Ramification groups of local fields with imperfect residue class fields

(To appear in the Journal of Number Theory)

Bart de Smit

Department of Mathematics University of California Berkeley, CA 94720

Abstract. The Galois group of a Galois extension of local fields with an inseparable residue class field extension has two intertwined filtrations with ramification groups. This note contains some elementary results on the structure of these filtrations, that are similar to those given by Serre in *Corps Locaux*, chapter IV, §3, for the case that the residue class field extension is separable.

Key words: ramification groups, local fields.

1980 Mathematics subject classification (1985): 11S15.

Acknowledgement. The author was supported by a John and Elliot Wheeler Fellowship from the University of California and NSF contract DMS 90-02939.

1. Introduction.

A local field is a complete field with respect to a discrete valuation. It is usually assumed in the theory of Galois extensions of local fields that the residue class field extension is separable, which holds for completions of number fields and function fields with a perfect field of constants (see e.g. [7, ch. IV]). We refer to this case as the classical case. There are many examples of imperfect residue class fields though, for instance the residue field of the local ring of a prime divisor on an algebraic surface in non-zero characteristic. This note is concerned with Galois extensions of local fields with an inseparable residue class field extension. As indicated in Zariski-Samuel [8], this leads to considering two intertwined filtrations of the Galois group with ramification groups. We will introduce this double filtration in section 2.

For the classical case, some basic results on the location of jumps in the sequence of ramification groups can be found in Serre [7, ch. IV, §3]. For instance, it is shown there that the jumps are all congruent modulo the residue characteristic. The goal of this note is to generalize these elementary statements in terms of the double filtration. See Fontaine [4] for an improvement for the case of a perfect residue field.

Deeper results like Hasse-Arf's theorem (see [7]) are even impossible to formulate for inseparable residue field extensions, because there is no satisfactory definition of an "upper numbering" in this case (see [3] and [5]). The most advanced result for local fields with imperfect residue class fields is probably Kato's local class field theory in [6] for "*n*dimensional local fields" F, in which a canonical homomorphism, the norm residue map, from a certain Milnor K-group to $\operatorname{Gal}(F^{\mathrm{ab}}/F)$ is constructed. Hyodo defines ramification groups in the upper numbering by looking at a filtration of this K-group (see [5]), but results on their relation to the usual ramification groups in lower numbering seem to be lacking.

2. Ramification groups.

For a local field K, we denote the valuation ring by A_K , its maximal ideal by \mathfrak{p}_K and its residue class field by \overline{K} . Let $K \subset L$ be a finite Galois extension of local fields with group G. Assume that char $\overline{K} = p > 0$ and let $f = f_{sep} f_{insep}$ be the degree of \overline{L} over \overline{K} , where f_{sep} is the degree of the separable part. Let $e = e_{tame} e_{wild}$ be the ramification index of Lover K, where e_{tame} is the tame ramification index (i.e., the *p*-prime part of *e*).

2.1 Definition. For $n, i \in \mathbb{Z}_{\geq 0}$ the (n, i)-ramification group $G_{n,i}$ of L over K is the subgroup of $G = \operatorname{Gal}(L/K)$ consisting of those K-automorphisms of L that induce the identity on $\mathfrak{p}_L^i/\mathfrak{p}_L^{n+i}$, i.e. $G_{n,i} = \{\sigma \in G : \forall x \in \mathfrak{p}_L^i : x - \sigma(x) \in \mathfrak{p}_L^{n+i}\}.$

Note that $G_{n,i}$ is a normal subgroup of G, as it is the kernel of the homomorphism $G \to \operatorname{Aut}(\mathfrak{p}_L^i/\mathfrak{p}_L^{n+i})$. For $n \ge 0$ we will use the notation $G_n = G_{n+1,0}$ and $H_n = G_{n,1}$, so that the usual ramification groups in the classical case, as in Serre [7], are the G_n . We have $H_0 = G$, and $G_n \subset H_n$.

