doi: 10.2478/v10062-012-0027-8

ANNALES
UNIVERSITATIS MARIAE CURIE-SKŁODOWSKA
LUBLIN – POLONIA

VOL. LXVII, NO. 2, 2013 SECTIO A 17–32

AKRAM LBEKKOURI

Some results on local fields

Abstract. Let K be a local field with finite residue field of characteristic p. This paper is devoted to the study of the maximal abelian extension of K of exponent $p-1$ and its maximal p-abelian extension, especially the description of their Galois groups in solvable case. Then some properties of local fields in general case are studied too.

1. Presentation. Let us make a description of some standard over-extensions. But, first let us specify some important, although well-known remarks concerning the characteristics of a local field and its residue field.

Let K be a complete field with respect to a discrete valuation.

1.1. Characteristics.

1.1.1. The case of mixed characteristics. In this case, necessarily $char(K) = 0$ and the residue field is necessarily of characteristic $p > 0$. Therefore, K contains necessarily the $(p-1)$-th roots of unity.

It is worthy to note that in this case the residue field may be finite or infinite. Indeed, for the infinite case consider the following example.

Let p be an arbitrary but fixed prime number, let K be the completion of $\mathbb{Q}_{nr}$, the field generated over $\mathbb{Q}_p$ by all roots of unity of order prime to p (i.e., the maximal unramified extension of $\mathbb{Q}_p$) which is a complete discrete valued field of characteristic 0 with infinite residue field of characteristic $p > 0$. Then the residue field is equal to the algebraic closure of $\mathbb{F}_p$ (namely

2000 *Mathematics Subject Classification.* 11S15.

Key words and phrases. Local fields, local number fields, Wild ramification, intermediate extension, standard p-over-extensions, semi-direct product, inertia group.

the field generated by all $\mathbb{F}_{p^{l^n}}$ with l prime and n any strictly positive integer), which is infinite.

1.1.2. The case of equal characteristics. In this case we may have $char(K) = 0$ with a residue field necessarily infinite. In such case K may contain the $(p-1)$-th roots of unity or not, as well as the p-th roots of unity.

Or we may have $char(K) = p > 0$ with a residue field that may be finite or infinite. In such case K contains necessarily the $(p-1)$-th roots of unity, but does not contain the p-th roots of unity.

1.2. Presentation of the standard p-over-extensions. *By "standard p-over-extensions" of a local field K with finite residue field of characteristic p, we mean the maximal abelian extension M of K of exponent $p-1$, and the maximal p-abelian extension of M.*

Some needed theorems on groups. Schur–Zassenhaus theorem, 1937 (first version):

Theorem 1.1. *If G is a finite group, N is an invariant (not necessarily abelian) subgroup of G, and if $(\#N, \#G/N) = 1$, then the following sequence:*

$$1 \mapsto N \mapsto G \mapsto G/N \mapsto 1$$

is exact, also N has a complement M in G, that is G is a semi-direct product of N by M.

Schur–Zassenhaus theorem (second version), see [6], Chap. 7, Th. 7.24., page 151:

Theorem 1.2. *If N and M are finite groups of relatively prime orders, then every extension of N by M is a semi-direct product.*

Generalized Schur–Zassenhaus theorem, see [5], § 2.3, page 41:

Theorem 1.3. *Let K be a closed normal Hall subgroup of a profinite group G. Then K has a complement L in G (i.e., L is a closed subgroup of G such that $G = KL$ and $K \cap L = \{1\}$). Moreover, any two complements of K are conjugate.*

Note. A closed subgroup K of a profinite group G is a π-Hall subgroup if $\#K$ is a π-number and $|G : K|$ is a π'-number. When $\pi = \{p\}$, a π-Hall subgroup is simply called p-Sylow subgroup.

In particular, if the exponent and the index of K are relatively, prime then K is a π-Hall subgroup.

1.2.1. Case of finite residue field. Let p be a prime number and K be a local field with finite residue field of characteristic p, $K = \mathbb{F}_{p^f}$. Therefore, the maximal abelian extension of exponent $p-1$ of K is $M = K((K^\star)^{1/p-1})$, regardless of the characteristic of K.

Write $\Gamma = gal(M/K)$ for the Galois group. From Kummer Theory for abelian extensions we have that the group Γ is dual to the group $K^\star/K^{\star(p-1)}$, under the pairing:

$$\begin{array}{rccc} \varphi: & \Gamma \times \left(K^\star/K^{\star(p-1)}\right) & \longmapsto & \mathbb{F}_p^\star \\ & (\sigma, \overline{x}) & \longmapsto & \sigma(y)/y \end{array}$$

with $(y^{p-1} = x)$ where $\mathbb{F}_p^\star \subset K^\star$ has been identified with the group of the $(p-1)$-th roots of unity.

Write N for the maximal abelian extension of exponent p of M (i.e., the maximal p-abelian extension of M). The expression of N depends essentially on the characteristic of K:

1. If $char(K) = 0$, K is a finite extension of $\mathbb{Q}_p$ of residual degree f and ramification index e, then $N = M(\sqrt[p]{M^\star})$. Furthermore we have the tower:

$$K \text{ ——— } M = K\left(\sqrt[p-1]{K^\star}\right) \text{ ——— } N = M(\sqrt[p]{M^\star}).$$

The group $\Delta = gal(N/M)$ is isomorphic to the filtered Γ-module $M^\star/M^{\star p}$ of $\mathbb{F}_p$-dimension $2 + (p-1)^2 ef$.

2. If $char(K) = p > 0$, $K = k((T))$, we can not take the same extension as above. Indeed extracting p-th roots in characteristic p gives rise to purely inseparable extensions, in nontrivial case. In such case, the field N is obtained by adjoining the zeroes of polynomials of the form $X^p - X - a$ with $a \in M$, (Artin–Schreier polynomials). Then we have $N = M(\wp^{-1}(M))$, where $\wp$ is the endomorphism of M defined by $\wp : x \to x^p - x$. So, we have the tower:

$$K \text{ ——— } M = K\left(\sqrt[p-1]{K^\star}\right) \text{ ——— } N = M(\wp^{-1}(M)).$$

$\Delta = gal(N/M)$ is isomorphic to the filtered Γ-module $M/(\wp(M))$ of $\mathbb{F}_p$-dimension $+\infty$.

Clearly all extensions of the two towers above are normal, so we write the different Galois groups as follows:

• $\Gamma = gal(M/K)$, which is abelian of degree $(p-1)^2$ isomorphic to $(\mathbb{Z}/(p-1)\mathbb{Z})^2$.

• $\Delta = gal(N/M)$, which is abelian too of exponent p, isomorphic to a product of a nonnecessarily countable number of copies of $\mathbb{Z}/p\mathbb{Z}$, in general see §2.4., (but in mixed characteristics case this number is finite).

• $\mathcal{G} = gal\,(N/K)$, which is not necessarily abelian. Furthermore, it is a semi-direct product $\mathcal{G} = \Delta \rtimes \Gamma$. Indeed, according to Schur–Zassenhaus Theorems 1.1, 1.2, we get the result for finite case. For general case, from Krull topology, Δ is a closed normal subgroup of $\mathcal{G}$ and the exponents are relatively prime, then according to the generalized Schur–Zassenhaus Theorem 1.3, we get the result too.

