Canad. J. Math. Vol. **52** (6), 2000 pp. 1269–1309

Well Ramified Extensions of Complete Discrete Valuation Fields with Applications to the Kato Conductor

Luca Spriano

Abstract. We study extensions L/K of complete discrete valuation fields K with residue field $\overline{K}$ of characteristic $p > 0$, which we do not assume to be perfect. Our work concerns ramification theory for such extensions, in particular we show that all classical properties which are true under the hypothesis *"the residue field extension $\overline{L}/\overline{K}$ is separable"* are still valid under the more general hypothesis that the valuation ring extension is monogenic. We also show that conversely, if classical ramification properties hold true for an extension L/K, then the extension of valuation rings is monogenic. These are the "*well ramified*" extensions. We show that there are only three possible types of well ramified extensions and we give examples. In the last part of the paper we consider, for the three types, Kato's generalization of the conductor, which we show how to bound in certain cases.

Contents

Received by the editors July 6, 1999; revised February 16, 2000.
AMS subject classification: 11S, 11S15, 11S20.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

Introduction

We consider complete discrete valuation fields which we shall call simply complete fields. The notations we use are at the end of this introduction and are (fairly) standard. For a finite extension L/K we mean by "classical case", "classical theory" and so on, that the residue field extension $\overline{L}/\overline{K}$ is separable (this is the hypothesis in, *e.g.*, [S1, ch. IV]).

Ramification theory for complete fields, is essentially a theory about invariants attached to an extension L/K which measure the deviation of L/K from being unramified.

The interest in complete fields with imperfect residue field is not new; in the paper of Epp [E], we find *weakly unramified extensions* (*i.e.*, extensions with $\mathfrak{p}_K\mathcal{O}_L = \mathfrak{p}_L$). In Miki's paper [M], one finds a general study of complete fields with imperfect residue field. At the end of the seventies Kato and Paršin, independently, were interested in n-dimensional local fields in relation with generalized class field theory, see [K1] and [P]. For example, the field $K = k((t))$, where $k = \mathbb{F}_p((X))$, is a 2-dimensional local field and its residue field $\overline{K}$ is $\mathbb{F}_p((X))$, which is imperfect.

When the residue field $\overline{K}$ is not perfect, the situation is very complicated. Look at the following example. Let K be a complete field with $\overline{K} = \mathbb{F}_p(x, y)$ and suppose that the characteristic of K is zero. Let A, B be two integral elements with their residue in $\overline{K}$ equal to x and y respectively. Then consider the extension $L = K(\alpha, \beta)$ where $\alpha^p = A$ and $\beta^p = B$. The situation is the following:

$$\begin{array}{ccccccc} L & \supset & \mathcal{O}_L & \supset & \mathfrak{p}_L = \mathfrak{p}_K\mathcal{O}_L & & \overline{L} = \mathbb{F}_p(\sqrt[p]{x}, \sqrt[p]{y}) \\ | & & | & & | & & | \\ K & \supset & \mathcal{O}_K & \supset & \mathfrak{p}_K & & \overline{K} = \mathbb{F}_p(x, y) \end{array} .$$

Here we have

$$e_{L/K} = 1, \quad f_{L/K} = f^{\mathrm{ins}}_{L/K} = [L : K].$$

This extension is not unramified because $\overline{L}/\overline{K}$ is not separable. The ramification index $e_{L/K}$ equals 1, however other ramification invariants, like the different, are *not* trivial. Observe that the extension of valuation rings *is not monogenic*. An extension L/K such that $e_{L/K} = 1$ and $[L : K] = f^{\mathrm{ins}}_{L/K}$ will be called *ferociously ramified*.

In Section 3 we verify, by examples, that, basically, all good properties of classical invariants are lost when considering general extensions, see Theorem 3.1. So we cannot establish a ramification theory, like in [S1], if we only use these invariants. We will show that a natural limit for establishing such a theory, is given by the monogenity of $\mathcal{O}_L/\mathcal{O}_K$. More precisely, one can define a filtration of $G = \mathrm{Gal}(L/K)$ by means of the classical function i_G (*cf.* Section 1). In the classical case if one considers a normal subgroup H of G, then one can obtain information on the filtration of G/H in terms of that of G. In general this is not possible. The reason is precisely that, in general, the valuation ring $\mathcal{O}_L$ is not monogenic over $\mathcal{O}_K$ (see Examples 3.3, 3.4 and Theorem 5.1). So, before studying the general situation, it is natural to analyze the extensions L/K which have $\mathcal{O}_L/\mathcal{O}_K$ monogenic.

It turns out that there are only three types of well ramified extensions L/K which are *completely ramified*, by this we mean that they do not contain tamely ramified subextensions (see also the definition in the beginning of Section 1):

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

I- totally ramified extensions;
II- ferociously ramified extensions such that $\overline{L}/\overline{K}$ is generated by only one element (f.r-1);
III- towers of extensions of the above two types, more precisely: extensions L/K containing a totally ramified subextension T/K (non-trivial) such that L/T is f.r-1.

The characterization of case III is established in Section 6 and in particular in Theorem 6.1. For well ramified extensions, we define a "modified" Hasse-Herbrand function $\varphi_{L/K}$ (analogous to the classical function) and for it we show Herbrand's theorem, *cf.* Section 7. In case III above, the Hasse-Arf theorem (stated in terms of $\varphi_{L/K}$) is shown by J. Borger (see [B] and also Section 10.4.3). This is equivalent to the fact that the Artin function a_G is a character of $\mathrm{Gal}(L/K)$, see Section 8.

In Section 9 we give a new proof of a result of Miki [M], giving a necessary condition for the existence of certain cyclic extensions of a complete field. We apply this result in our study of Kato's conductor, which we consider in Section 10 comparing it to the "naïve" conductor defined in terms of a variant of the classical function s_G; in particular we will deal with well ramified extensions in Section 10.4 and with cyclic extensions in Section 10.5.

Section 10 has undergone major changes after the first submission, and after we learnt of the work of J. Borger. His ideas allowed us to improve the results in that section.

To conclude this introduction, we would like to thank I. Fesenko, M. Kurihara, I. Zhukov and B. de Smit for the interest they have shown in my work. We are thankful to J. Borger for communicating us his proof of the Hasse-Arf theorem. We are also deeply grateful to Boas Erez for his help and constant encouragements.

The work presented here is part of the author's thesis [Sp].

Notation The letter p always indicates a prime in $\mathbb{Z}$. If G is a finite set, then $|G|$ indicates the number of elements of G.

If K is a field, $\mathrm{ch}(K)$ denotes the characteristic of K and K_s is a separable closure of K. A *complete field* K is a field K complete with respect to a discrete valuation with residue field $\overline{K}$ of characteristic $p > 0$. It is well-known that either $\mathrm{ch}(K) = 0$ or $\mathrm{ch}(K) = \mathrm{ch}(\overline{K})$. If K is a complete field,

- $\overline{K}$ denotes the residue field of K;
- v_K the normalized additive valuation of K, *i.e.*, $v_K(K^*) = \mathbb{Z}$;
- $\mathcal{O}_K = \{x \in K : v_K(x) \geq 0\}$ the valuation ring of K;
- $\mathfrak{p}_K = \{x \in K : v_K(x) > 0\}$ the maximal ideal of $\mathcal{O}_K$;
- π a prime element of $\mathcal{O}_K$;
- $U_K = \{x \in K : v_K(x) = 0\}$ the group of units and $U_K^i = 1 + \pi^i \mathcal{O}_K$, $i \geq 1$;
- e_K the absolute ramification index, *i.e.*, $e_K = v_K(p)$; throughout the paper we also use the notation: $e' = e_K/(p-1)$; if $\mathrm{ch}(K) = p$, we put $e_K = +\infty$;
- $\overline{x}$ the residue class mod $\mathfrak{p}_K$ of $x \in \mathcal{O}_K$;
- ζ_n a primitive n-th root of unity in a separable closure K_s;
- $\wp$ the map on K sending x to $x^p - x$.

If L is a finite extension of the complete field K,

- $e_{L/K}$ denotes the ramification index of L/K;
- $f_{L/K} = [\overline{L} : \overline{K}] = f_{L/K}^{\mathrm{sep}} \cdot f_{L/K}^{\mathrm{ins}}$ the residue degree;

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

- $\mathfrak{D}_{L/K}$ the different.

1 Definitions and Terminology

We rapidly recall some more notations and introduce definitions to be used below. Let K be a complete field which, we recall, we assume to have residue field of characteristic $p > 0$. If B is a ring, always assumed unitary, which contains a ring A, we say that B is *monogenic* over A when there exists α in B such that $B = A[\alpha]$. For an extension L/K of complete fields we shall say that L/K is monogenic if the extension of valuation ring is.

Definition Let L/K be a finite extension of complete fields. Then we have the following possibilities:

L/K	$f^{\text{sep}}_{L/K}$	$f^{\text{ins}}_{L/K}$	$e_{L/K}$
unramified	arb.	1	1
tamely ram.	arb.	1	$p \nmid e_{L/K}$
totally ram.	1	1	arb.
tot. wildly ram.	1	1	a power of p
weakly unram.	arb.	arb.	1
ferociously ram.	1	arb.	1
completely ram.	1	arb.	a power of p

Furthermore, let L/K be a ferociously ramified extension. If the residue field extension $\overline{L}/\overline{K}$ is generated by $x_1, \dots, x_n$ then we call L/K ferociously ramified of type n (f.r-n).

Remark 1.1 The definition of *weakly unramified* comes from [E]; in [Ku] there is the definition of *fiercely ramified*, but already in [Wi] one can find a first definition of fiercely ramified extension.[1] We use the adjective "ferocious" for "fierce". The classical definition of wildly ramified extension is that $p|e_{L/K}$, here we consider *totally wildly* ramified extensions: they are p-extensions. The terminology *"completely ramified"* is new.

Let L/K be a finite Galois extension with Galois group G. We do not assume that the residue field $\overline{K}$ is perfect. In [S1], the function $i_G \colon G \to \mathbb{Z} \cup \{\infty\}$ is defined by $i_G(1) = \infty$ and by

$$i_G(\sigma) = \inf_{x \in \mathcal{O}_L \setminus \{0\}} v_L\big(\sigma(x) - x\big), \quad \sigma \neq 1.$$

We also use the notation $i_{L/K}$ for i_G. By definition, an automorphism σ belongs to G_i if and only if $i_G(\sigma) \geq i + 1$. One can see that, if $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, then $i_G(\sigma) = v_L\big(\sigma(\alpha) - \alpha\big)$. More generally we have the following

Lemma 1.2 *Let L/K be a Galois extension of complete fields and $\sigma \in \mathrm{Gal}(L/K)$. If $\mathcal{O}_L = \mathcal{O}_K[x_1, \dots, x_n]$, then $i_G(\sigma) = \min_{1 \leq j \leq n}\{v_L\big(\sigma(x_j) - x_j\big)\}$.*

[1] Here is Williamson's definition: *The quotient field extension of an extension of discrete rank one valuation rings is said to be ferociously ramified if the residue class field extension has nontrivial inseparable part.* Clearly it is not the definition which we use.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

Proof In fact, for $\alpha = \sum_I a_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n} \in \mathcal{O}_L$ (the sum is taken over a finite set $I \subset \mathbb{N}^n$) we have $\sigma(\alpha) - \alpha = \sum_I a_{i_1,\dots,i_n} [\sigma(x_1^{i_1} \cdots x_n^{i_n}) - x_1^{i_1} \cdots x_n^{i_n}]$. So we have to consider the case $v_L\big(\sigma(\alpha\beta) - \alpha\beta\big)$ with $\alpha, \beta \in \mathcal{O}_L$. We have

$$\begin{aligned} v_L\big(\sigma(\alpha\beta) - \alpha\beta\big) &= v_L\big(\sigma(\alpha\beta) - \alpha\beta + \beta\sigma(\alpha) - \beta\sigma(\alpha)\big) \\ &= v_L\Big(\sigma(\alpha)\big(\sigma(\beta) - \beta\big) + \beta\big(\sigma(\alpha) - \alpha\big)\Big) \\ &\geq \min\{v_L\big(\sigma(\beta) - \beta\big), v_L\big(\sigma(\alpha) - \alpha\big)\}, \end{aligned}$$

because $v_L\big(\sigma(\alpha)\big) \geq 0$ and $v_L(\beta) \geq 0$. ■

One can also consider the function $s_G \colon G \to \mathbb{Z} \cup \{\infty\}$ defined by $s_G(1) = \infty$ and by

$$\begin{cases} s_G(\sigma) = \inf_{x \in \mathcal{O}_L \setminus \{0\}} v_L\big(\frac{\sigma(x)}{x} - 1\big), & \sigma \neq 1, \sigma \in G_0 \\ s_G(\sigma) = 0 & \text{if } \sigma \notin G_0. \end{cases}$$

In the classical case, if $\sigma \in G_0$, then $i_G(\sigma) = s_G(\sigma) + 1$; in general we only have

$$s_G(\sigma) \leq i_G(\sigma) \leq s_G(\sigma) + 1.$$

We have two intertwined filtrations of ramification groups (as indicated in [Z-S, ch. V]). Given two integers $n, i \geq 0$ one defines the (n, i)-ramification group $G_{n,i}$ of L/K as

$$G_{n,i} = \{\sigma \in G : v_L\big(\sigma(x) - x\big) \geq n + i, \text{ for all } x \in \mathfrak{p}_L^i\}.$$

Put $G_n = G_{n+1,0}$ and $H_n = G_{n,1}$, so that the classical ramification groups (see [S1, ch. IV]) are the G_n. We also define the ramification subgroup G_u (resp. H_u) for a positive real number u as G_i (resp. H_i) where i is the smallest integer $\geq u$. We have a filtration of G (*cf.* Props. 2.2–2.3 in [BDS2]) $G \supseteq G_0 \supseteq H_1 \supseteq G_1 \supseteq H_2 \supseteq \cdots \supseteq \{1\}$. We observe that if $\overline{L}/\overline{K}$ is separable, then $H_i = G_i$ for $i \geq 1$. Note that $G_{n,i}$ is a normal subgroup of G, as it is the kernel of the homomorphism $G \longrightarrow \mathrm{Aut}(\mathfrak{p}_L^i/\mathfrak{p}_L^{n+i})$. The group G_0/H_1 is cyclic and its order is e_{tame}, H_1 is a p-group of order $e_{\text{wild}} f_{L/K}^{\text{ins}}$. If we consider the sequence of ramification subgroups $G \supset G_0 \supset H_1 \supset \{1\}$, we have the associated tower of subfields

$$K \overset{f_{L/K}^{\text{sep}}}{\subseteq} L_0 \overset{e_{\text{tame}}}{\subseteq} L_1 \overset{f_{L/K}^{\text{ins}} e_{\text{wild}}}{\subseteq} L,$$

where L_0/K is unramified, L_1/L_0 is tamely ramified and L/L_1 is completely ramified. Indeed, the ramification groups are normal and so all of the intermediate extensions are Galois. Note that there are extensions where $f_{L/K}^{\text{ins}} > 1$ and $e_{L/K} > 1$, but for which there does not exist a subgroup which can "separate" ferocious from wild ramification.

The problems of ramification theory which we consider, come from the study of the extension L/L_1 which is completely ramified, so most of the time we will deal with the case $G = H_1$.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

2 Review of Results of Ramification Theory

We keep the notation of the preceding section, in particular we consider a finite, Galois extensions L/K; we do not make any assumptions on the residue field $\overline{K}$. Here we collect some more or less well known results; the proofs are in [S1, ch. IV] if $\overline{L}/\overline{K}$ is separable, in the general case see [BDS2].

Proposition 2.1 *Let L/K be a finite extension of complete fields.*

(i) *Suppose that $\overline{L}/\overline{K}$ is separable. Then there exists $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, i.e., $\mathcal{O}_L$ is monogenic as $\mathcal{O}_K$-algebra.*
(ii) *The quotient groups H_i/H_{i+1} are Abelian groups annihilated by p;*
(iii) *If G is Abelian, then all $i > 0$ with $G_i \neq H_{i+1}$ are congruent* mod *p and if there exists such an i, then all m with $H_m \neq G_m$ are divisible by p. If $\overline{L}/\overline{K}$ is separable, the jumps i such that $G_i \neq G_{i+1}$ are congruent* mod *p for any group G.*
(iv) *If $e_{L/K} = 1$, then $G_i = H_{i+1}$ for all $i \geq 1$.*

In the classical case there is a well-known connection between the different and the ramification groups: the *Hilbert formula* for the valuation of the different, which amounts to

$$v_L(\mathfrak{D}_{L/K}) = \sum_{\sigma \neq 1} i_G(\sigma) = \sum_{i \geq 0} (|G_i| - 1) = v_L\big(f'(\alpha)\big),$$

where $f(x)$ is the minimal polynomial of α over K and α is such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, (for a proof see [S1, ch. IV, Proposition 4]). We will note a formula due to de Smit generalizing this and valid in the non monogenic case, *cf.* Remark 5.4.

Now let us look at the ramification of L^H/K for H a normal subgroup of G. The following theorem holds under the more general hypothesis that the extension of valuation rings is monogenic. As can be seen by inspection, the same proof of [S1, ch. IV, Proposition 3] applies.