The inertia group of L over K is G_0 . In other words, the field of invariants $T = L^{G_0}$ is the maximal subfield of L that is unramified over K, so \overline{T} is the separable closure of \overline{K} in \overline{L} , and $G/G_0 \cong \operatorname{Gal}(\overline{T}/\overline{K})$, which has order f_{sep} . The tame ramification group, corresponding to the maximal tamely ramified subfield of L, is $H_1 \cap G_0$ (see e.g. [2]), which is just H_1 by the next proposition. The group G_0/H_1 is cyclic, as it maps injectively to $\operatorname{Aut}_{\overline{L}}(\mathfrak{p}_L/\mathfrak{p}_L^2) \cong \overline{L}^*$, and its order is e_{tame} . Finally, H_1 is a p-group of order $e_{\operatorname{wild}}f_{\operatorname{insep}}$.

For $n, i \in Z_{\geq 0}$ we define $B_i^n = \mathfrak{p}_L^i/\mathfrak{p}_L^{i+n}$, so that $B^n = \bigoplus_{i\geq 0} B_i^n$ becomes a graded A_K -algebra with the obvious multiplication map. The action of G on each B_i^n induces an A_K -algebra action on B^n . Note that B^n is isomorphic to the tensor algebra of the B_0^n -module B_1^n , and that the isomorphism is canonical (in particular, it preserves the G-action). An element $\sigma \in G$ lies in $G_{n,i}$ if and only it acts trivially on B_i^n .

2.2 Proposition. For all $n \ge 1$ and $i \ge 0$ we have $H_n \subset G_{n,i} \subset G_{n-1}$.

Proof. The induced action of an element $\sigma \in G_{n,i}$ on the ring B_0^n is compatible with the trivial action of σ on the B_0^n -module B_i^n . As B_i^n is a faithful B_0^n -module it follows that σ operates trivially on B_0^n , so $\sigma \in G_{n-1}$, which proves the inclusion on the right.

Now let $\sigma \in H_n$, then we see that $\sigma \in G_{n-1}$, and σ operates trivially on B_0^n as well as on B_1^n . Therefore, σ acts trivially on the tensor algebra B^n , and in particular on the homogeneous part of degree i, so $\sigma \in G_{n,i}$. This proves the other inclusion. **2.3 Proposition.** If n > 1 in the proposition above then we have equality on the left if pi and on the right if $p \mid i$. In the case n = 1, the quotient group $G_{1,i}/H_1$ is the *i*-torsion of G_0/H_1 , which is cyclic of order gcd(e_{tame}, i).

Proof. Let $\sigma \in G_{n-1}$, so that σ operates trivially on B_0^n . The B_0^n -module B_1^n is free of rank 1, so the B_0^n -automorphism of B_1^n induced by σ is multiplication by a unit u of B_0^n . Consequently, σ induces multiplication by u^i on the *i*-th tensor power B_i^n of the B_0^n -module B_1^n , and it follows that $\sigma \in G_{n,i} \Leftrightarrow u^i = 1 \Leftrightarrow \sigma^i \in H_n$. In particular $G_{1,i}/H_1$ is the kernel of multiplication by i on the cyclic group G_0/H_1 .

Now suppose that n > 1. As σ acts trivially on $B_1^{n-1} \subset B_0^n$, we must have $u \in 1 + \mathfrak{p}_L^{n-1}/\mathfrak{p}_L^n \subset B_0^n$, so that $u^p = 1$. It follows that we have $\sigma \in G_{n,i}$ if and only if $p \mid i$ or u = 1, and the first statement of the proposition follows at once.

We thus have a filtration of G as in Zariski-Samuel [8, ch. V, $\S10$, theorem 25]:

$$G = H_0 \supset G_0 \supset H_1 \supset G_1 \supset H_2 \supset G_2 \supset \cdots$$

and every ramification group $G_{n,i}$ with n > 1 occurs in this sequence, in the sense that it equals G_{n-1} or H_n .

In the classical case $(f_{\text{insep}} = 1)$ we have $H_n = G_n$ for $n \ge 1$, so we do not have a strict refinement of the usual chain of ramification groups. This can be shown as follows. Let $T = L^{G_0}$ be the inertia field. Then we have $A_L = A_T + \mathfrak{p}_L$ as $\overline{T} = \overline{L}$. If $\sigma \in H_n$ with $n \ge 1$, then σ operates trivially on $\mathfrak{p}_L/\mathfrak{p}_L^{n+1}$ and on A_T (as $H_n \subset G_0$), so it must act trivially on A_L/\mathfrak{p}_L^{n+1} which shows that $\sigma \in G_n$.