1.2.2. On the case of equal and prime characteristics. Let K be a local field having the same characteristic $p > 0$ as its residue field which is neither assumed to be finite nor perfect. In this case we still have the tower:

$$K \text{ ——— } M = K\big(\sqrt[p-1]{K^\star}\big) \text{ ——— } N = M(\wp^{-1}(M)).$$

The group $\Gamma = gal(M/K)$ is not necessarily finite but abelian of exponent $p-1$. The group $\Delta = gal(N/M)$ is isomorphic to an infinite but not necessarily countable number of copies of $\mathbb{Z}/p\mathbb{Z}$.

Proposition 1.4. *If $K = F((T))$, where F is a field of characteristic p which is not perfect, then $K/\wp(K)$ is infinite. Here $\wp$ is the endomorphism defined by $\wp : x \to x^p - x$.*

Proof. Consider $\frac{1}{T^n}$, where $n > 0$ and p does not divide n. If $\frac{1}{T^n} - \frac{1}{T^{n'}} \in \wp(K)$, with $n \neq n'$ and p does not divide nn', then $\frac{1}{T^n} - \frac{1}{T^{n'}} = f^p - f$, for some $f \in K = k((T))$. But $f \notin K = k[[T]]$ necessarily (since $n, n' > 0$ and distinct). Thus f has a leading polar term with degree $-r < 0$, so f^p has a pole with degree $-rp < -r$, that is $f^p - f$ has a pole of order rp that is divisible by p yet the difference $\frac{1}{T^n} - \frac{1}{T^{n'}}$ does not have this property, since n and n' are distinct and not divisible by p, which ends the proof. □

1.2.3. The field $M = K((K^\star)^{1/p-1})/K$ in the general case.

• In the local case with finite residue field of characteristic p we have seen that $M = K((K^\star)^{1/p-1})/K$ is an abelian extension of degree $(p-1)^2$, the Galois group of which is isomorphic to $(\mathbb{Z}/(p-1)\mathbb{Z})^2$.

• Meanwhile, if K is a complete field with respect to a discrete valuation having a residue field of characteristic p not necessarily finite, then $M = K((K^\star)^{1/p-1})/K$ is not necessarily finite, but it is abelian of exponent $p-1$, since K contains the $(p-1)$-th roots of unity.

• Otherwise, for such M/K, this extension need not be finite; if it is finite it need not be Galois; and if it is finite and Galois it need not have that Galois group. Some examples follow.

Examples.

1. Let $K = k((t))$, where $k = \mathbb{Q}(\xi_3)$ and ξ_3 is a primitive cube root of unity. So K is a complete discretely valued field.

Let $p = 3$. Then $k((k^\star)^{1/p-1})/k$ is infinite. Hence so is $K((K^\star)^{1/p-1})/K$.

2. Let k be an algebraically closed field of characteristic 0, and let $K = k((t))$. Then $K((K^\star)^{1/p-1})/K$ is Galois with group $\mathbb{Z}/(p-1)\mathbb{Z}$, not $(\mathbb{Z}/(p-1)\mathbb{Z})^2$.

3. Let k be the field of 3 elements, and let $K = k((t))$.

Let $p = 11$. Then $K((K^\star)^{1/p-1})/K$ is Galois with group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

4. Let k be the field of 3 elements, and let $K = k((t))$.

Let $p = 7$. Then $K((K^\star)^{1/p-1})/K$ has degree 12 (not 36), but it is not Galois because it is not separable, since $t^{1/3}$ is in this field.

5. $K = \mathbb{Q}(\xi_3)$ where ξ_3 is a 3-rd root of unity. Therefore, $M/K = K((K^\star)^{1/p-1})/K = \mathbb{Q}(\xi_3)((\mathbb{Q}(\xi_3)^\star)^{1/2})/\mathbb{Q}(\xi_3)$ is infinite, since adjoining to K the square roots of different prime elements of $\mathbb{Z}[\xi_3]$ will lead to disjoint

quadratic extensions whose composite has the degree equal to a large power of 2 (the power being the number of primes).

More generally we have the following results:

6. *Consider $K = \mathbb{Q}(\xi_p)$ where ξ_p is a p-th root of unity, p being an odd prime number. Then*

$$K\big(\sqrt[1/p-1]{K^\star}\big)/K = \mathbb{Q}(\xi_p)\Big(\sqrt[1/p-1]{\mathbb{Q}(\xi_p)^\star}\Big)/\mathbb{Q}(\xi_p)$$

is infinite.

Indeed, from the well-known result: *For relatively prime integers $a_1, \ldots, a_n$, the 2^n algebraic numbers $\sqrt{a_{i_1}, \ldots, a_{i_k}}$ with $i_1 < \cdots < i_k$ and $0 \le k \le n$ are linearly independent over $\mathbb{Q}$, so are a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{a_{i_1}}, \ldots, \sqrt{a_{i_k}})$. In particular, the degree of that field over $\mathbb{Q}$ is the maximum possible 2^n*, we can deduce that $\mathbb{Q}((\mathbb{Q}^\star)^{1/2})/\mathbb{Q}$ is infinite. Since $\mathbb{Q}(\xi_p)/\mathbb{Q}$ is finite, then $Q(\xi_p)((Q(\xi_p)^\star)^{1/2})/\mathbb{Q}(\xi_p)$ is infinite, therefore $\mathbb{Q}(\xi_p)((\mathbb{Q}(\xi_p)^\star)^{1/p-1})/\mathbb{Q}(\xi_p)$ is infinite too. The result is proved.

Note that the degree of $\mathbb{Q}(\xi_p)(\sqrt{a_{i_1}}, \ldots, \sqrt{a_{i_k}})$ over $\mathbb{Q}(\xi_p)$ is 2^n or 2^{n-1}; it depends on whether the set the numbers a_i union $+p$ or $-p$ is still independent or not and $\sqrt{+p}$ or $\sqrt{-p}$ belongs to $\mathbb{Q}(\xi_p)$ depending on whether $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$.

Furthermore, we have the following generalization:

7. *For any fractions field K, with characteristic not equal to 2, of a Dedkind ring $\mathfrak{A}$ having infinite many prime ideals and any odd prime number p, we have that $M = K((K^\star)^{1/p-1})/K$ is infinite.*

Indeed, it suffices to notice that when adjoining to K the square roots of two different prime elements of $\mathfrak{A}$ will lead to disjoint quadratic extensions. In fact, let $L = K(\sqrt{p})$ and $L' = K(\sqrt{q})$. They are both quadratic. Necessarily $L \cap L' = K$ otherwise $L = L'$, this means that $\sqrt{q} = a + b\sqrt{p}$ for $a, b \in K$, thus $q = a^2 + 2ab\sqrt{p} + b^2 p$. Clearly b has to be non-zero. If a is also non-zero, then this formula shows that $\sqrt{p} \in K$, so a has to be zero. Then $q = b^2 p$, but once we localize at the ideal generated by the prime number q; the prime number p is then a unit and q is a uniformizer so this cannot happen.

