On standard extensions of local fields

Akram Lbekkouri

BP: 10507, Casa-Bandoeng Casablanca, 20002 - Morocco

E-mail: `lbeka11@gmail.com`

Abstract

Let L/K be any separable extension of complete discrete valued fields of degree p. This work, is a study of some "standard over-extensions" of L/K, with the description of their Galois groups. The second target, which is the aim of this work, concerns the Galois closure of L/K. The study of the normal case has been done in some former work.

2010 Mathematics Subject Classification. **11S15**.

Keywords. Wild ramification, Discriminant , Eisenstein polynomials, Standard extensions of a local field , Intermediate extension, Semi-direct product.

Introduction

Let L/K be a separable extension of degree p of complete discrete valued fields having residue fields of characteristic $p > 0$. The content of this paper is as follows:

Section 1 is a general view of the standard over-extensions of K. Some specific results and examples on the extension $M = K((K^{\star})^{1/p-1})/K$, in general, are also given.

Section 2 is a description of the Galois groups of the standard extensions, the question of the finitude of the Number of Galois extensions having a given degree is studied and a Method for the determination of some cyclic extensions of a local number field is given.

Section 3 is the study of the Galois closure of L/K (the aim of this work). The existence of the intermediate extension and an explicit determination of it are studied.

1 Standard over-extensions

By "local field" we mean a complete discrete valued field, meanwhile "standard over-extensions" of a local field K are, the maximal abelian extension M of K of exponent $p-1$, the maximal p-abelian extension of M, and the Galois closure of a p-extension of K.

1.1 Case of finite residue field

Let K a local field with finite residue field, $k = \mathbb{F}_{p^f}$. The maximal abelian extension of exponent $p-1$ of K is $M = K((K^{\star})^{1/p-1})$, regardless of the characteristic of K, that is the compositum of two cyclic Kummer linearly disjoint extensions of K both of degree $p-1$. The unramified and a totally ramified $K(\sqrt[p-1]{\pi})$ (π uniformizer of K). M/K is the compositum of all cyclic extensions of K of degree dividing $p-1$. From Kummer Theory for abelian extensions (see [12] ch:VI), $\Gamma = gal(M/K)$

Tbilisi Mathematical Journal 8(2) (2015), pp. 49–67.
Tbilisi Centre for Mathematical Sciences.

Received by the editors: 11 September 2014.
Accepted for publication: 08 April 2015.

(the Galois group of M/K) is dual to $K^\star/K^{\star(p-1)}$, under the pairing:

$$\varphi: \begin{array}{ccc} \Gamma \times (K^\star/K^{\star(p-1)}) & \longmapsto & \mathbb{F}_p^\star \\ (\sigma, \overline{x}) & \longmapsto & \sigma(y)/y \end{array} \text{ with } (y^{p-1} = x);$$

so $\mathbb{F}_p^\star \subset K^\star$, is identified with the group of the $p-1$-th roots of unity. N the maximal abelian extension of exponent p of M is compositum of all extensions of K of degree p.

<u>*First*</u> <u>*case*</u> $char(K) = 0$

Here, $N = M(\sqrt[p]{M^\star})$; furthermore M/K, and N/M are normal.

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

• Write $\Delta = gal(N/M)$ seen as Γ -module (from the action of Γ on it, Γ acts on $M^\star/M^{\star p}$ and on $\mu_p \subset M$. $\Delta \simeq Hom(M^\star/M^{\star p}, <\zeta_p>)$ so it is isomorphic to the filtered Γ-module $M^\star/M^{\star p}$ of $\mathbb{F}_p$-dimension $p^{2+[M:\mathbb{Q}_p]}$. See Remark (1.1).

• $\mathcal{G} = gal\,(N/K)$, need not be nilpotent. It is a semidirect product $\mathcal{G} = \Delta \rtimes \Gamma_0$, where Γ_0 is a subgroup of $\mathcal{G}$ isomorphic to Γ (Schur-Zassenhaus Theorem, see [14]Chap.7. Th.7.24).

Remark 1.1. If the extension $L/\mathbb{Q}_p$ is finite then the order of the group $L^\star/L^{\star p}$ is

• 1. If L contains the p-th roots of unity then the order of the group $L^\star/L^{\star p}$ is $p^{2+[L:\mathbb{Q}_p]}$.

• 2. If L does not contain the p-th roots of unity $p^{1+[L:\mathbb{Q}_p]}$

Set $[L:\mathbb{Q}_p] = ef$, from $L^\star = \pi^{\mathbb{Z}} \times \mu_{p^f-1} \times \mathbb{U}_1$ for π a uniformizer of L, μ_n the group of the n-th roots of unity and $\mathbb{U}_1$ the group $U_1 = \{a \in L; a-1 \in \mathcal{M}_L\}$, so $L^\star \simeq \mathbb{Z} \times \mu_{p^f-1} \times \mathbb{U}_1$. From Prop. 10, Ch.XIV §.4 in [17], $\mathbb{U}_1$ is a direct product of a cyclic p-group and a $\mathbb{Z}_p$-module of rank $[L:\mathbb{Q}_p]$, so $\mathbb{U}_1 \simeq \mu_{p^h} \times \mathbb{Z}_p^{[L:\mathbb{Q}_p]}$ with $h \geq 0$, $\mu_{p^h} \subset L$ and $\mu_{p^{h+1}}$ not in L, so $h = 0$ if and only if L does not contain μ_p (see the following Note). So,

$$\begin{gathered} L^\star \simeq \mathbb{Z} \times \mu_{p^f-1} \times \mu_{p^h} \times \mathbb{Z}_p^{[L:\mathbb{Q}_p]} \\ L^\star/L^{\star p} \simeq \mathbb{Z}/p\mathbb{Z} \times \{1\} \times \mu_{p^h}/\mu_{p^h}^p \times (\mathbb{Z}/p\mathbb{Z})^{[L:\mathbb{Q}_p]} \end{gathered} \tag{1.1}$$

• If $h = 0$ then $\mu_{p^h}/\mu_{p^h}^p$ is of dimension zero.

• If $h > 0$ then $\mu_{p^h}/\mu_{p^h}^p \simeq \mathbb{Z}/p\mathbb{Z}$ that is of dimension 1.

In consequence $dim(L^\star/L^{\star p}) = 1 + 1 + [L:\mathbb{Q}_p]$ if $h > 0$ meanwhile $dim(L^\star/L^{\star p})$ $= 1 + [L:\mathbb{Q}_p]$ if $h = 0$. See for example Corollary of Proposition 6 §.3 Ch.II in [7].

<u>**Note:**</u> we prove, $\mathbb{U}_1 \simeq \mu_{p^h} \times \mathbb{Z}_p^{[L:\mathbb{Q}_p]}$.

For $L/\mathbb{Q}_p$ finite, the p-adic logarithm is a $\mathbb{Z}_p$-module homomorphism $log: \mathbb{U}_1 \to \mathcal{M}_L$, and $ker(log)$ is the p-th power roots of unity in L. This kernel is finite, since high p-th power order roots of unity have high degree over $\mathbb{Q}_p$, and can't lie in a finite extension of $\mathbb{Q}_p$ if the order is sufficiently large. The p-adic logarithm is an isomorphism from a sufficiently small closed disc $\mathcal{D}$ around 1 to a sufficiently small closed disc around 0, with its inverse being the p-adic exponential. A closed disc around 0 in $\mathcal{M}_L$ is a scalar multiple of $\mathcal{M}_L$, and $\mathcal{M}_L \simeq \mathbb{Z}_p^{[L:\mathbb{Q}_p]}$, so $\mathcal{D} \simeq \mathbb{Z}_p^{[L:\mathbb{Q}_p]}$. Since $\mathcal{D}$ is a $\mathbb{Z}_p$-submodule of $\mathbb{U}_1$ with finite index, $\mathbb{U}_1$ is a finitely generated (multiplicative) $\mathbb{Z}_p$-module that contains a submodule of finite index which is free of rank $[L:\mathbb{Q}_p]$, so by the structure theorem for finitely generated modules of a PID, $\mathbb{U}_1$ as a $\mathbb{Z}_p$-module is $\mathbb{T} \times \mathbb{Z}_p^{[L:\mathbb{Q}_p]}$, $\mathbb{T}$ is the torsion submodule of $\mathbb{U}_1$. The submodule $\mathbb{T}$ is $\mathbb{T} = \mu_{p^h} \subset \mathbb{U}_1$. Thus $\mathbb{U}_1 \simeq \mu_{p^h} \times \mathbb{Z}_p^{[L:\mathbb{Q}_p]}$. A special case is for $p = 2$, since all 2-adic field contains the 2-th roots of unity nevertheless the result still holds. For example, if $L = \mathbb{Q}_2$, $\mathbb{Q}_2^\star \simeq \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z} \times \mathbb{U}$, $(\mathbb{U} = \mathbb{U}_1)$, and $\mathbb{U}_1 = \mathbb{Z}_2^\star = \{+/-1\} \times (1+4\mathbb{Z}_2) \simeq \{+/-1\} \times \mathbb{Z}_2$ since the 2-adic logarithm is an isomorphism between $1 + 4\mathbb{Z}_2$ and $4\mathbb{Z}_2 \simeq \mathbb{Z}_2$.