***Theorem 2.2* (Herbrand property)** *Let L/K be a monogenic extension; for all $\tau \in G/H$ we have*

$$i_{G/H}(\tau) = \frac{1}{e_{L/L^H}} \sum_{\sigma \to \tau} i_G(\sigma), \tag{1}$$

where the sum is taken over all automorphisms $\sigma \in G$ which equal τ mod *H.*

The image of a ramification subgroup G_u in G/H is given by the Herbrand theorem, which amounts to the following equality

$$G_u H/H = (G/H)_v, \quad v = \phi_{L/L^H}(u),$$

where the function $\phi_{L/K}$ is defined by $\phi_{L/K}(0) = 0$ and

$$\phi_{L/K}(u) = \frac{1}{g_0}\big(g_1 + \cdots + g_m + (u - m)g_{m+1}\big), \quad g_i = |G_i|,$$

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

for $m \leq u \leq m+1$, m a nonnegative integer and u a real number. The function $\phi_{L/K}$ is piecewise linear, increasing and convex and it is a homeomorphism of $[0,+\infty)$. It is called *Hasse-Herbrand function*. At this point one can define an upper numbering of the ramification groups by

$$G^{\phi_{L/K}(i)} = G_i \quad \text{or} \quad G^j = G_{\psi_{L/K}(j)},$$

where $\psi_{L/K}$ is the inverse function of $\phi_{L/K}$. We say that j is a jump if $G^j \neq G^{j+\epsilon}$ for all $\epsilon > 0$. Note that the upper jumps are not necessarily integers, see, *e.g.* [S1, exercise 2, p. 84] or see the explicit computation in [S3, Section 4]; we recall that they are integers if the extension L/K is Abelian, in fact we have (see a proof in [S1, ch. V, Section 7]):

Theorem 2.3 **(Hasse-Arf)** *Suppose L/K is a finite, Abelian extension and suppose $\overline{L}/\overline{K}$ separable. If $G_i \neq G_{i+1}$, then $\phi_{L/K}(i)$ is an integer. Equivalently, the jumps of the upper filtration $\{G^\nu\}_{\nu\geq 0}$ are integers.*

There is a generalization of the Hasse-Arf theorem for cyclic extensions: Sen's theorem which was conjectured by Grothendieck, *cf.* [Sen]. It goes as follows. Let L be a complete field with perfect residue field $\overline{L}$. We say that an automorphism σ of L is wildly ramified if $v_L\big(\sigma(x) - x\big) > 1$ for all $x \in \mathcal{O}_L$. Note that if σ is of finite order, which is always the case if $\mathrm{ch}(L) = 0$, and if σ is wildly ramified, then p divides the order of σ. Put $i(\sigma) = v_L\big(\sigma(\pi_L) - \pi_L\big)$.

Theorem 2.4 **(Sen)** *Let L be a complete field with perfect residue field.*[2] *Let σ be a wildly ramified automorphism of L. Then, for all $n > 0$ we have*

$$i(\sigma^{p^{n-1}}) \equiv i(\sigma^{p^n}) (\bmod p^n).$$

Sen's theorem has to be considered as a generalization of Hasse-Arf theorem because infinite extensions are also permitted. Note that Sen's theorem implies the Hasse-Arf theorem, see [S1, Proposition 11, Section 7, ch. V]. Of course, the Hasse-Arf theorem implies the congruences in Sen's theorem if σ is of finite order.

3 General Ramification Theory, Two Non Classical Examples

We now show that the properties, listed in the preceding paragraph, do not hold in general.

Theorem 3.1 *There exist Galois extensions L/K for which*

(1) the property about monogenic valuation rings is not true;
(2) the ramification jumps are not congruent mod *p;*
(3) the Hilbert formula does not hold;
(4) the function i_G does not verify the Herbrand property;
(5) the Herbrand, Hasse-Arf and Sen theorems do not hold.

[2] As Sen observes, this hypothesis can be replaced with the weaker hypothesis: there exists a system of representatives $\mathcal{R}$ for $\mathcal{O}_L$ which is invariant under σ.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

The proof is achieved by producing two examples, see Ex. 3.3 and Ex. 3.4. We must give some explanations about Herbrand's and Sen's theorems when the residue field extension $\overline{L}/\overline{K}$ is not separable (note that Sen's theorem is stated with perfect residue field). We check whether the Hasse-Arf and Herbrand theorems hold true with the function $\phi_{L/K}$ which can be defined when $\overline{L}/\overline{K}$ is not separable formally in the same manner.

If we want an analog of Sen's theorem in the general case, we have to redefine wildly ramified automorphisms. If the extension L/K is cyclic with $G = \langle\sigma\rangle$, and ferociously ramified we can have either

$$i_G(\sigma) = 1, \quad \text{or} \quad i_G(\sigma) > 1.$$

So, for a completely ramified extension, we define σ to be a *wildly ramified automorphism* if $i_G(\sigma) \geq 1$. In what follows we need some results about Galois extensions of complete fields of degree p; we collect them in the proposition below. We define the *ramification number* of a cyclic extension L/K of degree p as the number $s_G(\sigma)$ (note that it does not depend on the chosen generator σ of $\mathrm{Gal}(L/K)$).

Proposition 3.2 *I. Kummer theory. Suppose* $\mathrm{ch}(K) = 0$ *and* $\zeta = \zeta_p \in K$. *Let* $e' = e_K/(p-1)$. *The cyclic extensions L/K of degree p are classified as follows*

$L = K(\alpha)$	$f_{L/K}$	*ramif. number*
$\alpha^p = 1 + v\cdot(\zeta-1)^p$	$f^{\mathrm{sep}}_{L/K} = p$	0
$\alpha^p = w\pi$	$\overline{L} = \overline{K}$	e'
$\alpha^p = 1 + w\pi^s$, $1 \leq s < e'p$, $p \nmid s$	$\overline{L} = \overline{K}$	$pe' - s$
$\alpha^p = u$	$f^{\mathrm{ins}}_{L/K} = p$	e'
$\alpha^p = 1 + u\pi^{tp}$, $1 \leq t < e'$	$f^{\mathrm{ins}}_{L/K} = p$	$e' - t$

where $v \in U_K$ *and* $\overline{v} \notin \wp(\overline{K})$, $w \in U_K$, $u \in U_K$ *and* $\overline{u} \notin \overline{K}^p$.

II. Artin-Schreier theory.

A) Let L/K be a cyclic extension of degree p and let σ a generator of $G := \mathrm{Gal}(L/K)$. *Then the ramification number* $s := s_G(\sigma)$ *is zero if and only if L/K is unramified. If L/K is completely ramified we have the following possibilities for s:*

(i) Let $\mathrm{ch}(K) = p > 0$.

- *If L/K is totally ramified, then* $s \geq 1$ *and* $p \nmid s$.
- *If L/K is ferociously ramified, then* $s \geq 1$.

(ii) Let $\mathrm{ch}(K) = 0$.

- *If L/K is totally ramified, then* $1 \leq s \leq pe_K/(p-1)$. *If $p|s$, then a primitive p-th root of unity belongs to K and* $s = pe_K/(p-1)$.
- *If L/K is ferociously ramified, then* $1 \leq s \leq e_K/(p-1)$.

B) Let K be of characteristic zero. Suppose that $x^p - x - a$, $a \in K$ *is irreducible. Let α be a root of* $x^p - x - a$. *Then* $L = K(\alpha)$ *is cyclic. If s is its ramification number, we have:*

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

(i) *If* $a \in U_K$, $\overline{a} \notin \wp(\overline{K})$, *then* L/K *is unramified.*

(ii) *If* $a \notin \mathcal{O}_K$, $p \nmid v_K(a)$ *and* $v_K(a) \geq -pe_K/(p-1)$, *then* L/K *is totally ramified and* $s = -v_K(a)$.

(iii) *If* $a = u\pi^{-t}$, $t > 0$, $p|t$, $\overline{u} \notin \overline{K}^p$ *and* $t/p < e_K/(p-1)$, *then* L/K *is ferociously ramified and* $s = t/p$.

If $\mathrm{ch}(K) = p > 0$, *then the same statements are true, the only difference being that if* $a = u\pi^{-t}$, $\overline{u} \notin \overline{K}^p$, *then* $s = t/p$ *is not bounded.*

The proof of the first part is Lemma (2-16) in [H]. Part II is in ch. III of [F-V] (see also [M-W]).

Example 3.3 We realize a Galois extension L/K with the following characteristics:

(1) $[L : K] = 8$, $e_{L/K} = 2$, $f_{L/K} = f^{\mathrm{ins}}_{L/K} = 4$;
(2) $\mathcal{O}_L$ is not monogenic over $\mathcal{O}_K$;
(3) The ramification jumps are not congruent mod 2 and Herbrand's theorem doesn't hold.

Let K be a complete field of characteristic zero. Let $\overline{K} = \mathbb{F}_2(u, v)$ be the field of rational functions in two variables over $\mathbb{F}_2$, and let $A, B \in \mathcal{O}_K$ be such that $\overline{A} = u$, $\overline{B} = v$. Suppose also $e_K = 2$. Consider the irreducible polynomial

$$f(X) = X^4 - A\pi X^2 + B.$$

We define the field L as the splitting field of $f(X)$. Let α be a root of $f(X)$. Then $K(\alpha)/K$ is ferociously ramified of degree 4. Let β be another root of $f(X)$ such that $\beta \neq \pm\alpha$. So, $\gamma = \alpha + \beta$ is such that $L = K(\gamma, \alpha)/K(\alpha)$ is totally ramified, indeed the minimal polynomial of γ over $K(\alpha)$ is

$$X^2 - 2\alpha X - \pi(A - 2\alpha^2/\pi),$$

which is an Eisenstein polynomial, thus $e_{L/K} = 2$; this last argument also shows that $[L : K] = 8$, in fact it suffices to consider the tower of field extensions $L \supset K(\alpha) \supset K$. We show the statement (2) about the non monogenity of $\mathcal{O}_L$ below, by showing that the Hilbert formula does not hold (*cf.* Theorem 5.1). However, by using Proposition 4.1 (A) below, we can write $\mathcal{O}_L = \mathcal{O}_K[\alpha, \gamma]$. In the calculations below, we use Lemma 1.2.

Now, define the K-automorphism $\sigma: L \to L$ by

$$\begin{cases} \sigma(\alpha) = -\beta & \sigma^2(\alpha) = -\alpha \quad \sigma(\beta) = \alpha \\ \sigma^3(\alpha) = \beta & \sigma^4(\alpha) = \alpha, \end{cases}$$

and $\tau: L \to L$ by $\tau(\alpha) = \alpha$, $\tau(\beta) = -\beta$. The group G is dihedral because $\tau\sigma = \sigma^3\tau$.

In order to show Herbrand's theorem we have to compute $i_G(\sigma)$ for σ in G. After some calculations one finds $i_G(\sigma) = 1$, $i_G(\tau) = 4$, $i_G(\sigma^2) = 4$ (indeed, $v_L := v$; we have $i_G(\sigma) : v(\sigma\alpha - \alpha) = v(\alpha + \beta) = 1$, $v(\sigma\gamma - \gamma) = v(-2\beta) = 4$; $i_G(\tau) : v(\tau\alpha - \alpha) = +\infty$, $v(\tau\gamma - \gamma) = 4$; $i_G(\sigma^2) : v(\sigma^2\alpha - \alpha) = 4$, $i_G(\sigma^2) = 5$).

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

The different is computed by considering the tower of extensions $L \supset K(\alpha) \supset K$. So we have:

$$v_L(\mathfrak{D}_{L/K}) = v_L(\mathfrak{D}_{L/K(\alpha)}) + v_L(\mathfrak{D}_{K(\alpha)/K}) = 2e_K + 2v_L\big(f'(\alpha)\big) = 4 + 6 = 10.$$

Hilbert's formula states that $v_L(\mathfrak{D}_{L/K}) = \sum_{\sigma\neq 1} i_G(\sigma) = 16$, so the extension $\mathcal{O}_L/\mathcal{O}_K$ is not monogenic (*cf.* Theorem 5.1).

We check Herbrand's theorem for the normal subgroup $H = \langle\sigma\rangle$. It fixes the f.r-1 extension $L' = K\big((\alpha^2 - \beta^2)\alpha\beta\big)/K$. For G/H we have[3]

$$(G/H)_1 \supset (G/H)_2 = \{1\}.$$

For $u = 3$ we have

$$G_3H/H = G/H \neq \{1\}.$$

We also have $H_0 \supset H_1 = H_2 = H_3 \supset H_4 = \{1\}$, so $\phi_{L/L'}(3) = 3/2$, but $(G/H)_{3/2} = (G/H)_2 = \{1\}$, which means that

$$G_3H/H \neq (G/H)_{3/2} = (G/H)_2 = \{1\}.$$

Thus Herbrand's theorem doesn't hold.

Example 3.4 Let K be a complete field of characteristic zero. Here we construct a Kummer extension L/K which is cyclic of degree p^2 with the following characteristics:

(1) $e_{L/K} = 1$, $f^{\mathrm{ins}}_{L/K} = p^2$;
(2) $\mathcal{O}_L$ is not monogenic over $\mathcal{O}_K$; more precisely $\mathcal{O}_L$ is generated by two elements over $\mathcal{O}_K$; thus L/K is f.r-2;
(3) The ramification jumps are not congruent mod p, so an analog of Sen's theorem does not hold;
(4) Hilbert's formula is not verified.
(5) The Hasse-Arf theorem does not hold.

Suppose $\zeta_{p^2} \in K$ and let $\overline{K} = \mathbb{F}_p(u, v)$ be the field of rational functions in two variables over $\mathbb{F}_p$. The extension $L = K(x)$ is defined by

$$x^{p^2} = (1 + U\pi^{ps})(1 + V\pi^{pt})^p,$$

where $U, V \in U_K$ are such that $\overline{U} = u$, $\overline{V} = v$ and $p \leq pt < s < e'$, $e' = e_K/(p-1)$. Let $G = \langle\sigma\rangle$ where $\sigma(x) = \zeta_{p^2}x$. Put $y = x^p$, then $K(y)/K$ is f.r-1 with ramification number equal $e' - s$. Now consider $Y = y/(1 + V\pi^{pt})$ and $\alpha = (Y-1)/\pi^s$, then

$$\mathcal{O}_{K(y)} = \mathcal{O}_K[\alpha], \quad \overline{K(y)} = \mathbb{F}_p(\sqrt[p]{u}, v).$$

[3]In fact the minimal polynomial of $(\alpha^2 - \beta^2)\alpha\beta$ is $X^2 = B(A^2 - 4B)$, from which one deduces that the ramification jump of L'/K is 1.

Note that $y = (1+\alpha\pi^s)(1+V\pi^{pt})$, thus, as above, we see that $L = K(x)/K(y)$ is f.r-1 with ramification number $e' - t$. Put $\beta = (x-1)/\pi^t$, then

$$\mathcal{O}_L = \mathcal{O}_{K(y)}[\beta], \quad \overline{L} = \mathbb{F}_p(\sqrt[p]{u}, \sqrt[p]{v}).$$

One can show that $\mathcal{O}_L = \mathcal{O}_K[\alpha, \beta]$ (see Proposition 4.1 (A) below). Now we compute $i_G(\sigma)$ and $i_G(\sigma^p)$. We have to evaluate $v_L\big(\sigma(\beta) - \beta\big)$ (recall Lemma 1.2):

$$v_L\big(\sigma(\beta) - \beta\big) = v_L\left(\frac{\sigma(x)-1}{\pi^t} - \frac{x-1}{\pi^t}\right) = \frac{e_K}{p(p-1)} - t.$$

The value of $i_G(\sigma)$ is the minimum between $v_L\big(\sigma(\alpha)-\alpha\big) = e' - s$ and $v_L\big(\sigma(\beta)-\beta\big) = e'/p - t$. This minimum clearly depends on the values of s and t. Assume $s - t > e_K/p$, then $i_G(\sigma) = e' - s =: a$ and $i_G(\sigma^p) = e' - t =: b$. Note that the Herbrand property is far from being true, indeed $i_{K(y)/K}(\sigma|_{K(y)}) = i_G(\sigma)$.

Of course, one can choose s and t such that the ramification jumps are not congruent mod p, so an analog of Sen's theorem does not hold (note that σ is a wildly ramified automorphism). The Hilbert formula is not verified, indeed

$$v_L(\mathfrak{D}_{L/K}) = (p-1)(a+b) \neq \sum_{\sigma \neq 1} i_G(\sigma) = (p^2 - p)a + (p-1)b.$$

The last ramification jump is $b-1$, the Hasse-Arf theorem would state that $\phi_{L/K}(b-1)$ is an integer, but

$$\phi_{L/K}(b-1) = \sum_{i=1}^{b-1} \frac{g_i}{p^2} = a - 1 + \frac{b-a}{p},$$

and we have just said that a, b can be chosen not congruent mod p.

4 Three Types of Monogenic Extensions

In this section we study the $\mathcal{O}_K$-module $\mathcal{O}_L$. It is well-known that $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module ($\mathcal{O}_L$ being a finitely generated module over a principal ring), but one can be more precise.