8. In contrast, in characteristic 2 we have the counter-example

$$\mathbb{F}_2(T)\big(\sqrt{T}\big) = \mathbb{F}_2(T)\big(\sqrt{T+1}\big).$$

Note. Concerning items 7 and 8, the different result for characteristic 2 is really just an artifact. More generally, if p is any prime and a positive integer n is not a power of p, then $M = K((K^{\star 1/n})/K$ is infinite for rings as in item 7. Of course if p is prime and $n = p - 1$, then n cannot be a power of a prime q unless $q = 2$, which leads to the item 8. But if we take a different n (e.g. take $n = p - 2$), then characteristic 2 need not be the exception.

2. Description of the over-extensions (case of finite residue field).

2.1. Sundries on groups. First let us prove some necessary results:

Proposition 2.1. *Let G_0 be a subgroup of $\mathcal{G} = (\mathbb{Z}/p\mathbb{Z})^n \rtimes_\varphi (\mathbb{Z}/(p-1)\mathbb{Z})^2$ of index p, then $G_0 \cap (\mathbb{Z}/p\mathbb{Z})^n$ is normal in $\mathcal{G}$.*

Proof. First note that $(\mathbb{Z}/p\mathbb{Z})^n$ is the p-Sylow subgroup of $\mathcal{G}$ and is normal in it. Since G_0 contains a copy of $(\mathbb{Z}/(p-1)\mathbb{Z})^2$, then $(\mathbb{Z}/(p-1)\mathbb{Z})^2$ normalizes G_0 and therefore normalizes $G_0 \cap (\mathbb{Z}/p\mathbb{Z})^n$. On the other hand $(\mathbb{Z}/p\mathbb{Z})^n$ normalizes $G_0 \cap (\mathbb{Z}/p\mathbb{Z})^n$, since $(\mathbb{Z}/p\mathbb{Z})^n$ is abelian. In consequence $G_0 \cap (\mathbb{Z}/p\mathbb{Z})^n$ is normal in $\mathcal{G}$. □

Remark 2.2. The result above does not mean that any subgroup of index p of $(\mathbb{Z}/p\mathbb{Z})^n$ is normal in $\mathcal{G} = (\mathbb{Z}/p\mathbb{Z})^n \rtimes_\varphi (\mathbb{Z}/(p-1)\mathbb{Z})^2$. See the following counter-example.

Example 2.3 (Counter-example). Let $K = \mathbb{Q}_3$, consider $M = K\left(\sqrt{K^\star}\right) = \mathbb{Q}_3\left(i, \sqrt{3}\right)$, and consider $E = M\left(\sqrt[3]{1+\sqrt{3}}\right)$, that is a normal 3-extension of M. The Galois closure of E/K is $N = M\left(\sqrt[3]{M^\star}\right)$, i.e.,

$$N = M\left(\sqrt[3]{1+\sqrt{3}}, \sqrt[3]{1-\sqrt{3}}\right)$$

and $gal\,(N/M) = (\mathbb{Z}/3\mathbb{Z})^2$. But E/K is not normal, otherwise there should be an intermediate subextension E'/K of degree 3 of E/K and an automorphism σ of E that maps $\sqrt{3}$ to $-\sqrt{3}$, which is the identity on E', furthermore $\sigma\left(\sqrt[3]{1+\sqrt{3}}\right)$ must be a cubic root of $\sigma(1+\sqrt{3}) = 1-\sqrt{3}$, but E contains no such root, since E is strictly contained in N. Hence the subgroup $gal\,(N/E)$ is not normal in $gal\,(N/K)$.

2.2. Case of mixed characteristic.

Remark 2.4. From the expression of Γ above, we know that Γ is of exponent $p-1$, that is M/K is abelian Kummer extension relatively to the number $p-1$. Furthermore, the multiplicative group $\sqrt[p-1]{K^\star}/K^\star$ contains a finite number of coclasses $c_i K^\star$ likewise the multiplicative group $K^\star/K^{\star p-1}$, with the coclasses $c_i K^{\star p-1}$. Δ being seen as Γ-module, from the action of Γ on it, in fact Γ acts on M, on $M^\star$, on $M^{\star p}$ too, and on $M^\star/M^{\star p}$, as well as on μ_p which is included in M; μ_p being the group of p-th roots of unity. So, $\Delta \simeq Hom\,(M^\star/M^{\star p}, \langle\zeta_p\rangle)$. $M^\star/M^{\star p}$ is known to be a vector space on $\mathbb{F}_p$ of dimension $2 + [M:K][K:\mathbb{Q}_p]$ then it is a finite p-elementary abelian group that is a vector space over $\mathbb{F}_p$ having the same dimension, thus $\#\Delta = p^{2+[M:K][K:\mathbb{Q}_p]} = p^{2+n}$ where $n = [M:K][K:\mathbb{Q}_p] = (p-1)^2 ef$ and Δ is p-elementary abelian having $2+n$ generators that is $\Delta = \langle\alpha_1, \alpha_2, \ldots, \alpha_{n+2}\rangle$.

Since $M^\star/M^{\star p}$ is a $\mathbb{F}_p[\Gamma]$-module of dimension $n+2$, we can assert that N can be generated over M by $n+2$ elements b_i such that $b_i^p \in M$, that

is $N = M(b_1, b_2, \ldots, b_{n+2})$, hence we can consider $\Delta = \langle \alpha_1, \alpha_2, \ldots, \alpha_{n+2} \rangle$ such that $\alpha_i(b_i) = \zeta_p^i b_i$, and $\alpha_i(b_j) = b_j$ if $i \neq j$, where ζ_p is a primitive p-th root of unity. To sum up we have the result:

Proposition 2.5. *When writing $N = M(b_1, b_2, \ldots, b_{n+2})$, with $b_i^p \in M$, the group $\Delta = gal(N/M) = \langle \alpha_1, \alpha_2, \ldots, \alpha_{n+2} \rangle$ can be defined by $\alpha_i(b_i) = \varepsilon^i b_i$ and $\alpha_i(b_j) = b_j$ if $i \neq j$, where ε is a primitive p-th root of unity.*

Here we need to construct the semi-direct product

$$(\mathbb{Z}/p\mathbb{Z})^n \rtimes_\phi (\mathbb{Z}/(p-1)\mathbb{Z})^2,$$

that is to write down a non-trivial homomorphism $\phi : (\mathbb{Z}/(p-1)\mathbb{Z})^2 \to Aut((\mathbb{Z}/p\mathbb{Z})^n)$. (The trivial homomorphism $\phi(g) = Id$, where Id is the identity automorphism of $(\mathbb{Z}/p\mathbb{Z})^n$, corresponds to the direct product). The group $Aut((\mathbb{Z}/p\mathbb{Z})^n)$ can be identified with the group $GL_n(\mathbb{Z}/p\mathbb{Z})$, the group of invertible n-dimensional matrices over $\mathbb{Z}/p\mathbb{Z}$. To write down a group homomorphism:

$$\phi : (\mathbb{Z}/(p-1)\mathbb{Z})^2 \to GL_n(\mathbb{Z}/p\mathbb{Z})$$

we just need to decide where the two standard generators, say g_1, g_2, of $(\mathbb{Z}/(p-1)\mathbb{Z})^2$ are sent, and the only constraints are that their images commute and they have order dividing $p-1$. Thus to describe all possible homomorphism φ we need to find all pairs of matrices A and B in $GL_n(\mathbb{Z}/p\mathbb{Z})$ such that $A^{p-1} = I_n$, $B^{p-1} = I_n$, where I_n is the identity matrix and $AB = BA$.