Remark 1.2. Since N/M a p-elementary abelian, $gal(N/M) = \Delta \simeq (\mathbb{Z}/p\mathbb{Z})^n$ with $n = 2+[M : \mathbb{Q}_p]$ and from classical group theory $(\mathbb{Z}/p\mathbb{Z})^n$ has exactly

$$\binom{n}{i}_p = \frac{(p^n-1)(p^{n-1}-1)\ldots(p^{n-i+1}-1)}{(p^i-1)(p^{i-1}-1)\ldots(p-1)}$$

subgroups of order p^i, ($\binom{n}{i}_p$ the Gaussian p-binomial coefficient (n choose $i)_p$ for $i \leq n$). (The number of i-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_p$). By the theorem of classical Galois theory, N/M contains $\binom{n}{i}_p$ extensions of M of degree p^{n-i}.

Second case: $char(K) = p > 0$, $K = F((T))$, with F a finite field. Then $N = M(\wp^{-1}(M))$; $(\wp : x \to x^p - x)$(Artin-Schreier).

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

• $\Delta = gal(N/M)$ is isomorphic to the filtered Γ-module $M/(\wp(M))$ of $\mathbb{F}_p$-dimension $+\infty$, which is abelian too of exponent p, isomorphic to a countably infinite product of copies of $\mathbb{Z}/p\mathbb{Z}$ in general see Proposition (1.5).

• $\mathcal{G} = gal\,(N/K)$, $\mathcal{G}$ need not be nilpotent, since $\mathcal{G} = \Delta \rtimes \Gamma_0$, $\Gamma \simeq \Gamma_0 \subset \mathcal{G}$, (Generalized Schur-Zassenhaus [13]. §.2.3; page: 41)). Indeed from Krull topology, (see [12] ch:VII), Δ is a closed normal subgroup of $\mathcal{G}$ and the exponents are relatively prime. So, we have a split short exact sequence $1 \to \Delta \to \mathcal{G} \to \Gamma_0 \to 1$.

Note: Having $\Gamma \simeq \Gamma_0$, in the next, we write Γ instead of Γ_0 since no confusion can occur.

Remark 1.3. Δ is the single Sylow p-subgroup of $\mathcal{G}$, so the number of subgroups of $\mathcal{G}$ of order p^i equals the number of subgroups of Δ of order p^i for all i, namely,

$$\binom{n}{i}_p = \frac{(p^n-1)(p^{n-1}-1)\ldots(p^{n-i+1}-1)}{(p^i-1)(p^{i-1}-1)\ldots(p-1)}$$

1.2 On the prime and Equi-characteristic Case

Remain that for a complete discrete valued field K having the same characteristic p as its residue field F we can write $K = F((T))$ with T a transcendental element over F.

1.2.1 Infinitude of $K/\wp(K)$

Proposition 1.4. $K = F((T))$, with F a complete discrete valued field of characteristic p then $K/\wp(K)$, is countably infinite, ($\wp : x \to x^p - x$).

Proof. Consider $\frac{1}{T^n}$, for $n > 0$ 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 $f \in K = F((T))$ but $f \notin K = F[[T]]$,

necessarily (since $n, n' > 0$ and distinct) (which is no more true if F is finite). 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. So, we found infinitely many different elements outside of a subspace.
For the infinity of the codimension. $(T^n)_n$ with n negative prime to p numbers is free in $K/\wp(K)$. Let $n_1 < \cdots < n_m$ be negative prime to p integers, and $a_1, \ldots, a_m \in F$ non-zero. We have to prove that $f = a_1 T^{n_1} + \cdots + a_m T^{n_m}$ does not lie in $\wp(K)$. Let v be the canonical valuation of $K = F((T))$. Then $v(f) = n_1 < 0$. By contradiction, suppose that $f = g^p - g$ for some $g \in K$. Then $v(g) < 0$, so $v(g^p - g) = pv(g)$. $f = g^p - g$ implies that $n_1 = v(f) = v(g^p - g) = pv(g)$, thus p divides n_1. So, we get the contradiction. Now, by Hensel's Lemma $\wp(K)$ contains an open neighborhood of 0 so $K/\wp(K)$ is just countably infinite. Q.E.D.

Note: Prop.(1.4) can be generalized to any infinite and commutative field K, $char(K) = p$ with $\wp(K) \subsetneq K$ (strict inclusion). Indeed, the equality can occur, for example if K is algebraically closed, the equation $T^p - T - t$ is separable, with K separably closed and $char(K) = p$ we get $\wp(K) = K$, $K/\wp(K)$ is then trivial.
Let K be a commutative and infinite field and L/K finite with $[L : K] > 1$. The element 1 can be extended to a K-basis $e_1, ..., e_n$ of L, with $e_1 = 1$ and $n > 1$. Then $L = Ke_1 + Ke_2 + ... + Ke_n = K + Ke_2 + ... + Ke_n$ (the sums are direct sums). Passing to additive quotient groups, L/K is isomorphic to $Ke_2 + ... + Ke_n$, which is infinite since K is infinite. So, a similar argument works when L is any field extension of K that is larger than K (not just finite extensions of K) by using a K-basis of L that contains K.

1.2.2 Description of the product Δ

Proposition 1.5. For $L = \mathbb{F}((T))$ a local functional field with $\mathbb{F}$ a finite field of characteristic p, let N be the maximal exponent-p abelian extension of L. Then $gal(N/L)$ is a product of an countable infinite product of copies of $\mathbb{Z}/p\mathbb{Z}$.

Proof. By Kummer's theory, $gal(N/L)$ embeds into $Hom(L/\wp(L), \mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^{(\alpha)}$, and is a direct product of a non-necessarily countable number of copies of $\mathbb{Z}/p\mathbb{Z}$, of course $L/\wp(L) \simeq gal(N/L)$ and $L/\wp(L)$ embeds into $(\mathbb{Z}/p\mathbb{Z})^{(\alpha)}$. Since $L/\wp(L)$ is just countably infinite (see Prop.1.4) and thus has only countably infinite dimension then with Pontryagin duality that swaps direct sums for direct products we see that $gal(N/L)$ is thereby obtained as a countably infinite product. Q.E.D.

By use of the notations of §.1.2. $K = \mathbb{F}((T))$ ($\mathbb{F}$ finite of characteristic p), M/K is Kummer-abelian of degree $(p-1)^2$, then $M = K\left(\sqrt[p-1]{K^\star}\right)$ with $M = V((X))$ too (V finite)$V = \mathbb{F}(\sqrt[p-1]{(\varepsilon)})$ (ε a generator of $\mathbb{F}^\star$, and $X = \sqrt[p-1]{T}$). Now, by "continuity of roots" for separable monic polynomials, there are only countably many finite separable extensions of a local function fields see Example(2.9) (as such fields have a countable dense subset), Δ is necessarily a countable infinite product of copies of $\mathbb{Z}/p\mathbb{Z}$. Furthermore, Prop. (1.5) gives a direct proof of

Corollary 1.6. From Prop.(1.5). The group $\Delta = gal(N/M)$ (where $N = M(\wp^{-1}(M))$ and $M = K\left(\sqrt[p-1]{K^\star}\right)$), is a product of an countable infinite product of copies of $\mathbb{Z}/p\mathbb{Z}$.

1.3 Remarks on the extension $M = K((K^\star)^{1/p-1})/K$ in general

• In 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 not necessarily finite of characteristic p, then we have $M = K((K^\star)^{1/p-1})/K$ is not necessarily finite, but it is still abelian of exponent $p-1$, since K contains the $p-1$-th roots of unity.
• Otherwise, the extension M/K 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. Indeed see the following.

