An. Şt. Univ. Ovidius Constanţa Vol. 9(2), 2001, 69–86

TAMELY RAMIFIED EXTENSION'S STRUCTURE

Denis Ibadula

Dedicated to Professor Mirela Ştefănescu on the occasion of her 60th birthday

Abstract

The structure of an algebraic tamely ramified extension of a henselian valued field is studied. We will prove, in theorem 3.2, the following statement: *A finite extension L/K is tamely ramified if and only if the field L is obtained from the maximal unramified extension T by adjoining the radicals* $\sqrt[m]{t}$, with $t \in T, m \in \mathbb{N}, \quad m \geq 1, \quad (m,p) = 1,$ *where p is the characteristic of the residue class field .*

At the end of the paper some examples are presented.

1. Preliminaries

In this paper we fix a base valued field $K = (K, v)$ which is henselian with respect to a nonarchimedean valuation v. We denote the valuation ring, the maximal ideal and the residue class field by $O_K, \underline{m}_K, \overline{K}$ respectively. If L/K is an algebraic extension, the valuation v extend uniquely to a valuation on L, denoted v too. The corresponding invariants are labelled $O_L, \underline{m}_L, \overline{L}$ respectively.

Definition 1.1. Let L/K be a finite extension of valued fields.
$e := e(L/K) := (vL : vK)$ is called the **ramification index**.
$f := f(L/K) := [\overline{L} : \overline{K}]$ is called the **inertia degree**.

Definition 1.2. An extension of valued fields L/K is called **immediate** if $e(L/K) = f(L/K) = 1$ (i.e. $vK = vL$ and $\overline{L} = \overline{K}$).

Received: June, 2001

Definition 1.3. A finite extension L/K of valued fields is called **defectless** if $[L : K] = e(L/K) \cdot f(L/K)$. An extension L/K (not necessary finite) of valued fields is called **defectless** if each finite subextension of L is defectless.

2. Unramified Extensions

A particularly important role in theory of valued fields is played by the unramified extensions, which are defined as follows.

Definition 2.1. A finite extension L/K of valued fields is called **unramified** if the extension $\overline{L}/\overline{K}$ of the residue class fields is separable and one has

$$[L : K] = [\overline{L} : \overline{K}].$$

An arbitrary algebraic extension L/K is called **unramified** if any finite subextension F of L/K is unramified.

We are presenting now, without proofs, a few results concerning the unramified extension.

Proposition 2.2. *Let L/K and $K^{'}/K$ be two algebraic extensions of the same valued henselian field K and let $L^{'} = LK^{'}$. If L/K is unramified, then $L^{'}/K^{'}$ is unramified too. Each subextension of an unramified extension is unramified.*□

Corollary 2.3. *The composite of two unramified extensions of K is again unramified.* □

Definition 2.4. Let L/K be an algebraic extension. The composite T/K of all unramified subextensions is called the **maximal unramified subextension of L/K .**

Proposition 2.5. *The residue class field of T, denoted $\overline{T}$,is the separable closure of $\bar{K}$ in the residue class field extension $\overline{L}/\overline{K}$ of L/K, whereas the value group of T equals that of K (i.e. $vT = vK$).*□

3. Tamely Ramified Extensions

If the characteristic $p = char(\overline{K})$ of the residue class field is positive, then one has the following weaker notion accompanying that of an unramified extension.

Definition 3.1. An algebraic extension L/K is called **tamely ramified** if the extension $\overline{L}/\overline{K}$ of the residue class field is separable and one has $([L : T], p) = 1$, where p is the characteristic of $\overline{K}$ and T denotes the maximal unramified extension of L/K.

In the infinite case this latter condition is taken to mean that the degree of each finite subextension of L/T is prime to p.

Theorem 3.2. (The structure theorem of the tamely ramified extensions). *Let L/K be an algebraic extension. Then L/K is tamely ramified if and only if the extension L/T is generated by radicals:*

$$L = T(\alpha \in L | \exists m \geq 1,\, \alpha^m \in T, (m,p) = 1\},$$

where p is the characteristic of $\overline{K}$ and T is the maximal unramified extension of L/K.

Moreover, if L/K is tamely ramified,then L/K is defectless.

Proof. Before we start proving the theorem, we must make a few remarks. We may reduce the problem to a finite extension L/K because, if L/K is an arbitrary algebraic extension, we may represent L as an filtrated inductive limit of his finite subextensions. We may also assume that $K = T$ because L/K is obviously tamely ramified if and only if L/T is tamely ramified.

Let's prove the necessity: we suppose that L/K is tamely ramified. Let $L' := T(t(L/K)^{(p')})$, where

$$t(L/K) := \{x \in L^\times | \exists m \geq 1 \text{ such that } x^m \in K\}$$

contains the elements of L, which are radicals over K. We consider now a subgroup of this set:

$$t(L/K)^{(p')} := \{x \in L^\times | \exists m \geq 1,\ (m,p) = 1 \text{ such that } x^m \in K\}.$$

The results obtained may be summarized in the following picture:

$$\begin{aligned} K &= T \subseteq L' := T(t(L/K)^{(p')}) \subseteq L \\ \overline{K} &= \overline{T} = \overline{L'} = \overline{L} \\ vK &= vT \subseteq vL' \subseteq vL. \end{aligned}$$

To justify that $L = L'$, which proves the first implication, we will use a few lemmata.

Lemma 3.3. *Let L/K be an immediate and tamely ramified extension. Then one has $L = K$.*

Lemma 3.4. *Let L/K be an immediate and tamely ramified extension and let T be the maximal unramified extension of L/K. Then the composite*

$$t(L/K)^{(p')} \to vL \twoheadrightarrow \frac{vL}{vK}$$

$$x \longmapsto vx \longmapsto vx \bmod vK$$

induces a group isomorphism $t(L/K)^{(p')}/T^{\times} \tilde{\to} vL/vK = vL/vT$.

