^*/(1+\mathfrak{p}) = \bigcup_{\mathfrak{a}\in\mathcal{I}_K} (\mathfrak{a}/\mathfrak{a}\mathfrak{p})^\circ, \tag{5.2}$$

the union being disjoint, and the notation $^\circ$ being as declared in the introduction. If the residue characteristic p is positive, then $\mathbb{F}_p^*$ is a subgroup of $(A/\mathfrak{p})^*$. The exact sequence above shows that $\mathbb{F}_p^*$ may also be viewed as a subgroup of $K^*/(1+\mathfrak{p})$.

Proposition 5.3. *Let K be a local field with positive residue characteristic p. Then:*

(i) *for each $m \in \mathbb{Z}$ coprime to p, the map $1+\mathfrak{p} \to 1+\mathfrak{p}$ sending ζ to ζ^m is a group automorphism;*

(ii) *for each $\lambda \in K^*$ and each $\theta \in K^*/(1+\mathfrak{p})$ with $\lambda \cdot (1+\mathfrak{p}) = \theta^{p-1}$ there is a unique element $\eta \in K^*$ with $\eta \cdot (1+\mathfrak{p}) = \theta$ and $\eta^{p-1} = \lambda$;*

(iii) *the group of $(p-1)$st roots of unity in K^* has order $p-1$, and under the natural map $K^* \to K^*/(1+\mathfrak{p})$ it maps isomorphically to the subgroup $\mathbb{F}_p^*$ of $K^*/(1+\mathfrak{p})$.*

Proof. Our definition of Henselian shows that for each $\lambda \in 1+\mathfrak{p}$ and for each $m \in \mathbb{Z}$, $m \notin p\mathbb{Z}$, the polynomial $f = X^{|m|} - \lambda$ has a unique zero in $1+\mathfrak{p}$, which implies (i).

Part (ii) follows from (i), because θ^{p-1}/λ has a unique $(p-1)$-st root in $1+\mathfrak{p}$.

Applying (ii) with $\lambda = 1$ and θ equal to a generator of the subgroup $\mathbb{F}_p^*$ of $K^*/(1+\mathfrak{p})$ one finds that K^* has a subgroup mapping isomorphically to $\mathbb{F}_p^*$ under the map $K^* \to K^*/(1+\mathfrak{p})$. Since $X^{p-1}-1$ has no more than $p-1$ zeros in K, this subgroup must be the group of $(p-1)$st roots of unity in K^*. This proves (iii) and completes this proof of Proposition 5.3. □

Using Proposition 5.3(iii) we shall identify the group of $(p-1)$st roots of unity in K^* with $\mathbb{F}_p^*$.

6 Totally wild extensions

In this section, let K be a local field with valuation ring A, as defined in the previous section. Let $\mathfrak{p}$ be the maximal ideal of A, and let p be the characteristic of $A/\mathfrak{p}$.

Let L be a finite extension of K, let B be the integral closure of A in L, and let $\mathfrak{q}$ be the maximal ideal of B. We write $f(L/K)$ for the field extension degree $[B/\mathfrak{q} : A/\mathfrak{p}]$. The *ramification index* of L over K is the group index $e(L/K) = (\mathcal{I}_L : \mathcal{I}_K)$. According to a Lemma of Ostrowski [8, Section 38; 5, Chapter I, Proposition 7.1], one has

$$[L:K] = d(L/K)e(L/K)f(L/K) \tag{6.1}$$

for some $d(L/K) \in \mathbb{Z}$ called the *defect* of L over K. If p is positive, $d(L/K)$ is a power of p, and if $p = 0$ then $d(L/K) = 1$. The extension L of K is called *tame* if

$$d(L/K) = 1,\ e(L/K) \not\equiv 0 \bmod p, \text{ and } B/\mathfrak{q} \text{ is separable over } A/\mathfrak{p}.$$

If L is tame over K and M is tame over L, then M is tame over K. If $p = 0$, then every finite extension is tame. If p is non-zero, we call L *totally wild* over K if

$$e(L/K) \text{ is a power of } p \text{ and } B/\mathfrak{q} \text{ is purely inseparable over } A/\mathfrak{p};$$

if $p = 0$, then L is totally wild over K if and only if $L = K$. Clearly, the degree of a totally wild extension is a power of p. The extension L over K is totally wild if and only if the only subextension of L over K that is tame is K itself [3]. If L is

purely inseparable over K, then L is totally wild over K. Generally, L is totally wild over K if and only if the maximal intermediate field of L over K that is separable over K is totally wild over K; in the separable case, Proposition 6.3 below gives a Galois-theoretic criterion for total wildness.

Let M be a finite Galois extension of K, and G the Galois group of M over K. Let C be the integral closure of A in M, and $\mathfrak{r}$ its maximal ideal. We define the *ramification group* V of M over K to be the kernel of the map $G \to \mathrm{Aut}(M^*/(1+\mathfrak{r}))$ induced by the action of G on M. The ramification group is normal in G, it is a p-group if $p > 0$, and if $p = 0$ it is trivial [5, Chapter I, Theorem 3.6].

Proposition 6.2. *Let L be a finite extension of K. Then there exists a unique maximal subextension L_t of L that is tame over K. If L' is a subextension of L over K, then $L'_\mathrm{t} = L_\mathrm{t} \cap L'$. If M is Galois over K, then M_t is the fixed field of V in M.*

Proof. [5, Chapter I, Theorem 3.15]. □

Proposition 6.3. *Let L be a finite separable extension of K. Let M be a finite Galois extension of K such that the set X of field embeddings $L \to M$ that are the identity on K is non-empty. Let $x \in X$ and let G and H be the Galois groups of M over K and M over xL respectively. Then the following are equivalent:*

(i) *the field L is totally wild over K;*

(ii) *one has $G = V \cdot H$;*

(iii) *$\#(V/(V \cap H)) = [L : K]$;*

(iv) *the natural action of V on X is transitive.*

Proof. By Proposition 6.2, the field L_t is the intersection of L (the fixed field of H) with the fixed field of V in M. The extension L of K is totally wild if and only if L_t is equal to K. Thus, L is totally wild over K if and only if $V \cdot H = G$. We may identify the set X with the set G/H, so $\#X = [L : K]$. It is immediate that $H \cdot V = G$ is equivalent to (iii) and to (iv). The proposition follows. □

We end the present section with two auxiliary result on totally wild extensions.