Proposition 4.1

(A) Let L/K be an extension of complete fields. Let v_K, v_L be discrete valuations of K and L respectively. Let $e = e_{L/K} < +\infty$ and $f = f_{L/K}$. Let π_L be a prime with respect to v_L and let $\vartheta_1, \dots, \vartheta_f$ be elements of $\mathcal{O}_L$ such that their residues form a basis of $\overline{L}$ over $\overline{K}$. Then $\{\vartheta_i \pi_L^j\}_{1 \le i \le f, 0 \le j \le e-1}$ form a basis of the K-space L and of the $\mathcal{O}_K$-module $\mathcal{O}_L$. If $f < +\infty$, then L/K is a finite extension of degree $n = ef$.

(B) In particular, $\mathcal{O}_L$ is monogenic over $\mathcal{O}_K$ in the following two cases:

(i) the extension L/K is of prime degree;

(ii) the extension L/K is ferociously ramified and $\overline{L}/\overline{K}$ is generated by only one element (f.r-1).

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

Proof Part (A) is [F-V, ch. II, Proposition (2.4)]. For part (B) (i) we only have to consider the ferociously ramified case (in the other case see Proposition 2.1). In this case we have $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, where α is a lifting of a such that $\overline{L} = \overline{K}(a)$, by part (A). (B) (ii) immediately follows from (A). ■

In order to study monogenic extensions L/K, we introduce the following terminology.

Definition We say that the extension L/K is in

- Case I: If $\overline{L}/\overline{K}$ is separable.
- Case II: If L/K is ferociously ramified with $\overline{L}/\overline{K}$ generated by one element (f.r-1).
- Case III: If $\mathcal{O}_L/\mathcal{O}_K$ is monogenic and L/K is neither in case I nor in case II.

We recall that the extensions in case I (resp. case II) are monogenic by Proposition 2.1 (resp. Proposition 4.1 (B) (ii)).

4.0.1 The Case III

We show that case III is not empty. Let $f(X) \in \mathcal{O}_K[X]$ be a monic, irreducible polynomial of degree n and $L = K[X]/\big(f(X)\big)$. As always, $\mathfrak{p}_K$ denotes the maximal ideal of $\mathcal{O}_K$. We consider the $\mathcal{O}_K$-algebra

$$B = \mathcal{O}_K[X]/\big(f(X)\big) = \mathcal{O}_K[\alpha].$$

We want to see when $B = \mathcal{O}_L$. We denote $\overline{f(X)}$ the image of $f(X)$ in $\overline{K}[X]$. Let $\overline{f(X)} = \prod_{i\in I} g_i(X)^{e_i}$ be the decomposition of $\overline{f(X)}$ into irreducible factors in $\overline{K}[X]$ and choose a polynomial $G_i(X) \in \mathcal{O}_K[X]$ such that $\overline{G_i} = g_i$. We can determine the maximal ideals of B, as in the following lemma (for a proof *cf.* [S1, Lemme 4, Section 6, ch. I]).

Lemma 4.2 *Let $\mathfrak{p}_i = (\mathfrak{p}_K, G_i)$ be the ideal of B generated by $\mathfrak{p}_K$ and by the canonical image of G_i. The ideals $\mathfrak{p}_i$, $i \in I$ are maximal and distinct ideals and every maximal ideal of B is equal to some $\mathfrak{p}_i$. The quotient $B/\mathfrak{p}_i$ equals the field $k_i = \overline{K}[X]/\big(g_i(X)\big)$.*

Now, we are ready to study the monogenity of $\mathcal{O}_L/\mathcal{O}_K$.

Proposition 4.3

(A) *Let L/K be a completely ramified extension in case III of degree $n = p^{r+s}$ with $r, s \geq 1$ and assume that both $e_{L/K} = p^s$ and $f^{\text{ins}}_{L/K} = p^r$. Suppose that there exists $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Then, the minimal polynomial $f(X)$ of α over K is of the following form*

$$(*) \qquad f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + b, \quad a_i \in \mathfrak{p}_K, \quad b \in U_K$$

and it has the following properties:

(i) $\overline{f(X)} = (X^{p^r} - A)^{p^s} = g(X)^{p^s}$, $\overline{b} = A^{p^s}$, $A \notin \overline{K}^p$.

(ii) For all liftings $G(X) \in \mathcal{O}_K[X]$ of $g(X)$ we have $v_L\big(G(\alpha)\big) = 1$.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

(B) Let $f(X) \in \mathcal{O}_K[X]$ be the polynomial $(*)$ with $n = p^{r+s}$, $r, s \geq 1$. Let α be a root of $f(X)$ and suppose that

(i) $f(X)$ is irreducible;

(ii) $\overline{f(X)} = (X^{p^r} - A)^{p^s}$, $\overline{b} = A^{p^s}$ and $A \notin \overline{K}^p$.

(iii) There exists a lifting $a \in \mathcal{O}_K$ of A such that $v_L(\alpha^{p^r} - a) = 1$.

If we let $L = K[X]/\big(f(X)\big)$, then L/K is in case III and

$$\mathcal{O}_L = \mathcal{O}_K[\alpha], \quad \textit{and} \quad e_{L/K} = p^s, \quad f^{\text{ins}}_{L/K} = p^r.$$

Proof of Proposition 4.3 (A) By hypothesis, $\overline{L}/\overline{K}$ is purely inseparable generated by $\overline{\alpha}$, so $\overline{L} = \overline{K}(\overline{\alpha})$, which means $\overline{\alpha}^{p^r} = A$ for some $A \notin \overline{K}^p$ and for some $r \geq 1$. The minimal polynomial of α is like in $(*)$ and property (i) is clear. We prove (ii). Let π_L be a prime of $\mathcal{O}_L$. Now, suppose by contradiction that there exists G a lifting of g such that $v_L\big(G(\alpha)\big) = E > 1$. Then $\big(\mathfrak{p}_K, G(\alpha)\big) = (\pi_L^{\min\{E, e_{L/K}\}})$ which is not maximal. This contradicts Lemma 4.2 which stated that the ideal $\big(\mathfrak{p}_K, G(\alpha)\big)$ is the maximal ideal of $\mathcal{O}_L$.

(B) The element $\alpha^{p^r} - a$ is a prime of L, hence (*cf.* Proposition 4.1 (A) above) $\mathcal{O}_L = \mathcal{O}_K[\alpha^{p^r} - a, \alpha] = \mathcal{O}_K[\alpha]$. The statements $e_{L/K} = p^s$, $f^{\text{ins}}_{L/K} = p^r$ are clear. ■

The following example (see also Section 6) shows that the class of monogenic extensions of valuation rings is wider than cases I, II.

Example 4.4 Here, we have an extension of monogenic valuation rings which is not in case I or II. Let K be a complete field of characteristic zero. Let $\zeta_{p^2} \in K$. Consider the cyclic extension of degree p^2 defined by $L = K(x)$ where x a root of the polynomial

$$f(X) = X^{p^2} - (1 + u\pi)A^p, \quad A \in U_K, \quad \overline{A} \notin \overline{K}^p, \quad u \in U_K.$$

One sees that $e_{L/K} = p = f^{\text{ins}}_{L/K}$, so L/K is not of case I or II. We show that $\mathcal{O}_L = \mathcal{O}_K[x]$. The conditions of Proposition 4.3 (B) are clearly verified as we now show. Put $Y = x^p$. Now consider $G(X) = X^p - A$, clearly $\overline{f(X)} = \overline{G(X)}^p$ in $\overline{K}[X]$. It is not difficult to see that $x^p = A(1 + U\pi_1)$, where $U \in U_{K(Y)}$ and π_1 is a prime of $K(Y)$. So $v_L\big(G(x)\big) = 1$ and $\mathcal{O}_L = \mathcal{O}_K[x]$. Below (Lemma 5.2) we will also see that the monogenity of valuation rings can be established by using the Herbrand's property, in particular for this example we have $i_G(\sigma) = e_K/(p-1)$ and $i_G(\sigma^p) = pe_K/(p-1)$.

5 Well Ramified Extensions

Here we show that monogenic extensions can be characterized by Herbrand's property (1) as well as other ramification properties.

***Theorem 5.1* (Definition)** *Let L/K be a Galois completely ramified extension. If one of the following equivalent conditions is satisfied, we say that L/K is well ramified.*

(1) The extension $\mathcal{O}_L/\mathcal{O}_K$ is monogenic.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

(2) The Hilbert formula holds.
(3) The Herbrand property holds for all normal subgroups H of G.

Furthermore, for a well ramified extension the ramification jumps are not always congruent mod p.

The implications (1) $\Rightarrow$ (2) and (1) $\Rightarrow$ (3) are classical and explained in the preceding paragraphs. (1) $\Leftrightarrow$ (2) by Remark 5.4 below. The implication (3) $\Rightarrow$ (1) is given by the following lemma.

Lemma 5.2 *Let L/K be a Galois, completely ramified extension of complete fields of degree p^n. Then the following three conditions are equivalent:*

(i) The valuation ring $\mathcal{O}_L$ is monogenic over $\mathcal{O}_K$.
(ii) For every normal subgroup H of G we have $i_{G/H}(\tau) = \frac{1}{e_{L/L^H}} \sum_{\sigma\to\tau} i_G(\sigma)$, for all $\tau \in G/H$, i.e., Herbrand's property holds true for every normal subgroup H of G.
(iii) There exists a normal subgroup H of G such that $\mathcal{O}_L/\mathcal{O}_{L^H}$ and $\mathcal{O}_{L^H}/\mathcal{O}_K$ are monogenic and $i_{G/H}(\tau) = \frac{1}{e_{L/L^H}} \sum_{\sigma\to\tau} i_G(\sigma)$, for all $\tau \in G/H$.

The proof of Lemma 5.2 is based on some notation and results from [BDS1], which we now recall. If L/K is Galois put $\mathfrak{a}_L(\sigma) = \mathfrak{p}_L^{i_G(\sigma)}$. Let $B = \mathcal{O}_L$ and $A = \mathcal{O}_K$. The following definition is due to de Smit.

Definition The *monogenity conductor* $\mathfrak{r}_{B/A}$ of B over A is the ideal $\mathfrak{p}_L^n$ where n is the smallest integer for which there is an $\alpha \in B$ with $\mathfrak{p}_L^n \subset A[\alpha]$. We also write $\mathfrak{r}_{L/K}$ for $\mathfrak{r}_{B/A}$.

Therefore $\mathfrak{r}_{B/A} = B$ if and only if B/A is monogenic. Let H be a subgroup of G (not necessarily normal), one can show[4] that for $K \subset L^H \subset L$

$$\mathfrak{a}_{L^H}(\tau) \mid \prod_{\sigma\to\tau} \mathfrak{a}_L(\sigma).$$

For all K-embeddings τ of L^H in L that are not the inclusion, let $\mathfrak{d}(\tau)$ be the ideal of $\mathcal{O}_L$ such that

$$\mathfrak{d}(\tau)\mathfrak{a}_{L^H}(\tau) = \prod_{\sigma\to\tau} \mathfrak{a}_L(\sigma).$$

We have the following proposition (for a proof see Th. 2.2 and Proposition 3.2 in [BDS1]).

Proposition 5.3 *Let L/K be a finite, Galois extension. Recall that $\mathfrak{D}_{L/K}$ denotes the different of L/K.*

(i) We have

$$\mathfrak{D}_{L/K} \cdot \mathfrak{r}_{L/K} = \prod_{\sigma\neq 1} \mathfrak{a}_L(\sigma).$$

[4] All the statements which follow are shown in [BDS1].

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

(ii) We have

$$\mathfrak{r}_{L/L^H}\cdot\mathfrak{r}_{L^H/K}\prod_{\tau\neq 1}\mathfrak{d}(\tau)=\mathfrak{r}_{L/K},$$

where τ runs over all K-embeddings of L^H in L that are not the inclusion.

Remark 5.4 Proposition 5.3 (i) gives Hilbert's formula in general. In fact if we take the valuation (in L) we obtain

$$v_L(\mathfrak{D}_{L/K})+n=\sum_{\sigma\neq 1}i_G(\sigma)=\sum_{i\geq 0}(|G_i|-1),$$

where n is the valuation (in L) of the monogenity conductor $\mathfrak{r}_{L/K}$.

The above remark shows that (1) is equivalent to (2), in fact the number n in the formula is zero if and only if L/K is monogenic.

Proof of Lemma 5.2 We use the above notations. The implications (i) $\Rightarrow$ (ii) and (i) $\Rightarrow$ (iii) are Herbrand's property. We show (ii) $\Rightarrow$ (i) and (iii) $\Rightarrow$ (i).

(ii) $\Rightarrow$ (i). We have to show that

$$\Big\{\forall H\lhd G, i_{G/H}(\tau)=\frac{1}{e_{L/L^H}}\sum_{\sigma\to\tau}i_G(\sigma)\Big\}\quad\Rightarrow\quad\{\mathcal{O}_L/\mathcal{O}_K\text{ is monogenic}\}.$$

By induction on p^n, the degree of L/K. For $n=1$ it is verified. Now, let H be a normal subgroup of G of order p^{n-1}. Since $i_{G/H}(\tau)=1/e_{L/L^H}\sum_{\sigma\to\tau}i_G(\sigma)$ we have $\mathfrak{d}(\tau)=1$ for all $\tau\neq 1$ in G/H, therefore

$$(*)\qquad \mathfrak{r}_{L/L^H}\cdot\mathfrak{r}_{L^H/K}=\mathfrak{r}_{L/K}.$$

We know that $\mathfrak{r}_{L^H/K}=(1)$, because L^H/K is of degree p and now we show that $\mathfrak{r}_{L/L^H}=(1)$. The inductive hypothesis on H is

$$\Big\{\forall T\lhd H, i_{H/T}(\gamma)=\frac{1}{e_{L/L^T}}\sum_{\substack{s\in H\\ s\to\gamma}}i_H(s)\Big\}\quad\Rightarrow\quad\{\mathcal{O}_L/\mathcal{O}_{L^H}\text{ is monogenic}\}.$$

We show that for any $T\lhd H$, $i_{H/T}(\gamma)=\frac{1}{e_{L/L^T}}\sum i_H(s)$. Let $\gamma\in H/T$ and let $s\in H$ be such that $s\equiv\gamma \bmod T$, then

$$i_{H/T}(\gamma)=\inf_{x\in\mathcal{O}_{L^T}\setminus\{0\}}v_{L^T}\big(\gamma(x)-x\big)=i_{G/T}(\gamma).$$

By hypothesis we also have

$$\begin{aligned}i_{H/T}(\gamma)=i_{G/T}(\gamma)&=\frac{1}{e_{L/L^T}}\sum_{\substack{s\to\gamma\\ s\in G}}i_G(s)=\frac{1}{e_{L/L^T}}\sum_{\substack{s\to\gamma\\ s\in H}}i_G(s)+\frac{1}{e_{L/L^T}}\sum_{\substack{s\to\gamma\\ s\in G\setminus H}}i_G(s)\\ &=\frac{1}{e_{L/L^T}}\sum_{\substack{s\to\gamma\\ s\in H}}i_H(s),\end{aligned}$$

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

because the sum over $s \in G \setminus H$ is empty (in fact if $x \in G$ such that $x \equiv \gamma \bmod T$, then $x \equiv s \bmod T$ which implies that $x \in H$). Hence the inductive hypothesis is verified and the extension L/L^H is well ramified which means that $\mathfrak{r}_{L/L^H} = 1$ and by $(*)$ we are done.

Now consider (iii) $\Rightarrow$ (i). Let H be a subgroup like in the hypothesis. Since $i_{G/H}(\tau) = 1/e_{L/L^H} \sum_{\sigma \to \tau} i_G(\sigma)$ we have $\mathfrak{d}(\tau) = 1$ for all $\tau \neq 1$ in G/H, therefore

$$\mathfrak{r}_{L/L^H} \cdot \mathfrak{r}_{L^H/K} = \mathfrak{r}_{L/K}.$$

But, by hypothesis, we have $\mathfrak{r}_{L/L^H} = B$ and $\mathfrak{r}_{L^H/K} = \mathcal{O}_{L^H}$ involving $\mathfrak{r}_{L/K} = (1)$, *i.e.*, B/A is monogenic. So we are done. ■

The proof of Theorem 5.1 will be achieved by explaining the remark about ramification jumps. Naturally we should not consider a classical extension, because we know that in this case the ramification jumps are congruent mod p (Proposition 2.1 (iii)). Take K with $e_K = p(p-1)m$, and m prime to p. For example take K' with $e_{K'} = m$ and adjoin a p^2 root of unity. Consider $x^{p^2} = 1 + u\pi^{p^2 s}$, $\overline{u} \notin \overline{K}^p$ and $s < e_K/p^2$ (this last condition implies that the first ramification number is $> e_K/\big(p(p-1)\big)$). Let $L = K(x)$. The extension L/K is clearly f.r-1 so well ramified. We find $i_G(\sigma^p) = e' - s$ and $i_G(\sigma) = e'/p - s$ (recall $e' = e_K/(p-1)$) hence we have $i_G(\sigma^p) - i_G(\sigma) = m(p-1) \not\equiv 0 \pmod p$.

Remark 5.5 *The analog of the Herbrand property for the function s_G is not true.* Let L/K be a completely and well ramified extension. We show that for a normal subgroup H of G we might have

$$s_{G/H}(\tau) \neq \frac{1}{e_{L/L^H}} \sum_{\sigma \to \tau} s_G(\sigma).$$

This is seen by considering Example 4.4 (case III), where we have $s_G(\sigma) = e'$ and $s_{G/H}(\sigma) = pe' - 1$. For this reason, below, we will only consider the function i_G.