First of all, let's see how we apply this two lemmata to prove that $L = L'$. In accordance with lemma 3.3., we have to show that the extension L/L' is tamely ramified and immediate. Because the degree of extension $[L : T(L/L')]$ (where $T(L/L')$ is the maximal unramified extension of L/L') divides $[L : T]$, which is prime with p, we have $([L : T(L/L')], p) = 1$. Since the residue class field extension is trivial ($\overline{L} = \overline{L'}$), we conclude that $L/L'$is tamely ramified.

We have to show now that L/L' is immediate, which means $\overline{L} = \overline{L'}$ and $vL = vL'$. As L/K is tamely ramified, the extension $\overline{L}/\overline{K}$ is separable and, by proposition 2.5, we have $\overline{L} = \overline{T} = \overline{K}$, so that $\overline{L} = \overline{L'}$. Let's prove now that $vL = vL'$. Because it is obvious that $vL' \subseteq vL$, we will show that $vL \subseteq vL'$, which will result from the surjectivity of the homomorphism from lemma 3.4.

Let $\gamma \in vL$. The surjectivity of the homomorphism from lemma 3.4 implies that there exists $a \in t(L/K)^{(p')}$ such that $v(a) \equiv \gamma (\bmod vK)$,i.e. $v(a) = \gamma + v(b)$, $b \in K$. We have $\gamma = v(ab^{-1})$,where $ab^{-1} \in t(L/K)^{(p')}$,so that $\gamma \in v(t(L/K)^{(p')})$, which shows that $vL \subseteq v(t(L/K)^{(p')})$. As $vL' \subseteq vL \subseteq v(t(L/K)^{(p')}) \subseteq vL'$, we may conclude that $vL' = vL$, which implies that L/L' is an immediate extension, so that $L = L'$.

We have now to justify the two lemmata which will prove this first implication.

Proof (of lemma 3.3). Let's first remark that L/K is a separable extension. Let now $m := [L : K]$, with $(m, p) = 1$, and $Hom_K(L, \tilde{K}) = \{\sigma_1, ..., \sigma_m\}$,where $\tilde{K}$ is an algebraic closure of K. The additive homomorphism

$$\begin{array}{rcl} Tr & : & L \to K \\ x & \longmapsto & Tr(x) := \sum_{i=1}^{m} \sigma_i(x) \end{array}$$

induces the additive homomorphism

$$\begin{array}{rcl} \overline{Tr} & : & \overline{L} = \overline{K} \to \overline{K} \\ \overline{x} & \longmapsto & \overline{Tr}(\overline{x}) := \overline{Tr(x)} \end{array}$$

Let us show $\overline{Tr(x)} = m\overline{x}$. Let $\overline{x} \equiv x (\mathrm{mod}\, \underline{m}_L) \in \overline{L}, x \in O_{L.}$ As $\overline{K} = \overline{L}$, there exists $a \in O_K$ such that $\overline{x} = \overline{a}$, which means $x - a \in \underline{m}_L$. Let $x - a = b$, with $b \in \underline{m}_L$. We have $Tr(x) = Tr(a) + Tr(b) = \sum_{i=1}^{m} \sigma_i(a) + Tr(b)$, so that $\overline{Tr}(\overline{x}) = \overline{Tr(x)} = m \cdot \overline{a} = m \cdot \overline{x}$. Since $(m, p) = 1$, the additive homomorphism $\overline{Tr}$ is injective.

We have to show now that $L = K$. Suppose that there exists an element $a \in L \setminus K$. As $vL^\times = vK^\times$, we may choose $b \in K^\times$ such that $va = vb$ and obtain the unit $u := a/b \in O_L^\times$. Because $a - \frac{1}{m}Tr(a) \in L \setminus K$ has the trace zero, we may assume that $a \in L \setminus K$ and $Tr(a) = 0$. The unit $u \in O_L^\times$ has the trace $Tr(u) = \frac{0}{b} = 0$. Hence $\overline{Tr}(\overline{u}) = \overline{Tr(u)} = \overline{0}$, and thus $m \cdot \overline{u} = \overline{0}$, $m \equiv 0 (\mathrm{mod}\, p)$, which contradicts $(m, p) = 1$. $\square$

Proof (of lemma 3.4). Let's show first that the composite homomorphism has the kernel equal to $T^\times$. Assume that x is an element from the kernel, $x = a \cdot u$, with $a \in K^\times$ and $u \in O_L^\times$ such that there exists $m \geq 1$ with $x^m = b, b \in K, (m, p) = 1$. Since $x^m = b = a^m u^m$, we may denote $u^m = c$, for some c in K. We have to prove now $u \in K^\times$,which implies immediately $x \in K^\times$. As $\overline{L} = \overline{K}$, we may write $u = d \cdot u^{'}$, where $d \in O_K^\times$ and u' is a unit in $O_L^\times$, $\overline{u'} = \overline{1} \equiv 1 (\mathrm{mod}\, \underline{m}_L)$. Since $u^{'m} = \frac{u^m}{d^m} = \frac{c}{d^m}$, with $\overline{u'} = \overline{1}$,we may assume that $u \in O_L^\times$ and $\overline{u} = \overline{1}$. By Hensel's lemma the equation $x^m - c = 0$ has a solution $\alpha \in O_K$ such that $\overline{\alpha} = \overline{1}$. Moreover, since $u\alpha^{-1}$ is a root of unity of order m, $(m, p) = 1$, we have $u\alpha^{-1} \in T = K$, which implies $u \in K$ and $x \in K$. Because the other implication is trivial, we obtain that the homomorphism has the kernel equal to $T^{\times}$.

We want to check now the surjectivity of the homomorphism

$$\begin{array}{rcl} t(L/K)^{(p')} & \longrightarrow & vL \\ x & \longmapsto & vx \end{array}$$

which will end the proof.