Proposition 6.4. *Let M be a finite Galois extension of K, let C be the integral closure of A in M, and $\mathfrak{r}$ the maximal ideal of C. Then:*

(i) *the natural action of G on the group $\mathcal{I}_M$ of fractional C-ideals is trivial;*

(ii) *for each fractional C-ideal $\mathfrak{a}$ the natural action of V on the group $\mathfrak{a}/\mathfrak{a}\mathfrak{r}$ is trivial.*

Proof. Let $\sigma \in G$ and $\mathfrak{a} \in \mathcal{I}_M$. Since $\mathcal{I}_M$ is torsion-free, and $\mathcal{I}_M/\mathcal{I}_K$ is finite and thus torsion, we have $\sigma(\mathfrak{a})/\mathfrak{a} = C$ in $\mathcal{I}_M$. This proves (i).

Using the short exact sequence (5.2) and (i), it is immediate that V acts trivially on $(\mathfrak{a}/\mathfrak{a}\mathfrak{r})^\circ$. This finishes this proof of Proposition 6.4. □

Proposition 6.5. *Let L be a finite, totally wild field extension of K and let m be an integer coprime to p. Then the norm map $\mathrm{N}_{L/K} \colon L^* \to K^*$ and the inclusion $\iota_{L/K} \colon K^* \to L^*$ induce group isomorphisms*

$$L^*/L^{*m} \to K^*/K^{*m} \text{ and } K^*/K^{*m} \to L^*/L^{*m}.$$

Moreover, if $[L : K] \equiv 1 \bmod m$ then these isomorphisms are mutually inverse.

Proof. If $p = 0$, the statement is trivial, because in this case the only totally wild extension of K is K itself. Assume $p > 0$. The composition of the inclusion $K^* \to L^*$ and the norm $L^* \to K^*$ is the map $K^* \to K^*$ sending each $\lambda \in K^*$ to $\lambda^{[L:K]}$.

If L is purely inseparable over K, then the composition of the norm $L^* \to K^*$ with the inclusion $K^* \to L^*$ again maps each $\lambda \in L^*$ to $\lambda^{[L:K]}$.

Next, suppose L is separable over K. Let M be a finite Galois extension of K containing L. Let V be the ramification group of M over K, let H be the Galois group of M over L and write W for $V \cap H$. Then the composition of the norm map $\mathrm{N}_{L/K} \colon L^* \to K^*$ with the inclusion $\iota_{M/K} \colon K^* \subseteq M^*$ sends each $y \in L^*$ to $\prod_{\tau W \in V/W} \tau(y) \in M^*$. The definition of V shows that V acts trivially on the group $M^*/(1+\mathfrak{r})$. So $\iota_{M/K} \circ \mathrm{N}_{L/K}$ induces the map $L^* \to M^*/(1+\mathfrak{r})$, $y \mapsto y^{[L:K]} \cdot (1+\mathfrak{r})$; since $\mathfrak{q} = \mathfrak{r} \cap L$, we obtain that $\iota_{L/K} \circ \mathrm{N}_{L/K}$ induces the map $\lambda \mapsto \lambda^{[L:K]}$ on $L^*/(1+\mathfrak{q})$. By Proposition 5.3 applied to m and L, every element of $(1+\mathfrak{q})$ is an m-th power, so the induced map on L^*/L^{*m} is exactly defined by $\lambda \mapsto \lambda^{[L:K]}$.

In the general case, we write L as a purely inseparable extension of a separable extension L' of K. In this case, the norm $\mathrm{N}_{L/K} = \mathrm{N}_{L'/K} \circ \mathrm{N}_{L/L'}$ and the inclusion map $\iota_{L/L'} \circ \iota_{L'/K}$ induce the map $\lambda \mapsto (\lambda^{[L:L']})^{[L':K]} = \lambda^{[L:K]}$ on L^*/L^{*m}.

Since m is coprime to p and $[L : K]$ is a power of p, the maps defined by $\lambda \mapsto \lambda^{[L:K]}$ are automorphisms of K^*/K^{*m} and L^*/L^{*m} respectively, thus, the norm and inclusion induce isomorphisms $L^*/L^{*m} \to K^*/K^{*m}$ and $K^*/K^{*m} \to L^*/L^{*m}$ respectively. If moreover $[L : K] \equiv 1 \bmod m$, then these maps are the identity on their domain, which proves the proposition. □

7 Constructing a root of the discriminant

In this section, K is a local field of residue characteristic $p > 2$, and L a finite, separable, totally wild extension of K. Let n be defined by $[L : K] = p^n$. Write A for the Henselian valuation ring of K, and B for the integral closure of A in L. Fix a finite Galois extension M of K containing L, and denote by C the integral closure of A in M. Let $\mathfrak{r}$ be the maximal ideal of C. The Galois group of M over K is denoted by G and the ramification group by V. By Proposition 6.3, the group V acts transitively on the set X of ring homomorphisms $L \to M$ that are the identity on K, so $X \in \mathcal{S}_G$. From Proposition 4.1, we obtain the homomorphism $\epsilon_X \colon G \to \mathbb{F}_p^*$. Choose $\alpha \in L$ such that $K(\alpha) = L$. We denote the Galois group of M over L by H. Let $\iota_{M/L} \colon L \to M$ denote the inclusion map, viewed as an element of X. The stabilizer of $\iota_{M/L}$ in G is exactly $H \subseteq G$. Write f for the irreducible polynomial of α over K. Write $\Delta(\alpha)$ for the discriminant of f.