Example 1.7. 1). • Let $K = k((t))$, where $k = \mathbb{Q}(\zeta_3)$ and ζ_3 is a primitive cube root of unity. So K is a complete discretely valued field.
Let $p = 3$. $k((k^\star)^{1/p-1})/k$ is infinite. Hence so is $K((K^\star)^{1/p-1})/K$.
2). • $K = \mathbb{Q}(\zeta_3)$ where ζ_3 is a 3-th root of unity. Therefore, $M/K = K((K^\star)^{1/p-1})/K = \mathbb{Q}(\zeta_3)((\mathbb{Q}(\zeta_3)^\star)^{1/2})/\mathbb{Q}(\zeta_3)$, is infinite, since adjoining to K the square roots of different prime elements of $\mathbb{Z}[\zeta_3]$ will lead to disjoint quadratic extensions whose composite has degree a large power of 2 (the power being the number of primes).
More generally we have the following result:
3). • *"Consider $K = \mathbb{Q}(\zeta_p)$ where ζ_p is a p-th root of unity, p being an odd prime number. Then $K(\sqrt[1/p-1]{K^\star})/K = \mathbb{Q}(\zeta_p)(\sqrt[1/p-1]{\mathbb{Q}(\zeta_p)^\star})/\mathbb{Q}(\zeta_p)$, is infinite".*
Indeed, from the well known result "For relatively prime integers $a_1, ..., a_n$, the 2^n algebraic numbers $\sqrt{a_{i_1}, ..., a_{i_k}}$ with $i_1 < ... < i_k$ and $0 \leq k \leq n$ are linearly independent over $\mathbb{Q}$, so are a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{a_{i_1}}, ..., \sqrt{a_{i_k}})$. 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 $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is finite then $Q(\zeta_p)((Q(\zeta_p)^\star)^{1/2})/\mathbb{Q}(\zeta_p)$ is infinite, therefore $\mathbb{Q}(\zeta_p)((\mathbb{Q}(\zeta_p)^\star)^{1/p-1})/\mathbb{Q}(\zeta_p)$is infinite too. The result is proved.
Note that the degree of $\mathbb{Q}(\zeta_p)(\sqrt{a_{i_1}}, ..., \sqrt{a_{i_k}})$ over $\mathbb{Q}(\zeta_p)$ 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 $\mathbb{Q}(\zeta_p)$, depends on whether $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$.
4). • 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 $(\mathbb{Z}/(p-1)\mathbb{Z})^2$.
5). • 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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

6). • 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.
7). • *" For any fractions field K, with characteristic $p \neq 2$, of a Dedkind ring $\mathfrak{A}$ having infinite many prime ideals , we have $M = K((K^\star)^{1/p-1})/K$, 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 $\sqrt{p} \in K$, so a has to be zero. Then $q = b^2 p$, localizing at q, p is a unit and q is a uniformizer so this cannot happen.
8). • In contrary, in characteristic 2 $\mathbb{F}_2(T)(\sqrt{T}) = \mathbb{F}_2(T)(\sqrt{T+1})$ Is a counter-example.

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

2.1 Case of mixed characteristic

2.1.1 Explicit description of the semidirect product

From §.1.1 First case, $\Gamma \simeq (\mathbb{Z}/(p-1)\mathbb{Z})^2$, and $\Delta \simeq (\mathbb{Z}/p\mathbb{Z})^n$. Write $\Delta =< \alpha_1, \alpha_2, ..., \alpha_n >$. $M^\star/M^{\star p}$ being a $\mathbb{F}_p[\Gamma]$-module of dimension n, by local class field theory $M^\star/M^{\star p} \simeq \Delta = gal(N/M)$. Furthermore, $\Delta \simeq Hom\,(M^\star/M^{\star p}, <\zeta>)$ with ζ a primitive p-th root of unity. So, N is generated over M by n elements b_i such that $b_i^p \in M$ that is $N = M(b_1, b_2, ..., b_n)$, so consider $\Delta =< \alpha_1, \alpha_2, ..., \alpha_n >$ such that $\alpha_i(b_i) = \zeta_i b_i$ with ζ_i a p-th root of unity, and $\alpha_i(b_j) = b_j$ if $i \neq j$. To sum up we have the result:

Proposition 2.1. For $N = M(b_1, b_2, ..., b_n)$, with $b_i^p \in M$. Then
$\Delta = gal(N/M) =< \alpha_1, \alpha_2, ..., \alpha_n >$ is defined by $\alpha_i(b_i) = \zeta_i b_i$ with $\alpha_i(b_j) = b_j$ if $i \neq j$.

Let $\varphi : (\mathbb{Z}/(p-1)\mathbb{Z})^2 \to Aut((\mathbb{Z}/p\mathbb{Z})^n)$ a non trivial homomorphism.
Set $\Delta \rtimes_\varphi \Gamma = (\mathbb{Z}/p\mathbb{Z})^n \rtimes_\varphi (\mathbb{Z}/(p-1)\mathbb{Z})^2 =< \alpha_1, \alpha_2, ..., \alpha_n > \rtimes_\varphi < g_1, g_2 >$, by use of the basic representation theory, every representation of Γ is completely reducible by the theorem of Maschke see [4]. Further $|Hom(\Gamma, \mathbb{F}_p^\star)| = |\Gamma|$, so every irreducible representation of Γ over $\mathbb{F}_p$ has dimension 1. then, if V is a vector space over $\mathbb{F}_p$ and $\varphi : \Gamma \to Aut(V_{\mathbb{F}_p})$ a homomorphism, there exists a basis

B of V and homomorphisms $\varphi_b : \Gamma \to \mathbb{F}_p^\star$, $b \in B$ such that $\varphi(g)(b) = \varphi_b(g)b$ for every $g \in \Gamma$ and every $b \in B$. So we get:

Proposition 2.2. The semi-direct product $\mathcal{G}$,
$\mathcal{G} = \Delta \rtimes_\varphi \Gamma = (\mathbb{Z}/p\mathbb{Z})^n \rtimes_\varphi (\mathbb{Z}/(p-1)\mathbb{Z})^2 =< \alpha_1, \alpha_2, ..., \alpha_n > \rtimes_\varphi < \sigma, \tau >$,
is defined by the $2n$ relations:
$\sigma\alpha_i\sigma^{-1} = \zeta_i\alpha_i$, and $\tau\alpha_i\tau^{-1} = \xi_i\alpha_i$, for $i = 1, ..., n$; ζ_i, ξ_i being elements of $(\mathbb{Z}/p\mathbb{Z})^\star$.
That is by terms of characters, for $\chi_i \in \hat{\Gamma} = Hom(\Gamma, \mathbb{F}_p^\star)$ (dual of Γ); write
$M_1 = diag(\chi_1(\sigma), \chi_2(\sigma), ..., \chi_n(\sigma))$, and $M_2 = diag(\chi_1(\tau), \chi_2(\tau), ..., \chi_n(\tau))$,
for the diagonal matrices images of σ and τ, then the action above becomes:
$\sigma\alpha_i\sigma^{-1} = \chi_i(\sigma)\alpha_i$, and $\tau\alpha_i\tau^{-1} = \chi_i(\tau)\alpha_i$.

2.1.2 Noticeable remarks on the group $\mathcal{G}$

Remark 2.3. :
• 1. In general such groups are metabelian, but nonnilpotent. Meanwhile, they can be nilpotent, then abelian, if and only if for all i; $\zeta_i = \xi_i = 1$ ($\mathcal{G}$ is then a direct product).
Concerning the center $Z(\mathcal{G})$ of $\mathcal{G}$. Since $(\mathbb{Z}/p\mathbb{Z})^n$ and $(\mathbb{Z}/(p-1)\mathbb{Z})^2$ are abelian, any generator of the first subgroup that commutes with the generators of the second lies in the center and vis versa. So:
• 2. $\mathcal{G} = \Delta \rtimes_\varphi \Gamma = (\mathbb{Z}/p\mathbb{Z})^n \rtimes_\varphi (\mathbb{Z}/(p-1)\mathbb{Z})$ note the action of Γ on Δ the homomorphism $\varphi : \Gamma \to Aut(\Delta)$ then $ker(\varphi)$ consists of all $\sigma^a\tau^b$ for which $\zeta_i^a\xi_i^b = 1$ for all i. Put $C = C_\Delta(\Gamma) = C_\Delta(\sigma) \cap C_\Delta(\tau)$ it is described in terms of the i such that $\zeta_i = \xi_i = 1$. Then $C = \Delta \cap Z(\mathcal{G})$. For $\sigma\tau \in \mathcal{G}$ with $\sigma \in \Delta$ and $\tau \in \Gamma$ then $\sigma\tau \in C_\mathcal{G}(\Gamma) \Leftrightarrow \sigma \in C$. On the other hand $\sigma\tau \in C_\mathcal{G}(\Delta) \Leftrightarrow \tau \in C_\Gamma(\Delta) = ker(\varphi)$. Finally $Z(\mathcal{G}) = C_\mathcal{G}(\Gamma) \cap C_\mathcal{G}(\Delta)$.
• 4. For $m < n$ if there are exactly m indices i with $\zeta_i = \xi_i = 1$ then $\#Z(\mathcal{G}) \geq p^m$.
• 5. $\#Z(\mathcal{G}) > p^m$ if and only if there exist a, b not both are zero, such that $0 \leq a, b < p-1$, and $\zeta_i^a \cdot \xi_i^b = 1$ for all i. Indeed, for $g \in \mathcal{G}$, $g = nh$ with $n \in (\mathbb{Z}/p\mathbb{Z})^n$ and $h \in (\mathbb{Z}/(p-1)\mathbb{Z})^2$, g is central if and only if both n and h are central. Since, central elements in $\mathcal{G}$ contained in $(\mathbb{Z}/p\mathbb{Z})^n$ are generated by the α_i for which $\zeta_i = \xi_i = 1$. So $h = \sigma^a\tau^b$ is central if and only if the condition above holds, so there can be more than p^m elements in the center. Also, $\#Z(Z(\mathcal{G})) = p^m \cdot c$ with c a proper divisor of $(p-1)^2$.
• 6. Particularly if $\zeta_i = \xi_i$ for all i; then $\sigma^{-1}\tau$ lies in the center that is $(p-1)|\#Z(\mathcal{G})$. Likewise if $\zeta_i = \xi_i^{-1}$ for all i; then $\tau\sigma$ lies in the center that is $(p-1)|\#Z(\mathcal{G})$ too.
• 7. If none of the conditions 4.), 5.) and 6.) hold then $\mathcal{G}$ is centerless.