Let $\alpha \in vL$, $\alpha = v(a), a \in L$. Then $v(N_{L/K}(a)) = v(\prod\limits_{i=1}^{m} \sigma_i(a)) = \sum\limits_{i=1}^{m} v(\sigma_i(a)) = m \cdot \alpha$, where $m := [L : T]$, $(m, p) = 1$ and $Hom_K(L, \tilde{K}) = \{\sigma_1, ..., \sigma_m\}$. Now let $b := N_{L/K}(a) \in K^{\times}$; since $v(b) = m \cdot v(a) = v(a^m)$, $a^m = b \cdot u$, with $u \in O_L^{\times}$. As $\overline{L} = \overline{K}$ we may write $u = c \cdot u'$, with $u' \in O_L^{\times}$, $\overline{u'} = \overline{1}$. So we have $a^m = b \cdot u = b \cdot c \cdot u' = d \cdot u'$, with $d \in T^{\times}$. We want to show now that $u' = u''^m$, with $u'' \in O_K^{\times}$, which will implies that there exists $\frac{x}{u''}$ such that $(\frac{x}{u''})^m = \frac{x}{u'} = d \in T^{\times}$,i.e. that an radical over T of order m, prime with p, with $v(\frac{x}{u''}) = \alpha$. It suffices to show that $1 + m_K \subseteq O_K^{\times m}$, where $(m, p) = 1, p = char\ \overline{K} > 0$. Let $u \equiv 1 (\mathrm{mod}\, \underline{m}_K)$. Consider the polynomial $f(X) = X^m - u \in O_K[X]$. Since $1 \in \overline{K}$ is a simple root of $\overline{f}$, by Hensel's lemma there exists one and only one $\omega \in O_K$ such that $f(\omega) = 0$, and so $\omega^m = u$, $\overline{\omega} = 1$.□

An immediate consequence of this lemma is the fact that the tamely ramified extension has no defect. Assume that L/K is tamely ramified and, by the first proved implication, $L = L' := T(t(L/K)^{(p')})$. Let's prove now that

$$[L' : T] = (vL' : vT),$$

in fact, that $[L' : T] \leq m$, where $m := (vL' : vT)$. Since L/K is a finite extension, $t(L/K)^{(p')}/K^{\times}$ and vL/vK are finite too and L' is obtained from T by adjoining a finite number of elements. We want to find some generators $t_1, ..., t_m \in L'$ such that any element from L' may be written as a combination of $t_1, ..., t_m$ with coefficients in T. This will implies $m \geq [L' : T]$ which will prove the fact that a tamely ramified extension is defectless.

Now, let $t_1, ..., t_m \in t(L/K)^{(p')}$, with $v(t_i)(\mathrm{mod}\ vT)$, for $i = \overline{1, m}$, be a system of representatives for the quotient vL/vT. By the isomorphism from lemma 3.5, we have $t(L/K)^{(p')} = \bigcup\limits_{i=1}^{m} t_i T^{\times}$,which implies $L' = T(t_1, ..., t_m)$.

It remains to show that $L' = \sum_{i=1}^{m} Tt_i$. A polynomial from L' is a sum of monomials of form $c \cdot \prod_{i=1}^{m} t_i^{r_i}$, $c \in T$. Since any product of two elements $t_i t_j$, $1 \leq i, j \leq m$ can be written as $t_K \cdot \lambda$, with $\lambda \in T^\times$, $1 \leq k \leq m$, it follows that $[L' : T] = (vL' : vT)$.

Before we prove the other implication of theorem 3.2, let's make a few comments. Since $\frac{t(L/K)^{(p')}}{T^\times} \simeq \frac{vL}{vK}$ and the quotient vL/vK may be written as a direct sum of cyclical groups $\frac{vL}{vK} = \bigoplus_{i=1}^{r} \frac{\mathbb{Z}}{m_i\mathbb{Z}}$, we have

$$t(L/K)^{(p')} = \left\{ \left(\prod_{i=1}^{r} t_i^{s_i} \right) x |\ 0 \leq s_i < m_i,\ x \in T^\times \right\},$$

where t_i are the generators of cyclical groups $\mathbb{Z}/m_i\mathbb{Z}$, for $i = \overline{1, m}$. Then $L = T(t_1, ..., t_r)$, with $t_i^{m_i} = c_i \in T^\times$, $m_i | [L : T]$; therefore $(m_i, p) = 1$.

In order to prove that an extension $L = T(t_1, ..., t_r)$ is tamely ramified, it suffices to look at the case $r = 1$, i.e. $L = K(t)$, with $t^m = a$, $a \in T$, $(m, p) = 1$. The general case then follows by induction.

We may assume, without loss of generality, that $\overline{K}$ is separably closed. This is seen by passing to the maximal unramified extension $T' := K_{nr}$, which has the separable closure $\overline{T'} = \overline{K}_{nr} = \overline{K}^{sep}$ as its residue class field. We obtain the following diagram

$$\begin{array}{ccccc} & & L = T(t) & & \\ & \nearrow & & \searrow & \\ K = T & & & & L \cdot T' = T'(t) =: L', \\ & \searrow & & \nearrow & \\ & & K_{nr} =: T' & & \end{array}$$

where $L \cap T' = T = K$ and $L' := L \cdot T' = T'(t)$. If now L'/T' is tamely ramified, then $\overline{L'}/\overline{T'}$ is separable; therefor $\overline{L'} = \overline{T'}$. Hence $\overline{T} \subseteq \overline{L} \subseteq \overline{L'} = \overline{T'}$ and $\overline{T'}/\overline{T}$ is separable, $\overline{L}/\overline{T}$ is also separable. Moreover, since $p \nmid [L' : T'] = [L : T]$ it follows that L/T is also tamely ramified.

We may assume, without loss of generality, that $[L : K] = m$, i.e. a can't be written as $a = a'^d$, where d is the greatest divisor of m such that $a' \in T$. Otherwise, since $t^m = \left(t^{\frac{m}{d}}\right)^d = a'^d$, and $\left(\frac{t^{\frac{m}{d}}}{a'}\right)^d = 1$, we have $\zeta := \frac{t^{\frac{m}{d}}}{a'}$ a root of unity of order d, with $(d, p) = 1$ and therefore ζ is an element of the residue class field which is separable closed and contains all roots of unity of order prime with the characteristic. So, $t^{\frac{m}{d}} = \zeta \cdot a' \in K$ and we can make this assumption.

