Proceedings of the Edinburgh Mathematical Society (1997) **40**, 353–365 ©

THE DIFFERENT AND DIFFERENTIALS OF LOCAL FIELDS WITH IMPERFECT RESIDUE FIELDS

by BART DE SMIT

(Received 28th August 1995)

Let K be a complete field with respect to a discrete valuation and let L be a finite Galois extension of K. If the residue field extension is separable then the different of L/K can be expressed in terms of the ramification groups by a well-known formula of Hilbert. We will identify the necessary correction term in the general case, and we give inequalities for ramification groups of subextensions L'/K in terms of those of L/K. A question of Krasner in this context is settled with a counterexample. These ramification phenomena can be related to the structure of the module of differentials of the extension of valuation rings. For the case that $[L:K]=p^2$, where p is the residue characteristic, this module is shown to determine the correction term in Hilbert's formula.

1991 *Mathematics subject classification:* 11S15, 13N05.

1. Introduction

By a local field we mean a complete field with respect to a discrete valuation. In this note we study ramification groups, the different and differentials for finite separable extensions of local fields with inseparable residue class field extensions.

For the case that the residue class field extension is separable, which we will call the *classical case*, there is a beautiful theory of ramification groups for which we refer to Serre [**11**, Ch. III, IV]. The classical results, such as Hilbert's formula for the different in terms of ramification groups, do not hold in general. In the classical case one has the "upper numbering" of ramification groups [**11**, Ch. IV, §3], which is preserved under restriction to subextensions, but the examples in (3.7) below show that no such renumbering exists in our context.

Known results on the non-classical case include Kato's class field theory for "n-dimensional complete discrete valuation fields," see [**6**] and [**4**]. In Zariski–Samuel [**12**, Vol. I, Ch. V, §10] two intertwined filtrations with ramification groups are defined, and some classical results on where the jumps can be, have been generalized to this double filtration [**2**]. Krasner [**7**] focuses on the different, and some of the present results can be inferred from his paper.

For any local field K we denote the prime ideal by $\mathfrak{p}_K$ and the residue class field by $\bar{K}$. Let v_K be the normalized valuation on K and let the valuation of a fractional ideal of K be the valuation of a generator, so that $v_K(\mathfrak{p}_K)=1$. In this introduction the results will be formulated for Galois extensions L/K with Galois group G. With the

https://doi.org/10.1017/S0013091500023798 Published online by Cambridge University Press

exception of Section 5, all results will be shown for non-Galois extensions too.

In the classical case, the different $\mathcal{D}_{B/A}$ can be expressed in terms of ramification groups by the following formula that is due to Hilbert

$$v_L(\mathcal{D}_{B/A}) = \sum_{i=0}^{\infty}(\#G_i - 1). \tag{1}$$

Recall that the ramification groups G_i are defined by $G_i = \{\sigma \in G : i_G(\sigma) \geq i+1\}$ where $i_G(\sigma) = \inf\{v_L(\sigma x - x) : x \in B\}$. Hilbert's formula holds under the weaker condition that B is *monogenic* over A, i.e., that $B = A[\alpha]$ for some $\alpha \in B$. For the non-monogenic case we will show that one needs to add a term on the left hand side of (1), namely the smallest integer n for which there is an $\alpha \in B$ with $\mathfrak{p}_L^n \subset A[\alpha]$. We call the ideal $\mathfrak{p}_L^n$ the monogenity conductor of B over A.

Suppose L' is an intermediate field of the extension L/K corresponding to a normal subgroup H of G. In the classical case, the ramification numbers $i_{G/H}(\tau)$ of L'/K can be computed from the $i_G(\sigma)$ by the well-known formula

$$i_{G/H}(\tau) = \frac{1}{e'}\sum_{\sigma \mapsto \tau} i_G(\sigma), \tag{2}$$

where e' is the ramification index of L over L'. Again, the same formula holds if B is monogenic over A. We can only give inequalities for the general case (see (3.6)), and examples showing that they are optimal if one only wants to take the ramification groups into account. It follows that the ramification groups of L' over K are not in general determined by those of L over K.

Krasner [7] raises a question which in our terminology asks whether an extension for which the monogenity conductor is multiplicative in towers, is necessarily monogenic. We give an example that shows that this is not the case (see (3.5) below).

In Section 4 we look at the module $\Omega_{B/A}$ of A-differentials of B. Using derivations rather than differentials, Moriya [10] showed that the length of the B-module $\Omega_{B/A}$ is $v_L(\mathcal{D}_{B/A})$. Such a statement holds in the much more general ring theoretic context of locally complete intersections [8, Prop. 10.17]. We will give an alternative proof, and we show that for any ring homomorphism $\Lambda \to A$, there is a canonical short exact sequence of B-modules:

$$0 \to \Omega_{A/\Lambda} \otimes_A B \to \Omega_{B/\Lambda} \to \Omega_{B/A} \to 0.$$

Like Moriya's proof, our proof is a reduction to the monogenic case. The module $\Omega_{B/A}$ contains more information than the different, namely its structure as a B-module. We will show that the number of elements needed to generate $\Omega_{B/A}$ as a B-module is equal to the number of elements needed to generate B as an algebra over A if B is not unramified over A.

One can hope that there is some relation between the correction terms needed in

https://doi.org/10.1017/S0013091500023798 Published online by Cambridge University Press

(1) and (2) and the B-module structure of $\Omega_{B/A}$. In Section 5, we give such results under the assumption that L is Galois over K of degree p^2, where p is the residue characteristic.