Proposition 2.4. 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

$G_0 \cap (\mathbb{Z}/p\mathbb{Z})^n$. By 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 $\mathcal{G}$. Q.E.D.

Remark 2.5. 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-examples.

Example 2.6. (Counter-example)
In Proposition (2.4) when considering $p = 3$, $n = 2$ take for example for the action defining the semi-direct product $[\varphi(x,y)](a,b) = (a, yb)$ (here we identified $\mathbb{Z}/(p-1)\mathbb{Z}$ with $\mathbb{F}_p^\star$). The subgroup $\{(a,a) | a \in \mathbb{Z}_3\}$ is obviously not normal in $\mathcal{G}$.

Example 2.7. (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 $\sigma(\sqrt[3]{1+\sqrt{3}})$, must be a cubic root of $\sigma(1+\sqrt{3}) = 1-\sqrt{3}$, but E contains no such root, since E is strictly contains in N. Hence the subgroup $gal\,(N/E)$ is not normal in $gal\,(N/K)$.

2.2 Equi-characteristic Case

For Δ a p-profinite group, product of a countable number of copies of $\mathbb{Z}/p\mathbb{Z}$, N is generated over M by a countable number of elements b_i such that $b_i^p - b_i \in M$. So, Δ is generated by α_i of order p with $\alpha_i^j(b_i) = b_i + j$ for $0 \le j < p$, $i \in N$ and $\alpha_i(b_k) = b_k$ for $i \ne k$. So:

Proposition 2.8. With a countable number of relations, we define $\mathcal{G} = \Delta \rtimes_\varphi \Gamma = < \alpha_1, \alpha_2, ..., \alpha_n, ... > \rtimes_\varphi < \sigma, \tau >$, is $\sigma\alpha_i\sigma^{-1} = \zeta_i\alpha_i$, and $\tau\alpha_i\tau^{-1} = \xi_i\alpha_i$; for $i \in N$; and $\zeta_i, \xi_i \in (\mathbb{Z}/p\mathbb{Z})^\star$. That are, $\sigma\alpha_i\sigma^{-1} = \chi_i(\sigma)\alpha_i$, and $\tau\alpha_i\tau^{-1} = \chi_i(\tau)\alpha_i$ where $\chi_i \in \hat{\Gamma}$.

2.3 On the Number of Galois extensions having a given degree

The finitude of the number of all extensions of a local number field having a given degree" was studied and explicitly computed first by I.R.Safarevič in [15], M.Krasner in [6] then by J.P.Serre in [16]. In characteristic $p > 0$ this result holds no more. See the Example:

Example 2.9. For instance,
• The field $\mathbb{F}_p((X))$, ($\mathbb{F}_p$ of p elements), has only one inseparable extension of degree p. Indeed for L an inseparable extension of degree p, $L^p = \mathbb{F}_p((X))$, of course p-th power in $K = \mathbb{F}_p((X))$ are Laurent series in X^p ($\mathbb{F}_p$ is perfect). So, if $f \in K$, $f = a_0 + a_1X + \ + a_{p-1}X^{p-1}$ each a_i is a p-th power. $K(\sqrt[p]{f})$ lies in $K(\sqrt[p]{X})$, and so $K(\sqrt[p]{X})$ is the only purely inseparable extension of degree p, and $L = \mathbb{F}_p((X)^{1/p}))$. Meanwhile, it has infinitely many separable ones (Artin-Schreier) of this

degree. In fact the question reduces to whether , $K/\wp(K)$, ($\wp: x \to x^p - x$), is infinite? which is true. Prop. (1.4).
• In imperfect residue field case, we have the following beautiful example. $K = k(x)((z))$ (k is algebraically closed of characteristic p) has infinitely many extensions of degree p. Extensions given by $y^p - y = x^j$, ($j \in \mathbb{N}$ and $j \nmid p$), are all disjoint Galois p-extensions.

Now, let us first state some important results on groups:

Lemma 2.10. A finitely generated group G has only finitely many normal subgroups of a given index n, and only finitely many subgroups of G of bounded index.

PROOF. Let $G =< x_1, ..., x_k >$ be a finitely generated group and H a fixed finite group. There are finitely many homomorphisms from G to H (for each tuple $g_1, ..., g_k$ there is at most one sending x_i to g_i). So there are finitely many normal subgroups N of G such that $G/N \simeq H$ (for each such N there exists at least one homomorphism from G to H with kernel N). As, up to isomorphism there are finitely many groups of fixed order, then there are finitely many normal subgroup of G having fixed (or even bounded index). Let K be a subgroup of G of finite index m, it has at most m conjugates $K_1, ..., K_l$ and the intersection of all K_i is a normal subgroup of index at most $m^l \leq m^m$. (The normal core of K). As for a normal subgroup N of index s there are at most 2^s subgroups containing N, then the number of subgroups of bounded index in G is bounded. Q.E.D.

Theorem 2.11. Let G be a topologically finitely generated profinite group, then:
• For each natural number n the number of open subgroups of G of index n is finite.
• Identity element 1 of G has a fundamental system of neighborhoods consisting of countable chain of open characteristic subgroups of $G = V_0 \supseteq V_1 \supseteq V_2$... See [13] (Prop. 2.5.1)

The Galois group of any infinite extension is a profinite group, the converse is also true. So in case of Theorem (2.11), "the finitude" still holds.

Corollary 2.12. If $gal(K^s/K)$ is topologically finitely generated, then there are only finitely many Galois extensions of a given degree of K. Particularly if K is quasi-finite.

In "Serre's sense" a field is said to be quasi-finite if it is perfect and $gal(K^s/K) \simeq \widehat{\mathbb{Z}}$.

2.4 Method for the determination of some cyclic extensions of a local number field

Let $K/\mathbb{Q}_p$ be a finite extension, $[K : \mathbb{Q}_p] = r$. Set K_c the compositum of all cyclic extensions of K of degree p.

2.4.1 On the compositum of all cyclic p-extensions

Proposition 2.13. With the hypothesis above,
1 • $[K_c : K] = p^{r+1}$ and $gal(K_c/K) \simeq (\mathbb{Z}/p\mathbb{Z})^{r+1}$, if the $p-th$ roots of unity are in K. 2 • $[K_c : K] = p^{r+2}$ and $gal(K_c/K) \simeq (\mathbb{Z}/p\mathbb{Z})^{r+2}$, if K contains the $p-th$ roots of unity.

Proof. By local class field theory, $K^\star/K^{\star p}$ is isomorphic to the Galois group of the maximal elementary abelian p-extension of K ie. K_c. Remark.(1.1) gives the result. Q.E.D.

2.4.2 Explicitness for the case $K = \mathbb{Q}_p$

Application: The Maximal p-abelian extension of $\mathbb{Q}_p$

For $p \neq 2$, $\mathbb{Q}_p$ has exactly $p+1$ cyclic extensions of degree p, all are totally ramified except one is unramified. For $p = 2$ a detailed classification of the quadratic and the quartic extensions is given in [10]. Put $r = 1$ in Prop.(2.13) to determine the compositum of all cyclic extensions of $\mathbb{Q}_p$ of degree p. Exhibit two cyclic linearly disjoint extensions of degree p of $\mathbb{Q}_p$ (the unramified $\mathbb{Q}_p(\lambda)$, and the subextension $\mathbb{Q}_p(\eta)$ (totally ramified) of degree p of $\mathbb{Q}_p(\zeta_{p^2})$; ζ_{p^2} is a primitive p^2-th root of unity). The $p+1$ cyclic extensions of degree p of $\mathbb{Q}_p$ are the subextensions of $\mathbb{Q}_p(\lambda,\eta)$. Respectively write, $G_\lambda = gal(\mathbb{Q}_p(\lambda))/\mathbb{Q}_p$ and $G_\eta = gal(\mathbb{Q}_p(\eta))/\mathbb{Q}_p$. There are natural isomorphisms from G_λ and G_η into $\mathbb{F}_p$.