Proposition 7.1. *In the situation above, there exists $\delta(\alpha) \in M$ such that*

(i) $\delta(\alpha)^{p-1} = (-1)^{n(p+1)/2} \cdot \Delta(\alpha)$, *and*

(ii) *for each $\sigma \in G$ one has $\sigma(\delta(\alpha))/\delta(\alpha) = \epsilon_X(\sigma)$.*

The setup for proving Proposition 7.1 will take up most of this section; a proof is given after Lemma 7.4. We give a number of definitions that depend on α. The set J is defined by

$$J = \{\mathfrak{j} \subseteq M : \text{ there exists } \tau \in G \text{ such that } \mathfrak{j} = (\alpha - \tau\alpha) \cdot C\}.$$

Clearly, J is finite and non-empty, and because C is a valuation ring, J is totally ordered by inclusion. The minimal element of J equals (0), and the maximal element

$\max J$ equals $\sum_{\tau\in G}(\alpha-\tau\alpha)\cdot C$. To simplify notation, we will write $J^\circ = J\setminus\{(0)\}$. For $\mathfrak{j}\in J^\circ$, we denote by $\mathfrak{j}'$ the predecessor of $\mathfrak{j}$ in J. For any $\mathfrak{j}\in J$, we write

$$G_\mathfrak{j} = \{\tau\in G : \alpha-\tau\alpha\in\mathfrak{j}\},\ V_\mathfrak{j} = V\cap G_\mathfrak{j}.$$

For example, one has $G_{\max J} = G$, $V_{\max J} = V$, $G_{(0)} = H$, and $V_{(0)} = V\cap H$. By Proposition 6.4(i), each $G_\mathfrak{j}$ is a subgroup of G, and each $G_\mathfrak{j}$ contains H. Since V is normal in G, each $V_\mathfrak{j}$ is a subgroup of V that is normalized by $G_\mathfrak{j}$ and therefore also by the subgroup H of $G_\mathfrak{j}$.

Until Lemma 7.3, we fix an element $\mathfrak{j}\in J^\circ$. We define the map $c\colon V_\mathfrak{j}\to\mathfrak{j}/\mathfrak{j}\cdot\mathfrak{r}$ by $c(\tau) = (\alpha-\tau\alpha \bmod \mathfrak{j}\cdot\mathfrak{r})$. From Proposition 6.4(ii) it follows that c is a group homomorphism. An element $\tau\in V_\mathfrak{j}$ belongs to the kernel of c if and only if $\alpha-\tau\alpha\in\mathfrak{j}\cdot\mathfrak{r}$. Since $\mathfrak{j}$ is isomorphic to C as a C-module, $\mathfrak{j}\cdot\mathfrak{r}$ is a proper C-submodule of $\mathfrak{j}$ that contains each proper C-submodule of $\mathfrak{j}$. Thus, for $\tau\in V_\mathfrak{j}$, one has $\alpha-\tau\alpha\in\mathfrak{j}\cdot\mathfrak{r}$ if and only if $(\alpha-\tau\alpha)\cdot C$ is properly contained in $\mathfrak{j}$; By definition of $\mathfrak{j}'$ this occurs if and only if $\alpha-\tau\alpha\in\mathfrak{j}'$. This proves $\ker c = V_{\mathfrak{j}'}$, so $V_{\mathfrak{j}'}$ is a normal subgroup of $V_\mathfrak{j}$. Since $\mathfrak{j}/\mathfrak{j}\cdot\mathfrak{r}$ is a vector space over the field $C/\mathfrak{r}$ of characteristic p, the group $V_\mathfrak{j}/V_{\mathfrak{j}'}$ is naturally a vector space over $\mathbb{F}_p$. We write $V_\mathfrak{j}/V_{\mathfrak{j}'}$ multiplicatively, so $\mathbb{F}_p$ acts on it via scalar exponentiation, while $\mathfrak{j}/\mathfrak{j}\cdot\mathfrak{r}$ is written additively, and $\mathbb{F}_p$ acts on it by scalar multiplication.

The group H acts on $V_\mathfrak{j}/V_{\mathfrak{j}'}$ by conjugation, so $V_\mathfrak{j}/V_{\mathfrak{j}'}$ is an H-module. For $\sigma\in H$, we write σ_* for the conjugation action of σ on $V_\mathfrak{j}$, $V_{\mathfrak{j}'}$, and $V_\mathfrak{j}/V_{\mathfrak{j}'}$. Let $\sigma\in H$. Then we have $\sigma\alpha=\alpha$, so for each $\tau\in V_\mathfrak{j}$ one has $\alpha-\sigma\tau\sigma^{-1}\alpha = \sigma(\alpha-\tau\alpha)$. It follows that the injective map $c\colon V_\mathfrak{j}/V_{\mathfrak{j}'}\to\mathfrak{j}/\mathfrak{j}\cdot\mathfrak{r}$ induced by c is H-linear. It maps the set $(V_\mathfrak{j}/V_{\mathfrak{j}'})^\circ$ of non-identity elements of $V_\mathfrak{j}/V_{\mathfrak{j}'}$ to the set $(\mathfrak{j}/\mathfrak{j}\cdot\mathfrak{r})^\circ$ of non-zero elements of $\mathfrak{j}/\mathfrak{j}\cdot\mathfrak{r}$, which by (5.2) is a subset of the multiplicative group $M^*/(1+\mathfrak{r})$.

Let $n_\mathfrak{j}$ be the dimension of $V_\mathfrak{j}/V_{\mathfrak{j}'}$ as an $\mathbb{F}_p$-vector space, which is finite because $V\subseteq G$ is finite, and let $S_\mathfrak{j}$ be a section of $(V_\mathfrak{j}/V_{\mathfrak{j}'})^\circ$ under $\mathbb{F}_p^*$.

Lemma 7.2. *Let $\theta_\mathfrak{j}$ be the element $\prod_{\tau\in S_\mathfrak{j}} c(\tau)$ of $M^*/(1+\mathfrak{r})$. Then we have*

(i) $\theta_\mathfrak{j}^{p-1} = (-1)^{n_\mathfrak{j}}\cdot\displaystyle\prod_{\rho\in(V_\mathfrak{j}/V_{\mathfrak{j}'})^\circ} c(\rho)$ *in* $M^*/(1+\mathfrak{r})$,

(ii) *for each $\sigma\in H$ one has*

$$\frac{\sigma(\theta_\mathfrak{j})}{\theta_\mathfrak{j}} = \det_{V_\mathfrak{j}/V_{\mathfrak{j}'}}(\sigma_*)$$

in the group $\mathbb{F}_p^*\subseteq(C/\mathfrak{r})^*\subseteq M^*/(1+\mathfrak{r})$.