2. The different and the monogenity conductor

Let L/K be a finite separable extension of local fields with valuation rings $A \subset B$. We recall the definition and some basic properties of the different $\mathcal{D}_{B/A}$ of B over A. For any subset S of L its *complementary set* $S^\dagger$ is defined by $S^\dagger = \{x \in L : \forall y \in S : \mathrm{Tr}_{L/K}(xy) \in A\}$. The different $\mathcal{D}_{B/A}$ of L over K is the inverse ideal of the fractional ideal $B^\dagger$. Let $\alpha \in B$ with $L = K(\alpha)$. It is a well-known result due to Euler, that $A[\alpha]^\dagger = f'(\alpha)^{-1}A[\alpha]$, where f' is the derivative of the minimal polynomial f of α over K. We say that B is *monogenic* over A if there is an α with $B = A[\alpha]$. The different can then be computed easily, namely $\mathcal{D}_{B/A} = f'(\alpha)B$.

In the classical case, i.e., if $\bar{L}$ is separable over $\bar{K}$, the ring B is monogenic over A. See [**11**, Ch. III, §6, Prop. 12] for a proof. Without the separability condition this need not hold. However, we always have a monogenic extension of rings of integers if $[L:K]$ is prime, because then the ring-generator can be taken to be either a prime element or a representative of a generator of the residue field extension.

(2.1) Notation. Fix a Galois extension M of K that contains L, and let C be the valuation ring of M. By a K-embedding we mean a K-algebra homomorphism between extension fields of K. For any K-embedding $\sigma : L \to M$ let $\mathfrak{a}_L(\sigma)$ be the C-ideal generated by the elements $x - \sigma x$ with $x \in B$. If L/K is normal we may take $M = L$ and then $\mathfrak{a}_L(\sigma) = \mathfrak{p}_L^{i_G(\sigma)}$. Thus the ideals $\mathfrak{a}_L(\sigma)$ provide an easy way to consider "ramification numbers" for non-normal extensions (cf. Deligne [**1**]). The *monogenity conductor* $\mathfrak{r}_{B/A}$ of B over A is defined as the largest ideal of B that is contained in $A[\alpha]$, for some $\alpha \in B$. Note that $A[\alpha]$ is open in L if $L = K(\alpha)$, so $\mathfrak{r}_{B/A} \neq 0$.

Theorem 2.2. *We have*

$$\mathcal{D}_{B/A}\mathfrak{r}_{B/A} \cdot C = \prod_{\sigma \neq 1} \mathfrak{a}_L(\sigma),$$

where the product ranges over all K-embeddings of L in M that are not the inclusion.

Proof. Let $\alpha \in B$ with $L = K(\alpha)$. Define the conductor $\mathfrak{r}_\alpha$ of $A[\alpha]$ in B as the largest ideal of B that is contained in $A[\alpha]$, so $\mathfrak{r}_\alpha = \{x \in B : xB \subset A[\alpha]\}$. As in [**11**, Ch. III §6], we show that $\mathfrak{r}_\alpha \cdot \mathcal{D}_{B/A} = f'(\alpha)B$, where f is the minimal polynomial of α over K:

$$\begin{aligned} x \in \mathfrak{r}_\alpha &\Leftrightarrow xB \subset A[\alpha] \Leftrightarrow f'(\alpha)^{-1}xB \subset A[\alpha]^\dagger \\ &\Leftrightarrow \mathrm{Tr}_{L/K}(f'(\alpha)^{-1}xB) \subset A \Leftrightarrow f'(\alpha)^{-1}x \in \mathcal{D}_{B/A}^{-1}. \end{aligned}$$

https://doi.org/10.1017/S0013091500023798 Published online by Cambridge University Press

Since $\mathfrak{t}_{B/A} = \mathfrak{t}_\alpha$ for some α, one inclusion of the theorem now follows from

$$f'(\alpha) = \prod_{\sigma \neq 1} (\alpha - \sigma(\alpha)) \in \prod_{\sigma \neq 1} \mathfrak{a}_L(\sigma).$$

To finish the proof, we need to show that there is an $\alpha \in B$ for which the ideal on the right is generated by $f'(\alpha)$, for it then follows from the inclusion that we showed already, that $\mathfrak{t}_\alpha = \mathfrak{t}_{B/A}$. Such an element α is provided by the following lemma.

Lemma 2.3. *There is an element $\alpha \in B$ such that for all K-embeddings $\sigma : L \to M$ we have $\mathfrak{a}_L(\sigma) = (\alpha - \sigma\alpha)C$.*

Proof. If B is monogenic, then we may take α to be a generator of the ring extension, because for any C-ideal $\mathfrak{a}$ the question whether σ and the inclusion induce the same A-algebra homomorphism $B \to C/\mathfrak{a}$, then depends only on the two images of α.

Now assume that B is not monogenic over A. Then $\bar{K}$ is imperfect and in particular infinite, because the residue field extension must be inseparable. For each $\sigma : L \to M$ that is not the inclusion, the mapping from $V = B/\mathfrak{p}_K B$ to $\mathfrak{a}_L(\sigma)/\mathfrak{p}_M \mathfrak{a}_L(\sigma)$ induced by $1 - \sigma$ is a non-zero $\bar{K}$-linear map, and for each $\alpha \in B$ the element $(\alpha \bmod \mathfrak{p}_K B)$ lies in the kernel V_σ of this map if and only if $(1-\sigma)(B) \not\subset (\alpha - \sigma\alpha)C$. It follows from the well-known fact that a vector space over an infinite field is not a finite union of strict subspaces, that there always exists an element $x \in V$ that is not contained in V_σ for any σ. Any representative α of x in B satisfies our conditions. □

(2.4) Remark. For a Galois extension L/K with Galois group G the theorem says

$$v_L(\mathcal{D}_{B/A}) + n = \sum_{\sigma \neq 1} i_G(\sigma) = \sum_{i=0}^{\infty} (\#G_i - 1),$$

where n is the smallest integer for which there is an $\alpha \in B$ with $\mathfrak{p}_L^n \subset A[\alpha]$.

3. Ramification groups of subextensions

Let $K \subset L' \subset L$ be finite separable extensions of local fields with valuation rings $A \subset B' \subset B$. We fix a finite Galois extension M of K that contains L with valuation ring C and we use the notation $\mathfrak{a}_L(\sigma)$ as in (2.1).