If $e_{\text{wild}} = 1$, then we have $G_n = H_{n+1}$ for $n \ge 1$, because multiplication by a prime element of the tame ramification field is an isomorphism of B_0^n to B_1^n , that preserves the action of H_1 .

We now derive some simple properties of the ramification groups by embedding the quotient groups G_n/G_{n+m} and H_n/H_{n+m} in groups of homomorphisms for $m \leq n$.

2.4 Proposition. Let $n, m \in Z$ with $0 \le m \le n$. The map $\phi : G_n \to \operatorname{Hom}_{A_K}(A_L, \mathfrak{p}_L^{n+1})$ defined by $\phi(\sigma)(x) = \sigma x - x$ induces an injective homomorphism of groups

$$G_n/G_{n+m}\operatorname{Hom}_{A_K}(B_0^{m+1}, B_{n+1}^m)$$

Proof. As $G_n \subset G_{n,m+1}$, the image of \mathfrak{p}_L^{m+1} under $\phi(\sigma)$ is contained in \mathfrak{p}_L^{n+m+1} for all $\sigma \in G_n$, so we obtain a mapping $G_n \to \operatorname{Hom}_{A_K}(B_0^{m+1}, B_{n+1}^m)$. In order to show that this is a homomorphism of groups, note that for $\sigma, \tau \in G_n$ and $x \in A_L$ we have $\phi(\sigma\tau)(x) - \phi(\sigma)(x) - \phi(\tau)(x) = \phi(\sigma)(\phi(\tau)(x)) \in \mathfrak{p}_L^{2n+1}$, because $\phi(\tau)(x) \in \mathfrak{p}_L^{n+1}$ and $\sigma \in G_n \subset G_{n,n+1}$. Finally, the kernel of this homomorphism is clearly G_{n+m} . Analogously, we have a canonical injection of groups $H_n/H_{n+m}\operatorname{Hom}_{A_K}(B_1^m, B_{n+1}^m)$. It follows that the groups G_n/G_{2n} and H_n/H_{2n} are abelian, which is also shown in [8]. Furthermore, the groups G_n/G_{n+1} and H_n/H_{n+1} are annihilated by p for all $n \ge 1$, and if char K = p, then the same holds for G_n/G_{2n} and H_n/H_{2n} .

2.5 Proposition. For all $n, m \ge 0$ we have $[G_n, G_m] \subset G_{n+m}$ and $[H_n, H_m] \subset H_{n+m}$.

Proof. We may assume that $m \leq n$. Recall that G acts on the set of homomorphisms f from a G-module M to a G-module N by $(\sigma f)(x) = \sigma(f(\sigma^{-1}x))$ for $x \in M$. Letting G act on G_n/G_{n+m} by conjugation, it is easy to check that the embedding in 2.4 preserves the action of G. But as G_m acts trivially on B_0^{m+1} and on B_{n+1}^m , it follows that G_m acts trivially on G_n/G_{n+m} , so $[G_n, G_m] \subset G_{n+m}$. The second statement can be deduced in the same way.

3. Derivations and commutators.

Let *m* and *n* be non-negative integers with $m \leq n$. The image of G_n/G_{n+m} under the embedding in proposition 2.4 lies in the subgroup $\text{Der}_{A_K}(B_0^{m+1}, B_{n+1}^m)$ of A_K -derivations of B_0^{m+1} to B_{n+1}^m . This follows from the fact that for $x, y \in A_L$ and $\sigma \in G_n$ we have

$$\sigma(xy) - xy = x(\sigma y - y) + y(\sigma x - x) + (\sigma y - y)(\sigma x - x),$$

and the last term on the right hand side lies in $\mathfrak{p}_L^{2n+2} \subset \mathfrak{p}_L^{n+m+1}$.

The following proposition shows that the image of H_n/H_{n+m} in $\operatorname{Hom}_{A_K}(B_1^m, B_{n+1}^m)$ is contained in a subgroup that can be described as a group of graded derivations. If Bis a graded algebra over a ring A, the A-module $\operatorname{Der}_A^n(B)$ of graded derivations of degree n from B to B consists of those graded A-endomorphisms d of degree n of B for which d(xy) = xd(y) + yd(x) for all $x, y \in B$.