To determine the primitive elements, set $\eta = 1 + \sum_{0<i<p^2; i^{p-1}\equiv 1 \mod p} \zeta_{p^2}^i$ an uniformizer (the trace), their conjugates $\eta_k = 1 + \sum_{0<i<p^2; i^{p-1}\equiv 1 \mod p} \zeta_{p^2}^{i+kp}$, with $0 \leq k \leq p-1$ (action of $\mathbb{F}_p$ on the conjugates of η). For a prime q, $q \equiv 1 \mod p$; and $p^{(q-1)/p}$ not congruent to 1 mod q and $p^{(q-1)/p}$ not congruent to 1 mod q, write $\lambda = \sum_{j \mod q; j^{(q-1)/p}\equiv 1 \mod q} \zeta_q^j$ the conjugates are $\lambda_k = \sum_{j \mod q; j^{(q-1)/p}\equiv 1 \mod q} \zeta_q^j \zeta_p^k$, with $0 \leq k \leq p-1$. The expression $\lambda_{r_1}\eta_{s_1} + ... + \lambda_{r_p}\eta_{s_p}$ gives the primitive elements for the p-cyclic extensions of $\mathbb{Q}_p$.

Example 2.14. For a numerical example, consider the case $p = 7$ we have $[\mathbb{Q}_7(\zeta_{49}) : \mathbb{Q}_7] = 42$, so we can take $\eta = 1 + \zeta_{49} + \zeta_{49}^{-1} + \zeta_{49}^{18} + \zeta_{49}^{-18} + \zeta_{49}^{19} + \zeta_{49}^{-19}$ thus we get $[\mathbb{Q}_7(\eta) : \mathbb{Q}_7] = 7$ with $\mathbb{Q}_7(\eta)/\mathbb{Q}_7$ cyclic totally ramified. Then by taking $q = 29$ we get $[\mathbb{Q}_7(\zeta_{29}) : \mathbb{Q}_7] = 28$ therefore, we can take $\lambda = \zeta_{29} + \zeta_{29}^{-1} + \zeta_{29}^{12} + \zeta_{29}^{-12}$ and thus $[\mathbb{Q}_7(\lambda) : \mathbb{Q}_7] = 7$ with $\mathbb{Q}_7(\lambda)/\mathbb{Q}_7$ cyclic unramified.

For a detailed study (see [8] §.3 page 139). With software Pari, for several values of p, the Eisenstein polynomials corresponding to the p cyclic extensions are determined, as well as their reduites (in Krasner's sense).

2.4.3 Determination of the cyclic extensions of degree d of $\mathbb{Q}_p$, with $d|p-1$)

p an odd prime, and $d = q_1^{r_1}.q_2^{r_2}...q_s^{r_s}$ (q_i prime) for $d|p-1$. By Kummer theory, the cyclic extensions of degree d of $\mathbb{Q}_p$ are in bijection with the cyclic subgroups of order d of $\mathbb{Q}_p^\star/\mathbb{Q}_p^{\star d}$. Since $\mathbb{Q}_p^\star = p^Z \times Z_p = p^Z \times \mu_{p-1} \times U_1$ (μ_n n-th roots of unity), and $U_1^d = U_1$, so $\mathbb{Q}_p^\star/\mathbb{Q}_p^{\star d} \simeq p^Z/p^{dZ} \times \mu_{p-1}/\mu_{(p-1)/d} \simeq < p > \times < \zeta >$ a product of two cyclic groups of order d. These extensions come from taking a d-th root of ξp^i, (i integer determined mod d, ξ is a $p-1$-th root of unity (determined up to multiplication by a $((p-1)/d)$-th root of unity). This gives the product of two cyclic groups of order d. Now The number of cyclic non-isomorphic extensions of degree d of $\mathbb{Q}_p$ is equal to the number of cyclic subgroups of order d of $(\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/d\mathbb{Z})$. Since, a cyclic group of order d contains $\varphi(d)$ elements of order d, (Euler's totient). For $g(d)$ the number of elements

of order d in a group, the number of cyclic subgroups is $g(d)/\varphi(d)$. The order of any element of G (direct product of two cyclic groups of order d) divides d. If m divides d, then the set of elements whose orders divide m is the subgroup of G which is the direct product of two cyclic groups of order m, whose order is m^2. So, if $g(m)$ is the number of elements of order exactly m, $m^2 = \sum_{k|m} g(k)$, and by möbius inversion (μ) $g(m) = \sum_{k|m} k^2\mu(m/k)$. For $m = d$ gives the number of elements of order d in G. The number of cyclic subgroups of order d in the group G is $g(d)/\varphi(d) = (\sum_{k|d} k^2\mu(d/k))/\varphi(d)$.
For $d = 60$, $\varphi(d) = 16$ and then the number of elements of order 60 is $60^2 - 30^2 - 20^2 - 12^2 + 10^2 + 6^2 + 4^2 - 2^2 = 2304$, so the number of cyclic subgroups of order 60 is 144.
For d a prime, it is $(d^2 - 1)/(d - 1) = d + 1$ see Huppert in [3] (Hilfssatz 8.5). The number of cyclic groups of order d in an elementary abelian d-group of rank n, is $(d^n - 1)/(d - 1)$.
Description of Galois groups of cyclic extensions of degree d of $\mathbb{Q}_p$ with $d|p-1$. For $r = 1$ and $s = 1$ then d is prime, these are in bijection with the pairs $(i, j) \in (\mathbb{Z}/d\mathbb{Z})^2$ with either $i = 1$ or $(i, j) = (0, 1)$, corresponding to the $\mathbb{F}_d$ points on the projective line.
A similar description for prime-powers, say q^r, the subgroups generated by pairs $(1, j)$ for all j and those generated by pairs $(i, 1)$ for all i divisible by the prime q.
For the general case use the canonic splitting into the direct product of the Sylow subgroups and combine for each Sylow subgroup.

Example 2.15. Description of cyclic extensions of degree 3 of $\mathbb{Q}_7$?
By local class field theory, this is the same as the number of one-dimensional subspaces of the $\mathbb{F}_3$-vector space $\mathbb{Q}_7^\star/(\mathbb{Q}_7^\star)^3$. As 3 divides $6 = 7 - 1$, this is 2-dimensional: the cubes in $\mathbb{Q}_7^\star$ are $7^{3n}\varepsilon$ where $\varepsilon = +-1 \pmod 7$. So there are 4 such extensions.
$\mathbb{Q}_7$ contains the cube roots of unity. So, the degree 3 cyclic extensions are Kummer extensions, they are generated by the cube roots of $2, 7, 14$ and 28.

3 Embedding of an extension of prime degree in its Galois closure

3.1 Existence of the intermediate extension

Proposition 3.1. Let K be a commutative field, for every separable extension L/K of degree p, p an odd prime, $G = gal(L_C)/K$ 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 (ie. $L_C = LF$). Furthermore if L/K is not cyclic (LF/K is hence not abelian), then L has exactly p conjugates over K in LF.

Proof. G is solvable, its order is divisible by p but not by p^2. Seen as a transitive subgroup of the symmetric group $\mathfrak{S}_p$, then according to ([1], ch.3, th.7) G contains a unique subgroup P of order p so it is normal in G. P is contained in its normalizer $N(P)$ in $\mathfrak{S}_p$. Also $N(P)$ seen as the affine linear group $GA_1(\mathbb{F}_p)$, we have the isomorphism $\mathbb{F}_p^\star \to Aut(P)$, and 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 semidirect product $G = P \rtimes M$ with M cyclic of order m.

If the semidirect product is a direct product then it is cyclic since m and p are co-prime.

Otherwise G is not abelian. In such case M being cyclic then all its conjugates are cyclic too. Write m in the form $m = \prod_{i=1}^{r} m_i^{\alpha_i}$, m_i being different prime numbers, and N for the number of the conjugates of M (note that according to Hall's theorem(see [14]Chap5. Th5.23. page 85) 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. So the number N must divide mp, being $N \equiv 1$ modulo m_i for all i , thus $(N, m) = 1$. So 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 $L_C = LF$. The proof is ended. Q.E.D.

Remark 3.2. F is unique. Now, L/K being of prime degree, from now on we can suppose that L/K is totally ramified (so LF/F is too) and write $LF = F(\pi)$.

3.2 Intermediate extension, explicit determination

From now on, assume that K has a finite residue field of characteristic p.

3.2.1 Description of the Galois closure

Recall that the compact group $\Gamma \simeq Hom(K^\star/K^{\star p-1}, \mu_{p-1})$ then by duality $\Gamma \simeq K^\star/K^{\star p-1}$. Hence Γ is of the exponent $p-1$, and M/K is Kummer abelian relatively to $p-1$. The subextension F of L_C/K (Prop. 3.1), and of M/K, is cyclic Kummer of degree m dividing $p-1$ then, $F = K\left(\sqrt[m]{b}\right)$, with $b \in K^\star$. So, $K\left(\sqrt[m]{b}\right) = K\left(\sqrt[m]{d}\right)$ if and only if there exists an integer $k \geq 1$; with $(k, m) = 1$ such that $d \in b^k K^{\star m}$.