Proof. Each $\rho\in(V_\mathfrak{j}/V_{\mathfrak{j}'})^\circ$ can be written uniquely as $\rho=\tau^\gamma$, with $\tau\in S_\mathfrak{j}$ and $\gamma\in\mathbb{F}_p^*$. Therefore one has

$$\prod_{\rho\in(V_\mathfrak{j}/V_{\mathfrak{j}'})^\circ} c(\rho) = \prod_{\gamma\in\mathbb{F}_p^*}\prod_{\tau\in S_\mathfrak{j}} c(\tau^\gamma).$$

Since c is a morphism of $\mathbb{F}_p^*$-sets, we have $c(\tau^\gamma)=\gamma c(\tau)$. In $\mathbb{F}_p$, one has $\prod_{\gamma\in\mathbb{F}_p^*}\gamma = -1$. We thus see

$$\prod_{\rho\in(V_\mathfrak{j}/V_{\mathfrak{j}'})^\circ} c(\rho) = \prod_{\tau\in S_\mathfrak{j}} -c(\tau)^{p-1} = (-1)^{\#S_\mathfrak{j}}\theta_\mathfrak{j}^{p-1}.$$

The order of the $\mathbb{F}_p$-vector space $V_\mathfrak{j}/V_{\mathfrak{j}'}$ is $p^{n_\mathfrak{j}}$, so $\#(V_\mathfrak{j}/V_{\mathfrak{j}'})^\circ = p^{n_\mathfrak{j}}-1$. Since p is odd, one has

$$\#S_\mathfrak{j} = \frac{p^{n_\mathfrak{j}}-1}{p-1} = p^{n_\mathfrak{j}-1}+\cdots+p+1\equiv n_\mathfrak{j} \bmod 2.$$

This proves Lemma 7.2(i).

For $\tau \in S_{\mathfrak{j}}$, there exist $\tau' \in S_{\mathfrak{j}}$ and $\gamma_\tau \in \mathbb{F}_p^*$ such that $\sigma(c(\tau)) \in \gamma_\tau c(S)$. We also have $\sigma_*(\tau) \in \gamma_\tau S$. The mapping $\tau \mapsto \tau'$ is a permutation of $S_{\mathfrak{j}}$, so

$$\det_{V_{\mathfrak{j}}/V_{\mathfrak{j}'}}(\sigma_*) = \prod_{\tau \in S_{\mathfrak{j}}} \gamma_\tau = \prod_{\tau \in S_{\mathfrak{j}}} \frac{\sigma(c(\tau))}{c(\tau')} = \frac{\sigma(\theta_{\mathfrak{j}})}{\theta_{\mathfrak{j}}}.$$

This concludes this proof of Lemma 7.2. □

Let f' be the derivative of f.

Lemma 7.3. *Let*

$$\theta = \prod_{\mathfrak{j} \in J^\circ} \theta_{\mathfrak{j}}^{\#(V_{\mathfrak{j}'}/V_{(0)})} \in M^*/(1+\mathfrak{r}).$$

Then the following holds in the group $M^*/(1+\mathfrak{r})$:

(i) $\theta^{p-1} = (-1)^n \cdot f'(\alpha) \cdot (1+\mathfrak{r})$,

(ii) *for each $\sigma \in H$ one has $\sigma(\theta)/\theta = \epsilon_X(\sigma)$.*

Proof. Since $V_{(0)}$ is the stabilizer of α under V, we have

$$f = \prod_{\rho \in V/V_{(0)}} (X - \rho(\alpha)), \quad f'(\alpha) = \prod_{\rho \in (V/V_{(0)}) \setminus \{V_{(0)}\}} (\alpha - \rho(\alpha)).$$

For $\mathfrak{j} \in J^\circ$ and $\tau \in V_{\mathfrak{j}} \setminus V_{\mathfrak{j}'}$, the coset $(\alpha - \tau(\alpha)) \cdot (1+\mathfrak{r})$ is equal to $c(\tau)$, and this value depends only on the coset $\tau V_{\mathfrak{j}'}$. Hence in $M^*/(1+\mathfrak{r})$, we have

$$f'(\alpha) \cdot (1+\mathfrak{r}) = \prod_{\mathfrak{j} \in J^\circ} \prod_{\tau V_{(0)} \in (V_{\mathfrak{j}} \setminus V_{\mathfrak{j}'})/V_{(0)}} c(\tau) = \prod_{\mathfrak{j} \in J^\circ} \prod_{\rho \in (V_{\mathfrak{j}}/V_{\mathfrak{j}'})^\circ} c(\rho)^{\#(V_{\mathfrak{j}'}/V_{(0)})}.$$

One has

$$p^{\sum_{\mathfrak{j} \in J^\circ} n_{\mathfrak{j}}} = \prod_{\mathfrak{j} \in J^\circ} \#(V_{\mathfrak{j}}/V_{\mathfrak{j}'}) = \#(V/V_{(0)}) = p^n.$$

Since $\#(V_{\mathfrak{j}'}/V_{(0)}) \equiv 1 \bmod 2$, Lemma 7.2(i) yields

$$(-1)^n f'(\alpha) \cdot (1+\mathfrak{r}) = \prod_{\mathfrak{j} \in J^\circ} (-1)^{n_{\mathfrak{j}}} \prod_{\rho \in (V_{\mathfrak{j}}/V_{\mathfrak{j}'})^\circ} c(\rho)^{\#(V_{\mathfrak{j}'}/V_{(0)})} = \prod_{\mathfrak{j} \in J^\circ} \theta_{\mathfrak{j}}^{(p-1)\cdot\#(V_{\mathfrak{j}'}/V_{(0)})} = \theta^{p-1}.$$

This proves Lemma 7.3(i).