Note that two commuting matrices are simultaneously diagonalizable. It comes to pick up two elements of $GL_n(\mathbb{Z}/p\mathbb{Z})$ of order dividing $p-1$. Indeed since $p-1$ is co-prime to $p = char(\mathbb{Z}/p\mathbb{Z})$, then every element of $GL_n(\mathbb{Z}/p\mathbb{Z})$ of order $p-1$ is diagonalizable. Furthermore, a diagonal matrix is of order dividing $p-1$ if the diagonal entries belong to $(\mathbb{Z}/p\mathbb{Z})^\star$. It suffices to consider the element M of GL_n in the form $M = diag(d_1, d_2, \ldots, d_n)$; a diagonal matrix such that $d_i \in (\mathbb{Z}/p\mathbb{Z})^\star$. Such M exists and verifies the needed properties of order and commutativity. Then for such M consider the element f_M of $Aut((\mathbb{Z}/p\mathbb{Z})^2)$ the matrix of which is exactly M. Then write

$$(\mathbb{Z}/(p-1)\mathbb{Z})^2 = \langle g_1, g_2 \rangle$$

with g_1, g_2 of order $p-1$ and $(\mathbb{Z}/p\mathbb{Z})^n = \langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle$ with the α_i of order p. Therefore, we have a group homomorphism:

$$\begin{array}{rccc} \phi : & (\mathbb{Z}/(p-1)\mathbb{Z})^2 & \mapsto & Aut((\mathbb{Z}/p\mathbb{Z})^n) \\ & g_i & \mapsto & \phi(g_i) = f(g_i) = f_{M_i} \end{array}$$

for $i = 1$ or 2 with $M_i = diag(\zeta_{i1}, \zeta_{i2}, \ldots, \zeta_{in})$; a diagonal matrix. ζ_{ij} being elements of $(\mathbb{Z}/p\mathbb{Z})^\star$, M_1 and M_2 being the matrices associated to ϕ. Thus we can define the semi-direct product as

$$(\mathbb{Z}/p\mathbb{Z})^n \rtimes_\phi (\mathbb{Z}/(p-1)\mathbb{Z})^2 = \langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle \rtimes_\phi \langle g_1, g_2 \rangle$$

with $2n$ relations $g_i\alpha_j g_i^{-1} = \zeta_{ij}\alpha_j$. Clearly we have several different actions ϕ and then several different semi-direct products.

Note that by considering the dual $\hat{\Gamma}$ of Γ; $\hat{\Gamma} = Hom(\Gamma, \mathbb{F}_p^\star)$; the matrices M_1 and M_2 can be written as $M_i = diag(\chi_1(g_i), \chi_2(g_i), \ldots, \chi_n(g_i))$ where $\chi_j \in \hat{\Gamma}$, and then the $2n$ relations can be written as $g_i\alpha_j g_i^{-1} = \chi_j(g_i)\alpha_j$. So, we have proved the following result:

Proposition 2.6. $(\mathbb{Z}/p\mathbb{Z})^n \rtimes_\phi (\mathbb{Z}/(p-1)\mathbb{Z})^2 = \langle \alpha_1, \alpha_2, \ldots, \alpha_n\rangle \rtimes_\phi \langle g_1, g_2\rangle$ *with* $2n$ *relations* $g_i\alpha_j g_i^{-1} = \zeta_{ij}\alpha_j$ *for* $i = 1, 2$ *and* $j = 1, \ldots, n$. *That is* $g_i\alpha_j g_i^{-1} = \chi_j(g_i)\alpha_j$ *with* $\chi_j \in \hat{\Gamma}$.

Therefore, by the use of the Proposition 2.6, we get the result:

Proposition 2.7. *Let* $\mathcal{G} = \Delta \rtimes_\phi \Gamma = (\mathbb{Z}/p\mathbb{Z})^{n+2} \rtimes_\phi (\mathbb{Z}/(p-1)\mathbb{Z})^2$. *Write* $\mathcal{G} = \langle \alpha_1, \alpha_2, \ldots, \alpha_{n+2}\rangle \rtimes_\phi \langle \sigma, \tau\rangle$. *Then the semi-direct product is defined by the* $2(n+2)$ *relations:* $\sigma\alpha_i\sigma^{-1} = \zeta_i\alpha_i$, *and* $\tau\alpha_i\tau^{-1} = \xi_i\alpha_i$, *for* $i = 1, \ldots, n+2$; ζ, ξ *being elements of* $(\mathbb{Z}/p\mathbb{Z})^\star$.

That is by considering the dual $\hat{\Gamma} = Hom(\Gamma, \mathbb{F}_p^\star)$ *of* Γ; *and by writing the matrices* M_1 *and* M_2, *images of* σ *and* τ *by the action defining the semi-direct product, as follows:* $M_1 = diag(\chi_1(\sigma), \chi_2(\sigma), \ldots, \chi_{n+2}(\sigma))$, *and* $M_2 = diag(\chi_1(\tau), \chi_2(\tau), \ldots, \chi_{n+2}(\tau))$, *where* $\chi_i \in \hat{\Gamma}$, *the* $2(n+2)$ *relations can be written as:* $\sigma\alpha_i\sigma^{-1} = \chi_i(\sigma)\alpha_i$, *and* $\tau\alpha_i\tau^{-1} = \chi_i(\tau)\alpha_i$.

2.3. Uncountability of the product Δ for local functional fields.

Proposition 2.8. *Let* $K = \mathbb{F}((T))$, *where* $\mathbb{F}$ *is a finite field. Then* $\Delta = gal(N/M)$ *(where* $N = M(\wp^{-1}(M))$ *and* $M = K\big(\sqrt[p-1]{K^\star}\big)$*) is a sum of an uncountable number of copies of* $\mathbb{Z}/p\mathbb{Z}$.

Proof. $\mathbb{F}$ is a finite field. The group $M/\wp(M)$ is a direct sum of a non-necessarily countable number of copies of $\mathbb{Z}/p\mathbb{Z}$ (with $\wp : x \to x^p - x$). Furthermore, $M/\wp(M)$ is isomorphic to Δ. M/K is Kummer and abelian of degree $(p-1)^2$. We can write $M = V((X))$; $V((X))$ being the field of Laurent series, where $V = \mathbb{F}(\sqrt[p-1]{(\varepsilon)})$ where ε is a generator of the multiplicative group $\mathbb{F}^\star$ and $X = \sqrt[p-1]{T}$.