Proposition 3.1 *For all K-embeddings $\tau : L' \to M$ we have*

$$\mathfrak{a}_{L'}(\tau) \mid \prod_{\sigma \mapsto \tau} \mathfrak{a}_L(\sigma),$$

where the product ranges over all K-embeddings $\sigma : L \to M$ with $\sigma|_{L'} = \tau$.

https://doi.org/10.1017/S0013091500023798 Published online by Cambridge University Press

Proof. By (2.3) there exists an element $\alpha \in B$ such that $\mathfrak{a}_L(\sigma) = (\alpha - \sigma\alpha)C$ for all σ. Let $f \in B'[X]$ be the minimal polynomial of α over L', and denote the polynomial that one obtains from f by applying τ to all its coefficients by τf. Then $f = \prod_\sigma (X - \sigma\alpha)$ with σ ranging over all L'-embeddings of L in M, and $\tau f = \prod_{\sigma\mapsto\tau}(X - \sigma\alpha)$. Since $\tau f - f$ has coefficients in $\mathfrak{a}_{L'}(\tau)$, we deduce

$$\prod_{\sigma\mapsto\tau} \mathfrak{a}_L(\sigma) = \prod_{\sigma\mapsto\tau}(\alpha - \sigma\alpha)\cdot C = (\tau f)(\alpha)C = (\tau f - f)(\alpha)C \subset \mathfrak{a}_{L'}(\tau).$$ □

For K-embeddings τ of L' in M that are not the inclusion, define the ideal $\mathfrak{d}(\tau)$ of C by $\mathfrak{d}(\tau)\mathfrak{a}_{L'}(\tau) = \prod_{\sigma\mapsto\tau} \mathfrak{a}_L(\sigma)$.

Proposition 3.2. *We have*

$$\mathfrak{t}_{B/B'}\mathfrak{t}_{B'/A}\prod_{\tau\neq 1}\mathfrak{d}(\tau) = \mathfrak{t}_{B/A}\cdot C,$$

with τ ranging over all K-embeddings of L' in M that are not the inclusion.

Proof. We can group the factors $\mathfrak{a}_L(\sigma)$ in (2.2) according to the restriction $\sigma|_{L'}$. Using (2.2) for L/L' and K/K' and the definition of $\mathfrak{d}(\tau)$ we get

$$\mathcal{D}_{B/A}\mathfrak{t}_{B/A}C = \mathfrak{t}_{B/B'}\mathcal{D}_{B/B'}\mathfrak{t}_{B'/A}\mathcal{D}_{B'/A}\prod_{\tau\neq 1}\mathfrak{d}(\tau).$$

Now use the transitivity of the different to cancel all three differents. □

Corollary 3.3. *We have $\mathfrak{t}_{B/B'}\mathfrak{t}_{B'/A} \mid \mathfrak{t}_{B/A}$. If B is monogenic over A, then B' is monogenic over A, equality holds in* (3.1), *and* $\mathfrak{d}(\tau) = (1)$.

Proof. The first statement follows from the fact that the ideals $\mathfrak{d}(\tau)$ are integral. If B is monogenic over A then $\mathfrak{t}_{B/A} = (1)$, and as monogenity conductors are integral ideals too, it then follows that all ideals on the left-hand side of (3.2) are all equal to (1). □

Corollary 3.4. *If L'/K is unramified then equality holds in* (3.1) *and* $\mathfrak{t}_{B/A} = \mathfrak{t}_{B/B'}$.

Proof. We can choose $\alpha \in L'$ with minimal polynomial $f \in A[X]$ such that $L' = K(\alpha)$, and $f \bmod \mathfrak{p}_K$ is separable. Let $\tau : L' \to M$ be a K-embedding which is not the inclusion. Since the zeros of f in M are distinct in $\bar{M}$, the map $\bar{L}' \to \bar{M}$ induced by τ, is not the inclusion. Therefore, $\mathfrak{a}_{L'}(\tau)$ is the unit ideal, and $\mathfrak{d}(\tau) = (1)$. The valuation ring of L' is monogenic over A, so it follows from (3.2) that $\mathfrak{t}_{B/A} = \mathfrak{t}_{B/B'}$. □

(3.5) A question of Krasner. Krasner [7] defines the "arithmetic different" $\delta_{B/A}$ as the B-ideal generated by the elements $f'_\alpha(\alpha)$, where α ranges over the elements of B that generate L as a field extension of K, and f_α is the minimal polynomial of α over K. It

https://doi.org/10.1017/S0013091500023798 Published online by Cambridge University Press

follows from the proof of (2.2) that $\delta_{B/A} = \mathcal{D}_{B/A}\mathfrak{r}_{B/A}$, and with (3.1) it follows that $\delta_{B/B'}\delta_{B'/A} \mid \delta_{B/A}$ (cf. [7, Thm. 9]). In Krasner's terminology, the extension L/K is said to be "Dedekindian" if $\delta_{B/A} = \mathcal{D}_{B/A}$, and it is called "Hilbertian" if $\delta_{B/A} = \delta_{B/B'}\delta_{B'/A}$ for all intermediate fields L'. Krasner asks the question whether all "Hilbertian" extensions are "Dedekindian." The answer is no, and to show this we will construct a non-monogenic extension without intermediate fields.

Suppose k is a field of characteristic $p > 0$ with elements $a, b \in k$ such that $k(a^{1/p}, b^{1/p})$ has degree p^2 over k. For instance, one may take $k = \mathbb{F}_p(U, V)$ with $a = U$ and $b = V$. Let $K = k((t))$ be the local field of Laurent series with valuation $v_K(\sum a_i t^i) = \inf\{i : a_i \neq 0\}$, and valuation ring $A = k[[t]]$. Consider the separable polynomial

$$f(X) = X^{p^2} + t^{p^2}X^p - t^{p^2}X - t^p b - a^p \in K[X]$$

and let $L = K(\alpha)$ where α is a zero of f in the separable closure K^{sep} of K. Then α is integral and $\alpha^p \equiv a \bmod \mathfrak{p}_L$. Put $\beta = (\alpha^p + t^p\alpha - a)/t$, then $\beta^p = t^{p^2-p}\alpha + b$, so that β is integral and $\beta^p \equiv b \bmod \mathfrak{p}_L$. It follows that $\bar{L} \supset k(a^{1/p}, b^{1/p})$, so that f is irreducible, and B is not monogenic over A.