6 Extensions in Case III

The example 4.4 shows that case III is not empty. For extensions in case III we can give a structure theorem.

Theorem 6.1 *Let L/K be a Galois, completely ramified extension in case III. Then there exists a Galois, totally ramified subextension T/K with $T \neq K$ and $T \neq L$, such that L/T is f.r-1.*

We need some lemmas. First of all we recall that a subextension of a well ramified extension is well ramified (see [BDS1, Corollary (4.3)]).

Lemma 6.2 *Let $K \subseteq L \subseteq M$ be finite separable extensions of complete fields. Then the number of elements needed to generate $\mathcal{O}_L$ as a $\mathcal{O}_K$-algebra is at most the number of elements needed to generate $\mathcal{O}_M$ over $\mathcal{O}_K$.*

The key lemma is the following.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

Lemma 6.3 *Let L/K be a Galois and completely ramified extension. Assume that there exists a Galois subextension T/K, $T \neq K$ and $T \neq L$ such that L/T is totally ramified and T/K is f.r-1. Then L/K cannot be well ramified.*

Proof Let π_1 be a prime of L such that $\mathcal{O}_L = \mathcal{O}_T[\pi_1]$. Let $\alpha \in T$ be such that $\mathcal{O}_T = \mathcal{O}_K[\alpha]$. By Proposition 4.1 we have $\mathcal{O}_L = \mathcal{O}_K[\alpha, \pi_1]$. Let σ be an automorphism of T and denote $\widetilde{\sigma}$ a lifting of σ to G. By Lemma 1.2 we have $i_G(\widetilde{\sigma}) = \min\{v_L(\widetilde{\sigma}\pi_1 - \pi_1), v_L(\sigma\alpha - \alpha)\}$. We show that $i_G(\widetilde{\sigma}) = v_L(\widetilde{\sigma}\pi_1 - \pi_1)$. Suppose we had $i_G(\widetilde{\sigma}) = v_L(\sigma\alpha - \alpha)$, then

$$(*) \qquad \frac{i_G(\widetilde{\sigma})}{e_{L/T}} = v_T(\sigma\alpha - \alpha) = i_{T/K}(\sigma).$$

But, by Herband's property we have

$$(**) \qquad i_{T/K}(\sigma) = \frac{1}{e_{L/T}} \sum_{s \to \sigma} i_G(s) = \frac{i_G(\widetilde{\sigma})}{e_{L/T}} + \frac{1}{e_{L/T}} \sum_{\substack{s \to \sigma \\ s \neq \widetilde{\sigma}}} i_G(s).$$

So from $(*)$ and $(**)$ we deduce that

$$\frac{1}{e_{L/T}} \sum_{\substack{s \to \sigma \\ s \neq \widetilde{\sigma}}} i_G(s) = 0,$$

but this is not possible because $i_G(s) \geq 1$ for all $s \in G$. We have shown that

$$(2) \qquad i_G(s) = v_L(s\pi_1 - \pi_1), \qquad \text{for all } s \in G.$$

Now, note that $\alpha \notin \mathcal{O}_K[\pi_1]$. Indeed, we should have $\alpha = \sum_{i \geq 0} a_i \pi_1^i$, $a_i \in \mathcal{O}_K$ (the sum $\sum_{i \geq 0}$ is finite), but passing mod π_1, we find $\alpha \equiv a_0 (\operatorname{mod} \pi_1)$ which is impossible.

By (2) and by Hilbert's formula we have

$$(3) \qquad v_L(\mathfrak{D}_{L/K}) = \sum_{\substack{s \in G \\ s \neq 1}} i_G(s) = \sum_{\substack{s \in G \\ s \neq 1}} v_L(s\pi_1 - \pi_1) = v_L\big(f'(\pi_1)\big),$$

where $f(X)$ denotes the minimal polynomial of π_1 over K.

Now we define (*cf.* [S1, ch. III, Section 6]) the ideal $\mathfrak{r}_{\pi_1} = \{x \in \mathcal{O}_L : x\mathcal{O}_L \subseteq \mathcal{O}_K[\pi_1]\}$ (note that $\mathfrak{r}_{\pi_1}$ is the largest ideal of $\mathcal{O}_L$ which is contained in $\mathcal{O}_K[\pi_1]$). We have (again [S1, ch. III, Section 6])

$$\mathfrak{D}_{L/K} = f'(\pi_1) \cdot \mathfrak{r}_{\pi_1},$$

but (3) implies $\mathfrak{r}_{\pi_1} = (1)$, which implies $\mathcal{O}_L = \mathcal{O}_K[\pi_1]$, but we have shown that this is not possible because $\alpha \notin \mathcal{O}_K[\pi_1]$. So we are done. ∎

Proof of Theorem 6.1 By induction on $[L : K]$. Let M/K be a Galois subextension of L/K such that $[L : M] = p$. Let T/K be a Galois subextension of M/K such that T/K is totally ramified and M/T in case II. Applying Lemma 6.3 to L/T we deduce that L/M is ferociously ramified, hence in case II. ∎

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

6.1 p-Elementary Extensions in Case III

We have seen cyclic extensions in case III (*cf.* Ex. 4.4). Here we explain how to construct examples of p-elementary extensions. This construction is independent of the characteristic of the field K. Let us consider two Galois, totally ramified extensions K_1/K and K_2/K of degree p. We study the compositum $L = K_1K_2/K$. We want to find conditions on K_1/K and K_2/K such that L/K is in case III. The notation is the following: $L = K(x, y)$, $K_1 = K(x)$, $K_2 = K(y)$, $\langle\sigma\rangle = \mathrm{Gal}(K_1/K)$, $\langle\tau\rangle = \mathrm{Gal}(K_2/K)$ where K_1/K and K_2/K. We choose the minimal polynomial of x and y as an Artin-Schreier polynomial, so let

$$X^p - X - \pi^{-(p-1)}A, \quad \overline{A} \in \overline{K}^p$$

be the minimal polynomial of x over K. For simplicity we choose $A := \alpha^p$, $\alpha \in U_K$. The ramification number of K_1/K is $p-1$, so $i_{K_1/K}(\sigma) = p$. Let $\widetilde{\sigma}, \widetilde{\tau}$ be liftings of σ, τ to G. Now let $f(Y) = Y^p - Y - \pi^{-(p-1)}B$ be the minimal polynomial of y over K. Note that by Herbrand's property we have $i_G(\widetilde{\sigma}) = i_G(\widetilde{\tau}) = 1$. In fact $i_{K_1/K}(\sigma) = p = \sum_{s\mapsto\sigma} i_G(s)$ and the sum is taken over p elements which are all ≥ 1. We want to impose conditions on the unit B in order to have L/K in case III. So we consider $f(Y)$ over K_1.

The element $\pi_1 = \pi x$ is a prime of K_1 (as one can see immediately) and we have

$$\pi_1^p = \pi^p x^p = \pi^p(x + \pi^{-(p-1)}A) = \pi A\Omega,$$

where $\Omega \in U_{K_1}^{(p-1)^2}$, so $\pi = A^{-1}\Omega^{-1} \cdot \pi_1^p$. So the polynomial $f(Y)$ over K_1 becomes

$$f(Y) = Y^p - Y - A^{p-1}\Omega^{p-1}B\pi_1^{-p(p-1)}.$$

Now consider the element $z = y\pi_1^{p-1}$, we have:

$$z^p - \pi_1^{(p-1)^2}z = A^{p-1}B\Omega^{p-1}. \tag{4}$$

Which properties must the unit B have in order to have L/K_1 f.r-1 and L/K in case III?

Suppose that $\overline{B} \notin \overline{K}^p$. Then L/K_1 is f.r-1 with ramification number equal to $p-1$, because we have chosen $A = \alpha^p$. Is it possible that L/K is in case III? We compute the value of the different of L/K in two different ways:

(1) by using the Hilbert formula (it holds because we are supposing that L/K is in case III, *i.e.*, well ramified!);
(2) by using the tower product formula for the different.

(1) From $i_G(\widetilde{\sigma}) = i_G(\widetilde{\tau}) = 1$, Hilbert formula implies

$$v_L(\mathfrak{D}_{L/K}) = (p^2 - 1).$$

(2) The explicit calculation shows that

$$v_L(\mathfrak{D}_{L/K}) = v_L(\mathfrak{D}_{L/K_1}) + v_L(\mathfrak{D}_{K_1/K}) = (p-1)^2 + p(p-1).$$

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

(Note that $v_L(\mathfrak{D}_{L/K_1}) = (p-1)^2$ is computed by using the polynomial (4).) So the two values are equal (*i.e.*, $p^2 - 1 = (p-1)^2 + p(p-1)$) if and only if $p = 1$ or $p = 2$. So in the case of the prime 2 the extension L/K is well ramified.

Now we continue the discussion in case $p \neq 2$. We have to consider a unit B such that $\overline{B} \in \overline{K}^p$. Take

$$B = \beta^p + \pi^{p-2}\gamma$$

where $\beta \in U_K \setminus U_K^1$ and $\gamma \in U_K$ such that $\overline{\gamma} \notin \overline{K}^p$. We consider the element $\omega = (z - \beta\alpha)/(\pi_1^{p-2})$, the condition on B (in particular $\overline{\gamma} \notin \overline{K}^p$) shows that $\mathcal{O}_L = \mathcal{O}_{K_1}[\omega]$. By computing the minimal polynomial of ω over K_1 we find

$$v_L(\mathfrak{D}_{L/K_1}) = (p-1)^2 - (p-2)(p-1) = p - 1.$$

Now we compute the different of L/K.

$$v_L(\mathfrak{D}_{L/K}) = v_L(\mathfrak{D}_{L/K_1}) + v_L(\mathfrak{D}_{K_1/K}) = (p-1) + p(p-1) = p^2 - 1,$$

which is the value given by Hilbert formula, so by Theorem 5.1 the extension L/K is well ramified.

7 Ramification Theory for Well Ramified Extensions

Here, we assume that L/K is completely, well ramified and Galois. In the well ramified case one can show that the double filtration defined in Section 1 is reduced to a single filtration, *i.e.*,

- case I: $G_i = H_i$, $i \geq 1$.
- case II: $G_i = H_{i+1}$, $i \geq 1$ (*cf.* Proposition 2.1 (iv)).
- case III: $G_i = H_{i+1}$, $i \geq 1$.

We don't show the above statement in case III because we consider another filtration which allows us to simultaneously deal with cases I, II and III.

Definition Let L/K be a finite Galois extension. The modified i-th ramification group $G[i]$ for $i \geq 1$ is defined by

$$G[i] = \{\sigma \in \mathrm{Gal}(L/K) : i_{L/K}(\sigma) \geq i\}.$$

We also define a modified upper numbering for ramification groups by $G\big(\varphi_{L/K}(u)\big) = G[u]$.

7.1 The Modified Hasse-Herbrand Function

Definition The modified Hasse-Herbrand function $\varphi_{L/K}(u)$, $u \in \mathbb{R}_{\geq 0}$ is defined as follows

$$\varphi_{L/K}(u) = \int_0^u \frac{|G[t]|}{e_{L/K}} \mathrm{d}t.$$

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

If $m \le u \le m+1$, where m is a nonnegative integer, we have

$$\varphi_{L/K}(u) = \frac{1}{e_{L/K}}\big(g_1 + \cdots + g_m + g_{m+1}(u-m)\big), \quad g_i = |G[i]|$$

and clearly $\varphi_{L/K}(m) = \sum_{i=1}^{m} g_i/e_{L/K}$ for $m \ge 1$. We drop the index L/K in $\varphi_{L/K}$ if there is no risk of confusion. Note that in case I we have $\varphi_{L/K}(u) = 1 + \phi_{L/K}(u-1)$, where $\phi_{L/K}$ is the classical Hasse-Herbrand function.

Proposition 7.1

(a) *The function φ is continuous, piecewise linear, increasing and convex.*
(b) $\varphi(0) = 0$.
(c) *If φ'_r and φ'_l denote the right and the left derivatives then:*

$$\varphi'_r(u) = \varphi'_l(u) = g_u/e_{L/K},$$

if $u \notin \mathbb{N}$;

$$\varphi'_l(u) = g_u/e_{L/K} \quad \text{and} \quad \varphi'_r(u) = g_{u+1}/e_{L/K} \quad \text{if } u \in \mathbb{N}.$$

(d) *The map φ is a homeomorphism of $[0,+\infty)$ onto $[0,+\infty)$.*
(e) *The preceding properties (a)–(d) characterize the function φ.*

The inverse map of φ is denoted by ψ. There is an analog of the above proposition for the map ψ, see [S1, Prop. 13]. The next goal is to show Herbrand's theorem for well ramified extensions. We need some lemmas.

Lemma 7.2 $\varphi_{L/K}(u) = \frac{1}{e_{L/K}} \sum_{\sigma \in G} \inf\big(i_G(\sigma), u\big)$.

Proof Let $\vartheta(u)$ be the function defined by the right hand. It is a continuous and piecewise linear function and $\vartheta(0) = 0$. If $m < u < m+1$, $m \in \mathbb{N}$, then the derivative $\vartheta'(u)$ equals the number of $\sigma \in G$ such that $i_G(\sigma) \ge m+1$ multiplies by $1/e_{L/K}$; so we have $\vartheta'(u) = g_{m+1}/e_{L/K}$ which is $\varphi'(u)$; so by Proposition 7.1 φ and ϑ coincide. ■

Now let T be a normal subgroup of G.

Lemma 7.3 *Let $\sigma \in G/T$ and put $j(\sigma) = \sup\{i_G(s) : s \in G \text{ and } s \equiv \sigma \bmod T\}$. Then*

$$i_{G/T}(\sigma) = \varphi_{L/L^T}\big(j(\sigma)\big).$$

Proof Let $s \in G$ be an element such that $s \equiv \sigma \bmod T$ and $i_G(s) = j(\sigma)$. Put $m = i_G(\sigma)$. If $t \in T$ belongs to $T[m]$ we have $i_G(t) \ge m$, hence $i_G(st) \ge m$ and $i_G(st) = m$. On the other hand, if t does not belong to $T[m]$, then $i_G(t) < m$ and $i_G(st) = i_G(t)$. In both cases we have $i_G(st) = \inf\big(i_G(t), m\big)$. By Herbrand's property we have

$$i_{G/T}(\sigma) = \frac{1}{e_{L/L^T}} \sum_{t \in T} \inf\big(i_G(t), m\big)$$

and by applying the preceding lemma to the group T, we have $i_{G/T}(\sigma) = \varphi_{L/L^T}(m)$. ■

Finally we can state and prove the analog of Herbrand theorem.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

Theorem 7.4 *Let L/K be a well ramified extension. The ramification for a quotient G/T is given by*

Lower numbering: $G[u]T/T = (G/T)[v]$, $v = \varphi_{L/L^T}(u)$.
Upper numbering: $G(\nu)T/T = (G/T)(\nu)$, *for all* $\nu \geq 0$.

Proof For the lower numbering we have

$$\sigma \in G[u]T/T \Leftrightarrow j(\sigma) \geq u \Leftrightarrow \varphi_{L/L^T}\big(j(\sigma)\big) \geq \varphi_{L/L^T}(u)$$
$$\Leftrightarrow i_{G/T}(\sigma) \geq \varphi_{L/L^T}(u) \Leftrightarrow \sigma \in (G/T)[v].$$

For the modified upper numbering one can show an analog of the multiplicativity in tower for the functions φ and ψ (the proof goes exactly as in [S1, ch. IV, Prop. 15]).

Proposition 7.5 *We have*

$$\varphi_{L/K} = \varphi_{L^T/K} \circ \varphi_{L/L^T}, \quad \psi_{L/K} = \psi_{L/L^T} \circ \psi_{L^T/K}.$$

Now we proceed as in the proof of Prop. 14 in *loc. cit.* ■

The Hasse-Arf theorem with respect to the modified upper numbering was shown by J. Borger. For the reader's convenience, we reproduce his proof in Section 10.4.3.

Theorem 7.6 **(Borger)** *The modified upper ramification jumps of abelian well ramified extensions are integers.*

As we have already noted, a general ramification theory does not exist yet. In [Zh], Zhukov gives a good ramification theory under the hypothesis $[\overline{K} : \overline{K}^p] = p$. This hypothesis is, however, quite restrictive; in fact, in some sense, it reduces to the theory of well ramified extensions. Roughly speaking, Zhukov, by "eliminating wild ramification" à la Epp (*cf.* [E]) can reduce, in a canonical way, the study of a completely ramified extension to a ferociously ramified one. For a ferociously ramified extension the hypothesis on $[\overline{K} : \overline{K}^p]$ imply that the extension to consider is in fact f.r-1 and for this there exists a good ramification theory as we have seen.