For $\sigma \in H$, we use Lemma 7.2(ii) and the fact that $\#(V_{\mathfrak{j}}/V_{(0)}) \equiv 1 \bmod p-1$ to obtain

$$\frac{\sigma(\theta)}{\theta} = \prod_{\mathfrak{j} \in J^\circ} \left(\frac{\sigma(\theta_{\mathfrak{j}})}{\theta_{\mathfrak{j}}}\right)^{\#(V_{\mathfrak{j}'}/V_{(0)})} = \prod_{\mathfrak{j} \in J^\circ} \det_{V_{\mathfrak{j}}/V_{\mathfrak{j}'}}(\sigma_*)^{\#(V_{\mathfrak{j}'}/V_{(0)})} = \prod_{\mathfrak{j} \in J^\circ} \det_{V_{\mathfrak{j}}/V_{\mathfrak{j}'}}(\sigma_*)$$

Using (3.2), we see that

$$\prod_{\mathfrak{j} \in J^\circ} \det_{V_{\mathfrak{j}}/V_{\mathfrak{j}'}}(\sigma_*) = \frac{\det_V(\sigma_*)}{\det_{V_{(0)}}(\sigma_*)} = \epsilon_X(\sigma).$$

This proves Lemma 7.3. □

Lemma 7.4. *There exists $\eta \in M^*$ such that*

(i) $\eta^{p-1} = (-1)^n \cdot f'(\alpha)$,

(ii) *for each* $\sigma \in H$ *one has* $\sigma(\eta)/\eta = \epsilon_X(\sigma)$ *in* M^*.

Proof. Proposition 5.3(ii), with $(-1)^n f'(\alpha)$, M^*, $\mathfrak{r}$, and the element θ from Lemma 7.3 in the roles of λ, K^*, $\mathfrak{p}$, and θ, yields a unique element $\eta \in M^*$ with $\eta \cdot (1+\mathfrak{r}) = \theta$ and $\eta^{p-1} = (-1)^n f'(\alpha)$. This element satisfies (i), and we will now prove that it also satisfies (ii). Let $\sigma \in H$. Because $f'(\alpha)$ is an element of L, we have $\sigma(\eta^{p-1}) = \eta^{p-1}$. Therefore $\frac{\sigma(\eta)}{\eta}$ is a $(p-1)$st root of unity. By Lemma 7.3(ii) one has $\frac{\sigma(\eta)}{\eta} \cdot (1+\mathfrak{r}) = \epsilon_X(\sigma) \in M^*/(1+\mathfrak{r})$. Thus, by Proposition 5.3(iii), one has $\frac{\sigma(\eta)}{\eta} = \epsilon_X(\sigma)$. This proves Lemma 7.4. □

Proof of Proposition 7.1. Let $\mathrm{N}\colon L \to K$ denote the norm map. One has

$$\mathrm{N}(f'(\alpha)) = (-1)^{p^n(p^n-1)/2}\Delta(\alpha).$$

Since p is odd, one obtains

$$\mathrm{N}((-1)^n f'(\alpha)) = (-1)^{np^n}\,\mathrm{N}(f'(\alpha))$$
$$= (-1)^{np^n}(-1)^{p^n(p^n-1)/2}\Delta(\alpha) = (-1)^{n(p+1)/2}\Delta(\alpha).$$

By Proposition 6.5 applied to $m = p-1$, one has $\mathrm{N}(\lambda) \in \lambda L^{*p-1}$ for every $\lambda \in L^*$. Therefore, there exists $\zeta \in L^*$ such that $\mathrm{N}((-1)^n f'(\alpha)) = (-1)^n f'(\alpha)\zeta^{p-1}$. One obtains

$$(-1)^{n(p+1)/2}\Delta(\alpha) = (-1)^n f'(\alpha)\zeta^{p-1} = \eta^{p-1}\zeta^{p-1}$$

with η as in Lemma 7.4. Set $\delta(\alpha) = \eta\zeta$. Then $\delta(\alpha)$ satisfies 7.1(i). We prove that it also satisfies 7.1(ii). From $\delta(\alpha)^{p-1} = (-1)^{p^n(p^n-1)/2}\Delta(\alpha) \in K^*$ and Proposition 5.3(iii), it follows that the map $\sigma \mapsto \frac{\sigma(\delta(\alpha))}{\delta(\alpha)}$ is a homomorphism of groups $G \to \mathbb{F}_p^* \subseteq K^*$. For $\sigma \in H$, we have $\sigma(\zeta) = \zeta$ since ζ is an element of L; by Lemma 7.4(ii),

$$\frac{\sigma(\delta(\alpha))}{\delta(\alpha)} = \frac{\sigma(\eta\zeta)}{\eta\zeta} = \frac{\sigma(\eta)}{\eta} = \epsilon_X(\sigma).$$

By Lemma 4.2, there is a unique extension of the homomorphism $\epsilon_X|_H = (\sigma \mapsto \frac{\sigma(\delta(\alpha))}{\delta(\alpha)})$ to a homomorphism $G \to \mathbb{F}_p^*$. Hence ϵ_X and $\sigma \mapsto \frac{\sigma(\delta(\alpha))}{\delta(\alpha)}$ coincide on all of G. This proves Proposition 7.1. □

Proof of Theorem 1.2. As noted in the introduction, we may assume p to be odd, as we do in this section. Let $\alpha, \beta \in L$ be such that $K(\alpha) = L = K(\beta)$, and let $\delta(\alpha), \delta(\beta)$ be as in Proposition 7.1. From Proposition 7.1(ii), we see that for every $\sigma \in G$, we have

$$\frac{\sigma(\delta(\alpha))}{\delta(\alpha)} = \epsilon_X(\sigma) = \frac{\sigma(\delta(\beta))}{\delta(\beta)},$$

and therefore $\sigma(\delta(\alpha)/\delta(\beta)) = \delta(\alpha)/\delta(\beta)$. This implies that $\delta(\alpha)/\delta(\beta)$ is an element of K^*. Raising $\delta(\alpha)/\delta(\beta)$ the $(p-1)$st power and using Proposition 7.1(i), we find

$$(-1)^{n(p-1)/2}\Delta(\alpha) \cdot K^{*p-1} = (-1)^{n(p-1)/2}\Delta(\beta) \cdot K^{*p-1}.$$

This proves Theorem 1.2. □

Corollary 7.5. *The element* $(-1)^{n(p+1)/2} \cdot \Delta(\alpha)$ *of* K^* *has a* $(p-1)$*st root in the maximal tame subextension of any Galois closure of* L *over* K.