3.1 Proposition. For all $n, m \in Z$ with $1 \le m \le n$ we have a canonical embedding

$$\phi_n: H_n/H_{n+m} \mathrm{Der}^n_{A_K}(B^m)$$

given by $\phi_n(\overline{\sigma})(\overline{x}) = \sigma x - x \mod \mathfrak{p}_L^{i+n+m}$ for $\overline{\sigma} \in H_n/H_{n+m}$ with representative $\sigma \in H_n$, and $\overline{x} \in B_i^m$ with representative $x \in \mathfrak{p}_L^i$.

The straightforward proof is left to the reader. We may view $\operatorname{Der}_{A_K}^n(B^m)$ as a subgroup of $\operatorname{Hom}_{A_K}(B_1^m, B_{n+1}^m)$ as it is easy to check that the restriction map from the first to the second is injective. Furthermore, an A_K -homomorphism $d_1: B_1^m \to B_{n+1}^m$ lies in its image if and only if there exists a $d_0 \in \operatorname{Der}_{A_K}(B_0^m, B_n^m)$ such that $\forall x \in B_0^m \forall y \in B_1^m : d_1(xy) =$ $d_0(x)y + xd_1(y)$ (cf. Bourbaki [1, ch. III, §10, proposition 14]).

The direct sum $\bigoplus_{i\geq 0} \operatorname{Der}_{A_K}^i(B^m)$ has a structure of a graded Lie-algebra over A_K , with Lie-brackets $[\cdot, \cdot]$ defined by $[d_1, d_2] = d_1 \circ d_2 - d_2 \circ d_1$. From 2.5 we know that we

have a commutator mapping $H_a \times H_b \to H_{a+b}$ defined by $(\sigma, \tau) \mapsto [\sigma, \tau] = \sigma \tau \sigma^{-1} \tau^{-1}$. These two bracket operations are compatible in the sense of the following theorem.

3.2 Theorem. If $m \ge 0$ and $a, b \ge m$, then the commutator map induces a Z-bilinear map $H_a/H_{a+m} \times H_b/H_{b+m} \to H_{a+b}/H_{a+b+m}$, and the following diagram commutes:

$$\begin{array}{cccc} H_a/H_{a+m} & \times & H_b/H_{b+m} & \xrightarrow{[\cdot,\cdot]} & H_{a+b}/H_{a+b+m} \\ & & & & \downarrow \phi_a \times \phi_b & & & \downarrow \phi_{a+b} \\ \operatorname{Der}^a_{A_K}(B^m) & \times & \operatorname{Der}^b_{A_K}(B^m) & \xrightarrow{[\cdot,\cdot]} & \operatorname{Der}^{a+b}_{A_K}(B^m) \end{array}$$

Proof. Let $\overline{x} \in B_i^m$ and let x be a representative of \overline{x} in \mathfrak{p}_L^i . For $\sigma \in H_a$ and $\tau \in H_b$ we have $\phi_a(\sigma)(\phi_b(\tau)(\overline{x})) = x - \tau x - \sigma x + \sigma \tau x \mod \mathfrak{p}_L^{i+m+a+b}$. Subtracting the same equality with σ and τ interchanged gives

$$[\phi_a(\sigma),\phi_b(\tau)](\overline{x}) = \sigma\tau x - \tau\sigma x \mod \mathfrak{p}_L^{i+m+a+b} = \phi_{a+b}([\sigma,\tau])(\tau\sigma\overline{x}) = \phi_{a+b}([\sigma,\tau])(\overline{x}),$$

as both σ and τ operate trivially on B^m . The bottom horizontal map in the diagram is A_K -bilinear and the vertical maps are injective. It now follows immediately that the diagram is commutative and that the top horizontal map is well-defined and Z-bilinear (which can also be shown by suitable identities with commutators).