Let $\alpha := v(t) \in vL$ and let $n := ord\ (\alpha\ mod\ vK)$. Since $m \cdot \alpha = m \cdot v(t) = v(t^m) = v(a) \in vK$, we have $m = d \cdot n$. It follows that $n \cdot \alpha = v(t^n) = v(b), b \in K$ and $v(b^d) = v(t^m) = v(a)$ and consequently $t^m = a = b^d u$, with $u \in O_K^{\times}$. As $(d,p) = 1$, the polynomial $\overline{f}(X) = X^d - u \in \overline{K}[X]$ is separable one. Since $\overline{K}$ is separable closed, $\overline{f}$ admits a solution $w \in \overline{K}$, hence also over K by Hensel's lemma. So there exists $c \in O_K$ such that $c^d - u = 0$ and $\overline{c} = w$. Therefore $t^m = a = b^d u = b^d c^d = (bc)^d$ and, by made assumption, we obtain $d = 1$, and hence $m = n$. Thus

$$m \leq (vL : vK) \leq m := [L : K],$$

in other words $(vL : vK) = [L : K]$, and so $[\overline{L} : \overline{K}] = 1$,i.e.$\overline{L} = \overline{K}$. This shows that L/K is tamely ramified.□

Corollary 3.5. *Let L/K and K'/K be two algebraic extensions over K and $L' := L \cdot K'$. Then we have*

$$L/K \textit{ tamely ramified} \Longrightarrow L'/K' \textit{ tamely ramified.}$$

Proof. We may assume, without loss of generality, that L/K is finite and consider the diagram

$$\begin{tikzcd}
 & & L \arrow[dr, dash] & \\
 & T \arrow[ur, dash] \arrow[dr, dash] & & L \cdot K' =: L'. \\
K \arrow[ur, dash] \arrow[dr, dash] & & T \cdot K' \arrow[ur, dash] & \\
 & K' \arrow[ur, dash] & &
\end{tikzcd}$$

The inclusion $T \subseteq TK'$ follows from Proposition 2.2. If L/K is tamely ramified, then $L = T(\sqrt[m_1]{a_1}, ..., \sqrt[m_r]{a_r})$, $(m_i, p) = 1$; hence $L' = LK' = TK'(\sqrt[m_1]{a_1}, ..., \sqrt[m_r]{a_r}) \subseteq T''(\sqrt[m_1]{a_1}, ..., \sqrt[m_r]{a_r}) \subseteq L'$, where T' is the maximal unramified extension of L'/K', we have $L' = T'(\sqrt[m_1]{a_1}, ..., \sqrt[m_r]{a_r})$, so that L'/K' is also tamely ramified.□

Definition 3.6. Let L/K be an algebraic extension. then the composite V/K of all tamely ramified subextensions is called the **maximal tamely ramified** subextension of L/K.

Definition 3.7. A finite extension L/K is called **totally** (or **purely**) **ramified** if $K = T$.

Definition 3.8. A finite extension. L/K is called **wildly ramified** if it is not tamely ramified, i.e. if $L \neq V$.

4.Applications

We will consider now a few important extensions for which we will calculate the maximal unramified and tamely ramified subextensions.

4.1: Consider the extension $L := \mathbb{Q}_p(\zeta)/K := \mathbb{Q}_p$, for a primitive $n-$th. root of unity ζ. In the two cases $(n,p) = 1$ and $n = p^s$, the extension behaves completely differently. Let us first look at the case $(n,p) = 1$.

Proposition 4.1.1 *(the case $(n,p) = 1$). Let $K := \mathbb{Q}_p, L := K(\zeta)$, and let O_L/O_K and L/K, be the extension of valuation rings, and respectively residue class fields, of L/K. Suppose that $(n,p) = 1$. Then one has:*

(i) The extension L/K is unramified of degree f, where f is the smallest natural number such that $q^f \equiv 1 \ mod \ n$, i.e. f is of order p mod n in the multiplicative group $(\frac{\mathbb{Z}}{n\mathbb{Z}})^{\times}$.

(ii) The Galois group $G(L/K)$ is canonically isomorphic to $G(\overline{L}/\overline{K})$ and is generated by the Frobenius automorphism $\zeta \mapsto \zeta^p$.

(iii) $O_L = O_K[\zeta]$, where O_K is the ring $\mathbb{Z}_p$ of *p-adic integers.*

Proof. (i) Let $P(X)$ be the minimal polynomial of ζ over K and $\overline{P}(X)$ its reduction modulo $\underline{m}_K$. Being a divisor of the separable polynomial $X^n - \overline{1}$, $P(X)$ is separable; by henselianity of $\mathbb{Q}_p$, the polynomial $\overline{P}(X)$ is irreductible (any factorization of $\overline{P}(X)$ over residue class field "lifts" to a factorization of $P(X)$ which is irreductible). So, the reduction $\overline{P}(X)$ is the minimal polynomial of $\overline{\zeta} \equiv \zeta \ mod \ m_L$. P and $\bar{P}$ have the same degree, so that $[L : K] = [\overline{K}(\zeta) : \overline{K}] = [\overline{L} : \overline{K}] =: f$. L/K is therefore unramified.

Because the polynomial $X^n - 1$ splits over O_L (ζ is integral over O_K, so it's in O_L, the integral closure of O_K in L. Therefore all the roots of polynomial $X^n - 1$ are in O_L since they are powers of the primitive root ζ), and because $X^n - \overline{1}$ is separable, $X^n - 1$ splits over $\overline{L}$ into distinct linear factors, so that $\overline{L} = \mathbb{F}_{p^f}$ contains the group of roots of unity of orders divisors of n and is obtained by adjoining them to $\overline{K} = \mathbb{F}_p$ (equivalently of n-th. primitive root $\overline{\zeta}$). Consequently, f is the smallest number such that the group of n-th unity roots is included in the cyclic group $\overline{L}^{\times}$ of order $p^f - 1$, i.e. $n | \ p^f - 1$.This shows (i).