Proof. Let M be a Galois closure of L over K. The element $\delta(\alpha)$ is a zero of the polynomial $X^{p-1} - (-1)^{n(p+1)/2}\Delta(\alpha) \in K[X]$, so the degree $[K(\delta(\alpha)) : K]$ is at most $p-1$ and thus prime to p. Therefore $K(\delta(\alpha))$ is tame over K, by [5, Chapter I, Proposition 3.1]. This proves Corollary 7.5. □

8 Constructing an extension with given invariant

Let K be a local field of positive residue characteristic p with valuation ring A. Write $\mathfrak{p}$ for the maximal ideal of A. For an integer m and a group G, we say G is *m-divisible* if for each $g \in G$ there exists $h \in G$ such that $h^m = g$. Let

$$K_{\mathrm{f}} = \{a \in K : \text{ there exists } k \in \mathbb{Z}_{\geq 0} \text{ such that } ap^k, a^{-1}p^k \in A\},$$

which is a subgroup of K^*. It is immediate that $A^* \subseteq K_{\mathrm{f}}$. In this section, we assume that K^*/K_{f} is $(p-1)$-divisible and $K \neq A$. If K has characteristic p, then $p = 0$ in K and $K^* = K_{\mathrm{f}}$, so the first assumption is satisfied. Furthermore, if $\mathcal{I}_K \cong K^*/A^*$ is isomorphic as an ordered group to a subgroup of the additive group of real numbers, then the first assumption is also satisfied.

Theorem 8.1. *With the assumptions above, suppose $K_{\mathrm{f}}/(1+\mathfrak{p})$ is not p-divisible. Then the map*

$$\Phi\colon \mathcal{L}(K, p^n) \to K^*/K^{*p-1}$$

defined in the introduction is surjective for every positive integer n.

The remainder of this section is devoted to our proof of Theorem 8.1. As an immediate consequence, we obtain Theorem 1.3. Our general strategy for proving Theorem 8.1 is to construct elements of $\mathcal{L}(K, p^n)$ with a given invariant using polynomials of the form $T^{p^n} + aT + b$ for $a, b \in K^*$. We will begin with two lemmas on polynomials of this form. For g a polynomial, we write $\Delta(g)$ for the discriminant of g.

Lemma 8.2. *Let n be a positive integer, let $a, b \in K^*$, and let $g \in K[T]$ be the polynomial $T^{p^n} + aT + b$. If K has characteristic zero, assume $a^{p^n} \notin p^{np^n} b^{p^n-1} \cdot A$. Then*

$$\Delta(g) \in (-1)^{p^n(p^n-1)/2} a \cdot K^{*p-1}.$$

Proof. Swan [11, Theorem 2] gives the following formula:

$$\Delta(g) = (-1)^{p^n(p^n-1)/2}(p^{np^n} b^{p^n-1} + (1-p^n)^{p^n-1} a^{p^n}).$$

If K has characteristic p, then this formula reduces to

$$\Delta(g) = (-1)^{p^n(p^n-1)/2} \cdot a^{p^n},$$

which lies in $(-1)^{p^n(p^n-1)/2} a \cdot K^{*p-1}$.

If K has characteristic zero and $p^{np^n} b^{p^n-1} \notin a^{p^n} \cdot A$, then one has

$$x = \frac{p^{np^n} b^{p^n-1}}{(1-p^n)^{p^n-1} a^{p^n}} \in \mathfrak{p}.$$

By Proposition 5.3(i) applied to $m = p-1$, all elements of $1+\mathfrak{p}$ are $(p-1)$st powers. One computes

$$\Delta(g) = (-1)^{p^n(p^n-1)/2} \cdot (1+x) \cdot (1-p^n)^{p^n-1} a^{p^n}.$$

Thus $\Delta(g)$ is an element of $(-1)^{p^n(p^n-1)/2} \cdot a \cdot K^{*p-1}$. This proves the Lemma. □

Lemma 8.3. *Let n be a positive integer, and let $a, b \in K^*$ be such that*

(i) $b^{p^n-1} \notin a^{p^n} \cdot A$

(ii) $b \cdot (1+\mathfrak{p})$ *is not a* p*-th power in the group* $K^*/(1+\mathfrak{p})$.

Let α *in some extension field of* K *satisfy*

$$\alpha^{p^n} + a\alpha + b = 0.$$

Then $K(\alpha)$ *is a separable, totally wild extension of* K *of degree* p^n.

Proof. The field $K(\alpha)$ is separable over K, because if K has characteristic p, then the polynomial $T^{p^n} + aT + b$ and its derivative a are coprime in $K[T]$.

It is clear that $[K(\alpha) : K]$ is at most p^n. In this proof, let B be the integral closure of A in $K(\alpha)$, and let $\mathfrak{q}$ be the maximal ideal of B. The plan of this proof is to show that the ramification index $e = e(K(\alpha)/K)$ multiplied by the inseparability degree f_i of $B/\mathfrak{q}$ over $A/\mathfrak{p}$ is divisible by p^n. By the definition of totally wild and Ostrowski's lemma 6.1, that will clearly suffice.