By considering the quotient group $K^\star/K^{\star m}$ the order of the class $bK^{\star m}$; in it is m. Since m is dividing $(p-1)$, $K^\star/K^{\star m} \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$; 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, 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 this number equals to $\left(p_1^{\alpha_1} + p_1^{\alpha_1 - 1}\right) \dots \left(p_r^{\alpha_r} + p_r^{\alpha_r - 1}\right)$. Furthermore $gal\,(F/K) \simeq H$; H being a subgroup of $gal\,(L_C/K)$ and L_C the Galois closure of L/K; is 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. So, Schur-Zassenhaus theorem ([14]Chap.7. Th.7.24., page:151) ensures the semi direct product $gal\,(L_C/K) \simeq gal\,(L_C/F) \rtimes H$. From local class field theory see [2] the isomorphism between the three groups $gal\,(F/K) \simeq H \simeq K^\star/N_{F/K}\,(F^\star)$ of order m, and the surjective homomorphism $s: K^\star/K^{\star m} \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \mapsto K^\star/N_{F/K}\,(F^\star)$.

3.2.2 The group $gal\,(LF/K)$

Since $gal\,(F/K)$ is cyclic of order m dividing $p-1$, write $gal(F/K) =< \varepsilon >$ with $\varepsilon(\sqrt[m]{b}) = \xi_m(\sqrt[m]{b})$, where ξ_m a primitive m-th root of unity and name the extension of ε to $F(\pi)$, ε too. Since $gal(F(\pi)/F)$ is cyclic of order p write $gal(F(\pi)/F) =< \sigma >$. LF/K being Galois, consider τ any element of $gal(LF/K)$, thus $\tau = \sigma^i\varepsilon^j$, 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

$$\tau\sigma\tau^{-1} = \sigma^t \text{ with } 1 \leq t \leq p-1. \tag{1.2}$$

Consider the affine group $AGL\,(1,p)$, of all maps from $\mathbb{F}_p$ to itself in the form $x \mapsto ux+v$ where $u \neq 0$ 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 $GL_2\,(\mathbb{Z}/p\mathbb{Z})$, of the matrices in form $\begin{pmatrix} u & v \\ 0 & 1 \end{pmatrix}$ an automorphism δ corresponds to $\begin{pmatrix} u & v \\ 0 & 1 \end{pmatrix}$; $\delta\,(\xi_p) = \xi_p^u$, and $\delta(x) = \xi_p^v x$; ξ_p, is a primitive p-th root of unity. Pick a generator g of $(\mathbb{Z}/p\mathbb{Z})^\star$, for a generator of $gal\,(F/K)$ take, $\varepsilon : x \mapsto gx$ that corresponds to $\begin{pmatrix} g & 0 \\ 0 & 1 \end{pmatrix}$ and for a generator σ of $gal(LF/F)$, $\sigma : x \mapsto x+1$ that corresponds to $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ then $\varepsilon\sigma\varepsilon^{-1} = \sigma^g$. For any τ of $gal(LF/K)$; $\tau = \sigma^i\varepsilon^j$, 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 $\mathbb{F}_p$. $(\mathbb{Z}/p\mathbb{Z})^\star$, has $\varphi\,(m)$ elements of order m, $\varphi\,(.)$ (Euler's totient). Meanwhile the equation $x^m = 1 \bmod p$ has exactly m solutions in $(\mathbb{Z}/p\mathbb{Z})^\star$, ($m$ 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 isomorphic to the group of the m-th roots of unity.

3.3 Generation of the intermediate extension

3.3.1 Ramification elements of LF/K :

$LF = F(\pi)$, π uniformizer of L and of LF too. $d_{(.)}$, $e_{(.)}$ and $f_{(.)}$ the respective discriminant, ramification index and residual degree. So $e_{LF/F} = e_{L/K} = p$; $f_{LF/F} = f_{L/K} = 1$.

Write $e_{F/K} = e_{LF/L} = t = \#|G_0/G_1|$ and $f_{F/K} = f_{LF/L} = r$ that is the order of G/G_1 (with respectively G the Galois G_0 the inertia and G_1 the ramification groups).

For any K-homomorphism σ of L, define the break relative to σ as $v = v_L(\frac{\sigma(\pi)}{\pi} - 1)$. v is independent of π and σ and depends of L/K only, see [5]. With a prime degree it is unique with $v \leq \frac{ep}{p-1}$. Its integrity is a necessary condition for the normality of L/K.

By computing $v_K(d_{LF/K})$ in two different ways, along the towers $LF/F/K$ and $LF/L/K$ we get $v_F\left(d_{LF/F}\right) = (p-1)\,(1+v)$; furthermore we have $v_K\left(d_{F/K}\right) = v_L\left(d_{LF/L}\right) = (t-1)\,r = m-r$.

In conclusion we get $v_K\left(d_{L/K}\right)=(p-1)\left(1+\frac{v}{t}\right)$. So,

$$gcd\,(v,t)=1. \tag{1.3}$$

3.3.2 Explicit computation of the break

Let $f(X)=\sum_{i=0}^{p}a_iX^i$, be an Eisenstein polynomial of degree p $a_i\in K$ $(f(\pi)=0)$, write $\pi=\pi_1,\pi_2,\ldots,\pi_p$, for the roots of $f(X)=0$. Set $f_0(X)=X^{-1}f(\pi(X+1))=X^{-1}\sum_{i=0}^{p}a_i\pi^i(X+1)^i=X^{-1}\sum_{i=0}^{p}\sum_{t=0}^{i}a_i\pi^i\binom{i}{t}X^t=\sum_{j=0}^{p-1}\sum_{i=j+1}^{p}\binom{i}{j+1}a_i\pi^iX^j=\sum_{j=0}^{p-1}d_jX^j$, with $d_j=\sum_{i=j+1}^{p}\binom{i}{j+1}a_i\pi^i$, $d_{p-1}=\pi^p$, and $d_0=\sum_{i=1}^{p}\binom{i}{1}a_i\pi^i=\sum_{i=1}^{p}ia_i\pi^i$. Then $w=\frac{v_L(d_0)-v_L(d_{p-1})}{p-1}$, so $v_L(d_0)=(p-1)w+p$ ($v_L(.)$ normalized valuation of L).
Since $v_L(d_0)=\inf_{1\le t\le p}(v_L(ta_t)+t)$, there exists a_k ***the principal coefficient*** of f, such that $w=\frac{v_L(k)+v_L(a_k)+k-p}{p-1}$. Having $d_0\equiv ka_k\pi^k$, modulo $\pi^{v_L(ka_k)+k+1}$, two cases can be distinguished. First case, $k\neq p$, and then $w=\frac{v_L(ka_k)+k-p}{p-1}$, with $k=(p-1)w-v_L(a_k)+p$, in the Second $k=p$ (necessarily $char(K)=0$) so $w=\frac{pe}{p-1}$. With $w=\frac{v}{t}$ we have:

$$d_0\equiv\left(ka_k\pi^{-v_L(a_k)}\right)\left(\pi^{(p-1)w+p}\right)\ \text{modulo}\pi^{(p-1)w+p+1}. \tag{1.4}$$

($ka_k\pi^{-v_L(a_k)}$ being an unit of L).

3.3.3 Explicit computation of the primitive element

Consider $g(X)=X^{-1}f(\pi+X)=\sum_{t=0}^{p-1}b_tX^t$, its roots are $\theta_i=\sigma^i(\pi)-\pi$, for $1\le i\le p-1$. ($\sigma^i(\theta)\equiv\theta\mod\pi$, so, $N_{LF/F}(\theta)\equiv\theta^p\equiv\theta\mod\pi$), then $L(\theta_2,\ldots,\theta_p)$ is the splitting field of f over K. $g(X)=\sum_{t=0}^{p-1}\sum_{i=t+1}^{p}\binom{i}{t+1}a_i\pi^{i-t-1}X^t$; $b_t=\sum_{i=t+1}^{p}\binom{i}{t+1}a_i\pi^{i-t-1}$, $b_{p-1}=1$ and $\prod_{i=1}^{p-1}\theta_i=b_0=\sum_{i=1}^{p}\binom{i}{1}a_i\pi^{i-1}=\sum_{i=1}^{p}ia_i\pi^{i-1}$, so $d_0=b_0\pi$.
$v_L(b_0)=\inf_{1\le t\le p}\ (v(ta_t)+t-1)=v(d_0)-1=(p-1)(w+1)$. So, $v_L(a_k)=(p-1)w-k+p$. Then $\prod_{i=1}^{p-1}\theta_i=b_0\equiv ka_k\pi^{k-1}=(ka_k\pi^{-v_L(a_k)})(\pi^{(p-1)(w+1)})$ modulo $\pi^{(p-1)w+p}$.
Write $\gamma=-b_0=-ka_k\pi^{k-1}$, and extend the normalized valuation $v_L(.)$ of L to LF in a nonnormalized way ($v_{LF}(\pi)=1$). Denote by $g_1(X)=X^{p-1}-\gamma$ (its roots are the $\zeta_{p-1}^i\sqrt[p-1]{\gamma}$, where ζ_{p-1} is a $(p-1)$-th root of unity), and by θ' any root of $g_1(X)=0$. Compute the expression $g(\theta')-g_1(\theta')=g(\theta')$ in two different ways:

$$\begin{aligned} g(\theta')-g_1(\theta') &= \theta'^{p-1}-\theta'^{p-1}+\textstyle\sum_{i=1}^{p-2}b_i\theta'^i+\sum_{i=1}^{p}ia_i\pi^{i-1}+\gamma \\ &= \textstyle\sum_{i=1}^{p-2}b_i\theta'^i+\sum_{i=1,i\neq k}^{p}ia_i\pi^{i-1}. \end{aligned} \tag{1.5}$$