(ii)is immediate from (i).

(iii) Since L/K is unramified, we have $\underline{m}_K \cdot O_K = \underline{m}_L$, and since $1, \overline{\zeta}, ..., \overline{\zeta}^{f-1}$ represents a basis of $\overline{L}/\overline{K}$, we have $O_L = O_K[\zeta] + \underline{m}_K \cdot O_L$, and $O_L = O_K[\zeta]$ by Nakayama's lemma (if A is local ring with maximal ideal $\underline{m}$, N an A-module finitely generated and $M \subseteq N$ a submodule such that $N = M + \underline{m}N$, then $M = N$)..

Proposition 4.1.2 *(the case $n = p^m$) Let ζ be a primitive p^m-th root of the unity. Then one has:*

(i) L/K is purely ramified of degree $\varphi(p^m) = (p-1)p^{m-1}$.

(ii) $G(L/K) \simeq \left(\frac{\mathbb{Z}}{p^m\mathbb{Z}}\right)^{\times}$.

(iii) $O_L = O_K[\zeta]$, i.e. $\mathbb{Z}_p[\zeta]$ is the valuation ring of $\mathbb{Q}_p(\zeta)$.

(iv) $1-\zeta$ is a prime element (a local uniformizer) of $O_L = \mathbb{Z}_p[\zeta]$ which means that generates the maximal ideal $\underline{m}_L$ of the discrete valuation ring O_L, i.e. is an element of minimal positive valuation) with norm over K equal to p.

Proof: $\mu = \zeta^{p^{m-1}}$ is a primitive p-th root of the unity, i.e.

$$\begin{aligned} \mu^{p-1} + \mu^{p-2} + ... + 1 &= 0, \text{ hence} \\ \zeta^{(p-1)p^{m-1}} + \zeta^{(p-2)p^{m-1}} + ... + 1 &= 0. \end{aligned}$$

Therefore, $\zeta - 1$ is a root of the polynomial

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

Since $P(0) = p$ and $\bar{P}(X) = X^{(p-1)p^{m-1}}$, $P(X)$ satisfies Eisenstein's criterion and is irreducible over K. Therefore $[L:K] = [\mathbb{Q}_p(\zeta) : \mathbb{Q}_p] = \varphi(p^m)$. The canonical injection

$$\begin{aligned} G(L/K) &\rightarrow \left(\frac{\mathbb{Z}}{p^m\mathbb{Z}}\right)^{\times} \\ \sigma &\longmapsto n(\sigma), \end{aligned}$$

where $\sigma(\zeta) = \zeta^{n(\sigma)}$, is therefore bijective, since both groups have order $\varphi(p^m)$. Thus

$$N_{L/K}(1-\zeta) = \prod_{\sigma \in G(L/K)} \sigma(1-\zeta) = \prod_{\sigma \in G(L/K)} (1-\sigma(\zeta)) = P(0) = p.$$

Writing w for the extension of the p-adic valuation v_p to L,we find furthermore that

$$\begin{aligned} 1 &= v_p(p) = w(p) = w(\prod_{\sigma\in G(L/K)} \sigma(1-\zeta)) = \sum_{\sigma\in G(L/K)} w(\sigma(1-\zeta)) = \\ &= \sum_{\sigma\in G(L/K)} w(\zeta-1) = \varphi(p^m)w(\zeta-1), \end{aligned}$$

i.e. L/K is totally ramified and $1-\zeta$ is a prime element (a local uniformizer) of the (discrete) valued field L. The powers $(\zeta-1)^i$, for $i=0,1,...,\varphi(p^m)-1$, determine a base of L/K. Denoting by M the O_K-module generated by this base, we obtain easily:

$$O_L = M + (\zeta-1)^{\varphi(p^m)}O_L = M + \underline{m}_K O_L.$$

Since L/K is separable, O_L is a finitely generated O_K – module and, by Nakayama's Lemma, $O_L = M$. This concludes the proof.

Remark 4.1.3. Since L/K is separable, the discriminant of every base of L/K is a nonzero element of K. In particular, the discriminant of the above base is a nonzero element of O_K, $dO_L \subseteq M$ and $\frac{O_L}{dO_L}$ finitely generated over $\frac{O_K}{dO_K}$ and finite too. Consequently, O_L is a finitely generated O_K-module. We can avoid Nakayama's Lemma here (in case 1, iii, too) if we consider the fact that L is complete and so O_L is a projective limit of quotient rings $\frac{O_L}{p^iO_L}$ which determines a cofinal system in the family of quotient rings of O_L .

Case 3 $(n = n'p^m, (n',p) = 1, m \in \mathbb{N})$.The general case of a n-th root of the unity ζ, with $n = n'p^m$, $(n',p) = 1$, $m \in \mathbb{N}$) yields from the two extreme cases, above treated.

We can assume $m \neq 0$ (otherwise we obtain the case 1). The maximal unramified extension of L/K is $T = K(\zeta_{n'}) = \mathbb{Q}_p(\zeta_{n'})$, the cyclotomic extension of K, of order n, and the maximal tamely ramified extension of L/K is $V = T(\zeta_p) = K(\zeta^{p^{m-1}}) = \mathbb{Q}_p(\zeta^{p^{m-1}})$, the cyclotomic extension of K, with degree $n'p$. We have :

$$K = \mathbb{Q}_p \subseteq T = \mathbb{Q}_p(\zeta_{n'}) \subseteq V = T(\zeta_p) \subseteq \mathbb{Q}_p(\zeta_n) = L.$$

The results obtained may be summarized in the following way:

$$\begin{array}{rcl} L/K \text{ unramified} & \Longleftrightarrow & m=0; \\ L/K \text{ tamely ramified} & \Longleftrightarrow & m=0 \text{ or } m=1; \\ L/K \text{ purely ramified} & \Longleftrightarrow & n'=1; \\ L/K \text{ nontrivial, tamely and purely ramified} & \Longleftrightarrow & m=1; \text{ and } n'=1, \text{i.e. } n=p. \end{array}$$

At limit, if n tends to ∞, we have that L is the maximal cyclotomic extension of K, $\mathbb{Q}_p$, the maximal unramified extension is $T = K_{nr} = K(\zeta_n|(n,p)=1)$, with $G(L/K)$ isomorphic with $\hat{\mathbb{Z}}$, topologically generated by Frobenius automorphism $\zeta_n \mapsto \zeta_n^p$, $(n,p)=1$, and the maximal tamely ramified extension $V = T(\zeta_p)$, with Galois group $G(V/T)$ of order $p-1$ (to remark that for $p=2$, we have $V=T$).