The equation satisfied by α shows that the two largest of the fractional B-ideals $\alpha^{p^n} \cdot B$, $a\alpha \cdot B$, bB coincide. If $a\alpha \cdot B$ is one of these, then it contains α^{p^n} and b, so $(a\alpha)^{p^n} \cdot B = (a\alpha)(a\alpha)^{p^n-1} \cdot B$ contains $\alpha^{p^n} \cdot b^{p^n-1}$ and consequently $a^{p^n} \cdot B$ contains b^{p^n-1}; but $B \cap K = A$ then implies that $a^{p^n} \cdot A$ already contains b^{p^n-1}, contradicting (i). Thus we conclude that the two largest fractional ideals can only be $\alpha^{p^n} \cdot B$ and bB, and that $a\alpha$ belongs to $b\mathfrak{q}$. Thus the equation satisfied by α shows that we have

$$\alpha^{p^n} = -b \cdot (1+x) \text{ with } x \in \mathfrak{q}. \tag{8.4}$$

Let now k be the largest integer with $0 \le k \le n$ for which we can write $-b = c^{p^k} \cdot u$ with $c \in A$ and $u \in A^*$. (Note that for $k = 0$, we can take $c = b$ and $u = -1$.) Choose such c and u. We are going to show that e is divisible by p^{n-k} and f_i by p^k. That will do.

As for e, we may clearly assume $k < n$. Then the maximality of k implies that cA is not a p-th power in the group of fractional ideals $\mathcal{I}_K$. But $\alpha^{p^n} \cdot B = bB = (cB)^{p^k}$ shows that $\alpha^{p^{n-k}} \cdot B = cB$, so cB is a p^{n-k}-th power in $\mathcal{I}_{K(\alpha)}$. This implies that the cokernel of the natural map $\mathcal{I}_K \to \mathcal{I}_{K(\alpha)}$ has an element of order p^{n-k}, and therefore p^{n-k} divides e.

As for f_i, we may clearly assume $k > 0$. Then c^{p^k} is a p-th power in K^*, so condition (ii) implies that the element $u \in A^*$ with $-b = c^{p^k} \cdot u$ is not in $(A^*)^p \cdot (1+\mathfrak{p})$ or, equivalently, that the image $\bar{u}$ of u in the field $A/\mathfrak{p}$ is not a p-th power in that field. From (8.4), we see that the element $\beta = \alpha^{p^{n-k}}/c$ satisfies $\beta^{p^k} = u \cdot (1+x)$ with $x \in \mathfrak{q}$. Hence $\beta \in B^*$, and the image $\bar{\beta}$ of β in $B/\mathfrak{q}$ is a zero of the polynomial $T^{p^k} - \bar{u}$. By what we just proved about $\bar{u}$, it follows that $\bar{\beta}$ is purely inseparable of degree p^k over $A/\mathfrak{p}$. Hence f_i is divisible by p^k, as required. This completes our proof. □

We prove Theorem 8.1 in the case that K has characteristic p.

Lemma 8.5. *Suppose* K *has characteristic* p *and* $K^*/(1+\mathfrak{p})$ *is not* p*-divisible. Then the map* $\Phi\colon \mathcal{L}(K, p^n) \to K^*/K^{*p^{n-1}}$ *from the introduction is surjective.*

Proof. Fix a class $\xi \in K^*/K^{*p^{n-1}}$. Choose $b \in K^*$ such that $b \cdot (1+\mathfrak{p})$ is not a p-th power in $K^*/(1+\mathfrak{p})$. If $b \in A^*$, let $c \in K^* \setminus A^*$, which is possible because $K \ne A$, and multiply b by c^p to obtain $b(1+\mathfrak{p})$ not a p-th power in $K^*/(1+\mathfrak{p})$ and $b \notin A^*$. Choose $a \in K^*$ with $(-1)^{p^n(p^n-1)/2} a \in \xi$ and $b^{p^n-1} \notin a^{p^n} \cdot A$; for example, for $x' \in \xi$, one of $-x'b^{p-1}$, $-x'b^{1-p}$, $-x'^{-p}b^{p-1}$ and $-x'^{-p}b^{1-p}$ will do. Let α in some extension of K satisfy $\alpha^{p^n} + a\alpha + b = 0$. By Lemma 8.3, the extension L is totally wild and separable over K of degree p^n. By Lemma 8.2, the invariant associated to L is ξ. Lemma 8.5 follows. □

Until our proof of Theorem 8.1, suppose that K has characteristic zero. The strategy in characteristic zero follows the same lines as in characteristic p, but we need to be more careful when choosing the elements a and b of K^*. To aid this choice, we introduce some notation and prove a lemma. Let $\mathrm{ord}\colon K_{\mathrm{f}} \to \mathbb{R}$ be the group homomorphism that preserves the order defined by $p \mapsto 1$; that is, for $c \in K_{\mathrm{f}}$, $s \in \mathbb{Z}$ and $t \in \mathbb{Z}_{>0}$, we have $\mathrm{ord}(c) > \frac{s}{t}$ if and only if $p^s \notin c^t \cdot A$.

Lemma 8.6. *Let $\xi' \in K^*/K^{*p-1}$. Let $c \in K_{\mathrm{f}}$ with $\mathrm{ord}(c) > 0$. Let $y, z \in \mathbb{R}$ such that $y - z \geq (p-1)\mathrm{ord}(c)$. Then there exists $a \in \xi'$ with $z \leq \mathrm{ord}(a) < y$.*

Proof. Because we assume K^*/K_{f} is $(p-1)$-divisible, $K_{\mathrm{f}} \cap \xi'$ is non-empty. Let $a' \in K_{\mathrm{f}} \cap \xi'$, then for every integer k, also $a'c^{(p-1)k} \in \xi'$. Choose k minimal such that $z \leq \mathrm{ord}(a'c^{(p-1)k})$ and put $a = a'c^{(p-1)k}$. By minimality of k, we have $\mathrm{ord}(a) < z + \mathrm{ord}(c^{p-1}) \leq y$, which proves the lemma. □

Now we are ready to prove the characteristic zero case.