Note that under the hypothesis $[\overline{K} : \overline{K}^p] = p$, case III can always be reduced to case II by "eliminating wild ramification"; by this we mean that there exists a finite extension K_1/K such that LK_1/K_1 is f.r-1. But in general this is not possible. For instance take Ex. 4.4 with the following additional hypotheses: (i) $\overline{u} \notin \overline{K}^p$, (ii) $[\overline{K}(\sqrt[p]{\overline{u}}, \sqrt[p]{\overline{A}}) : \overline{K}] = p^2$. Now consider the extension $K_1 = K(\sqrt[p]{\pi})$. Then LK_1/K_1 is ferociously ramified (we have eliminated the wild ramification), and in particular it is f.r-2, *i.e.*, not in case II.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

8 Artin Character, Representation and Conductor

Let L/K be a finite Galois extension. The Artin function a_G and the Swan function Sw_G are defined as follows

$$\text{Artin function:} \quad \begin{cases} a_G(\sigma) = -f_{L/K}i_G(\sigma) & \sigma \neq 1 \\ a_G(1) = -\sum_{\sigma\neq 1} a_G(\sigma) \end{cases}$$

$$\text{Swan function:} \quad \begin{cases} Sw_G(\sigma) = -f_{L/K}s_G(\sigma) & \sigma \neq 1, \sigma \in G_0, \\ Sw_G(1) = -\sum_{\sigma\neq 1} Sw_G(\sigma) \\ Sw_G(\sigma) = 0, & \text{if } \sigma \notin G_0. \end{cases}$$

In [K3], Kato considers the function $S_G = 1/f_{L/K}Sw_G$ instead of the function Sw_G (see Remark (6.7), *loc. cit.*). In what follows we will use both functions, S_G and Sw_G.

Clearly a_G and Sw_G are class functions (because i_G and s_G are) so they are sums with complex coefficients of irreducible characters of G. It is a fundamental theorem of Artin that a_G is an actual character of G (*i.e.*, sum with nonnegative integers as coefficients), see [S1, ch. VI]. From this one can deduce that Sw_G is also a character. The representation (defined up to isomorphism) affording the character a_G (resp. Sw_G) is called the Artin (resp. Swan) representation of group G attached to the extension L/K.

The Artin conductor $A_G(\chi)$ (resp. the Swan conductor $SW_G(\chi)$) of a character χ of G is the integer

$$(5) \qquad A_G(\chi) = (a_G, \chi) = \frac{1}{|G|}\sum_{\sigma\in G} a_G(\sigma)\chi(\sigma)$$
$$(\text{resp. } SW_G(\chi) = (Sw_G, \chi) = \frac{1}{|G|}\sum_{\sigma\in G} Sw_G(\sigma)\chi(\sigma)).$$

We show that in general (5) is not (neither for Sw_G nor for a_G) an integer, *cf.* Example 8.1 below. In [K3], Kato gives a definition of a Swan conductor for characters of degree 1, without assuming $\overline{L}/\overline{K}$ separable. In case I and II he shows that his conductor equals the formula (5) for Sw_G.

One can ask whether the Artin function a_G is a character of G in the well ramified case. We will see that (as in the classical case) this is equivalent to show the Hasse-Arf theorem for cyclic extensions. Note that in order to show that a_G *is not* a character we show that for an irreducible character χ of G, the Schur product (a_G, χ) *is not* a nonnegative integer.

Example 8.1 We consider a Galois extension L/K which is not well ramified, having the following properties:

(1) $[L : K] = 8$, $e_{L/K} = 4$, $f_{L/K} = f^{\text{ins}}_{L/K} = 2$;
(2) the functions Sw_G and a_G are not characters of G.

Assume that $e_K = 2$ and $\overline{K} = \mathbb{F}_2(u, v)$ as in ex. 3.3. Let L be the splitting field of the following polynomial

$$f(X) = X^4 - A\pi^2X^2 + \pi B, \quad A, B \in U_K, \quad \overline{A} = u, \quad \overline{B} = v.$$

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

Let α and β be two distinct roots of $f(X)$ and $\alpha \neq -\beta$. Then $K(\alpha)/K$ is totally ramified and the element $\gamma = (\alpha+\beta)/\pi$ proves that $f^{\mathrm{ins}}_{L/K} = 2$, in fact we have

$$\gamma^2 = \frac{\alpha^2+\beta^2+2\alpha\beta}{\pi^2} = A + \frac{2}{\pi^2}\alpha\beta,$$

and if we see this polynomial mod $\mathfrak{p}_{K(\alpha)}$, we obtain that $L = K(\gamma,\alpha)/K(\alpha)$ is ferociously ramified. So, $e_{L/K} = 4$ and $f^{\mathrm{ins}}_{L/K} = 2$. For a description of the Galois group $\mathrm{Gal}(L/K)$ see Ex. 3.3. A lengthy calculation[5] gives the following values of s_G and i_G

$$s_G(\sigma) = 3, \quad s_G(\tau) = 5, \quad s_G(\sigma^2) = 8,$$
$$i_G(\sigma) = 4, \quad i_G(\tau) = 5, \quad i_G(\sigma^2) = 8.$$

We show that neither a_G nor Sw_G are characters. In fact consider the character (of degree 1) $\psi\colon G \to \mathbb{C}^*$ defined by $\psi(\sigma) = i$, $\psi(\tau) = 1$. We find $(a_G,\psi) = 21/2$ and $(Sw_G,\psi) = 19/2$, we only compute (a_G,ψ) the other being similar.

$$(a_G,\psi) = \frac{1}{8}\Big[a_G(1) + \sum_{\sigma\neq 1} a_G(\sigma)\psi(\sigma)\Big] = \frac{1}{4}\Big[\sum_{\sigma\neq 1} i_G(\sigma)\big(1-\psi(\sigma)\big)\Big]$$
$$= \frac{1}{4}[4(1-i) + 2\cdot 8 + 4(1+i) + 4(1-i) + 2\cdot 5 + 4(1+i)] = \frac{21}{2}.$$

Note that L/K is not well ramified because the Hilbert formula does not hold for such an extension, see Theorem 5.1.

8.1 Artin Character in the Well Ramified Case

We show that in the well ramified case a_G is an actual character of G by using Borger's theorem (*cf.* Theorem 7.6). As in the classical case, we have to show congruences satisfied by the differences of ramification jumps for cyclic extensions (like Sen's theorem).

Proposition 8.2 *Let L/K be a cyclic, well ramified extension. The following are equivalent:*

(i) (Hasse-Arf) The upper modified ramification jumps are integers.
(ii) The function a_G is an actual character of G.

Proof The implication (ii) ⇒ (i) is clear. For the implication (i) ⇒ (ii), at first we observe that if H is a normal subgroup of G, then for $\sigma \in G/H$ we have

$$(*) \qquad a_{G/H} = \#(a_G),$$

this comes from the Herbrand property, indeed

$$\#a_G(\sigma) = \frac{1}{|H|}\sum_{s\to\sigma} a_G(s) = -\frac{1}{e_{L/L^H}}\sum_{s\to\sigma} i_G(s) = a_{G/H}(\sigma).$$

[5]It is similar to that in Ex. 3.3, by considering $\mathcal{O}_L = \mathcal{O}_K[\gamma,\alpha]$.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

Lemma 8.3 *Let H be a subgroup of G. Then we have*[6]

$$a_G|_H = \lambda r_H + f_{L^H/K} a_H, \quad \lambda = f_{L^H/K} v_{L^H}(\mathfrak{D}_{L^H/K})$$

where r_H is the character of the regular representation of H.

Proof If $\sigma \in H$, $\sigma \neq 1$, we have

$$a_G(\sigma) = -f_{L/K} i_G(\sigma), \quad a_H(\sigma) = -f_{L/L^H} i_H(\sigma), \quad r_H(\sigma) = 0,$$

so, by $i_H(\sigma) = i_G(\sigma)$, we have $a_G(\sigma) = \lambda r_H(\sigma) + f_{L^H/K} a_H(\sigma)$.

Take $\sigma = 1$. We have $a_G(1) = f_{L/K} v_L(\mathfrak{D}_{L/K})$ because L/K is well ramified, similarly we have $a_H(1) = f_{L/L^H} v_L(\mathfrak{D}_{L/L^H})$, so

$$a_G(1) = \lambda r_H(1) + a_H(1) = f_{L/K} v_L(\mathfrak{D}_{L^H/K}) + f_{L/K} v_L(\mathfrak{D}_{L/L^H}) = f_{L/K} v_L(\mathfrak{D}_{L/K}).$$

So we are done. ■

Corollary 8.4 *Let ψ be a character of H, then*

$$\big(a_G, \operatorname{Ind}_H^G(\psi)\big) = \lambda\psi(1) + f_{L^H/K}(a_H, \psi).$$

Proof It suffices to observe that $(a_G, \psi^*) = (a_G|_H, \psi)$. ■

We come back to the proof of Proposition 8.2. We have to show that (a_G, χ) is a nonnegative integer for any irreducible character χ. A theorem of Brauer states that every character of a finite group G is a linear combination with coefficients in $\mathbb{Z}$ of characters χ_i^* induced by characters χ_i of degree 1 of subgroups H_i of G, see [S2, ch. 10, Th. 19]. So $\chi = \sum n_i \chi_i^*$, where χ_i are characters of degree 1 of subgroups H_i of G and $n_i \in \mathbb{Z}$. Thus, by the above corollary, we have to show that (a_G, χ^*) is a nonnegative integer if χ is a character of degree 1. Let χ be a character of a cyclic group G and suppose $|G| = p^n$. Denote i_j the modified ramification jumps of G so that $G = G[i_1] \supset G[i_2] \supset \cdots \supset G[i_n] \neq \{1\}$ are the modified ramification groups and let i_χ be the biggest integer such that the restriction of χ to the ramification group $G[i_\chi]$ is not the trivial character. We have (put $g_i = |G[i]|$)

$$\begin{aligned}(a_G, \chi) &= \frac{1}{p^n} \sum_{\sigma \in G} a_G(\sigma)\chi(\sigma) = \frac{a_G(1) - \sum_{\sigma \neq 1} i_G(\sigma)\chi(\sigma)}{e_{L/K}} \\ &= \frac{1}{e_{L/K}} \sum_{j=1}^{n} \sum_{\sigma \in G[i_j] \setminus G[i_j+1]} \big(1 - \chi(\sigma)\big) \qquad (6) \\ &= \frac{g_{i_1}}{e_{L/K}} + \frac{(i_2 - i_1) g_{i_2}}{e_{L/K}} + \cdots + \frac{(i_\chi - i_{\chi-1}) g_{i_\chi}}{e_{L/K}} = \varphi_{L/K}(i_\chi),\end{aligned}$$

because $\sum_{\sigma \in G[i_j] \setminus G[i_j+1]} \big(1 - \chi(\sigma)\big) = 0$ for $j > i_\chi$; the number $\varphi_{L/K}(i_\chi)$ is integer because we suppose Hasse-Arf's theorem holds, so we are done. ■

[6] With $a_G|_H$ we denote the restriction of a_G to H, *i.e.*, if $\alpha\colon H \to G$ is the canonical injection, then $a_G|_H = a_G \circ \alpha$.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

9 A New Proof of a Result of Miki

We show how to deduce a result of Miki (*cf.* [M, Prop. 10]) by using [H] and [Wy]. We will need this result in Section 10. It can be read as saying that for small absolute ramification index the cyclic completely ramified extensions are always totally ramified. We introduce the genoma of a cyclic extension.

***Definition* (Genoma)** Let L/K be a cyclic extension of degree p^n. The genoma of L/K is the n-tuple $(A_1, \dots, A_n)$ where a letter A_i is associated to the extension K_i/K_{i-1}, $i = 1, \dots, n$ and $A_i = U$ (resp. $A_i = T$ or $A_i = F$) if K_i/K_{i-1} is unramified (resp. totally or ferociously ramified). We will write $\mathrm{gen}(L/K)$ to denote the genoma of L/K.

For instance, in Ex. 3.4 we have $\mathrm{gen}(L/K) = (F, F)$ and in Ex. 4.4 $\mathrm{gen}(L/K) = (T, F)$.

***Theorem 9.1* (Miki)** *Let L/K be a cyclic extension of degree p^n and let K be of characteristic zero. Suppose that $e_K < p - 1$. Then $\overline{L}/\overline{K}$ is separable.*

Proof We can suppose without loss of generality that L/K is completely ramified. If $[L : K] = p$, then the extension is totally ramified by Proposition 3.2, II. Suppose $[L : K] = p^2$, then we can suppose that the subextension K_1/K of degree p is totally ramified. Let t_0 (resp. t_1) be the ramification numbers of K_1/K (resp. of L/K_1). Now we use Hyodo's inequalities to have relations between t_0 and t_1.

Lemma 9.2 *Let L/K be a cyclic and completely ramified extension of degree p^2. Let t_0 (resp. t_1) the ramification number of K_1/K (resp. L/K_1).*

(i) *Assume* $\mathrm{gen}(L/K) = (F, F)$.
- *If* $t_0 \geq e_K/[p(p-1)]$, *then* $(t_0 + e_K)/p \leq t_1 \leq e_K/(p-1)$.
- *If* $t_0 \leq e_K/[p(p-1)]$, *then* $t_1 \geq t_0\big((p^2 - p + 1)/p\big)$.

(ii) *Assume* $\mathrm{gen}(L/K) = (F, T)$.
- *If* $t_0 \geq e_K/[p(p-1)]$, *then* $t_0 + e_K \leq t_1 \leq pe_K/(p-1)$.
- *If* $t_0 \leq e_K/[p(p-1)]$, *then* $t_1 \geq t_0(p^2 - p + 1)$.

(iii) *Assume* $\mathrm{gen}(L/K) = (T, F)$.
- *If* $t_0 \geq e_K/(p-1)$, *then* $t_0/p + e_K \leq t_1 \leq pe_K/(p-1)$.
- *If* $t_0 \leq e_K/(p-1)$, *then* $t_1 \geq t_0\big((p^2 - p + 1)/p\big)$.

(iv) *Assume* $\mathrm{gen}(L/K) = (T, T)$.
- *If* $t_0 \geq e_K/(p-1)$, *then* $t_0 + pe_K \leq t_1 \leq p^2 e_K/(p-1)$.
- *If* $t_0 \leq e_K/(p-1)$, *then* $t_1 \geq t_0(p^2 - p + 1)$.

Proof In [H, Lemma (4.1)], Hyodo gives these inequalities for the depth of ramification[7] $\mathrm{d}_K(L/K)$. We only have to rewrite those inequalities with $\mathrm{d}_K(K_1/K) = (p-1)t_0/e_{K_1/K}$ and $\mathrm{d}_K(L/K_1) = (p-1)t_1/e_{L/K}$. ■

[7] The depth of ramification is defined in [H], but see also Section 10.4.1.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

By (iii) of the above lemma, we have

$$\frac{t_0}{p} + e_K \leq t_1 \leq e_K + \frac{e_K}{p-1},$$

but $1 \leq t_0 \leq p-1$, so $e_K + 1 \leq t_1 \leq e_K$ which is impossible, so $e_{L/K} = p^2$.

Now consider an extension of degree p^n, $n \geq 3$ with $f^{\text{ins}}_{L/K_{n-1}} = p$ and $e_{K_{n-1}/K} = p^{n-1}$. Consider the subextension L/K_{n-2} where K_i/K is the subextension of degree p^i and let t_{i-1} be the ramification number of K_i/K_{i-1} for $i = 1, \ldots, n$ (here $K_0 = K$ and $K_n = L$). By using again the same Hyodo's inequalities for the extension L/K_{n-2}, we obtain

$$(*) \qquad \frac{t_{n-2}}{p} + e_{K_{n-2}} \leq t_{n-1} \leq \frac{pe_{K_{n-2}}}{p-1}.$$

Now we give an explicit computation of the ramification number t_{n-2}. In [Wy] we find many results about ramification jumps of cyclic totally wildly ramified extensions under the assumption that $\overline{K}$ is perfect. One can verify that the following result is true even if $\overline{K}$ is not perfect.

Lemma 9.3 *Let L/K be a cyclic wildly ramified extension of degree p^n. Let t_0 be the first ramification jump and assume that $t_0 \geq e_K/(p-1)$. Then the ramification jumps $t_1, t_2, \ldots, t_{n-1}$ are given by*

$$t_i = t_0 + pe_K + p^2 e_K + \cdots + p^i e_K, \quad i = 1, \ldots, n-1.$$

Proof Take [Wy] and see Prop. 25, Corollary 26, Th. 28, Corollary 29 and Th. 33; everything works even if $\overline{K}$ is imperfect. ■

Note that Lemma 9.3 gives the exact values of *ramification jumps* of a totally ramified extension; here we need the *ramification number* of K_{n-1}/K_{n-2}. In particular the $(n-1)$-th ramification jumps of K_{n-1}/K coincides with its $(n-1)$-th ramification number, *i.e.*, with the ramification number of K_{n-1}/K_{n-2}. So we apply Lemma 9.3 to the totally ramified extension K_{n-1}/K and we have $t_{n-2} = t_0 + pe_K + \cdots + p^{n-2}e_K$, so $(*)$ becomes

$$\frac{t_0}{p} + e_K + \cdots + p^{n-3}e_K + e_{K_{n-2}} \leq t_{n-1} \leq \frac{p^{n-1}e_K}{p-1},$$

or equivalently

$$\frac{t_0}{p} + e_K(1 + p + \cdots + p^{n-2}) \leq t_{n-1} \leq (p^{n-2} + \cdots + p + 1)e_K,$$

which is clearly impossible, so $e_{L/K} = p^n$ and we are done. ■

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

10 On the Kato Conductor

In the important works of Kato [K2]–[K3] there is a thorough discussion of the Swan conductor, see also [B-C-S] and [Sn]. In particular in [K2], Kato defines a conductor for well ramified extensions in cases I and II. In [K3], he succeeds in defining an integer valued conductor $\mathrm{Ksw}_{G_K}(\chi)$ for characters χ of degree one in the general case. In the next section we give an upper bound for this conductor in special cases.