The infinite galoissian extension L/T is purely ramified, with $\bar{T} = \bar{L} = \tilde{\bar{K}}$ (where denotes the algebraic closure of prime field $\bar{K} = \mathbb{F}_p$), abelian with $G(L/T)$, the inertia group of Galois (abelian) extension L/K, canonically isomorphic with $\varprojlim\limits_{m\geq 1} \left(\frac{\mathbb{Z}}{p^m\mathbb{Z}}\right)^{\times}$, the inversable elements group of $p-$adic integers ring. This extension has a unique $p-$Sylow closed subgroup, isomorphic (algebraic and topologic) to $\varprojlim\limits_{m\geq 1} \frac{\mathbb{Z}}{p^m\mathbb{Z}}$, the aditive group of p-adic integers.

Finally, let us remark that $G(L/V)$ is the kernel of canonical epimorphism

$$G(L/T) \simeq \mathbb{Z}_p^{\times} \to Hom(\frac{vL}{vK}, \bar{L}^{\times}) \simeq \mathbb{F}_p^{\times},$$

which leads an invertible element of the ring of $p-$adic integers to its class modulo the maximal ideal $p\mathbb{Z}_p$. Therefor $G(L/V)$ is identified with the subgroup $1+p\mathbb{Z}_p$ of $\mathbb{Z}_p$'s 1-units (the multiplicative profinite group $1+p\mathbb{Z}_p$ is canonically isomorphic - algebraically and topologically - with the profinite aditive group $\mathbb{Z}_p$,for $p \neq 2$)(cf.[N], chap.II, Prop.5.5).$\square$

4.2 . Let us study now the case of a tamely ramified Galois extension, with the base field henselian.

Proposition 4.2.1. *Let K be a valuated field, L/K a tamely ramified Galois extension (i.e. $L=V$), $G := G(L/K)$, $G_i = G_i(L/K)$ the extension inertia groups.*

Then:

(i) The inertia group G_i is abelian and it has a structure of $\frac{G}{G_i}$-module.

(ii) There exists a canonical isomorphism $G_i \simeq Hom(vL/vK, \bar{L}^{\times})$ of $\frac{G}{G_i}$-modules.

(iii) The group G is the semi-direct product of group $\chi\left(\frac{vL}{vK}\right)$ with Galois group $G(\bar{L}/\bar{K})$:

$$G \simeq \chi\left(\frac{vL}{vK}\right) \rtimes G(\bar{L}/\bar{K}),$$

where $\chi(A)$ denotes the profinite character group of torsion abelian group A.

Proof. (i) Since K is henselian and the extension L/K is Galois tamely ramified, we have the following result:

$$K = \mathbb{Z} \subseteq T \subseteq V = L$$

The sequence

$$1 \to G_r \to G_i \to Hom(vL/vK, \bar{L}^{\times}) \to 1$$

is exact and is induced by the surjective homomorphism:

$$\begin{array}{ccc} G_i & \to & Hom(vL/vK, \bar{L}^{\times}) \\ \sigma & \longmapsto & \chi_{\sigma}, \end{array}$$

where the associate homomorphism $\chi_{\sigma} : \bar{L}^{\times} \to \bar{L}^{\times}$ is given by $\chi_{\sigma}(x) := \frac{\overline{\sigma x}}{x} = \frac{\sigma x}{x}(\mathrm{mod})\underline{m}_L$. More, the group $Hom(vL/vK, \bar{L}^{\times})$ is canonically isomorphic with the character group $\chi\left(\frac{vL}{vK}\right) = \left(\frac{vL}{vK}\right)^{(p')}$, where $\left(\frac{vL}{vK}\right)^{(p')}$ denotes the group $\frac{vL}{vK}$ from which we eliminate the $p-$primary component, where p is the characteristic exponent of $\bar{K}$.

The exact sequence leads to the isomorphism $G_i \simeq Hom(vL/vK, \bar{L}^{\times})$ (since the extension is tamely ramified); in particular, the group G_i is abelian. Moreover, every finite quotient of G_i has the order prime with p.

The exact sequence is induced by the epimorphism :

$$\begin{array}{ccc} G(L/K) & \to & G(\bar{L}/\bar{K}) \\ \sigma & \longmapsto & \bar{\sigma}, \end{array}$$

where $\bar{\sigma}(\bar{x}) := \overline{\sigma(x)}$, for every $\bar{x} = x(\mathrm{mod}\,\underline{m}_L) \in \bar{L}$; we can now identify $\frac{G}{G_i} = \frac{G(L/K)}{G(L/T)} \simeq G(T/K)$ with $G(\bar{L}/\bar{K})$.

The group G_i is abelian and we have natural action

$$G(T/K) \times G(L/T) \rightarrow G(L/T)$$

given by

$$(\sigma, \tau) \longmapsto \sigma^{'} \circ \tau \circ \sigma^{'-1},$$

where $\sigma^{'} \in G := G(L/K)$ such that $\sigma^{'}|_T = \sigma$ (since $\sigma \in G(T/K)$, we can choose $\sigma^{'}$ as any prolongation to L; we can easily show that the definition do not depends of chosen prolongation). We can immediately show that the action is continue; it follows G_i becomes $\frac{G}{G_i}-$module.