To answer Krasner's question we still need to show that there are no intermediate fields of L/K. Let α' be a zero of f in K^{sep} with $x = \alpha - \alpha' \neq 0$. Since f is an additive polynomial, x is a zero of

$$X^{p^2} + t^{p^2}X^p - t^{p^2}X = X(X^{p^2-1} + t^{p^2}X^{p-1} - t^{p^2}).$$

One first sees that $v(x) > 0$ and then deduces that $v(x^{p^2-1}) = v(t^{p^2})$, so that $K(x)/K$ is a totally ramified extension of degree $p^2 - 1$. This implies that $K(\alpha, \alpha') = K(\alpha, x)$ has degree $p^2(p^2 - 1)$ over K. If there was an intermediate field L' of L/K, then α' could be taken to be conjugate with α over L', and the degree of $K(\alpha, \alpha')$ over K would be at most $p^2(p - 1)$.

(3.6) Inequalities. In addition to the bound on $\mathfrak{a}_{L'}(\tau)$ in (3.1) one has an obvious bound on the other side: choose an extension σ of τ to L, then $\mathfrak{a}_L(\sigma) \mid \mathfrak{a}_{L'}(\tau)$.

We can reformulate this if L is Galois over K with group G and L' corresponds to a normal subgroup H of G. If e' is the ramification index of L over L', then the restriction of v_L to L' is $e'v_{L'}$, so (3.1) and the bound given above can be stated as

$$\frac{1}{e'}\sup_{\sigma \mapsto \tau} i_G(\sigma) \leq i_{G/H}(\tau) \leq \frac{1}{e'}\sum_{\sigma \mapsto \tau} i_G(\sigma).$$

By (3.3) we have equality on the right in the monogenic case.

(3.7) Examples. To conclude this section, we give examples that show that these are the best bounds possible if one only wants to consider the ideals $\mathfrak{a}_L(\sigma)$.

https://doi.org/10.1017/S0013091500023798 Published online by Cambridge University Press

Furthermore, we will show that contrary to the classical case, the ramification numbers of L/K do not determine those of L'/K.

Let k be an imperfect field of characteristic p, and let K be the field $k((t))$ of Laurent series in t with coefficients in k. Fix an integer $s \in \{1, \dots, p\}$ and let $L' = K(\pi)$ where $\pi^p - t^{s(p-1)}\pi = t$. Then L' is a Galois extension of K of degree p, and the Galois group is generated by the automorphism τ of L' over K defined by $\pi \mapsto \pi + t^s$. Note that L' is wildly ramified over K with prime element π, so its valuation ring is $B' = A[\pi]$.

Suppose that $a \in k$ with $a \notin k^p$, and define the local field L as $L = L'(\alpha)$, where

$$\alpha^p - t^{2(p-1)}\alpha = a + t^{p-s}(1 - t^{p-1})\pi.$$

Then L is a Galois extension of L' of degree p, and the Galois group H of L over L' is generated by the map $\sigma : \alpha \mapsto \alpha + t^2$. By construction, $\bar{L} = \bar{L}'(\bar{\alpha})$ is a purely inseparable extension of $\bar{L}' = \bar{K}$ of degree p, and $B = B'[\alpha]$. We can extend τ to L by $\alpha \mapsto \alpha + t$, which shows that L is normal over K, and that $G = \mathrm{Gal}(L/K)$ is elementary abelian of order p^2, generated by σ and τ. The filtration with ramification groups is as follows:

$$G = G_0 = \cdots = G_{p-1} \neq G_p = \langle\sigma\rangle = G_{p+1} = \cdots = G_{2p-1} \neq G_{2p} = \{1\}.$$

Note that the first trivial ramification group of L' over K is $(G/H)_{ps}$, so the ramification groups of L' over K are not determined by those of L over K alone. With the given definition of τ, the inequalities in (3.6) read $p \leq ps \leq p^2$. In particular, we have equality on the right if $s = p$ (the monogenic case), and on the left if $s = 1$.

Using the fact that $B' = A[\pi]$ and $B = B'[\alpha]$ we see that

$$\mathcal{D}_{B/A} = \mathcal{D}_{B/B'}\mathcal{D}_{B'/A} = t^{2(p-1)}t^{s(p-1)}B = t^{(s+2)(p-1)}B.$$

By (2.2) we have $\mathfrak{t}_{B/A} = t^{(p-s)(p-1)}B$. We return to the case of Galois extensions of degree p^2 in Section 5.

4. Differentials

Let L/K be a finite separable extension of local fields with valuation rings $A \subset B$. In this section we study the B-module $\Omega_{B/A}$ of Kähler differentials of B over A, and its relation to the different and to questions about monogenity. See [9, Ch. 9] for definitions and fundamental properties of differentials.

The B-module $\Omega_{B/A}$ is finitely generated, because B is a finitely generated A-algebra. Since L is separable over K we have $\Omega_{B/A} \otimes_B L = \Omega_{L/K} = 0$, so the B-module $\Omega_{B/A}$ has finite length.