Let $\mathcal{M}_\mathcal{M}$ be the maximal ideal of M. Using Hensel's Lemma we can easily see that $\mathcal{M}_\mathcal{M} \subseteq \wp(M)$, (indeed by considering $b = -\sum_{i=0}^{\infty} a^{p^i}$, $b \in M$ and $b^p - b = a$). Then $M/\wp(M)$ is a quotient of $M/\mathcal{M}_\mathcal{M}$ which is a vector space of a countable dimension on $\mathbb{Z}/p\mathbb{Z}$. A base is given by all elements ζX^{-t}, where t are positive integers and ζ, ranging over a finite base of $\mathbb{F}$ over $\mathbb{Z}/p\mathbb{Z}$. Note that every element of $M/\mathcal{M}_\mathcal{M}$ is a finite linear combination of these elements. A countable product of copies of $\mathbb{Z}/p\mathbb{Z}$ will give infinite sums. Then Δ is necessarily an uncountable product of copies of $\mathbb{Z}/p\mathbb{Z}$, which ends the proof. □

3. The intermediate extension.

3.1. Some theorems on groups. P. Hall theorem (1928), see [6] Ch. 5, Th 5.23, page 85:

Theorem 3.1. *Let G be a solvable group of order nm where $(n, m) = 1$ then G contains at least one subgroup of order n and any such subgroups are conjugate.*

Lemma 3.2 (Galois, see for example [2], Ch. 3, Th. 7). *A transitive subgroup of $\mathfrak{S}_p$, the group of permutations of p elements, is solvable if and only if it contains a unique Sylow p-subgroup of order p.*

3.2. Existence of the intermediate extension.

Proposition 3.3. *Let K be any commutative field, for every separable extension L/K of degree p, where p is an odd prime number, such that $G = gal(L_C)/K$ the Galois group of the Galois closure of L/K is solvable. Then there exists a cyclic extension F/K of degree m dividing $p-1$ such that LF/F is cyclic of degree p and LF/K is Galois (i.e., $L_C = LF$).*

Furthermore, if L/K is not cyclic (LF/K is hence not abelian), then L has exactly p conjugates over K in LF.

Proof. Write G for the Galois group of its Galois closure. G is solvable, its order is divisible by p but not by p^2. Furthermore, it can be considered as transitive subgroup of the symmetric group $\mathfrak{S}_p$. According to Lemma 3.2 G contains a unique subgroup P of order p hence it is normal in G. P is contained in its normalizer $N(P)$ in $\mathfrak{S}_p$. Also $N(P)$ can be considered as the affine linear group $GA_1(\mathbb{F}_p)$, thus we have the isomorphism $\mathbb{F}_p^\star \to Aut(P)$, so we get a split short exact sequence:

$$1 \to P \to N(P) \to \mathbb{F}_p^\star \to 1.$$

Furthermore, $N(P)$ is isomorphic to the group of all 2×2 matrices over $GF(p)$ of the form $\begin{pmatrix} x & 0 \\ y & 1 \end{pmatrix}$. In consequence G/P is cyclic of order m dividing $p-1$. Therefore, and since $G \subset N(P)$, it is also a semi-direct product $G = P \rtimes M$ with M cyclic of order m. If the semi-direct product is a direct product, then it is cyclic since m and p are co-prime.

Otherwise G is not abelian. In such case since M is cyclic, all its conjugates are cyclic too. Write m in the form $m = \prod_{i=1}^{r} m_i^{\alpha_i}$, where m_i are different prime numbers, and N for the number of the conjugates of M (note that according to Hall's theorem (Theorem 3.1) all the subgroups of G of order m are conjugate). Since M is cyclic, it contains one and only one subgroup M_i of order $m_i^{\alpha_i}$ (Sylow m_i-subgroup of G) which is cyclic too. Conversely every Sylow m_i-subgroup of G can be embedded in some conjugate of M. Therefore, the number N must divide mp, being $N \equiv 1$ modulo m_i for every i, thus $(N, m) = 1$. In consequence the number of

conjugates of M is exactly p if G is not cyclic. Set F the field fixed by P, then the Galois closure of L/K is $L_C = LF$. This ends the proof. □

3.3. Intermediate extension, explicit determination. *We assume that K is a local field with a finite residue field of characteristic p.*

As seen before, the compact group Γ is $\Gamma \simeq Hom(K^\star/K^{\star p-1}, \mu_{p-1})$, then by duality $\Gamma \simeq K^\star/K^{\star p-1}$. Hence the exponent of Γ is just equal to $p-1$, and M/K is Kummer abelian extension relatively to the number $p-1$, and then the intermediate subextension F/K announced in Proposition 3.3 is cyclic Kummer.

3.4. Description of the Galois groups. Since F/K is Kummer, $F = K(\sqrt[m]{c})$, with $c \in K^\star$, $K^\star$ being the multiplicative group of nonzero elements of K. Furthermore, $K(\sqrt[m]{c}) = K\big(\sqrt[m]{d}\big)$ if and only if there exists an integer $k \geq 1$ with $(k, m) = 1$ such that $d \in c^k K^{\star m}$. By considering the quotient group $K^\star/K^{\star m}$, the order of the class $cK^{\star m}$ in it is m.

Since m divides $p-1$, $K^\star/K^{\star m} \approx (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$; therefore $K^\star/K^{\star m}$ is of order m^2. The number of the distinct Kummer cyclic extensions of K of degree m is exactly the number of cyclic subgroups of order m in $(K^\star/K^{\star m})$.

So it is easy to deduce that the number of the cyclic distinct Kummer extensions of K of degree m equals the number of the cyclic subgroups of order m included in $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, so by writing $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, we get that this number equals

$$\big(p_1^{\alpha_1} + p_1^{\alpha_1 - 1}\big) \dots \big(p_r^{\alpha_r} + p_r^{\alpha_r - 1}\big).$$

Furthermore, $gal\,(F/K) \approx H$, a cyclic group of order m dividing $p-1$ that can be embedded in μ_{p-1}, the group of the $(p-1)$-th roots of unity, and by considering the Galois closure L_C of L/K, $gal\,(L_C/K) \approx gal\,(L_C/F) \rtimes H$, (a semi-direct product). Then from local class field theory, see for example [3], we have the isomorphism between the three groups $gal\,(F/K) \approx H \approx K^\star/N_{F/K}\,(F^\star)$ of order m, and the surjective homomorphism

$$s : K^\star/K^{\star m} \approx (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \mapsto K^\star/N_{F/K}\,(F^\star)\,.$$

The group $gal\,(LF/K)$. Since $gal\,(F/K)$ is cyclic of order m dividing $p-1$, write $gal(F/K) =< \epsilon >$ with $\epsilon(\sqrt[m]{c}) = \xi_m(\sqrt[m]{c})$, where ξ_m a primitive m-th root of unity and name the extension of ϵ to $F(\pi)$ by ϵ too. Since $gal(F(\pi)/F)$ is cyclic of order p write $gal(F(\pi)/F) =< \sigma >$. LF/K is Galois, consider any element τ of $gal(LF/K)$, thus $\tau = \sigma^i \epsilon^j$, with $1 \leq i \leq p$ and $1 \leq j \leq m$, then from the normality of $< \sigma >$ in $gal(LF/K)$, we have the identity $\tau\sigma\tau^{-1} = \sigma^t$ with $1 \leq t \leq p-1$.