(ii) Since $G_i \simeq Hom(vL/vK, \bar{L}^{\times})$ and G_i is $\frac{G}{G_i}-$module, it remains to show that $Hom(vL/vK, \bar{L}^{\times})$ is $\frac{G}{G_i}-$module, i.e. $G(\bar{L}/\bar{K})$-module. Let $G(\bar{L}/\bar{K})$ operate on $Hom(vL/vK, \bar{L}^{\times})$

$$\begin{array}{rcl} G(\bar{L}/\bar{K}) \times Hom(vL/vK, \bar{L}^{\times}) & \rightarrow & Hom(vL/vK, \bar{L}^{\times}) \\ (\sigma, \varphi) & \mapsto & \sigma \circ \varphi, \\ \sigma \cdot \varphi & : & \dfrac{vL}{vK} \rightarrow \bar{L}^{\times} \\ \sigma \cdot \varphi(\alpha) & : & = \sigma(\varphi(\alpha)), \text{ for every } \alpha \in \dfrac{vL}{vK}. \end{array}$$

Therefore, the isomorphism $G_i \simeq Hom(vL/vK, \bar{L}^{\times})$ is a $\frac{G}{G_i}-$module isomorphism.

(iii) Since G_i is$\frac{G}{G_i}$, i.e. $G(T/K)-$module, we have an immediate description of $G(L/K)$ as semi-direct product:

$$G(L/K) \simeq G(L/T) \bowtie G(T/K) \simeq G_i \bowtie G(\bar{L}/\bar{K}) \simeq G_i \bowtie \frac{G}{G_i}.$$

Therefore, we have

$$G(L/K) \simeq \chi\left(\frac{vL}{vK}\right) \bowtie G(\bar{L}/\bar{K}),$$

and the proof is now complete. □

Consequently, given a tamely ramified Galois extension, with a henselian base field , we can calculate the value groups (so that $\frac{vL}{vK}$) and the residue class fields (and we know the normal extension $\bar{L}/\bar{K}$); so we know two important groups: $\chi\left(\frac{vL}{vK}\right)$ and $G(\bar{L}/\bar{K})$ which can describe the structure of group $G(L/K)$.

4.3. Let us now consider the power series field $K = \mathbb{C}((t))$ and $L = \tilde{K}$ its algebraic closure.

On K we have a discrete valuation defined as follows: if $f = \sum\limits_{i\geq n_0}^{\infty} a_i t^i$, with $n_0 \in \mathbb{Z}$, $a_i \in \mathbb{C}$, then

$$v(f) := \min\{\}\{i \in \mathbb{Z} \mid a_i \neq 0\},\ \text{if } f \neq 0{,}\infty,\ \text{if } f = 0.$$

The value group is $vK = Z$; let us now calculate the residue class field. The value ring, respectively the maximal ideal, are:

$$\begin{aligned} O_K &= \{f \in \mathbb{C}((t)) \mid v(f) \geq 0\} = \{\sum_{i\geq 0} a_i t^i \mid a_i \in \mathbb{C}\} = \mathbb{C}[[t]], \\ \underline{m}_K &= \{\sum_{i\geq 0} a_i t^i \mid a_i \in \mathbb{C}\}. \end{aligned}$$

The rings homomorphism:

$$\begin{aligned} O_K &\to \mathbb{C} \\ \sum_{i\geq 0} a_i t^i &\mapsto a_0, \end{aligned}$$

is injective and has the kernel $\underline{m}_K$; it follows that $K = \frac{O_K}{\underline{m}_K} \simeq \mathbb{C}$. Hence $K = \mathbb{C}((t))$ is the completion of discrete value field $\mathbb{C}(t)$, K is henselian, cf.[N], Chap.II, Lemma 4.6.

Proposition 4.3.1. *Let $K = d$ let $L = K$ be the algebraic closure of K. Then: (i) The extension L/K is purely and tamely ramified;*

(ii) The Galois group $G(L/K)$ is isomorphic to $\hat{\mathbb{Z}}$, the profinite completion of $\mathbb{Z}$.

Proof. (i) Since K is algebraically closed, we get that $\bar{L} = \bar{\tilde{K}} = \bar{K}$. Because $G(T/K)$ is isomorphic to Galois group of residue class field extension L/K, which in this case is identity, we have $T = K$, i.e. the extension is purely ramified.

Since the residue class field has the characteristic *char* $\bar{K} = 0$, $L = V$; therefore L/K is tamely ramified.

(ii) The Galois group $G(L/K)$, which identifies itself with $G(V/T)$, is isomorphic to abelian characters group $\chi\left(\frac{vL}{vK}\right)$. This implies that the extension L/K is abelian. Also, since the value group vK of K is $\mathbb{Z}$, vL is it's divisible closure, i.e.$\mathbb{Q}$. Hence the character group $\chi\left(\frac{vL}{vK}\right)$ is equal to $\chi\left(\frac{\mathbb{Q}}{\mathbb{Z}}\right)$, i.e. $\hat{\mathbb{Z}}$. It follows that $G(L/K) \simeq \hat{\mathbb{Z}}$.□

Remark 4.3.2. By Galois theory point of view, $\mathbb{C}((t))$ behaves like a finite group, since its Galois group is isomorphic to a finite Galois group. Therefore, for any $n \geq 1$, there exists a unique extension of K, of degree n; by tamely ramified extension structure's theorem, we have:

$$K = \mathbb{C}((t)) \text{---} K_n = \mathbb{C}((t))[t^{\frac{1}{n}}] = K(t^{\frac{1}{n}}).$$

To describe the Galois group $G(K_n/K)$ it suffices to show the action on the primitive element $t^{\frac{1}{n}}$:

$$\begin{array}{ccc} \left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, +\right) & \simeq & \mu_n \subseteq \mathbb{C}^\times \to G(K_n/K) \\ \zeta & \mapsto & \sigma_\zeta, \end{array}$$

where $\sigma_\zeta|_K = 1_K$ and $\sigma_\zeta(t^{\frac{1}{n}}) := \zeta \cdot t^{\frac{1}{n}}$.□

4.4. Let us now analyze the case of extension L/K, where K is the power series field in one undetermined t with coefficients in a field k of characteristic zero and $L = \tilde{K}$ is the algebraic closure of K.