Theorem 4.1. (1) *The length of the B-module $\Omega_{B/A}$ is $v_L(\mathcal{D}_{B/A})$.*
(2) *For any ring homomorphism $\Lambda \to A$ there is an exact sequence of B-modules:*

$$0 \to \Omega_{A/\Lambda} \otimes_A B \to \Omega_{B/\Lambda} \to \Omega_{B/A} \to 0.$$

https://doi.org/10.1017/S0013091500023798 Published online by Cambridge University Press

Proof. For (2) we only need to show injectivity of the map $\Omega_{A/\Lambda} \otimes_A B \rightarrow \Omega_{B/\Lambda}$, because exactness at the other places holds for arbitrary ring homomorphisms $\Lambda \rightarrow A \rightarrow B$ [**9**, Thm. 25.1].

Suppose A is generated as an Λ-algebra by a set $S \subset A$. We have a surjection of the polynomial algebra $\Lambda[X_s : s \in S]$ onto A sending a variable X_s to $s \in A$. Let R be a set of ideal generators of its kernel. Denoting the free A-module on a set X by $A^{(X)}$, we can describe $\Omega_{A/\Lambda}$ as the cokernel of the A-linear map $A^{(R)} \rightarrow A^{(S)}$, with matrix $(\partial r/\partial X_s)_{r \in R, s \in S}$.

Let us assume first that B is monogenic over A, so that $B = A[\alpha] \cong A[X]/(f)$, where $f \in A[X]$ is the minimal polynomial of α over K. Then the above argument for B over A instead of A over Λ implies that $\Omega_{B/A} \cong B/f'(\alpha)B$. We already knew that $\mathcal{D}_{B/A} = f'(\alpha)B$, so this shows (1). If we add the element α to S we find generators for B over Λ, and one more relation given by lifting f to a polynomial in $\Lambda[X_s][X]$. It follows that we have a diagram with exact rows and columns:

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
0 \arrow[r] & B^{(R)} \arrow[r] \arrow[d] & B^{(R)} \oplus B \arrow[r] \arrow[d] & B \arrow[r] \arrow[d, "f'(\alpha)"] & 0 \\
0 \arrow[r] & B^{(S)} \arrow[r] \arrow[d] & B^{(S)} \oplus B \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & 0 \\
 & \Omega_{A/\Lambda} \otimes_A B \arrow[r] \arrow[d] & \Omega_{B/\Lambda} \arrow[r] \arrow[d] & \Omega_{B/A} \arrow[d] & \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Statement (2) now follows from the snake lemma. This proves the theorem for the monogenic case.

We now show that the theorem is "transitive in towers", i.e., we show that the theorem holds for B over A, if it holds for B over B' and for B' over A, for some intermediate complete discrete valuation ring B'. Since the different is multiplicative in towers, statement (1) for B over A follows from (1) for each of the steps and (2) for B over B' with $\Lambda = A$. Furthermore, if (2) holds for each of the steps, then the map $\Omega_{A/\Lambda} \otimes_A B' \rightarrow \Omega_{B'/\Lambda}$ is injective, so after tensoring with the flat B'-algebra B we get injections

$$\Omega_{A/\Lambda} \otimes_A B \rightarrowtail \Omega_{B'/\Lambda} \otimes_{B'} B \rightarrowtail \Omega_{B/\Lambda},$$

which implies (2) for B over A. This proves "transitivity".

It follows that (4.1) holds if L/K is a tower of monogenic extensions. Not all extensions are of this type (cf. (3.5)), but Galois extensions L/K are. To see this, first note that the tame part T/K is monogenic. Furthermore, L is Galois over T of prime power degree. Every p-group has a chain of subgroups with steps of index p, and every extension of local fields of degree p is monogenic. This shows (4.1) for Galois extensions L/K.

For the general case, let M be a finite Galois extension of K containing L, and let C be its valuation ring. Then the theorem holds for C over A and for C over B. To get statement (1) for B over A we apply (2) for C over B by taking $\Lambda = A$ and using transitivity of the different. It remains to show (2) for B over A. Given a ring homomorphism $\Lambda \to A$, we let N be the kernel of the map $\Omega_{A/\Lambda} \otimes_A B \to \Omega_{B/\Lambda}$. Since C is flat over B, the C-module $N \otimes_B C$ is the kernel of the canonical map $\Omega_{A/\Lambda} \otimes_A C \to \Omega_{B/\Lambda} \otimes_B C$. We know that $\Omega_{A/\Lambda} \otimes_A C$ and $\Omega_{B/\Lambda} \otimes_B C$ both inject to $\Omega_{C/\Lambda}$, so $N \otimes_B C = 0$. But C is free over B, so we must have $N = 0$. □

The kernel $\Upsilon_{B/A/\Lambda}$ of the map $\Omega_{A/\Lambda} \otimes_A B \to \Omega_{B/\Lambda}$ is called the *module of imperfection*. Each of the reduction steps to the monogenic case in the above proof is an easy consequence of the following result, which has been proved by Grothendieck [**3**, Ch. 0, (20.6.18)]; for any flat B-algebra C there is a canonical exact sequence

$$0 \to \Upsilon_{B/A/\Lambda} \otimes_B C \to \Upsilon_{C/A/\Lambda} \to \Upsilon_{C/B/\Lambda}\Upsilon_{C/B/\Lambda} \to 0.$$

Kähler differentials are often used in commutative algebra to linearize ring theoretic problems. For instance, if the B-module $\Omega_{B/A}$ of Kähler differentials is not cyclic, then B is not monogenic over A. By the next proposition the converse holds too.

Proposition 4.2. *Suppose that L is not unramified over K. Then the smallest number of elements generating $\Omega_{B/A}$ as a B-module is equal to the smallest number of elements that generate B as an A-algebra.*

Proof. One inequality is clear: if $B = A[\alpha_1, \ldots, \alpha_k]$ then $\Omega_{B/A} = \sum_i B d\alpha_i$.