Theorem 10.1 *Let χ be a character of degree one of $G_K = \mathrm{Gal}(K_s/K)$ and suppose that $L = K_s^{\mathrm{Ker}(\chi)}/K$ is a completely ramified extension. Put $G = \mathrm{Gal}(L/K)$.*

(A) Suppose that L/K is well ramified. Then the Kato conductor of L/K is given by

$$\mathrm{Ksw}_{G_K}(\chi) = \left[\frac{1}{e_{L/K}} \Big(\sum_{\sigma \in G} S_G(\sigma)\chi(\sigma) - \mathfrak{M}_{L/K} \Big) \right], \tag{7}$$

where $\mathfrak{M}_{L/K}$ is a certain "normalized monogenic conductor" defined below in Section 10.4.1 and the function S_G was defined in Section 8. Here $[x]$ is the largest integer not exceeding x. We also have

$$\mathrm{Ksw}_{G_K}(\chi) = \begin{cases} \varphi_{L/K}(i_n) - 1 & \text{cases I and III} \\ \varphi_{L/K}(i_n) & \text{case II} \end{cases}$$

where i_n is the last modified ramification jump of $\mathrm{Gal}(L/K)$.

(B) If L/K is of degree p^n, then we have

$$\mathrm{Ksw}_{G_K}(\chi) \leq \left[\frac{1}{e_{L/K}} \Big(\sum_{\sigma \in G} S_G(\sigma)\chi(\sigma) - \mathfrak{M}_{L/K} \Big) \right].$$

10.1 The Norm Map

Let K be a complete field and let L/K be a Galois extension. The norm map $N_{L/K}$ is denoted by N when there is no risk of confusion. Throughout this chapter we assume that $[\overline{K} : \overline{K}^p]$ is finite. We recall some results about the norm map.

Proposition 10.2 *Let K be a complete field.*

(A) Let L/K be a cyclic, totally ramified extension of degree p and let $s := s_G(\sigma)$ be the ramification number. Then we have

- *(i) $NU_L^i \subseteq U_K^i$, for $0 \leq i \leq s$.*
- *(ii) $NU_L^{s+pi} = U_K^{s+i}$, for $i > 0$.*
- *(iii) $NU_L^{s+i} = NU_L^{s+i+1}$, for $i > 0$, $p \nmid i$.*

In particular $U_K^s \not\subset NL^*$ and $U_K^{s+1} \subset NL^*$.

(B) Let L/K be a cyclic, ferociously ramified extension of degree p and let $s = s_G(\sigma)$. Then we have

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

(i) $NU_L^i \subseteq U_K^{ip}$, *for* $0 \le i \le s$.

(ii) $NU_L^{s+i} = U_K^{sp+i}$, *for* $i > 0$.

In particular $U_K^{ps} \not\subset NL^*$ *and* $U_K^{ps+1} \subset NL^*$.

The case (A) is solved in Prop. 5, ch. V of [S1] or in Prop. (1.5), ch. III of [F-V]. For the ferociously ramified case see [K2, p. 332].

10.2 Definition of the Kato Conductor

In this section we want to give the definition of the Kato conductor, without introducing too much machinery. We only recall some notation and definitions.

Let $(\mathbb{Z}/n\mathbb{Z})(1)$ be the G_K-module of n-th roots of unity in K_s and for $r > 1$, let $(\mathbb{Z}/n\mathbb{Z})(r)$ be the r-th Tate twist of $(\mathbb{Z}/n\mathbb{Z})(1)$, *i.e.*, $(\mathbb{Z}/n\mathbb{Z})(r) = [(\mathbb{Z}/n\mathbb{Z})(1)]^{\otimes r}$ (with diagonal G_K action). Also, $(\mathbb{Z}/n\mathbb{Z})(0)$ is the G_K-module $\mathbb{Z}/n\mathbb{Z}$ with trivial action.

If K is a field of characteristic zero, for $n \neq 0$, Kato considers the following cohomology groups:

$$H_n^q(K) := H^q\big(K, (\mathbb{Z}/n\mathbb{Z})(q-1)\big).$$

By passing to the inductive limit with respect to the canonical transition maps $\mathbb{Z}/n\mathbb{Z}(r) \xrightarrow{m} \mathbb{Z}/nm\mathbb{Z}(r)$, we have

$$H^q(K) := H^q\big(K, (\mathbb{Q}/\mathbb{Z})(q-1)\big) = \varinjlim H_n^q(K).$$

If K is a field of characteristic $p > 0$, Kato defines again cohomology groups $H_n^q(K)$ by using more complicated objects related to the logarithmic part of the De Rham-Witt complex, but it is not important for understanding what follows, in fact we only consider H^1 and H^2 and in this case one can show (see [K1, II, p. 659])

$$H^1(K) \cong \mathrm{Hom}_c\big(\mathrm{Gal}(K^{ab}/K), \mathbb{Q}/\mathbb{Z}\big)$$
$$H^2(K) \cong \mathrm{Br}(K)$$

(K^{ab} denotes the maximal abelian extension of K and Hom_c means continuous homomorphism with respect to the Krull topology on $\mathrm{Gal}(K^{ab}/K)$ and the discrete topology on $\mathbb{Q}/\mathbb{Z}$; $\mathrm{Br}(K)$ is the Brauer group of K).

For $\chi \in H^q$ and $a_1, \ldots, a_r \in K^*$, Kato defines a symbol $\{\cdot, \cdot\}$ in H^{q+r}. This will be used to define a pairing between H^q and the Milnor K-group $K_r^M(K)$ of K.

We recall the definition of the Kato's pairing for field of characteristic zero, in characteristic $p > 0$ see [K3, (1.3)]. For $a \in K^*$ and a fixed $n \ge 0$, let $\{a\} \in H^1\big(K, (\mathbb{Z}/n\mathbb{Z})(1)\big)$ be the image under the connecting homomorphism $K^* \to H^1\big(K, (\mathbb{Z}/n\mathbb{Z})(1)\big)$ induced by the exact sequence of G_K-modules

$$1 \longrightarrow (\mathbb{Z}/n\mathbb{Z})(1) \longrightarrow K_s^* \xrightarrow{n} K_s^* \longrightarrow 1. \tag{8}$$

For $a_1, \ldots, a_r \in K^*$ the symbol

$$\{a_1, \ldots, a_r\} \in H^r\big(K, (\mathbb{Z}/n\mathbb{Z})(r)\big)$$

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

is the cup-product $\{a_1\} \cup \{a_2\} \cup \cdots \cup \{a_r\}$. For $\chi \in H^q(K)$ and $a_1, \ldots, a_r \in K^*$

$$\{\chi, a_1, \ldots, a_r\} \in H_n^{q+r}(K)$$

is the cup-product $\{\chi\} \cup \{a_1\} \cup \cdots \cup \{a_r\}$ By passage to the limit, we have for $\chi \in H^q(K)$ the element $\{\chi, a_1, \ldots, a_r\} \in H^{q+r}(K)$.

The q-th Milnor K-group $K_q^M(K)$ of K is defined for $q = 0, 1$ as $K_0^M(K) = \mathbb{Z}$, $K_1^M(K) = K^*$ and for $q > 1$ as

$$K_q^M(K) := \overbrace{(K^* \otimes \cdots \otimes K^*)}^{q \text{ times}} / J$$

where J is the subgroup generated by the elements of the form $a_1 \otimes \cdots \otimes a_q$ such that $a_i + a_j = 1$ for some $i \neq j$. The class of $a_1 \otimes \cdots \otimes a_q$ is also denoted by $\{a_1, \ldots, a_q\}$. All this defines the pairing

$$\begin{aligned} H^q(K) \otimes K_r^M(K) &\longrightarrow H^{q+r}(K) \\ \chi \otimes \{a_1, \ldots, a_r\} &\longrightarrow \{\chi, a_1, \ldots, a_r\}. \end{aligned} \tag{9}$$

We denote χ_L the image $\chi \in H^q(K)$ in $H^q(L)$. The definition of the Kato conductor is given by the following proposition (the proof is given in [K3, Prop. (6.3)]).

***Proposition 10.3* (Definition)** *For $\chi \in H^q(K)$ the Kato conductor $\mathrm{Ksw}_{G_K}(\chi)$ is the smallest integer $n \geq 0$ such that one of the following equivalent conditions (i)–(iii) holds.*

(i) $\{\chi_L, 1 + \pi^n \mathfrak{p}_L\} = 0$ *in $H^{q+1}(L)$ for all complete fields L over K such that $\mathcal{O}_K \subset \mathcal{O}_L$ and $\mathfrak{p}_K \subset \mathfrak{p}_L$.*
(ii) $\{\chi_L, 1 + \pi^{n+1} \mathcal{O}_L\} = 0$ *in $H^{q+1}(L)$ for all complete fields L over K such that $\mathcal{O}_K \subset \mathcal{O}_L$ and $\mathfrak{p}_L = \mathfrak{p}_K \mathcal{O}_L$.*
(iii) $\{\chi_{\mathcal{K}}, 1 + \pi^{n+1} T\} = 0$ *in $H^{q+1}(\mathcal{K})$ where $\mathcal{K}$ is the fraction field of the henselisation of $\mathcal{O}_K[T]_{(\pi)}$.*

The characters with Kato conductor zero are given in the following proposition (see [K3, Prop. (6.1)]).

Proposition 10.4 *Let K be a complete field. Then the subgroup of $H^q(K)$ composed by characters with Kato conductor equals zero is*

$$H^q(K)(non\text{-}p) \oplus \mathrm{Ker}\big(H^q(K)\{p\} \to H^q(K_{nr})\{p\}\big),$$

where K_{nr} denotes the maximal unramified extension of K, (non-p) means the part prime to p and $H^q(K)\{p\}$ denotes the p-primary part.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

10.3 The Kato Conductor of a Character

Here, we consider the case $q = 1$. In this case we show that the symbol defined by (9) coincides with the symbol $(\cdot,\cdot)$ defined in [S1, ch. XIV]; this allows to reduce the computation of the Kato conductor to a norm computation. Consider the exact sequence of trivial G_K-modules

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

and let δ be the connecting homomorphism $\delta\colon H^1(G_K, \mathbb{Q}/\mathbb{Z}) \to H^2(G_K, \mathbb{Z})$. If $b \in K^* = H^0(G_K, K_s^*)$ and $\chi \in H^1(G_K, \mathbb{Q}/\mathbb{Z})$, then the cup-product $b \cup \delta\chi$ is an element of the Brauer group $H^2(G_K, K_s^*) = \mathrm{Br}(K)$. The element $b \cup \delta\chi$ is denoted by (b, χ) and we now show that $\{b, \chi\} = (b, \chi)$.

Lemma 10.5 *With the above notation we have* $\{\chi, b\} = (b, \chi)$.

Proof Put $G_K = G$ and let $\chi \in H^1(K, \mathbb{Z}/n)$. Consider the following commutative diagram (see [Po p. 122])

$$\begin{array}{ccc} H^0(G, K_s^*) \times H^1(G, \mathbb{Z}/n) & \xrightarrow{(\delta,1)} & H^1\big(G, \mathbb{Z}/n(1)\big) \times H^1(G, \mathbb{Z}/n) \\ \cup\big\downarrow & & \cup\big\downarrow \\ H^1(G, K_s^* \otimes \mathbb{Z}/n) & \xrightarrow{\delta} & H^2\big(G, \mathbb{Z}/n(1) \otimes \mathbb{Z}/n\big) \end{array}$$

(the δ in $(\delta, 1)$ is induced by the exact sequence (8)). From this we obtain $\delta(b \cup \chi) = \delta b \cup \chi$. Now consider the commutative diagram

$$\begin{array}{ccc} H^0(G, K_s^*) \times H^1(G, \mathbb{Z}/n) & \xrightarrow{(1,\delta)} & H^0(G, K_s^*) \times H^2(G, \mathbb{Z}) \\ \cup\big\downarrow & & \cup\big\downarrow \\ H^1(G, K_s^* \otimes \mathbb{Z}/n) & \xrightarrow{\delta} & H^2(G, K_s^*) \end{array}$$

its commutativity gives $\delta(b \cup \chi) = b \cup \delta\chi$. Finally

$$\{b, \chi\} = \{b\} \cup \chi = \delta b \cup \chi = \delta(b \cup \chi) = b \cup \delta\chi = (b, \chi). \qquad \blacksquare$$

One of the fundamental properties of (χ, b) is stated in the following proposition (see [S1, ch. XIV, Section 1, Corollaire 1]).

Proposition 10.6 *The element $(b, \chi) = \{\chi, b\}$ vanishes if and only if b is a norm of the extension L_χ/K, where L_χ is the field fixed by* $\mathrm{Ker}(\chi)$.

Thus, by definition, in order to calculate $\mathrm{Ksw}_{G_K}(\chi)$ we have to compute the minimal integer n such that U_L^{n+1} is in the norm of the cyclic extension corresponding $\chi_{|_L}$ when L runs through all complete fields satisfying $\mathfrak{p}_L = \mathfrak{p}_K \mathcal{O}_L$. Note that the minimal integer n such that U_K^{n+1} is contained in the norm is not, in general, the Kato conductor (*e.g.* consider a field K with algebraically closed residue field).

Kato gives another characterization of $\mathrm{Ksw}(\chi)$ which does not involve extensions L/K as in the definition, *cf.* [K3, Proposition (6.5)].

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

Proposition 10.7 *Let K be a complete discrete valuation field and assume that $[\overline{K} : \overline{K}^p] = p^c < \infty$, and $H_p^{c+1}(\overline{K}) \neq 0$. Then, for $\chi \in H^1(K)$ and $n \geq 0$ the Kato conductor* $\mathrm{Ksw}(\chi)$ *is n if and only if n is the smallest integer such that*

$$\{\chi, U^{n+1}K_{c+1}^M(K)\} = 0 \quad \text{in } H^{c+1}(K),$$

where $U^iK_r^M(K)$ is the subgroup of $K_r^M(K)$ generated by the elements $\{x, y_1, \dots, y_{r-1}\}$ such that $x \in U_K^i$ and $y_1, \dots, y_{r-1} \in K^*$.

In the following we will only consider characters χ such that the corresponding cyclic extensions L/K are p-extensions, because for tame characters χ we have $\mathrm{Ksw}(\chi) = 0$, *cf.* Proposition 10.4. We can compute the Kato conductor in the following manner.

Corollary 10.8 *Let K be as in Proposition 10.7. Let $\chi \in H^1(K)$ and assume that the corresponding cyclic extension L/K is a p-extension. Then the minimal integer n such that*

$$U_K^{n+1} \subset N_{L/K}L^*$$

is the Kato conductor of χ.

Proof We can assume that $\overline{K}$ is imperfect, otherwise we have only totally ramified characters for which the Kato conductor is the Swan conductor $SW_G(\chi)$. Let $[\overline{K} : \overline{K}^p] = p^c < \infty$. By hypothesis (*i.e.*, $U_K^{n+1} \subset N_{L/K}L^*$) we have $\mathrm{Ksw}(\chi) \geq n$. Now $U_K^{n+1} \subset N_{L/K}L^*$, implies that $U^{n+1}K_{c+1}(K)$ is contained in the norm groups $N_{L/K}K_{c+1}(L)$. By Corollary p. 659 in [K1, II] we have that $\{\chi, U^{n+1}K_{c+1}(K)\} = 0$ in $H^{c+2}(K)$ and so, by Proposition 10.7, $\mathrm{Ksw}(\chi) \leq n$. ■

10.4 The Kato Conductor in the Well Ramified Case

As stated in [K3, Prop. (6.8)], if L/K is in case I or II and χ is a character of degree 1 of G, then

$$\mathrm{Ksw}_G(\chi) = \frac{1}{|G|}\sum_{\sigma\in G} Sw_G(\sigma)\chi(\sigma) = \frac{1}{e_{L/K}}\sum_{\sigma\in G} S_G(\sigma)\chi(\sigma). \tag{10}$$

Note that if t is the maximal modified ramification jump of L/K then we have

$$\mathrm{Ksw}(\chi) = \begin{cases} \varphi_{L/K}(t) - 1 & \text{case I} \\ \varphi_{L/K}(t) & \text{case II.} \end{cases} \tag{11}$$

The proof of the above formula is an easy computation left to the reader. These formulas do not work in general, as we have seen in Ex. 8.1, but see also Section 10.5.3.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

10.4.1 The Normalized Monogenic Conductor $\mathfrak{M}_{L/K}$

For complete fields the depth of ramification is defined by

$$\mathrm{d}_K(M/L) = v_K(\mathfrak{D}_{M/L}) - \big(v_K(\pi_L) - v_K(\pi_M)\big),$$

for algebraic extensions $K \subset L \subset M$. See [H] for more information. If $\overline{L}/\overline{K}$ is separable, $\mathrm{d}_L(L/K) = \sum_{\sigma\neq 1} s_G(\sigma)$. We define the integer $\mathfrak{M}_{L/K}$, called *normalized monogenic conductor* attached to an extension L/K by the formula:

$$\mathrm{d}_L(L/K) + \mathfrak{M}_{L/K} = \sum_{\sigma\neq 1} s_G(\sigma).$$

Note that in cases I, II we have $\mathfrak{M}_{L/K} = 0$, but in case III we have $\mathfrak{M}_{L/K} = e_{L/K} - 1$.