Proposition 4.4.1. *Let L/K be an extension given by $K = k((t))$, where k is a field of characteristic zero, and by $L = \tilde{K}$,where K is the algebraic closure of K.*

Then: (i) The maximal unramified extension is $T = \tilde{k}((t))$, where $\tilde{k}$ is the algebraic closure of k.

(ii) The maximal tamely ramified extension is $V = \tilde{k}((t))(t^{\frac{1}{n}} \mid n \geq 1)$.

(iii) The extension's Galois group is the semi-direct product of $\hat{\mathbb{Z}}$ with absolute Galois group $G(\tilde{k}/k)$.

Proof. As in case 4.3., we get $\bar{K} = k$, $\bar{L} = \tilde{k}$, $vK = vT = Z, vL = Q$; since *char* K = *char* $k = 0$, the extension is tamely ramified; therefor $V = L$. As $\frac{G(L/K)}{G(L/T)} \simeq G(\bar{L}/\bar{K})$, we certainly have $G(T/K) \simeq G(\tilde{k}/k)$; then the maximal unramified extension is $T = \tilde{k}((t))$. Thus, since the extension is tamely ramified, by structure theorem 3.3, we have $V = T(t^{\frac{1}{n}} \mid n \geq 1) = \tilde{k}((t))(t^{\frac{1}{n}} \mid n \geq 1)$. The results obtained above may be summarized as follows:

$$\begin{array}{rcl} K & = & k((t)) — T = \tilde{k}((t)) — V = \tilde{k}((t))(t^{\frac{1}{n}} | n \geq 1) = L \\ \bar{K} & = & k — \bar{T} = \tilde{k} = \bar{V} = \bar{L} \\ vK & = & \mathbb{Z} = vT — vV = vL = \mathbb{Q} \end{array}$$

Since $G(T/K)$ is isomorphic to absolute Galois group of coefficients field and $G(L/T)$ is isomorphic to $\hat{\mathbb{Z}}$, we get the following description of given extension Galois group:

$$G(L/K) \simeq \hat{\mathbb{Z}} \bowtie G(\tilde{k}/k)$$

□

4.5. In the previous case, if we consider the base field equal to power series field with real coefficients, we get:

$$\begin{array}{rcl} K & = & \mathbb{R}((t)) — T = \mathbb{C}((t)) — V = \mathbb{C}((t))(t^{\frac{1}{n}} | n \geq 1) = L \\ \bar{K} & = & \mathbb{R} — \bar{T} = \mathbb{C} = \bar{V} = \bar{L} \\ vK & = & \mathbb{Z} = vT — vV = vL = \mathbb{Q} \end{array}$$

In this particular case, the Galois group of extension L/K is

$$G(L/K) \simeq \hat{\mathbb{Z}} \bowtie \frac{\mathbb{Z}}{2\mathbb{Z}} \simeq \varprojlim_{n \geq 1} D_n = \hat{D}_\infty,$$

where $\hat{D}_\infty$ denotes the profinite completion of the infinite dihedral group.□

4.6. Finally, let us consider the power series field of a finite field $K = \mathbb{F}_q((t))$, where $q = p^s, s \geq 1, p$ is a prime number and $L = \tilde{K}^{sep}$, where $q = p^s$, $s \geq 1$, p is a prime number and $L = \tilde{K}^{sep}$, where $\tilde{K}^{sep}$ denotes the algebraic-separable closure of K.

Proposition 4.6.1. Let L/K be an extension with $K = \mathbb{F}_q((t))$, $q = p^s$, $s \geq 1$, p a prime number and $L = \tilde{K}^{sep}$.Then:

(i) The maximal unramified extension is given by $T = \widetilde{\mathbb{F}_p}((t))$, where $\widetilde{\mathbb{F}_p}$ *is* the algebraic closure of $\mathbb{F}_p$.

(ii) The maximal tamely ramified extension is $V = T(t^{\frac{1}{n}} \mid (n, p) = 1)$.

Proof. Since $\mathbb{F}_q$ is a finite field (and so perfect), the residue class field is $\bar{L} = \widetilde{\mathbb{F}_q} = \widetilde{\mathbb{F}_p}$; therefor the Galois group of residue class field extension is $G(\bar{L}/\bar{K}) = G(\widetilde{\mathbb{F}_q}/\mathbb{F}_q) = \hat{\mathbb{Z}}$. Let us remark that K is not a perfect field; the perfect closure is $K_{per} = K(t^{\frac{1}{p^n}} \mid n \geq 1)$. As before, we get $T = \mathbb{F}_q((t)) = \widetilde{\mathbb{F}_p}((t))$. In this case, the extension is not tamely ramified; the ramification group is $G_r \neq (0)$. Let us determine now the Galois group of extension V/T :

$$G(V/T) \simeq Hom(\frac{\mathbb{Q}}{\mathbb{Z}}, \bar{L} = \widetilde{\mathbb{F}_q}^{\times}) = Hom(\frac{\mathbb{Q}}{\mathbb{Z}}, \mu(\widetilde{\mathbb{F}_q})) = \chi((\frac{\mathbb{Q}}{\mathbb{Z}})^{(p')}) \simeq \prod_{p \neq p'} \hat{\mathbb{Z}}_p.$$

It follows that the maximal tamely ramified extension is $V = T(t^{\frac{1}{n}} \mid (n,p) = 1)$.□

References

[1] J. Ax, *A Metamathematical Approach to Some Problems in Number Theory*, AMS Symposium (73), 1969.

[2] S.Basarab, *Lectures notes*, Ovidius University, 1999.

[3] J. Neukirch, *Algebraic Number Theory*, Springer-Verlang, Berlin Heidelberg, 1999.

"Ovidius" University of Constanta,
Department of Mathematics,
8700 Constanta,
Romania
e-mail: denis@univ-ovidius.ro