All valuations in the sums are $\ge(p-1)w+p$. Since $g(\theta')=\prod_{i=1}^{p-1}(\theta'-\theta_i)$ then $v_{LF}\left(\prod_{i=1}^{p-1}(\theta'-\theta_i)\right)=\sum_{i=1}^{p-1}v_{LF}(\theta'-\theta_i)\ge(p-1)w+p=(p-1)(w+1)+1$, so there exists i_0 with $v_{LF}(\theta'-\theta_{i_0})\ge(w+1)+\frac{1}{p-1}$, that is $v_{LF}(\theta'-\theta_{i_0})>(w+1)$, by Krasner's Lemma (see [9]) $L(\theta')=L(\theta_{i_0})=L\left(\sqrt[p-1]{\gamma}\right)=L(\theta_2,\ldots,\theta_p)=K\left(\pi,\sqrt[p-1]{\gamma}\right)=LF$. Then:

Theorem 3.3. With the current notations, let L/K be a separable extension of degree p. If there exist an index k, $1\le k\le p-1$, such that $v_L(a_k)+k=\inf_{1\le i\le p}(v_L(a_i)+i)$, then

$K\left(\sqrt[p-1]{-ka_k\pi^{k-1}}\right)/K$ is cyclic Kummer extension of degree m, m dividing $p-1$. Furthermore, the splitting field of f over K is $K\left(\pi,\ \sqrt[p-1]{-ka_k\pi^{k-1}}\right)$.

Notice that $\theta' \equiv \theta_{i_0} \equiv \theta \mod \pi$ and take $\theta' = \sqrt[p-1]{\gamma}$, then

$$\theta' = \sqrt[p-1]{\gamma} \equiv \theta \text{ modulo } \pi \tag{1.6}$$

Furthermore, from the equality $k-1=(p-1)(w+1)-v_L(a_k)$, and since $w=\frac{v}{t}$:

$$\theta' = \sqrt[p-1]{\gamma} = \zeta_{p-1}\sqrt[p-1]{-ka_k\pi^{-v_L(a_k)}}\pi^{\frac{v}{t}+1}, \tag{1.7}$$

$(p-1)$ being prime to p then $L^\star/L^{\star(p-1)} \simeq K^\star/K^{\star(p-1)} \simeq \mathbb{Z}/(p-1)\mathbb{Z}\times\mathbb{Z}/(p-1)\mathbb{Z}$, so

$$\begin{array}{lcl} L^\star/L^{\star(p-1)} & \to & K^\star/K^{\star(p-1)} \\ \delta L^{\star(p-1)} & \to & N_{L/K}(\delta)K^{\star(p-1)}, \end{array} \tag{1.8}$$

is an isomorphism. Since $N_{L/K}(\frac{\gamma}{N_{L/K}(\gamma)}) \in K^{\star(p-1)}$, thus the pre-image $\frac{\gamma}{N_{L/K}(\gamma)} \in L^{\star(p-1)}$, that is $\sqrt[p-1]{\frac{\gamma}{N_{L/K}(\gamma)}} \in L^\star$. So $L\left(\sqrt[p-1]{\gamma}\right) = K\left(\pi,\ \sqrt[p-1]{\gamma}\right) = K\left(\pi,\ \sqrt[p-1]{N_{L/K}(\gamma)}\right)$, and then $F = K\left(\sqrt[p-1]{N_{L/K}(\gamma)}\right)$, and $LF = K\left(\pi,\ \sqrt[p-1]{N_{L/K}(\gamma)}\right)$. By other words we can take

$$\sqrt[p-1]{N_{L/K}(\gamma)} \text{ as primitive element of } \quad F/K \tag{1.9}$$

If the principal coefficient is $a_p = 1$ ($char(K) = 0$), $LF = L(\sqrt[p-1]{-p\pi}) = L(\sqrt[p-1]{-p}) = K(\pi,\ \sqrt[p-1]{-p}) = K(\pi,\zeta_p)$ is the splitting field of f over K. (where ζ_p is a primitive p-th root of unity). Furthermore, since $X^{p-1}+p$ is Eisenstein, $K(\pi,\zeta_p)/K$ is totally ramified of degree $p(p-1)$ (K with no the p-th roots of unity), otherwise L/K is normal. then:

Theorem 3.4. With the current notations, let L/K be a separable extension of degree p. If $v_L(a_i) \geq v_L(p)+p = p(e+1)$ for i , $1 \leq i \leq p-1$ then the splitting field of f over K is $K(\pi,\ \sqrt[p-1]{-p}) = K(\pi,\zeta_p)$. Furthermore $K(\pi,\zeta_p)/K$ is totally ramified of degree $p(p-1)$, (K with no p -th roots of unity). Otherwise $K(\pi)/K$ is normal of degree p.

Now let us generate the intermediate extension another way:

Theorem 3.5. With the current notations, let L/K be a separable extension of degree p. Then there exists $c \in K^\star$, unique up to $K^{\star(p-1)}$, such that the following hold:
- $L(\sqrt[p-1]{c})$ is the Galois closure of L/K
- For every $\tau \in Gal(L(\sqrt[p-1]{c})/K)$, and $\sigma \in Gal(L(\sqrt[p-1]{c})/K(\sqrt[p-1]{c}))$, we have

$\tau\sigma\tau^{-1} = \sigma^a$, with $a = \frac{\tau(\sqrt[p-1]{c})}{\sqrt[p-1]{c}}$ modulo p.

Proof. K contains the $p-1$-th roots of unity, F/K is Kummer cyclic of degree m, so $F = K\left(\sqrt[m]{b}\right)$, $b \in K^\star$. $K\left(\sqrt[m]{b}\right) = K\left(\sqrt[m]{d}\right)$; if and only if there exists an integer $k \geq 1$; with $(k,m)=1$

such that $d \in b^k K^{\star m}$. Up to take $c = b^{(p-1)/m}$, $LF = L\left(\sqrt[p-1]{c}\right)$.
Now $\tau(\sqrt[p-1]{c}) = \sigma^i(\varepsilon^j(\sqrt[p-1]{c})) = \sigma^i(\zeta_{p-1}^j \sqrt[p-1]{c}) = \zeta_{p-1}^j \sqrt[p-1]{c}$, for every $\tau \in gal\left(L\left(\sqrt[p-1]{c}\right) = LF/K\right)$.
So $\frac{\tau(\sqrt[p-1]{c})}{\sqrt[p-1]{c}}$ is a unit of L/F. ζ_{p-1}^j does not depend on c but on the coclass $cK^{\star p-1}$ only. Indeed $\frac{\tau(\sqrt[p-1]{c})}{\sqrt[p-1]{c}} = \frac{\tau(\sqrt[p-1]{d})}{\sqrt[p-1]{d}}$, if and only if $\tau\left(\sqrt[p-1]{\frac{c}{d}}\right) = \sqrt[p-1]{\frac{c}{d}}$, that is $\frac{c}{d} \in K^{\star p-1}$.
Set $\theta = \sigma(\pi) - \pi$ so $\theta \equiv 0 \mod \pi^{v+1}$ and $\pi_1 = \tau(\pi)$ it is uniformizer too. So $\sigma(\pi_1) - \pi_1 = u(\sigma(\pi) - \pi) = u\theta$ with u unit of LF. $u \equiv 1 \mod \pi$, as $\sigma(\tau(\pi) - \pi) \equiv \tau(\pi) - \pi \mod \pi$, so the class of $\frac{\tau(\theta)}{\theta}$ mod 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 $1 \le a \le p-1$, therefore $\tau(\theta) = (\sigma^a(\pi_1) - \pi_1)$. Since the equality between ideals $\sigma((\pi^t)) = (\pi^t)$ 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 $1 \le a \le p-1$, finally we get

$$\frac{\tau(\theta)}{\theta} \equiv a \ \text{ modulo } \ \pi^{v+1} \quad \text{that is modulo } p \quad \text{for} \quad 1 \le a \le p-1 \tag{1.10}$$

From (1.9); $c = N_{L/K}(\gamma) = N_{LF/F}(\gamma)$; $\gamma = -ka_k\pi^{k-1}$, a_k is the principal coefficient of f. By (1.6) $\sqrt[p-1]{\gamma} \equiv \theta \mod \pi \Rightarrow N_{LF/F}(\sqrt[p-1]{\gamma}) \equiv N_{LF/F}(\theta) \equiv \theta^p \equiv \theta \mod \pi$, then finally

$$\frac{\tau\left(N_{LF/F}(\sqrt[p-1]{\gamma})\right)}{N_{LF/F}(\sqrt[p-1]{\gamma})} \equiv a \ \text{ modulo } \ \pi^{v+1} \quad \text{that is modulo } p \quad \text{for} \quad 1 \le a \le p-1 \tag{1.11}$$

Q.E.D.