4. Jumps.

In this section we apply the ideas of the previous section to the case m = 1, in order to get results on where the jumps in the double filtration can occur. Consider the map $\phi_n : H_n/H_{n+1} \to \operatorname{Der}_{\overline{K}}^n(B^1)$. The preimage of the set $\operatorname{Der}_{\overline{L}}^n(B^1)$ of those derivations that are zero on $B_0^1 = \overline{L}$ is clearly G_n/H_{n+1} . Such a derivation must be multiplication by some $x \in B_n^1$ in degree 1, and then it is easy to deduce that it is multiplication by ix in degree i. In other words, we have an isomorphism $\alpha : B_n^1 \xrightarrow{\sim} \operatorname{Der}_{\overline{L}}^n(B^1)$ defined by $\alpha(x)(y) = ixy$ for $x \in B_n^1$ and $y \in B_i^1$. We thus get a canonical map $\theta_n : G_n/H_{n+1} \to B_n^1$ that can be given explicitly by $\sigma \mapsto \frac{\sigma \pi - \pi}{\pi} \mod \mathfrak{p}_L^{n+1}$, where π is any prime element of L. This can be summarized in the following commutative diagram in which the rows are exact and the vertical maps are injections.

First we look at the action of the tame ramification group. Denote the canonical map $G_0/H_1\overline{L}^*$ by θ_0 , so that $\sigma \in G_0$ induces multiplication by $\theta_0(\sigma)$ on $\mathfrak{p}_L/\mathfrak{p}_L^2 = B_1^1$.

4.1 Proposition. For $\sigma \in G_0$ and $\tau \in H_n$, we have $\kappa_n(\sigma\tau\sigma^{-1}) = \theta_0(\sigma)^n\kappa_n(\tau)$, and for $\sigma \in G_0$ and $\tau \in G_n$ we have $\theta_n(\sigma\tau\sigma^{-1}) = \theta_0(\sigma)^n\theta_n(\tau)$.

Proof. The mapping $\phi_n : H_n/H_{n+1} \to \operatorname{Der}_{\overline{K}}^n(B^1)$ respects the action of G_0/H_1 , where $\sigma \in G_0$ acts on H_n/H_{n+1} by conjugation, and on $\operatorname{Der}_{\overline{K}}^n(B^1)$ by conjugation with the automorphism of B^1 induced by σ , which multiplies an element $x \in B_i^1$ by $\theta_0(\sigma)^i$. So for $\sigma \in G_0, \tau \in H_n$ and $x \in B_0^1$ we get $\kappa_n(\sigma\tau\sigma^{-1})(x) = \sigma(\kappa_n(\tau)(\sigma^{-1}x)) = \theta_0(\sigma)^n\kappa_n(\tau)(x)$. For $\sigma \in G_0, \tau \in G_n$, and $x \in B_1^1$ we similarly obtain $\theta_n(\sigma\tau\sigma^{-1}) \cdot x = \phi_n(\sigma\tau\sigma^{-1})(x) = \sigma(\phi_n(\tau)(\sigma^{-1}x)) = \theta_0(\sigma)^{n+1}\theta_n(\tau)\theta_0(\sigma)^{-1} \cdot x = \theta_0(\sigma)^n\theta_n(\tau) \cdot x.$

4.2 Corollary. If G_0 is abelian, then $H_n = G_n = H_{n+1}$ for all $n \in \mathbb{Z}_{>0}$ that are not divisible by the tame ramification index.

Proof. If G_0 is abelian, then $\sigma\tau\sigma^{-1} = \tau$ for all $\sigma, \tau \in G_0$, so if θ_n or κ_n are not identically zero, this implies that $\theta_0(\sigma)^n = 1$ for all $\sigma \in G_0$. The statement therefore follows from the fact that G_0/H_1 is a cyclic group whose order is the tame ramification index.

Next, we look at commutators from higher ramification groups, and again we get some conditions on where the jumps can be in the filtration.

4.3 Proposition. Let $n, m \in \mathbb{Z}_{>1}$. If $\sigma \in G_n$ and $\tau \in H_m$, then

$$\kappa_{n+m}(\sigma\tau\sigma^{-1}\tau^{-1}) = m\theta_n(\sigma)\kappa_m(\tau),$$

and if in addition $\tau \in G_m$, then $\theta_{n+m}(\sigma\tau\sigma^{-1}\tau^{-1}) = (m-n)\theta_n(\sigma)\theta_m(\tau)$.