10.4.2 Case III: Degree p^2

We can suppose, without loss of generality, that $H_p^{c+1}(\overline{K}) \neq 0$, where $p^c = [\overline{K} : \overline{K}^p]$, otherwise we consider the extension $M = \bigcup_{i\geq 0} \overline{K}(T^{p^{-i}})$ of the residue field $\overline{K}$ preserving p-bases for which $H_p^{c+1}(\overline{M}) \neq 0$ (see [K2, Lemma (3.9)]). Let L/K be a cyclic extension of degree p^2 in case III, then $\mathrm{gen}(L/K) = (T, F)$ by Th. 6.1. We use the following notation:

- K_1/K is the subextension of degree p in L/K; the norm map $N_{K_1/K}$ is denoted by N_1;
- $G = \langle\sigma\rangle$ and $a := s_{K_1/K}(\sigma)$, $b := s_G(\sigma^p)$.

By Herbrand's property we have $a + 1 = p i_G(\sigma)$, *i.e.*, $i_G(\sigma) = (a + 1)/p$. We put $a = -1 + pa'$. The computation of the Kato conductor is as follows.

1. We show that $U_K^{b+(p-1)a'} \subset NL^*$;
2. We show that $U_K^{b+(p-1)a'-1} \not\subset NL^*$, so the Kato conductor is $b + (p - 1)a' - 1$ by Corollary 10.8;
3. We express the obtained value in terms of the function S_G and the normalized monogenity conductor.

1. A direct computation by using Proposition 10.2 gives:

$$N_{L/K_1} U_L^{b+1} = U_{K_1}^{pb+1} \subseteq N_{L/K_1} L^*$$
$$N_1 U_{K_1}^{a+(pb+1-a)} = N_1 U_{K_1}^{a+pb+p-pa'} \subseteq N_1 K_1^*,$$

which implies $U_K^{a+b+1-a'} \subset NL^*$.

2. The norm map induces

$$U_L^{b-1}/U_L^b \xrightarrow{N_{L/K_1}} U_{K_1}^{pb-p}/U_{K_1}^{pb-p+1} \xrightarrow{N_1} U_K^n/U_K^{n+1}.$$

Now we calculate the number n and we show that it is the Kato conductor. The first step is to show that $pb - p > a$.

Proof of $pb - p > a$ Consider Lemma 9.2, with our notation we have $t_0 = a$ and $t_1 = b$. So we have:

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

(i) If $a \geq e_K/(p-1)$, then $b \geq a/p + e_K$.
(ii) If $a \leq e_K/(p-1)$, then $b \geq a(p^2 - p + 1)/p$.

If (ii) holds, then $pb - p > a$ is clear. In the first case, observe that a is not divisible by p, so $b > a/p + e_K$. Or, note that L/K is cyclic of degree p^2 and by Miki's theorem (Theorem 9.1) we have that $e_K \geq p$. This shows $pb - p > a$.

Now we can write $pb - p = a + i$ with $i \geq 1$ and by Proposition 10.2 (A) (ii)–(iii) we have

$$N_1(U_{K_1}^{pb-p}) = N_1(U_{K_1}^{a+pb-a-p+(p-1)}) = U_K^{a+[pb-a-1]/p}.$$

So we have $n = a + [pb - a - 1]/p = a + b - a' = b + (p-1)a' - 1$. Now, we show that n is exactly the Kato conductor. The norm map $N_1 \colon U_{K_1}^{pb-p}/U_{K_1}^{pb-p+1} \to U_K^n/U_K^{n+1}$, is bijective (because $pb - p > a$ and K_1/K is totally ramified), but $N_{L/K_1} \colon U_L^{b-1}/U_L^b \to U_{K_1}^{pb-p}/U_{K_1}^{pb-p+1}$ is not surjective, so the composition $N_1 \circ N_{L/K_1}$ is not surjective, so $U_K^n \not\subseteq N_{L/K}L^*$. On the other hand we have $U_K^{n+1} \subseteq N_{L/K}L^*$, which, by Corollary 10.8, means that the Kato conductor is n.

3. Recall that the function S_G is defined for a completely ramified extension by $S_G(\sigma) = -s_G(\sigma)$ if $\sigma \neq 1$ and by $S_G(1) = -\sum_{\sigma \neq 1} S_G(\sigma)$. If we try to use the classical formula seen in (10) we find

$$\frac{1}{p} \sum_{\sigma \in G} S_G(\sigma)\chi(\sigma) = \frac{(p-1)(a+1)}{p} + b = (p-1)a' + b,$$

which is not $(p-1)a' + b - 1$, the Kato conductor. We try to use the normalized monogenity conductor:

$$\frac{1}{p}\Big(\sum_{\sigma \in G} S_G(\sigma)\chi(\sigma) - \mathfrak{M}_{L/K}\Big) = \frac{(p-1)a}{p} + b,$$

which is not the Kato conductor, but we observe that the integer part of this value is in fact the Kato conductor, so we have

$$\mathrm{Ksw}_{G_K}(\chi) = \left[\frac{1}{e_{L/K}}\Big(\sum_{\sigma \in G} S_G(\sigma)\chi(\sigma) - \mathfrak{M}_{L/K}\Big)\right].$$

10.4.3 Proof of the Theorem 10.1 (A)

Let L/K be a cyclic extension in case III and let $\chi \in H^1(K)$ be the corresponding character. As in the beginning of the preceding section we can suppose that $H_p^{c+1}(\overline{K}) \neq 0$. So by Corollary 10.8 we have to compute the minimal integer n such that $U_K^{n+1} \subset N_{L/K}L^*$.

Let T/K be the totally ramified extension defined by Theorem 6.1 (here T/K is uniquely determined because L/K is cyclic). Denote U_L^ν for $\nu \in \mathbb{R}$, $\nu \geq 0$ the group U_L^n where n is the smallest integer $\geq \nu$.

If t is the maximal modified ramification jump of L/K, then

$$U_T^{\varphi_{L/T}(t)+1} \subset N_{L/T}L^* \tag{12}$$

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

because L/T is in case II and its Kato conductor is $\varphi_{L/T}(t)$ by formula (11). Now consider the totally ramified extension T/K. By [S1, Ch. V, Cor. 3, Section 6] we have

$$N_{T/K}(U_T^s) = U_K^{\varphi_{T/K}(s+1)-1} \quad \text{if} \quad \mathrm{Gal}(T/K)[s+1] = \{1\}. \tag{13}$$

Let $t' = i_{T/K}(\tau)$ be the maximal modified ramification jumps of T/K. Let r be the maximum of $i_{L/K}(\sigma)$ for $\sigma \equiv \tau \bmod \mathrm{Gal}(L/T)$. By Lemma 7.3 we have $t' = \varphi_{L/T}(r)$. Note that $r < t$ (we explain this in the next paragraph), so

$$t' = \varphi_{L/T}(r) < \varphi_{L/T}(t). \tag{14}$$

To show $r < t$ note that $G[i] = H_{i+1}$ (see beginning of Section 7) and H_i/H_{i+1} are abelian groups annihilated by p (*cf.* Proposition 2.1) so $G[r] \supset G[t]$ and $G[r] \neq G[t]$ because L/K is cyclic.

Now we use the fact that the number $\varphi_{L/K}(t)$ is an integer (by Borger's Theorem 7.6). We shall show that $U_K^{\varphi_{L/K}(t)} \subset N_{L/K}L^*$.

By (14) we have $\mathrm{Gal}(T/K)[\varphi_{L/T}(t)] = \{1\}$ and so we can apply (13). By applying the norm map $N_{T/K}$ to (12) we have

$$N_{T/K}(U_T^{\varphi_{L/T}(t)+1}) = U_K^{\varphi_{T/K}(\varphi_{L/T}(t)+2)-1} \subset N_{L/K}L^*.$$

Thus it suffices to show that the smallest integer $\geq \varphi_{T/K}\big(\varphi_{L/T}(t)+2\big)-1$ is $\varphi_{L/K}(t)$. Indeed we have

$$\varphi_{T/K}\big(\varphi_{L/T}(t)+2\big) - 1 = \varphi_{T/K}\big(\varphi_{L/T}(t)\big) + \frac{2}{[T:K]} - 1 = \varphi_{L/K}(t) - 1 + \frac{2}{[T:K]},$$

where we have used Proposition 7.5. By Borger's theorem $\varphi_{L/K}(t)$ is an integer and thus we have shown that $\mathrm{Ksw}(\chi) \leq \varphi_{L/K}(t) - 1$.

Now we need a lemma which is a key tool to deduce Borger's theorem.

Lemma 10.9 *Let L/K be a Galois extension in case II. If $\overline{L} = \overline{K}(a^{1/f})$, then $a \in \overline{K} \setminus \overline{K}^p$ where $f = [L:K] = f_{L/K}^{\mathrm{ins}}$. Let α be a lifting of a in K and let $M = K(\beta)$ where $\beta^f = \alpha$. If $\sigma \in \mathrm{Gal}(L/K)$ and $\sigma' \in \mathrm{Gal}(LM/M)$ is such that $\sigma'|_L = \sigma$, then*

$$i_{LM/M}(\sigma') = e_{LM/L}\, i_{L/K}(\sigma).$$

Proof (after J. Borger) Note that the extension M/K is in case II and LM/M is in case I, in particular it is totally ramified. Let $x \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[x]$. One can check that $x^f - \alpha \in \mathfrak{p}_L \setminus \mathfrak{p}_L^2$. Let $g(X)$ be the minimal polynomial of β over K. Then $g(X+x)$ is an Eisenstein polynomial over L (because $g(X+x) \equiv X^f + x^f - \alpha \equiv X^f \bmod \mathfrak{p}_L$) and $\beta - x$ is a root of $g(X+x)$. So $\beta - x$ is a prime of LM and we have

$$i_{LM/M}(\sigma') = v_{LM}\big(\sigma'(\beta - x) - (\beta - x)\big) = v_{LM}\big(\sigma'(x) - x\big) = e_{LM/L}\, i_{L/K}(\sigma). \qquad \blacksquare$$

End of the Proof of Theorem 10.1 (A) and Proof of Borger's Theorem Now we simultaneously deduce the formula for the Kato conductor in case III and Borger's theorem.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

We compute the classical Artin's conductor $A(\chi|_M)$ for M as in the above lemma. By the preceding lemma we have

$$A(\chi|_M) = \frac{1}{e_{LM/M}} \sum_{\sigma' \in \mathrm{Gal}(LM/M)} \chi|_M(\sigma') i_{LM/M}(\sigma')$$
$$= \frac{e_{LM/L}}{e_{LM/M}} \sum_{\sigma' \in \mathrm{Gal}(LM/M)} \chi|_M(\sigma') i_{L/K}(\sigma) = \frac{1}{e_{L/K}} \sum_{\sigma \in G} \chi(\sigma) i_{L/K}(\sigma).$$

Since $A(\chi|_M)$ is an integer by Artin's theorem we deduce that the latter expression is an integer. Now by Proposition 8.2 one deduces the Hasse-Arf theorem for L/K.

The above argument also shows that the Swan conductor (= Kato conductor) of LM/M is equal to $A(\chi|_M) - 1$ which shows that $\mathrm{Ksw}(\chi) \geq \varphi_{L/K}(t) - 1$, so $\mathrm{Ksw}(\chi) = \varphi_{L/K}(t) - 1$ and Theorem 10.1 (A) follows. ■

10.5 An Upper Bound for the Kato Conductor

In this section we give a formula for the maximal value of the Kato conductor depending on S_G and $\mathfrak{M}_{L/K}$. In Section 10.5.3 we shall produce an example for which the Kato conductor is strictly smaller than the maximal value. Let L/K be a cyclic extension of degree p^n. We use the following notations:

- K_j is the subextension of degree p^j and $K_n = L$, $K_0 = K$.
- $G = \langle \sigma \rangle$, and t_j are the ramification numbers of L/K, *i.e.*, the ramification numbers of $\mathrm{Gal}(K_{j+1}/K_j)$, for $0 \leq j \leq n-1$.

Lemma 10.10 *Let L/K be a cyclic, completely ramified extension of degree p^n, $n \geq 2$ with the above notations. Then*

$$\mathfrak{M}_{L/K} = (p-1)\Big(\sum_{i=1}^{n-1} p^{n-i} s_G(\sigma^{p^{i-1}}) - e_{L/K_i} t_{i-1}\Big).$$

Let $\chi \in H^1(K, \mathbb{Q}/\mathbb{Z})$ be a character of the Galois group G_K, the *quasi-conductor* $\widetilde{\mathrm{Ksw}}(\chi) = \widetilde{\mathrm{Ksw}}(L/K)$ $(L = K_s^{\mathrm{Ker}(\chi)})$, is defined as the number given by the formula

$$\widetilde{\mathrm{Ksw}}(\chi) := \widetilde{\mathrm{Ksw}}(L/K) := \frac{1}{e_{L/K}} \Big(\sum_{\sigma \in G} S_G(\sigma)\chi(\sigma) - \mathfrak{M}_{L/K}\Big).$$

As we have already seen for extensions of degree p^2, this is not always an integer, it is a rational number and we show that the Kato conductor is at most the integer part of the quasi conductor, see Section 10.5.2.

10.5.1 Cyclic Extensions of Degree p^2

Now we consider cyclic, completely ramified extensions of degree p^2. We assume that $H_p^{c+1}(\overline{K}) \neq 0$ as in the beginning of Section 10.4.2. We have to consider three cases, depending on the ferocious and wild ramification of L/K:

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

A) $\mathrm{gen}(L/K) = (F, F)$;
B) $\mathrm{gen}(L/K) = (F, T)$;
C) $\mathrm{gen}(L/K) = (T, F)$.

Recall that the totally ramified case is classical and we know by Section 10.4 the formula of $\mathrm{Ksw}(L/K)$. Here we show how it is possible to calculate the maximal value of the Kato conductor by means of the function s_G and the normalized monogenity conductor.

Notation: a, b are the ramification numbers of the subextensions of L/K, *i.e.*, $a := s_{K_1/K}(\sigma)$, $b := s_G(\sigma^p)$.

A) Let L/K be a ferociously extension, either f.r-1 or f.r-2. We have $\mathrm{Ksw}(L/K) \leq pb + pa - a$. In fact (by Proposition 10.2)

$$N_{L/K_1} U_{K_1}^{b+1} = U_{K_1}^{pb+1} \subseteq N_{L/K_1} L^*$$
$$N_1 U_{K_1}^{a+i} = U_K^{pa+i} \subseteq N_1 K_1^*, \quad i > 0$$

so, for $pb + 1 = a + i$, *i.e.*, $i = pb - a + 1$, we have

$$U_K^{pa+pb-a+1} \subseteq N_{L/K} L^*.$$

If we use the formula for the Kato conductor in the well ramified case, *i.e.*, the formula (10), we see that $\sum_{\sigma \in G} S_G(\sigma)\chi(\sigma) = (p^2 - p)s_G(\sigma) + pb \neq pb + pa - a$. Now, the normalized monogenity conductor of L/K is $\mathfrak{M}_{L/K} = (p-1)\big(pi_G(\sigma) - a\big)$ (by using Lemma 10.10).

We can see that $\mathrm{Ksw}(L/K) \leq \widetilde{\mathrm{Ksw}}(L/K)$, indeed

$$\mathrm{Ksw}(L/K) \leq \sum_{\sigma \in G} S_G(\sigma)\chi(\sigma) - \mathfrak{M}_{L/K} = pb + pa - a.$$

B) In this case we have $\mathrm{Ksw}(L/K) \leq pa + b - a$. The norm calculation gives (*cf.* Proposition 10.2)

$$N_{L/K_1} U_L^{b+p} = U_{K_1}^{b+1} \subseteq N_{L/K_1} L^*$$
$$N_1 U_{K_1}^{a+i} = U_K^{pa+i} \subseteq N_1 K_1^*, \quad i > 0$$

so if we take $i = b + 1 - a$, we obtain $U_K^{pa+b-a+1} \subset N_{L/K} L^*$. Now we want to relate this value with the function S_G and $\mathfrak{M}_{L/K}$. Similarly to the preceding case we could consider the formula

$$\mathrm{Ksw}(L/K) \leq \widetilde{\mathrm{Ksw}}(L/K). \tag{15}$$

Let us verify this formula (recall that $b := s_G(\sigma^p)$).

$$\frac{1}{p}\Big(\sum_{\sigma \in G} S_G(\sigma)\chi(\sigma) - \mathfrak{M}_{L/K}\Big) = \frac{(p^2 - p)s_G(\sigma) + ps_G(\sigma^p) - (p-1)\big(ps_G(\sigma) - pa\big)}{p}$$
$$= pa - a + b.$$

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

C) We have: (*cf.* Proposition 10.2)

$$N_{L/K_1}U_L^{b+1} = U_{K_1}^{pb+1} \subseteq N_{L/K_1}L^*$$
$$N_1 U_{K_1}^{a+i} = N_1 U_{K_1}^{a+i+1} \subseteq N_1 K_1^*, \quad \text{for } i > 0 \quad \text{and} \quad p \nmid i.$$

For $i = pb - a + R_{K_1/K}$, where $R_{K_1/K}$ is the smallest nonnegative integer such that $pb - a + R_{K_1/K}$ is divisible by p, we have

$$N_1 U_{K_1}^{a+i} = N_1 U_{K_1}^{a+(pb-a+R_{K_1/K})} = U_K^{a+(pb+R_{K_1/K}-a)/p} \subset NL^*.$$

So we have

$$\mathrm{Ksw}(L/K) \leq a + \frac{pb + R_{K_1/K} - a}{p} - 1 = a + \left[\frac{pb-a}{p}\right].$$

The Kato conductor is exactly $a + [(pb-a)/p]$ because the composition of the norm maps

$$U_L^b/U_L^{b+1} \longrightarrow U_{K_1}^{pb}/U_{K_1}^{pb+1} \longrightarrow U_K^{a+[(pb-a)/p]}/U_K^{a+[(pb-a)/p]+1}$$

is not surjective, so $\mathrm{Ksw}(L/K) \leq [\widetilde{\mathrm{Ksw}}(L/K)]$.