Lemma 8.7. *Suppose K has characteristic zero, and that the group $K_{\mathrm{f}}/(1+\mathfrak{p})$ is not p-divisible. Let $\xi \in K^*/K^{*p-1}$ Then there exist $a, b \in K^*$ that satisfy*

$$(-1)^{p^n(p^n-1)/2}a \in \xi,\ b \cdot (1+\mathfrak{p}) \text{ is not a } p\text{-th power in } K^*/(1+\mathfrak{p}),$$
$$a^{p^n} \notin p^{np^n}b^{p^n-1} \cdot A \text{ and } b^{p^n-1} \notin a^{p^n} \cdot A.$$

Proof. Fix $\xi \in K^*/K^{*p-1}$. We distinguish two cases:

(i) there exists $N \in \mathbb{Z}_{>0}$ such that $\mathrm{ord}(K_{\mathrm{f}}) = \frac{1}{N}\mathbb{Z}$;

(ii) for every $x \in \mathbb{R}_{>0}$, the group K_{f} is generated by the set $\{u \in K_{\mathrm{f}} : |\mathrm{ord}(u)| < x\}$.

In case (i), let $c \in K_{\mathrm{f}}$ with $\mathrm{ord}(c) = \frac{1}{N}$. With Lemma 8.6 applied to $\xi' = (-1)^{p^n(p^n-1)/2}\xi$, c, $y = \frac{2p-1}{2N}$ and $z = \frac{1}{2N}$, choose $a \in (-1)^{p^n(p^n-1)/2}\xi$ with $\frac{1}{2N} \leq \mathrm{ord}(a) < \frac{2p-1}{2N}$. In this case, a is not a p-th power in $K^*/(1+\mathfrak{p})$. Put $b = a$, then a and b are as required.

In case (ii), for every real number $x > 0$, there exists $u \in K_{\mathrm{f}} \setminus (K_{\mathrm{f}}^p(1+\mathfrak{p}))$ with $|\mathrm{ord}(u)| < x$. With Lemma 8.6 applied to $\xi' = (-1)^{p^n(p^n-1)/2}\xi$, $c = p$, $y = p - \frac{1}{2}$, and $z = \frac{1}{2}$, choose $a \in \xi'$ with $\frac{1}{2} \leq \mathrm{ord}(a) < p - \frac{1}{2}$. If $a \cdot (1+\mathfrak{p})$ is not a p-th power in $K^*/(1+\mathfrak{p})$, set $b = a$, then a and b are as required. If $a \cdot (1+\mathfrak{p})$ is a p-th power in $K^*/(1+\mathfrak{p})$, choose $u \in K_{\mathrm{f}} \setminus K_{\mathrm{f}}^p(1+\mathfrak{p})$ with $|\mathrm{ord}(u)| < \frac{1}{2\cdot(p^n-1)}$. Set $b = au$, then a and b are as required. This proves the lemma. □

Proof of Theorem 8.1. If K has characteristic p, the statement follows from Lemma 8.5. Suppose K has characteristic zero. Let $\xi \in K^*/K^{*p-1}$ and choose $a, b \in K^*$ as in 8.7. Let α in some extension of K satisfy $\alpha^{p^n} + a\alpha + b = 0$. By Lemma 8.3, the extension $L = K(\alpha)$ is totally wild and separable over K of degree p^n. By Lemma 8.2, the invariant associated to L is ξ. The statement follows. □

We finish this section by giving a class of fields for which the invariant does not attain all values. Let K be a local field. Let K_{sep} be a separable closure of K and let G_K be the Galois group of K_{sep} over K. Let V be the kernel of the natural map $G_K \to \mathrm{Aut}(K_{\mathrm{sep}}^*/(1+\mathfrak{r}))$. By [5, Theorem 3.8ii], there is a subgroup $H \subseteq G_K$ with the properties $G_K = H \cdot V$ and $V \cap H$ is trivial. Write L for the fixed field of H in K_{sep}.

Proposition 8.8. *In the situation above, for $n > 0$, the set $\mathcal{L}(L, p^n)$ is empty and the map $\Phi\colon \mathcal{L}(L, p^n) \to L^*/L^{*p-1}$ from the introduction is not surjective.*

Proof. By [5, Theorem 3.6i, 3.10vi], the only extension of L that is totally wild is L itself. Therefore, $\mathcal{L}(L, p^n)$ is empty for all $n > 0$. The proposition follows. □

References

[1] Michael Artin. *Grothendieck topologies: notes on a seminar*. Cambridge, MA: Harvard University, Departement of mathematics, 1962.

[2] P. Cartier. "Sur une généralisation du transfert en théorie des groupes". In: *Enseignement mathématique* 16.1 (1970), pp. 49–57. ISSN: 0013-8584.

[3] Ido Efrat. *Valuations, orderings, and Milnor K-theory*. 1st ed. Vol. 124. Mathematical Surveys and Monographs. Providence, R.I: American Mathematical Society, 2006. ISBN: 9780821840412.

[4] Otto Endler. *Valuation Theory*. 1st ed. Universitext. Berlin, Heidelberg: Springer Berlin / Heidelberg, 1972. ISBN: 3540060707.

[5] Michiel Kosters. "Groups and fields in arithmetic". PhD thesis. Leiden University, Leiden, 2014. URL: https://hdl.handle.net/1887/25871 (visited on 03/31/2026).

[6] S. Lang. *Algebra*. Rev. Third edition. Graduate Texts in Mathematics, 211. New York, NY: Springer New York, 2002. ISBN: 9781461300410. URL: http://dx.doi.org/10.1007/978-1-4613-0041-0.

[7] Akram Lbekkouri. "On the discriminant in local number fields". In: *Lobachevskii journal of mathematics* 34.2 (2013), pp. 152–162. ISSN: 1995-0802.

[8] Alexander Ostrowski. "Untersuchungen zur arithmetischen Theorie der Körper". In: *Mathematische Zeitschrift* 39.1 (1935), pp. 321–404. ISSN: 0025-5874.

[9] Peter Scholze. "Perfectoid spaces". In: *Publications mathématiques de l'IHÉS* 116.1 (2012), pp. 245–313.

[10] Jean-Pierre Serre. *Cohomologie Galoisienne*. eng. 5ème éd., revisée et complétée 1994. Vol. 5. Lecture Notes in Mathematics. Springer, 2007. ISBN: 3540580026.

[11] Richard Swan. "Factorization of polynomials over finite fields". In: *Pacific journal of mathematics* 12.3 (1962), pp. 1099–1106. ISSN: 0030-8730.