Proof. Using the fact that $\phi_{n+m}(\sigma\tau\sigma^{-1}\tau^{-1}) = \phi_n(\sigma) \circ \phi_m(\tau) - \phi_m(\tau) \circ \phi_n(\sigma)$, and $\phi_n(\sigma)(x) = \alpha(\theta_n(\sigma))(x) = i\theta_n(\sigma) \cdot x$ for $x \in B_i^1$, it follows that for all $x \in B_0^1$ we have $\kappa_{n+m}(\sigma\tau\sigma^{-1}\tau^{-1})(x) = m\theta_n(\sigma) \cdot \kappa_n(\tau)(x) - \phi_m(\tau)(0\theta_n(\sigma) \cdot x) = m\theta_n(\sigma)\kappa_m(\tau)(x)$.

For $\tau \in G_m$ and $x \in B_1^1$ we similarly obtain $\theta_{n+m}(\sigma\tau\sigma^{-1}\tau^{-1})\cdot x = [\phi_n(\sigma), \phi_m(\tau)](x) = \phi_n(\sigma)(\theta_m(\tau)\cdot x) - \phi_m(\tau)(\theta_n(\sigma)\cdot x) = (m-n)\theta_n(\sigma)\theta_m(\tau)\cdot x$, as required.

4.4 Corollary. If G is abelian then all n > 0 with $G_n \neq H_{n+1}$ are congruent modulo p, and if there exists such an n, then all m with $H_m \neq G_m$ are divisible by p.

The following proposition shows that the first statement of 4.4 remains true in the not necessarily abelian case. For the second statement an additional condition seems necessary.

4.5 Proposition. Denote the set of n > 0 with $G_n \neq H_{n+1}$ by T, and the set of m > 0 with $H_m \neq G_m$ by S. Then all elements of T are congruent modulo p, and for $n \in T$ and $m \in S$ with pm we have $n + m \in T$. Furthermore, we have $S \subset pZ$ whenever $T \cap pZ \neq \emptyset$.

Proof. Suppose that $T \neq \emptyset$. As T is a finite set, it contains a maximal element n, so that $\theta_{n+n'}$ is the zero map for all n' > 0. It now follows from the second equality in 4.3 that every $n' \in T$ must be congruent to n modulo p.

Now let $n \in T$ and $m \in S$ with pm. Then the first equality in 4.3 shows that $n+m \in S$. For the last statement, assume that $S \not\subset pZ$, and let $n \in T$ with $p \mid n$. Let m be the biggest element of S that is not divisible by p, then $m + n \in S$ and pm + n, contradicting the choice of m.

4.6 Corollary. For all $n, m \ge 1$ we have $[G_n, G_m] \subset H_{n+m+1}$ and if $S \subset pZ$ then $[G_n, H_m] \subset G_{n+m}$ for n, m > 1.

Proof. It follows from 4.5 that at least one of the factors on the right in the second equation of 4.3 is zero, and if $S \subset pZ$ then the same holds for the first equation.

References.

- N. Bourbaki, Algèbre I, Hermann, Paris, 1970 [English translation: Algebra I, Addison Wesley, Reading, 1974].
- [2] J.W.S. Cassels and A. Fröhlich (eds.), Algebraic number theory, Academic Press, London-New York, 1967.
- [3] B. de Smit, The different and differentials for local fields with imperfect residue fields, in preparation, 1991.
- [4] J-M. Fontaine, Extensions finies Galoisiennes de corps valués complets à valuation discrète, Séminaire Delange-Pisot-Poitou (Théorie des nombres) 9, exposé 6 (1967/68).
- [5] O. Hyodo, Wild ramification in the imperfect residue field case, in Y. Ihara (ed.), Galois representations and arithmetic algebraic geometry, North-Holland, Advanced studies in pure mathematics 12, 1987, pp. 287–314.
- [6] K. Kato, A generalization of local class field theory by using K-groups II, J. Fac. Sci. Univ. Tokyo, 27 (1980), pp. 603–683.
- [7] J-P. Serre, Corps locaux, Hermann, Paris, 1962 [English translation: Local fields, Springer-Verlag GTM 67, New York, 1979].
- [8] O. Zariski and P. Samuel, Commutative algebra, Vol. I, Van Nostrand, Princeton, New Jersey, 1958 [Reprinted Springer-Verlag GTM 28, New York, 1960].