10.5.2 Proof of Theorem 10.1 (B)

We prove Theorem 10.1 part (B); this is equivalent to show that the Kato conductor of χ is at most the integer part of the "quasi-conductor" $\widetilde{\mathrm{Ksw}}(\chi)$. Let L/K be the cyclic extension of degree p^n, corresponding to $\chi \in H^1(K)$ and K_1 the subextension of degree p. We relate the Kato conductor of L/K with the Kato conductor of L/K_1, hence by induction we conclude. Put $X = \mathrm{Ksw}(L/K_1)$, $G = \langle\sigma\rangle$, and $H = \mathrm{Gal}(L/K_1)$.

At first we relate $\mathfrak{M}_{L/K}$ with $\mathfrak{M}_{L/K_1}$, then we calculate $\widetilde{\mathrm{Ksw}}(L/K)$. Here t_i indicates the ramification numbers of K_i/K_{i-1}, $1 \leq i \leq n$. By Lemma 10.10 we have

$$\begin{aligned}\mathfrak{M}_{L/K} &= (p-1)\sum_{i=1}^{n-1}\bigl(p^{n-i}s_G(\sigma^{p^{i-1}}) - e_{L/K_i}t_{i-1}\bigr)\\ &= (p-1)\bigl(p^{n-1}s_G(\sigma) - e_{L/K_1}t_0\bigr) + (p-1)\sum_{i=2}^{n-1}\bigl(p^{n-i}s_G(\sigma^{p^{n-i}}) - e_{L/K_i}t_{i-1}\bigr),\end{aligned}$$

now a simple change of index in the last sum shows that

$$\mathfrak{M}_{L/K} = (p-1)\bigl(p^{n-1}s_G(\sigma) - e_{L/K_1}t_0\bigr) + \mathfrak{M}_{L/K_1}. \tag{16}$$

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

Replacing the formula (16) in $\widetilde{\mathrm{Ksw}}(L/K)$, we have

$$\begin{aligned}\widetilde{\mathrm{Ksw}}(L/K) &= \frac{1}{e_{K_1/K}}\left(\frac{1}{e_{L/K_1}}\sum_{\tau\in H} S_H(\tau)\chi(\tau) + \frac{(p^n - p^{n-1})s_G(\sigma)}{e_{L/K_1}}\right)\\ &\quad - \frac{\mathfrak{M}_{L/K_1}}{e_{L/K}} - \frac{(p-1)(p^{n-1}s_G(\sigma) - e_{L/K}t_0)}{e_{L/K}}\\ &= \frac{1}{e_{K_1/K}}\left(\widetilde{\mathrm{Ksw}}(L/K_1) + \frac{(p-1)e_{L/K_1}t_0}{e_{L/K_1}}\right)\\ &= \frac{1}{e_{K_1/K}}\widetilde{\mathrm{Ksw}}(L/K_1) + \frac{(p-1)t_0}{e_{K_1/K}}.\end{aligned}$$

Now we have to consider two cases.

1. The extension K_1/K is ferociously ramified. A direct calculation gives

$$\begin{gathered} U_{K_1}^{X+1} \subset N_{L/K_1}L^*, \quad \text{(by def. of } X)\\ N_{K_1/K}U_{K_1}^{t_0+(X+1-t_0)} = U_K^{pt_0-t_0+X+1} \subset N_{L/K}L^*,\end{gathered}$$

so $\mathrm{Ksw}(L/K) \le pt_0 - t_0 + X$. But the calculation just done gives:

$$[\widetilde{\mathrm{Ksw}}(L/K)] = [\widetilde{\mathrm{Ksw}}(L/K_1) + pt_0 - t_0] = X + pt_0 - t_0,$$

so in this case we are done.

2. The extension K_1/K is wildly ramified. A direct calculation gives

$$\begin{gathered} U_{K_1}^{X+1} \subset N_{L/K_1}L^*, \quad \text{(by def. of } X)\\ N_{K_1/K}U_{K_1}^{t_0+(X+1-t_0+R_{K_1/K})} = U_K^{t_0+(X+1-t_0+R_{K_1/K})/p} \subset N_{L/K}L^*,\end{gathered}$$

where $R_{K_1/K}$ is the smallest non negative integer such that $X + 1 - t_0 + R_{K_1/K}$ is divisible by p. So $\mathrm{Ksw}(L/K) \le t_0 + [(X - t_0)/p]$. To conclude we need of the following lemma.

Lemma 10.11 *Let $a = t/p^b \in \mathbb{Q}$ with $b \ge 1$, $t \in \mathbb{N}$ and let s be a positive integer such that $[a] \ge s$. Then*

$$\left[\frac{[a]-s}{p}\right] = \left[\frac{a-s}{p}\right].$$

Proof Let $t = [a]p^b + r$, $0 \le r < p^b$. Replacing the value of a in the statement, we put $X := [(t - sp^b)/(p^{b+1})]$. So $t - p^b s = Xp^{b+1} + r_0$, $0 \le r_0 < p^{b+1}$, and we have

$$\left[\frac{[a]-s}{p}\right] = \left[\frac{Xp^{b+1} + r_0 - r}{p^{b+1}}\right].$$

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

We show that $r_0 - r \geq 0$. Indeed, $r_0 - r = p^b([a] - s - Xp)$, but

$$a - s - Xp = r/p^b \geq 0, \quad \text{and} \quad [a] \geq s,$$

hence $([a] - s - Xp) \geq 0$. Finally $[(r_0 - r)/p^{b+1}] = 0$. So the lemma is proved. ∎

We return to proof of the proposition. By the above lemma (with $a = \widetilde{\mathrm{Ksw}}(L/K_1)$) we have

$$[\widetilde{\mathrm{Ksw}}(L/K)] = t_0 + \left[\frac{\widetilde{\mathrm{Ksw}}(L/K_1) - t_0}{p}\right] = t_0 + \left[\frac{X - t_0}{p}\right]$$

and the proposition is proved. ∎

10.5.3 Example of Computation of the Kato Conductor

Here we show that the Kato conductor can be smaller than $[\widetilde{\mathrm{Ksw}}(L/K)]$. Let F be a complete field of characteristic zero with residue field $\mathbb{F}_p(y)$, $(p \neq 2)$ the field of rational function in one variable over $\mathbb{F}_p$ and assume $e_F = 1$. We study a particular cyclic extension over $K = F(\zeta_{p^2})$. We choose as a prime element in K the element $\pi = \zeta_{p^2} - 1$. Note that $e_K = p(p-1)$. Consider the cyclic extension $L = K(x)$ defined by

$$(*) \qquad x^{p^2} = (1 + A\pi^p)\pi^p, \quad \overline{A} = y.$$

Let $G = \langle \sigma \rangle$. We clearly have $f^{\text{ins}}_{K_1/K} = p = e_{L/K_1}$; note that L/K is not well ramified (*cf.* Theorem 6.1). In fact putting $x^p = z$, we find that the subextension $K_1 = K(z)/K$ is f.r-1 with $i_{K_1/K}(\sigma) = p - 1 := a$ and L/K_1 is totally ramified with $i_G(\sigma) = p^2 + 1$, by using the notation as in the preceding section we have $b = p^2$. The situation is like this:

$$\begin{array}{ccc} L & \overline{L} = \overline{K}_1 & \mathcal{O}_L = \mathcal{O}_{K_1}[x] \\ | & | & \\ K_1 & \overline{K}(\sqrt[p]{y}) & \mathcal{O}_{K_1} = \mathcal{O}_K[\alpha] \\ | & | & \\ K & \overline{K} & \end{array}$$

where the extension of valuation rings is $\mathcal{O}_L = \mathcal{O}_K[\alpha, x]$, with $\alpha = (z/\pi - 1)/\pi$. Note that x is a prime of $\mathcal{O}_L$. By the preceding section we know that the Kato conductor $\mathrm{Ksw}(L/K)$ is less than $pa + b - a$, we will show that in fact it is strictly smallest than this value.

Let us look at the norm map $N_{L/K}$.

$$\begin{array}{ccccc} U_L^b/U_L^{b+1} & \xrightarrow{N_{L/K_1}} & U_{K_1}^b/U_{K_1}^{b+1} & \xrightarrow{N_1} & U_K^{pa+b-a}/U_K^{pa+b-a+1} \\ \cong\downarrow & & \cong\downarrow & & \cong\downarrow \\ \overline{L} = \mathbb{F}_p(\sqrt[p^2]{y}) & \longrightarrow & \overline{K}_1 = \mathbb{F}_p(\sqrt[p]{y}) & \longrightarrow & \overline{K} = \mathbb{F}_p(y) \end{array}.$$

We investigate these maps and we show that the composition $N_1 \circ N_{L/K_1}$ is surjective, so we deduce that $U_K^{pa+b-a} \subset N_{L/K}L^*$ which implies $\mathrm{Ksw}(L/K) < pa + b - a$.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

Let us consider $N_{L/K_1}\colon U_L^b/U_L^{b+1} \longrightarrow U_{K_1}^b/U_{K_1}^{b+1}$. It suffices to compute the norm of the elements of the form $1+ux^b$ with $u \in \mathcal{O}_{K_1}$ (recall that x is the prime chosen in $\mathcal{O}_L$ and see [S1, ch. V]).

$$N_{L/K_1}(1+ux^b) \equiv 1 + N_{L/K_1}u \cdot N_{L/K_1}x^b + \mathrm{Tr}_{L/K_1}(ux^b) \bmod \mathfrak{p}_{K_1}^{b+1}$$
$$\equiv 1 + \big(u^p(1+A\pi^p)^p\pi^{p^2} - u(1+A\pi^p)p\pi^p\big) \bmod \mathfrak{p}_{K_1}^{b+1}.$$

Hence, the norm map on the residue fields induces the following homomorphism

$$N_{L/K_1}\colon \overline{L} \longrightarrow \overline{K}_1 \qquad (17)$$
$$\overline{u} \mapsto \overline{u}^p - \overline{u}.$$

This map is clearly not surjective.

Now we make explicit the norm map $N_1 = N_{K_1/K}\colon U_{K_1}^b/U_{K_1}^{b+1} \longrightarrow U_K^{pa+b-a}/U_K^{pa+b-a+1}$ (recall that a is the ramification number of K_1/K). The induced map

$$U_{K_1}^b/U_{K_1}^{b+1} \xrightarrow{N_1} U_K^{b+(p-1)a}/U_K^{b+(p-1)a+1}$$

is surjective (Proposition 10.2) and we explicitly determine it. For $v = \sum_{i=0}^{p-1} a_i\alpha^i \in \mathcal{O}_{K_1}$ we have

$$N_1(1+v\pi^b) \equiv 1 + \mathrm{Tr}(v\pi^b) \bmod \mathfrak{p}_K^{b+(p-1)a+1},$$

and we have $\mathrm{Tr}(v) = \sum a_i \,\mathrm{Tr}(\alpha^i)$. A direct computation gives

$$\mathrm{Tr}(\alpha^i) \equiv 0 \bmod \pi^{(p-1)a+1}, \quad \text{for } i = 1,2,\dots,p-2$$
$$\mathrm{Tr}(\alpha^{p-1}) \equiv \pi^{(p-1)a} \bmod \pi^{(p-1)a+1},$$
$$\mathrm{Tr}(a_0) \equiv 0 \bmod \pi^{(p-1)a+1}.$$

So the induced norm map on residue fields is given by

$$\overline{K}_1 \xrightarrow{N_1} \overline{K} \qquad (18)$$
$$\overline{v} \longrightarrow \overline{a}_{p-1}.$$

Now we consider the image of an element $\gamma = \sum_{i=0}^{p-1} b_i(\sqrt[p]{y})^i$, $b_i \in \mathbb{F}_p(y)$. By composing maps (17) and (18) we see that $\gamma \mapsto b_{p-1}$, which means that the composition is surjective and the Kato conductor is strictly smaller than $pa+b-a$.

References

[B-C-S] R. Boltje, G. Martin Cram and V. P. Snaith, *Conductors in the non-separable residue field case.* Algebraic K-Theory and Algebraic Topology, Kluwer Acad. Publ., 1993, 1–34.

[BDS1] B. de Smit, *The different and differentials of local fields with imperfect residue field.* Proc. Edinburgh Math. Soc. **40**(1997), 353–365.

https://doi.org/10.4153/CJM-2000-053-1 Published online by Cambridge University Press

[BDS2] ———, *Ramification groups of local fields with imperfect residue class field.* J. Number Theory (3) **44**(1993), 229–236.

[B] J. Borger, *A monogenic Hasse-Arf theorem.* Proceedings of the Conference on Ramification theory for arithmetic schemes, Luminy, 1999, to appear.

[E] H. P. Epp, *Eliminating wild ramification.* Invent. Math. **19**(1973), 235–249.

[F-V] I. Fesenko and V. Vostokov, *Local fields and their extensions.* Trans. Math. Monographs, Amer. Math. Soc., 1993.

[Her] M. J. Herbrand, *Sur la théorie des groupes de décomposition, d'inertie et de ramification.* J. de Liouville, 1931.

[H] O. Hyodo, *Wild ramification in the imperfect residue field case.* Galois Representations and Arithmetic Algebraic Geometry, Adv. Stud. Pure Math. **12**(1987), 287–314.

[K1] K. Kato, *A generalization of local class field theory by using K-groups I.* J. Fac. Sci. Univ. Tokyo, Sect. IA **26**(1979), 303–376; *II*, *ibid.*, **27**(1980), 603–683.

[K2] ———, *Swan conductors with differential values.* Adv. Stud. Pure Math. **12**(1987), 315–342.

[K3] ———, *Swan conductors for characters of degree one in the imperfect residue field case.* Contemp. Math. **83**(1989), 101–131.

[K4] ———, *Vanishing cycles, ramification of valuations, and class field theory.* Duke Math. J. (3) **55**(1987), 629–659.

[Ku] M. Kurihara, *On two types of discrete valuation fields.* Compositio Math. **63**(1987), 237–257.

[M-W] R. E. MacKenzie and G. Whaples, *Artin-Schreier equations in characteristic zero.* Amer. J. Math. **78**(1956), 473–485.

[M] H. Miki, *On $\mathbb{Z}_p$-extensions of complete p-adic power series fields and function fields.* J. Fac. Sci. Univ. Tokyo Sect. IA **21**(1974), 377–393.

[P] A. N. Paršin, *Abelian coverings of arithmetic schemes.* Soviet Math. Dokl. **19**(1978), 1438–1442.

[Po] G. Poitou, *Cohomologie Galoisienne des modules finis.* Sém. Inst. Math. Lille DUNOD, Paris, 1967.

[Sen] S. Sen, *On automorphisms of local fields.* Ann. of Math. **90**(1969), 33–46.

[S1] J.-P. Serre, *Corps Locaux.* 3rd edition, Hermann, Paris, 1967.

[S2] ———, *Représentations linéaires des groupes finis.* Hermann, Paris, 1967.

[S3] ———, *Sur la rationalité des représentations d'Artin.* Ann. of Math. **72**(1960), 406–420.

[Sn] V. P. Snaith, *Explicit Brauer induction.* Cambridge University Press, 1994.

[Sp] L. Spriano, *Well and fiercely ramified extensions of complete discrete valuation fields with application to the Kato conductor.* Université de Bordeaux 1, 1999.

[Wi] S. Williamson, *Ramification theory for extensions of degree p.* Nagoya Math. J. **41**(1971), 149–168.

[Wy] B. Wyman, *Wildly ramified gamma extensions.* Amer. J. Math. **91**(1969), 135–152.

[Z-S] O. Zariski and P. Samuel, *Commutative algebra, Vol. I.* Graduate Texts in Math. **28**, Springer, 1960.

[Zh] I. B. Zhukov, *On ramification theory in the imperfect residue field case.* Preprint, University of Nottingham, 1998.

Université Bordeaux I
351, Cours de la Libération
33405 Talence
France
email: spriano@math.u-bordeaux.fr