Consider the affine group $AGL\,(1, p)$, that is the set of all maps from $\mathbb{F}_p$ to itself of the form $x \mapsto ax + b$ where $a \neq 0$ in $\mathbb{F}_p$. $gal\,(LF/K)$ has order mp and is isomorphic to a subgroup of $AGL\,(1, p)$, which is isomorphic to the subgroup $GL_2\,(\mathbb{Z}/p\mathbb{Z})$, consisting of the matrices of the form

$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, where an automorphism δ corresponds to the matrix $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ when $\delta(\xi_p) = \xi_p^a$, and $\delta(x) = \xi_p^b x$ where ξ_p, is a primitive p-th root of unity. That is by picking a generator g of $(\mathbb{Z}/p\mathbb{Z})^\star$, we can use for a generator of $gal(F/K)$, $\epsilon : x \mapsto gx$ that corresponds to the matrix $\begin{pmatrix} g & 0 \\ 0 & 1 \end{pmatrix}$ and for a generator σ of $gal(LF/F)$, $\sigma : x \mapsto x+1$ that corresponds to the matrix $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ then $\epsilon\sigma\epsilon^{-1} = \sigma^g$.

For any element τ of $gal(LF/K)$ we have $\tau = \sigma^i\epsilon^j$, with $1 \leq i \leq p$ and $1 \leq j \leq m$, $\tau\sigma\tau^{-1} = \sigma^{g^j}$, also g must verify $g^m = 1$ in $\mathbb{F}_p$.

The group $(\mathbb{Z}/p\mathbb{Z})^\star$ has $\varphi(m)$ elements of order m, where $\varphi(\cdot)$ is the Euler's totient (indicator). Meanwhile the equation $x^m = 1$ modulo p has exactly m solutions in $(\mathbb{Z}/p\mathbb{Z})^\star$, since m divides $p-1$ which is the order of $(\mathbb{Z}/p\mathbb{Z})^\star$, these solutions are the elements of the cyclic subgroup of order m of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\star$, and is obviously isomorphic to the group of the m-th roots of unity.

On the other hand $\frac{\tau(c)}{c} = 1$ so $\frac{\tau(\sqrt[m]{c})}{\sqrt[m]{c}} = \xi_m^\beta$. Note that ξ_m^β does not depend on c but on the coclass $cK^{\star m}$ only. Indeed $\frac{\tau(\sqrt[m]{c})}{\sqrt[m]{c}} = \frac{\tau(\sqrt[m]{d})}{\sqrt[m]{d}}$ if and only if $\tau\left(\sqrt[m]{\frac{c}{d}}\right) = \sqrt[m]{\frac{c}{d}}$, that is $\frac{c}{d} \in K^{\star m}$. Now consider $\theta = \sigma(\pi) - \pi$ so $\theta \equiv 0$ modulo π^{v+1}. Set $\pi_1 = \tau(\pi)$ which is uniformizer too, since LF/F is normal and totally ramified, then $v_{LF/F}(\sigma(\pi) - \pi) = v_{LF/F}(\sigma(\pi_1) - \pi_1) > 0$ and integer v is the ramification number (= break=jump) of LF/F.

We can write $\sigma(\pi_1) - \pi_1 = u(\sigma(\pi) - \pi) = u\theta$ where u is the unit of LF. Note that $u \equiv 1 \mod \pi$, as $\sigma(\tau(\pi) - \pi) \equiv \tau(\pi) - \pi \mod \pi$, therefore it is worthy to note that the class of $\frac{\tau(\theta)}{\theta}$ modulo π is independent of π and depends on τ and σ only.

Then write $\theta = \sigma\tau^{-1}(\pi_1) - \tau^{-1}(\pi_1)$, that is $\tau(\theta) = \tau\sigma\tau^{-1}(\pi_1) - \pi_1$. Now, since $gal(LF/F) =< \sigma >$ is a normal subgroup of $gal(LF/K)$ which is not abelian we have $\tau\sigma\tau^{-1} = \sigma^a$, with $1 \leq a \leq p-1$, therefore $\tau(\theta) = (\sigma^a(\pi_1) - \pi_1)$. Since the equality between ideals $\sigma\left((\pi^t)\right) = (\pi^t)$ holds, by successive substitutions we get $\sigma^a(\pi_1) - \pi_1 \equiv a(\sigma(\pi_1) - \pi_1) \equiv a(\sigma(\pi) - \pi)$ modulo π^{v+2}, that is $\tau(\theta) \equiv a\theta$ modulo π^{v+2} for $1 \leq a \leq p-1$, finally we get $\frac{\tau(\theta)}{\theta} \equiv a \mod \pi^{v+1}$, that is modulo p for $1 \leq a \leq p-1$.

Now, we can take $c = N_{L/K}(\gamma) = N_{LF/F}(\gamma)$ where $\gamma = -ka_k\pi^{k-1}$ and a_k is the coefficient of f (the minimal polynomial of π over K that is over F too) such that k is the index t that achieves the minimum in the expression $\inf_{1\leq t\leq p}(v_L(ta_t) + t)$ (for more details on this method see [4] §.3.2, the proof of Proposition 3.1). Furthermore, we have $\sqrt[p-1]{\gamma} \equiv \theta \mod \pi \Rightarrow$

$N_{LF/F}(\sqrt[p-1]{\gamma}) \equiv N_{LF/F}(\theta) \equiv \theta^p \equiv \theta \mod \pi$, then we immediately get: $\frac{\tau\left(N_{LF/F}(\sqrt[p-1]{\gamma})\right)}{N_{LF/F}(\sqrt[p-1]{\gamma})} \equiv a \mod \pi^{v+1}$, that is modulo p for $1 \leq a \leq p-1$.

Therefore, we have proved the following result:

Theorem 3.4. *Let p be an odd prime number and K be a local field with $char(K) \equiv 0$ modulo p having a finite residue field. Consider any separable extension L/K of degree p.*

Then there exists $c \in K^\star$, unique up to $K^{\star(p-1)}$, such that the following holds:

- *$L(\sqrt[p-1]{c})$ is the Galois closure of L/K.*
- *For every $\tau \in gal\left(L(\sqrt[p-1]{c})\right)/K$, and $\sigma \in gal\left(L(\sqrt[p-1]{c})/K(\sqrt[p-1]{c})\right)$, we have $\tau\sigma\tau^{-1} = \sigma^a$, with $a = \frac{\tau\left(\sqrt[p-1]{c}\right)}{\sqrt[p-1]{c}}$ modulo p.*

In other words we have an explicit determination of the intermediate subextension announced in Proposition 3.3, namely $F = K(\sqrt[p-1]{c})$.

Note. Even if the decomposition of the Galois closure and the justification of the existence of the intermediate extension do not require the completion of the base field, the following description of the Galois groups and the intermediate extension require the completion of the base field and the finitude of the residue field obligatory. Indeed, $M = K(\sqrt[p-1]{K^\star})/K$ is not necessarily of degree $(p-1)^2$, much more it can be infinite as seen before. Furthermore the splitting field can be solvable much more cyclic over a local field and not solvable over a non-local field, see the following Example.