Now let n be the smallest number of elements that generate $\Omega_{B/A}$ as a B-module. We want to show that B is an A-algebra generated by n elements. The $\bar{L}$-vector space $\Omega_{B/A} \otimes_B \bar{L}$ has dimension n by Nakayama's lemma. It has a basis of the form $d\alpha_1 \otimes 1, \ldots, d\alpha_n \otimes 1$ for suitable $\alpha_1, \ldots, \alpha_n \in B$, and the elements $d\alpha_i$ generate $\Omega_{B/A}$. Put $S = A'[\alpha_1, \alpha_2, \ldots, \alpha_n]$, where A' is the valuation ring of the inertia field K' of L over K. We first show that $B = S$. It follows from the exact sequence

$$\Omega_{S/A} \otimes_S B \to \Omega_{B/A} \to \Omega_{B/S} \to 0$$

that $\Omega_{B/S} = 0$, so B has no derivations that are trivial on S. Since $\bar{L}$ is purely inseparable over $\overline{K'}$, and every inseparable extension of fields has a non-zero derivation, it follows that the reduction map $S \to \bar{L}$ is surjective. If S contains no prime element of B, then $S \cap \mathfrak{p}_L \subset \mathfrak{p}_L^2$, and we can construct a derivation of B over S by writing an element $x \in B$ as $x = r + y$, with $r \in S$ and $y \in \mathfrak{p}_L$, and mapping x to the class of y in $\mathfrak{p}_L/\mathfrak{p}_L^2$. So let $\pi \in S$ be a prime element of B and choose representatives $x_1, \ldots, x_f$ in S of a basis of $\bar{L}$ over $\overline{K'}$. Then the elements $x_i\pi^j$ of S with $1 \leq i \leq f$ and $0 \leq j < e$ form a basis of B as an A'-module, and therefore $B = S$.

Since L/K is not unramified, n is at least 1. We may assume that $\bar{K}$ is imperfect because otherwise B would be monogenic over A. We are done if we can find an

https://doi.org/10.1017/S0013091500023798 Published online by Cambridge University Press

element $\beta \in A'$ for which $A'[\alpha_1] = A[\alpha_1 + \beta]$, because we then have $B = A[\alpha_1 + \beta, \alpha_2, \ldots, \alpha_n]$. By the primitive element theorem (see Jacobson [**5**, Ch. I, §11]) we can find an element $\beta \in A'$ such that $\overline{K'} = \bar{K}(\bar{\beta})$ and $\bar{K}(\overline{\alpha_1} + \bar{\beta}) = \bar{K}(\bar{\alpha}_1, \bar{\beta})$. We then have $A' = A[\beta]$, and in order to deduce that $A'[\alpha_1] = A[\alpha_1 + \beta]$, we still need to show that the ring $R = A[\alpha_1 + \beta]$ contains the element β.

The ring R is a local ring, because B is a local ring that is integral over R (see [**12**, Ch. V, §2, Thm. 3]). Let $\mathfrak{m}$ be the maximal ideal of R. The $\mathfrak{m}$-adic topology on R is the same as the $\mathfrak{p}_K$-adic topology of the A-module R, and since R is a free A-module of finite rank, it is complete. Therefore, Hensel's lemma holds for R (see [**12**, Ch. VIII, §7]). Let h be the minimal polynomial of β over K, then the reduction of $h \bmod \mathfrak{p}_K$ has a simple zero $\bar{\beta}$ in $R/\mathfrak{m}$. By Hensel's lemma, h has a zero in R whose residue class is $\bar{\beta}$, so $\beta \in R$.

The following gives a generalization and an alternative proof for the fact from (3.3) that a subextension of a monogenic extension is monogenic.

Corollary 4.3. *Let $K \subset L \subset M$ be finite separable extensions of local fields, with rings of integers- $A \subset B \subset C$. Then the number of elements needed to generate B as an algebra over A is at most the number of elements needed to generate C over A.*

Proof. Assume that C can be generated as an A-algebra by n elements. By (4.2) the C-module $\Omega_{C/A}$ can be generated by n elements. By (4.1) we see that $\Omega_{B/A} \otimes C$ is a submodule. Looking at the $\mathfrak{p}_M$-torsion, we deduce that the C-module $\Omega_{B/A} \otimes C$ can also be generated by n elements, and then the same holds for the B-module $\Omega_{B/A}$. If L is unramified over K, then $n \leq 1$, and the statement is obvious. If L is not unramified over K, then (4.2) implies that B can be generated as an A-algebra by n elements. □

5. Galois extensions of degree p^2

In this section we suppose that L/K is a Galois extension of degree p^2 with $p = \operatorname{char} \bar{K}$. We will show that the defect in the classical formulas (1) and (2) in the introduction can be expressed in terms of the module structure of $\Omega_{B/A}$.

Put $G = \mathrm{Gal}(L/K)$, let L' be an intermediate field of degree p over K and let B' be the valuation ring of L'. Each of the steps in the extension $A \subset B' \subset B$ is monogenic, so the outer two modules in the exact sequence

$$0 \to \Omega_{B'/A} \otimes_{B'} B \to \Omega_{B/A} \to \Omega_{B/B'} \to 0$$

are cyclic. The B-module $\Omega_{B/A}$ is therefore isomorphic to $B/\mathfrak{p}_L^a \oplus B/\mathfrak{p}_L^b$, for unique integers a, b with $0 \leq a \leq b$. By (4.1) we have $\mathcal{D}_{B/A} = \mathfrak{p}_L^{a+b}$.

In (2.1) the monogenity conductor $\mathfrak{t}_{B/A}$ was defined. For $\tau \in \mathrm{Gal}(L'/K)$ with $r \neq 1$, the B-ideal $\mathfrak{d}(\tau)$ was given in Section 3 by $\prod_{\sigma \mapsto \tau} \mathfrak{a}_L(\sigma) = \mathfrak{a}_{L'}(\tau) \cdot \mathfrak{d}(\tau)$.

https://doi.org/10.1017/S0013091500023798 Published online by Cambridge University Press

Theorem 5.1. *We have* $\mathfrak{d}(\tau) = \mathfrak{p}_L^a$ *and* $\mathfrak{t}_{B/A} = \mathfrak{p}_L^{a(p-1)}$.