Example (Counter-example). Consider $f(X) = X^3 + 3X^2 + 24$ as a polynomial of $\mathbb{Q}_3[X]$ with $f(\alpha) = 0$. It is Eisenstein polynomial, and it defines a normal extension $\mathbb{Q}_3(\alpha)$ of $\mathbb{Q}_3$, see [4].

Meanwhile, when considering f as polynomial of $\mathbb{Q}[X]$, in spite of the fact that $\mathbb{Q}$ contains the $(p-1)$-th roots of unity for $p = 3$ and the Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$ is certainly solvable, the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not normal since the equation possesses complex roots.

4. On solvability in the general case. This section adjusts the focus on some general properties concerning local fields, especially the solvability of local finite extensions.

In case of local fields with finite residue fields the solvability can be easily proved. Meanwhile, in the general case, that is when the residue field is infinite, the problem is much more difficult, especially when it is not necessarily perfect, indeed we can have nonsolvable finite local extensions.

4.1. Sketch of the classical ramification. Let L/K be a finite Galois extension of local fields. In this paragraph especially, the residue fields are assumed to be perfect. In this case we can easily define two canonical filtrations (G_i) (the lower ramification groups) and (G^i) (the upper ramification

groups) in G that are decreasing sequences of subgroups of G. The i-th lower ramification group is defined to be

$$G_i = \{\sigma \in G; w(\sigma(\alpha) - \alpha) \geq i + 1 \text{ for all } \alpha \in \mathcal{R}_L\},$$

where $\mathcal{R}_L$ is the ring of the discrete valuation w.

The two filtrations of ramification subgroups are related by the formula $G^i = G_\psi(i)$, where ψ is the Hasse–Herbrand function used to be calculated in terms of orders of G_i. The said filtrations are compatible with the subextensions in L/K. In the sense that, if H is a normal subgroup of G, we can get the filtrations relative to H by taking $H_i = G_i \cap H$ and $(G/H)^i = (G^i H)/H$ (see [7], Ch. IV). Furthermore, if L/K is abelian when the residue fields is quasi-finite, the "upper" filtration of G is compatible with the reciprocity map $\theta : K^\star \to G$ in the sense that $\theta(U_i) = G^i$ for all $i = 0, 1, \ldots, n$, and (U_i) is the filtration of the units group in $K^\star$. The compatibility of the "upper" filtration of G with the class field theory is studied in [7], Ch. XV.

Consequently, in case of local fields with perfect residue fields, the solvability of G_0, the inertia subgroup of G is ensured, since the quotient of any two successive lower ramification groups is abelian. In fact it is either cyclic or a direct sum of groups of order p. Meanwhile, the solvability of G itself requires the finiteness of the residue field (see for example [7], Corollary 5 of §.2, Ch. IV page 68). Note that in this reference the residue field is not assumed to be perfect but it is assumed that the residue extension is separable only.

From now on, let K be a local field (that is a complete field with respect to a discrete valuation) having a non-necessarily perfect residue field k.

4.2. General case (imperfect residue field). First note that in the general case, a theory of upper numbering of ramification subgroups corresponding to a theory of the "lower" ramification subgroups by use of some means like the Hasse–Herbrand φ, ψ functions does not exist.

All that has been done till now is a "lower" ramification theory which is obtained from the double-filtration given in [8], see paragraph §.4.4 that comes. However, the ramification filtration in the group G does not determine that in H, for a normal subgroup H of G. In fact we do not have in this case a formula similar as in the separable case, (see [7], Ch. 4 §.1 Proposition 2). Indeed, for a finite Galois extension L/K of local fields, the discrete valuation ring $\mathcal{R}_L$ of L may not be generated by only one element over $\mathcal{R}_K$, when we are in the inseparable case in contrary to the separable case.

Moreover, recently for a theory of the upper numbering filtration, Abbes and Saito made a different interpretation that can be generalized in the general situation, giving rise to a quite well-behaved upper-number filtration.

To sum up, they define two decreasing filtrations by ramification groups on the absolute Galois group (the Galois group of the separable closure)

such that in the classical case where the residue field is perfect, we recover the classical upper numbering filtration. The definition uses rigid geometry and log-structures, see [1].

4.3. Description of the extension. Let K be any local field (i.e., a complete field with respect to a discrete valuation, the residue class field is imperfect), and let L/K be a finite Galois extension. Write $G = gal(L/K)$ for its Galois group. The discrete valuation ring of L is denoted by $\mathcal{R}_L$ and its maximal ideal by $\mathcal{M}_L$. In such case the degree of L/K splits in such a way $[L : K] = ef = e_{tame}e_{wild}f_{sep}f_{insep}$, ($e_{wild}$ and f_{insep} must be a power of p, e_{tame} is prime to p, meanwhile f_{sep} need not be necessarily prime to p).

Since L/K is a Galois extension, we get that the residue extension l/k is normal (see for example [7], Ch. 1, §.7, Proposition 20), but it need not be separable. Consider the set D of all automorphisms of l unvarying all elements of k, there is a natural surjective homomorphism from $\varphi : G \to D$. Indeed, let $g \in G$, g preserves $\mathcal{R}_L$ as well as $\mathcal{M}_L$. Therefore, g induces an automorphism of $l = \mathcal{R}_L/\mathcal{M}_L$. Since g fixes each element of K, it fixes each element of k as well, the surjectivity of φ is proved in the proposition referred above.

4.4. A filtration of the inertia group. The inertia group G_0 is given by $G_0 = \{\sigma \in G; \forall x \in \mathcal{R}_L, (x - \sigma(x)) \in \mathcal{M}_L\}$.

Let L_0 be the fixed field of G_0 that is the inertia field of L/K and the maximal subfield of L that is unramified over K. The residue class field l_0 of L_0 is the separable closure of k in l (the residue fields) hence l_0/k is Galois and its degree is f_{sep}, which is the order of $G/G_0 \simeq gal(l_0/k)$.

As it is usually done in this case when the residue class field is imperfect, for any positive integer $i \geq -1$ we define a filtration of the inertia group G_0 obtained from the double-filtration given in [8], where the authors consider a doubly indexed filtration $(G_{n,i})_{n,i\in\mathbb{N}}$ of the Galois group, from which a lower ramification filtration that generalizes the last one in the classical case (see for example [7]) can be deduced.

Namely $G_{n,i} = \{\sigma \in G; \forall x \in \mathcal{M}_L^i, (x - \sigma(x)) \in \mathcal{M}_L^{i+n}\}$, that is the subgroup of G consisting of the K-automorphisms of L that induce the identity on $\mathcal{M}_L^i/\mathcal{M}_L^{i+n}$. Whereas the classical lower ramification filtration is obtained by considering the sequence of the groups $G_{n+1,0}$.

So, we define $G_i = \{\sigma \in G; (\pi - \sigma(\pi)) \in \mathcal{M}_L^{i+1}\}$ for π an arbitrary but fixed prime element of L (in the definition of G_i, G can be replaced by G_0 since clearly $G_i \subseteq G_0$ for $i \geq 0$), that is the subgroup of G consisting of the K-automorphisms of L that act trivially on $\mathcal{R}_L/\mathcal{M}_L^{i+1}$.

By the way, $G = G_{-1}$ since σ satisfies $\sigma(\mathcal{R}_L) = \mathcal{R}_L$, $\sigma(\mathcal{M}_L) = \mathcal{M}_L$ and particularly $\sigma(\pi)$ is a prime element for any $\sigma \in G$. Then likewise for the classical case we have the filtration $G = G_{-1} \supseteq G_0 \supseteq G_1 \cdots \supseteq G_i \ldots$, with the existence of an integer r such that $G_i = \{1\}$ for $i \geq r$, since $\mathcal{R}_L \simeq \varprojlim \mathcal{R}_L/\mathcal{M}_L^i$.

4.5. Results. Then we have the result:

Proposition 4.1. *Let L/K be a finite Galois extension of local fields with imperfect residue class fields. Denote by G_0 the inertia group of $gal(L/K)$. Then G_0 is solvable, furthermore it is cyclic in characteristic zero case.*

Proof. First for any positive integer $i \geq 1$, let $\sigma \in G_i$. An uniformizer π of L being fixed we have $(\sigma(\pi) - \pi) \in \mathcal{M}_L^{i+1}$ hence $\pi - \sigma^{-1}(\pi) \in \sigma^{-1}(\mathcal{M}_L^{i+1})$, that is $\sigma^{-1} \in G_i$ so G_i is a subgroup of G. Furthermore, let $\sigma, \tau \in G_i$. Then $(\sigma\tau(\pi) - \pi) = \sigma(\tau(\pi) - \pi) + \sigma(\pi) - \pi \in \mathcal{M}_L^{i+1}$, i.e., $\sigma\tau \in G_i$, that is G_i is normal G. So, the above definition is well justified.

Now, let us fix a set of generators of the residue field extension and their lifts $u_1, \ldots, u_n$ to $\mathcal{R}_L$. Put it another way, $\mathcal{R}_L$ is generated by $\pi, u_1, \ldots, u_n$ as an $\mathcal{R}_K$-algebra, where π has valuation 1, and u_i are units.

Consider the map:

$$G \to k^\star,$$
$$g \mapsto \overline{g(\pi)/\pi}.$$

It is clear that this is a homomorphism, and G_1 is the kernel of this map. Then again consider the map:

$$G_1 \to k \oplus k \oplus \cdots \oplus k; \ \ (n+1 \text{ of them}),$$
$$g \mapsto (\overline{(g(\pi) - \pi)/\pi^2}, \overline{(g(u_1) - u_1)/\pi}, \ldots, \overline{(g(u_n) - u_n)/\pi}),$$

where $\overline{(g(\alpha) - \alpha)/\pi^i}$ is the residue class of $(g(\alpha) - \alpha)/\pi^i$ mod π, that is also a homomorphism, and G_2 is the kernel. Then we continue to consider:

$$G_2 \to k \oplus k \oplus \cdots \oplus k; \ \ (n+1 \text{ of them}),$$
$$g \mapsto (\overline{(g(\pi) - \pi)/\pi^3}, \overline{(g(u_1) - u_1)/\pi^2}, \ldots, \overline{(g(u_n) - u_n)/\pi^2}),$$

and so on and so forth, till we get a trivial G_r.

From this, in case of the residue fields having characteristic $p > 0$, it is clear that G_1 has a filtration by normal subgroups G_i where the subquotients G_i/G_{i+1} are p-elementary abelian groups as G_i/G_{i+1} injectively maps to $(1 + \mathcal{M}_L^i)/(1 + \mathcal{M}_L^{i+1})$ which is canonically isomorphic to $(l, +)$ for $i \geq 1$.

Furthermore, G_0/G_1 is cyclic of order prime to p as it injectively maps to $\mathcal{R}_L^\star/(1 + \mathcal{M}_L) \simeq (l^\star, \times)$, as well as to $Aut_l(\mathcal{M}_L/\mathcal{M}_L^2) \simeq (l^\star, \times)$, and the field l is of characteristic p. It is worthy to note that the maximal tamely ramified subfield T of L corresponds to the group $G_T = G_0 \cap G_1 = G_1$. Finally, G_1 is a p-group of order $e_{wild} f_{insep}$, therefore its solvability implies the last one of G_0.

In case the residue fields are of characteristic zero, since for $i \geq 1$ the subquotients G_i/G_{i+1} are isomorphic to a subgroup of $(l, +)$, considered as an additive group. $(l, +)$ has no finite subgroup except $\{0\}$, therefore G_i are trivial for all $i \geq 1$, in consequence G_0 is cyclic, $e_{wild} = 1$ and necessarily p does not divide e which ends the proof. $\square$

Note. The result of the solvability of the inertia group can be deduced from the work of I. B. Zhukov in [9] but not for the general case. Indeed, he added the strong hypothesis that $[k : k^p] = p$, where k is the residue field, that this K is particularly assumed to be a two-dimensional local field.

Proposition 4.2. *Let K be a local field, and let L/K be a finite Galois extension. Then L/K is solvable if and only if the maximal separable subextension of l/k is solvable.*

Proof. Consider $G = gal(L/K)$, and its inertia group G_0. By use of the current notations the isomorphism induced by the surjective homomorphism φ defined above makes G/G_0 isomorphic to the Galois group of the maximal separable subextension of l/k which equals D. From Proposition 4.1, G_0 is solvable, so the well-known result of classical group theory: G is solvable if and only if both G/G_0 and G_0 are solvable, ends the proof.

Thus L/K is solvable if and only if the Galois group of the maximal separable subextension of l/k is solvable. □

Acknowledgment. I heartily want to thank Professor I. Fesenko from Nottingham University (UK) for having read and approved the proof of Proposition 4.1.

References

[1] Abbes, A., Saito, T., *Ramification of local fields with imperfect residue fields*, Amer. J. Math. **124** (5) (2002), 879–920.
[2] Artin, E., *Galois Theory*, Univ. of Notre Dame Press, Notre Dame, 1942.
[3] Hazewinkel, M., *Local class field theory is easy*, Adv. Math. **18** (1975), 148–181.
[4] Lbekkouri, A., *On the construction of normal wildly ramified over Q_p, ($p \neq 2$)*, Arch. Math. (Basel) **93** (2009), 331–344.
[5] Ribes, L., Zalesskii, P., *Profinite Groups*, Springer-Verlag, Berlin, 2000.
[6] Rotman, J. J., *An Introduction to the Theory of Group*, Springer-Verlag, New York, 1995.
[7] Serre, J.-P., *Local Fields*, Springer-Verlag, New York–Berlin, 1979.
[8] Zariski, O., Samuel, P., *Commutative Algebra. Volume II*, Springer-Verlag, New York–Heidelberg, 1975.
[9] Zhukov, I. B., *On ramification theory in the imperfect residue field case*, Preprint No. 98-02, Nottingham Univ., 1998. Proceedings of the conference: Ramification Theory of Arithmetic Schemes (Luminy, 1999) (ed. B. Erez), http://family239.narod.ru/math/publ.htm.

Akram Lbekkouri
BP: 10507
Casa-Bandoeng 20002
Casablanca
Morocco
e-mail: lbeka11@gmail.com

Received August 11, 2012