Proof. It is easy to check that $\mathfrak{d}(\tau)$ does not depend on the choice of $\tau \in \mathrm{Gal}(L'/K)$, as long as $r \neq 1$, and we will just write $\mathfrak{d}$ for $\mathfrak{d}(\tau)$. Furthermore, we have $\mathfrak{t}_{B/A} = \mathfrak{d}^{p-1}$ by (3.2), so the first statement implies the second. It also follows that $\mathfrak{d}$ does not depend on the choice of the intermediate field L'.

First we give an explicit description of the A-algebra B in order to compute $\Omega_{B/A}$. We can write $B' = A[\alpha]$, where either α is a prime element of L' (if $[\overline{L'} : \bar{K}] = 1$), or the image of α in $\overline{L'}$ generates the residue class field extension (if $[\overline{L'} : \bar{K}] = p$). Let $f \in A[X]$ be the minimal polynomial of α over A. Now choose a generator β for B over B' in the same way, so that β is a prime element of B or $\bar{\beta}$ has degree p over $\overline{L'}$. Let

$$g = Y^p + c_{p-1}Y^{p-1} + \cdots + c_0 \in B'[Y]$$

be the minimal polynomial of β over L'. Then each coefficient c_i can be written as $g_i(\alpha)$ for some polynomial $g_i \in A[X]$ of degree less than p. It follows that the kernel of the surjective A-algebra homomorphism $A[X, Y] \to B$ that maps X to α and Y to β, is the ideal generated by f and $Y^p + g_{p-1}Y^{p-1} + \cdots + g_0$. Putting $\delta = \sum_{i=0}^{p-1} g_i'(\alpha)\beta^i$, we can now compute $\Omega_{B/A}$ as the cokernel of the B-linear map $B^2 \to B^2$ with the matrix

$$\begin{pmatrix} f'(\alpha) & \delta \\ 0 & g'(\beta) \end{pmatrix}.$$

The smallest invariant factor a of $\Omega_{B/A}$ is the largest integer for which the image of this map lies in $\mathfrak{p}_L^a \cdot B^2$. In other words,

$$\mathfrak{p}_L^a = \gcd(f'(\alpha), \delta, g'(\beta)) = \delta B + \mathcal{D}_{B'/A} \cdot B + \mathcal{D}_{B/B'}.$$

Since $\mathfrak{d}$ does not depend upon the choice of L', we may assume that $H = \mathrm{Gal}(L/L')$ lies in the highest non-trivial ramification group of L over K (in other words, take L' to be an intermediate field of degree p with $v_L(\mathcal{D}_{B'/A})$ minimal). In particular this means that there is a B-ideal $\mathfrak{b}$ such that $\mathfrak{a}_L(\sigma) = \mathfrak{b}$ for all $\sigma \notin H$, and $\mathfrak{b} \mid \mathfrak{a}_L(\sigma)$ for $\sigma \in H$.

The theorem follows from the following three statements, which are proved below.

(i) $\mathfrak{d} \mid \mathcal{D}_{B/B'}$ and $\mathfrak{d} \mid \mathcal{D}_{B'/A} \cdot B$;

(ii) $\mathfrak{d} \mid \delta B$;

(iii) $\mathfrak{d} = \delta B$ or $\mathfrak{d} = \mathcal{D}_{B'/A} \cdot B$.

In order to show (i), note that for $\tau \in \mathrm{Gal}(L'/K)$ with $\tau \neq 1$ we have

$$\mathfrak{d} = \mathfrak{a}_{L'}(\tau)^{-1} \prod_{\sigma \mapsto \tau} \mathfrak{a}_L(\sigma) \mid \mathfrak{a}_{L'}(\tau)^{-1}\mathfrak{a}_{L'}(\tau)^p = \mathcal{D}_{B'/A} \cdot B.$$

If σ_0 is any lift of τ to L, our choice of L' implies that

https://doi.org/10.1017/S0013091500023798 Published online by Cambridge University Press

$$\mathfrak{d} \mid \mathfrak{a}_{L'}(\tau)\mathfrak{a}_L(\sigma_0)^{-1}\mathfrak{d} = \prod_{\substack{\sigma\mapsto\tau \\ \sigma\neq\sigma_0}} \mathfrak{a}_L(\sigma) \mid \prod_{\substack{\sigma\in H \\ \sigma\neq 1}} \mathfrak{a}_L(\sigma) = \mathcal{D}_{B/B'}.$$

This proves statement (i). To prove (ii) we will use the following lemma.

Lemma 5.2. *Let $h \in A[X]$ be a polynomial of degree less than p and suppose that L' is not unramified over K. Then $h(\alpha) - \tau(h(\alpha))$ and $h'(\alpha)(\alpha - \tau\alpha)$ have the same valuation k in L', and they are congruent modulo $\mathfrak{p}_{L'}^{k+1}$.*

Proof. First consider the case that $h = X^i$ for some $i \in \{1, 2, \dots, p-1\}$. From

$$\alpha^i - \tau\alpha^i = (\alpha - \tau\alpha)(\alpha^{i-1} + \alpha^{i-2}\tau\alpha + \cdots + \tau\alpha^{i-1}),$$

and from $\alpha B' = \tau\alpha B'$, it is easy to infer that

$$\alpha^i - \tau\alpha^i \equiv i\alpha^{i-1}(\alpha - \tau\alpha) \bmod \alpha^{i-2}(\alpha - \tau\alpha)^2 B'.$$

If $e(L'/K) = 1$, then $\alpha \in B'^*$ and $\alpha \equiv \tau\alpha \bmod \mathfrak{p}_{L'}$ (as L' is not unramified over K), and the required congruence follows. Assume $e(L'/K) = p$, so that α is a prime element of B'. We claim that $\alpha \not\equiv 0 \bmod (\alpha - \tau\alpha)$. To see why this holds, note that the extension is not tamely ramified. This means that the tame ramification group of L' is the full group $\mathrm{Gal}(L'/K)$ and therefore $\alpha - \tau\alpha \in \mathfrak{p}_{L'}^2 = \alpha^2 B'$. This shows the claim, and the lemma follows for h of the special form X^i with $i < p$.

For the general case, write $h = \sum b_i X^i$ with $b_i \in K$. Our choice of α ensures that $v_{L'}(h'(\alpha)) = \inf_i v_{L'}(ib_i\alpha^{i-1})$. The lemma now follows from the next lemma, whose proof is left to the reader.

Lemma 5.3. *For $i = 1, 2, \dots, n$ let a_i and b_i be elements of a local field F, such that $a_i \equiv b_i \bmod a_i\mathfrak{p}_F$. Put $a = \sum_i a_i$ and $b = \sum_i b_i$. If $v_F(a) = \inf_i v_F(a_i)$, then we have $a \equiv b \bmod a\mathfrak{p}_F$, and in particular $v_F(a) = v_F(b)$.*

This proves (5.2). We return to the proof of (5.1). If L' is unramified over K then B is monogenic over A by (3.4), and (ii) and (iii) are trivial, so let us assume that L' is not unramified over K. We have $\delta = \sum_{i=0}^{p-1} a_i\beta^i$ where $a_i = g_i'(\alpha)$. By (5.2), we have $a_i(\alpha - \tau\alpha) \equiv b_i \bmod \mathfrak{p}_L b_i$, where the $b_i = g_i(\alpha) - \tau(g_i(\alpha))$ are the coefficients of $g - \alpha g$. Our choice of β implies that $v_L(\delta) = \inf_i v_L(a_i\beta^i)$. We can now apply (5.3) to get $\delta(\alpha - \tau\alpha)B = \epsilon B$, where $\epsilon = \sum b_i\beta^i$. We have $(\alpha - \tau\alpha)B = \mathfrak{a}_{L'}(\tau)$, and repeating the argument of the proof of (3.1) we get

$$\begin{aligned} \delta\mathfrak{a}_{L'}(\tau) &= \epsilon B = (\tau g - g)(\beta)B = (\tau g)(\beta)B \\ &= \prod_{\sigma\mapsto\tau}(\beta - \sigma\beta)B \subset \prod_{\sigma\mapsto\tau} \mathfrak{a}_L(\sigma) = \mathfrak{d}\mathfrak{a}_{L'}(\tau). \end{aligned}$$

https://doi.org/10.1017/S0013091500023798 Published online by Cambridge University Press

In particular this gives $\delta \in \mathfrak{d}$, which shows statement (ii).

Finally, we show (iii). If $\mathfrak{a}_L(\sigma) = (\beta - \sigma\beta)B$ for all $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma|_{L'} = \tau$, then the inclusion above is an equality, and we have $\delta B = \mathfrak{d}$. Alternatively, suppose $\mathfrak{a}_L(\sigma) \neq (\beta - \sigma\beta)B$ for some $\sigma \in G$ with $\sigma|_{L'} = \tau$. Since every element of $B = A[\alpha, \beta]$ is an A-linear combination of elements of the form $\alpha^i\beta^j$ it follows by an argument similar to the first paragraph of the proof of (2.3) that $\mathfrak{a}_L(\sigma) = (\alpha - \sigma\alpha)B = \mathfrak{a}_{L'}(\tau)$. By our choice of L', we then have $\mathfrak{a}_L(\sigma) = \mathfrak{a}_{L'}(\tau)$ for all $\sigma \in G$ with $\sigma|_{L'} = \tau$. The definition of $\mathfrak{d}$ and (2.2) now give $\mathfrak{d} = \mathfrak{a}_{L'}(\tau)^{p-1} = \mathcal{D}_{B'/A} \cdot B$. This concludes the proof of (iii) and of (5.1). □

REFERENCES

1. P. Deligne, Appendix in *Représentations des groupes réductifs sur un corps local* (by Bernstein, Deligne, Kazhdan and Vignéras, Travaux en cours, Hermann, Paris 1984).

2. B. de Smit, Ramification groups of local fields with imperfect residue class fields, *J. Number Theory* **44** (1993), 229–236.

3. A. Grothendieck (with J. Dieudonné), *Éléments de géométrie algébrique IV No. 1* (Publ. Math. I.H.E.S. **20**, 1964).

4. O. Hyodo, Wild ramification in the imperfect residue field case, in *Galois representations and arithmetic algebraic geometry*, Y. Ihara (ed.), (North-Holland, Adv. Stud. Pure Math. **12**, 1987).

5. N. Jacobson, *Lectures in abstract algebra, Vol. III* (Von Nostrand, Princeton, New Jersey, 1964).

6. K. Kato, A generalization of local class field theory by using *K*-groups II, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **27** (1980), 603–683.

7. M. Krasner, Local differents of algebraic and finite extensions of valued fields, *J. Number Theory* **28** (1988), 17–61.

8. E. Kunz, *Kähler differentials* (Vieweg, Braunschweig, 1986).

9. H. Matsumura, *Commutative ring theory* (Cambridge University Press, Cambridge, 1986).

10. M. Moriya, Theorie der Derivationen und Körperdifferenten, *Math. J. Okayama Univ.* **2** (1953), 111–148.

11. J.-P. Serre, *Corps locaux* (Hermann, Paris, 1962); English translation: *Local fields* (Graduate Texts in Math. **67**, Springer, New York, 1979).

12. O. Zariski and P. Samuel, *Commutative algebra, Vol. I, II* (Graduate Texts in Math. **28**, **29**, Springer-Verlag, New York, 1975.)

Vakgroep Wiskunde, Econometrisch Instituut
Erasmus Universiteit Rotterdam
Postbus 1738
3000 Dr Rotterdam
The Netherlands
E-mail address: dsmit@wis.few.eur.nl

https://doi.org/10.1017/S0013091500023798 Published online by Cambridge University Press