3.4 Explicit construction of the splitting field

3.4.1 Interpretation in case the principal coefficient is not a_p :

By a simple calculation we get the following Theorem (3.6) through the equality:

$$\sqrt[p-1]{N_{L/K}(\gamma)} = \xi_{p-1} k a_k (-a_0)^{\left(\frac{v}{t}+1\right)} \sqrt[p-1]{-ka_k(-a_0)^{-pv_K(a_k)}}. \tag{1.12}$$

Theorem 3.6. With the current notations, let L/K be a separable extension of degree p. If there exists an index k, $1 \le k \le p-1$ such that $v_L(a_k) + k = \inf_{1 \le i \le p}(pv_K(a_i) + i)$ (hence necessarily $v_L(a_k) + k < v_L(p) + p$) then the splitting field of f over K is
$K\left(\pi, (-a_0)^{\frac{v}{t}} \sqrt[p-1]{-ka_k(-a_0)^{-pv_K(a_k)}}\right)$.

Remark 3.7. It is clear that if the condition (1.13) is satisfied then $K(\pi)/K$ is normal.

$$\sqrt[p-1]{-ka_k(-a_0)^{-v_K(a_k)}} \in K(\pi). \tag{1.13}$$

Particular case $k = 1$.

Corollary 3.8. With the hypothesis and notations of theorem (3.3) , if:
1. $v_L(a_1) \le v_K(a_i)$ for every i , $2 \le i \le p-1$ and

2. $v_L(a_1) \le v_L(p)$,
then the splitting field of f over K is $K(\pi, \sqrt[p-1]{-a_1})$.

If $a_1 = p\alpha_1$; $\alpha_1 \equiv 1 \mod \mathfrak{P}_K$, (K a local number field) the splitting field of f over K is $K(\pi, \sqrt[p-1]{-a_1}) = K(\pi, \sqrt[p-1]{-p}) = K(\pi, \xi_p)$, where ξ_p is a primitive p-th root of unity.

Lemma 3.9. Let $(m,p) = 1$ and $x \in K^\star$, then $K(\sqrt[n]{x})/K$ is an unramified extension precisely if $x \in U_K K^{\star n}$. (See [11]Lemma 5.3.)

From Lemma (3.9) with $F = K\left((-a_0)^{\frac{v}{t}} \sqrt[p-1]{-ka_k(-a_0)^{-pv_K(a_k)}}\right)$, we have:

Lemma 3.10. With the conditions of Theorem (3.3)
$(p-1)$ divides $(v_K(a_k)+k-1)$ (ie. the break is integer), if and only if F/K is unramified.

Generation by discriminant:
We have $\Delta(f) = (-1)^{\frac{p(p-1)}{2}} N_{K(\pi)/K}(f'(\pi))$. $f'(\pi) = \sum_{i=1}^{p} ia_i\pi^{i-1}$
$= ka_k\pi^{k-1}\left(1+\sum_{i\neq k} r_i\pi^{i-1}\right)$, with r_i suitable choosen integers. Then it is clear that $v_L\left(r_i\pi^{i-1}\right) > 0$, for every i, $1 \le i \le p$ and $i \neq k$ and therefore, $(1+\sum_{i\neq k} r_i\pi^{i-1}) \in U_L^1$, thus $N_0 = N_{L/K}\left(1+\sum_{i\neq k} r_i\pi^{i-1}\right) \in U_K^1$, and then $\sqrt[p-1]{N_0} = N' \in K$. Indeed, since $U_K^1 \supseteq N_{L/K}(U_L^1)$ and if L/K is normal and totally ramified $N_{L/K}(U_L^1)$ is a subgroup of index p of U_K^1 . Now $N_{L/K}(-f'(\pi)) = N_{L/K}(-ka_k\pi^{k-1}).N_0$, therefore $\sqrt[p-1]{-N_{L/K}(f'(\pi))} = \xi_{p-1} \sqrt[p-1]{N_{L/K}(-ka_k\pi^{k-1})}.N'$, then $L\left(\sqrt[p-1]{-ka_k\pi^{k-1}}\right) = K\left(\pi, \sqrt[p-1]{-N_{L/K}(f'(\pi))}\right) = K\left(\pi, \sqrt[p-1]{(-1)^{\frac{p(p-1)}{2}+1}\Delta(f)}\right)$.

Theorem 3.11. With the conditions of Theorem (3.3). If there exists an index k, $1 \le k \le p-1$ such that $v_L(a_k) + k = \inf_{1\le i\le p}(v_L(a_i)+i)$. Then $K\left(\sqrt[p-1]{(-1)^{\frac{p(p-1)}{2}+1}\Delta(f)}\right)/K$ is a cyclic Kummer extension of degree m, m dividing $p-1$. Furthermore, the splitting field of f over K is $K\left(\pi, \sqrt[p-1]{(-1)^{\frac{p(p-1)}{2}+1}\Delta(f)}\right)$.

3.4.2 Interpretation in case the principal coefficient is a_p :

Generation by discriminant:
$f'(\pi) = \sum_{i=1}^{p} ia_i\pi^{i-1} = p\pi^{p-1}\left(1+\sum_{i=1}^{p-1} r_i\pi^{i-1}\right)$ with $v_L\left(r_i\pi^{i-1}\right) > 0$, for every i, $1 \le i \le p-1$, so $N_{L/K}(-f'(\pi)) = N_{L/K}\left(-p\pi^{p-1}\right).N_0 = (-p)^p(-a_0)^{p-1}.N_0$; that is $\sqrt[p-1]{-N_{L/K}(f'(\pi))} = p\zeta_{p-1}\sqrt[p-1]{-p}a_0N$, with $N \in K$ thus the splitting field is $K(\pi, \sqrt[p-1]{-p}) = K(\pi, \zeta_p) = K\left(\pi, \sqrt[p-1]{(-1)^{\frac{p(p-1)}{2}+1}\Delta(f)}\right)$. With the current notations:

Theorem 3.12. K being a finite extension of $\mathbb{Q}_p$. if $v_L(a_i) + i \ge v_L(p) + p = p(e+1)$ for every i , $1 \le i \le p-1$ then $K(\pi)/K$ is normal if and only if the p-th roots of unity lay in K, otherwise the splitting field of f over K is $K(\pi, \zeta_p) = K\left(\pi, \sqrt[p-1]{(-1)^{\frac{p(p-1)}{2}+1}\Delta(f)}\right)$.

3.5 Completeness and generation

The generation above by a $(p-1)$-th root of the discriminant in Propositions (3.11) and (3.12), was done in a local case with finite residue field, so the completeness is a necessary. Here, a counter-example of an Eisenstein polynomial defined on $\mathbb{Q}$ its splitting field can not be generated by a $(p-1)$-th root of the discriminant, even by adjoining the $(p-1)$-th roots of unity to $\mathbb{Q}$, and the splitting field has a solvable Galois group.

Example 3.13. (Counter-Example):
Consider the number $\alpha = \sqrt[5]{\sqrt{26}+5} - \sqrt[5]{\sqrt{26}-5}$.
By calculation of successive powers of α we get the minimal polynomial of α, $Irr(\alpha, \mathbb{Q})(X) = X^5 + 5X^3 + 5X - 10$ (Eisenstein), α the single real root, $(\mathbb{Q}(\alpha) \subset \mathbb{R})$. Set $r = \sqrt[5]{\sqrt{26}+5}$, so we have $\alpha = r - 1/r$, and $\alpha_j = r\zeta_5^j - 1/r\zeta_5^j$, ($\zeta_5$ is a primitive 5-th root of unity). By a similar calculation of successive powers of α_j we get that α_j and α are conjugate (same minimal polynomial). So $Irr(\alpha, \mathbb{Q})(X) = \prod_{j=0}^{4}(X - \alpha_j) = \prod_{j=0}^{4}(X - (r\zeta_5^j - 1/r\zeta_5^j))$.
1-st case:
Consider $K = \mathbb{Q}_5$. $Irr(\alpha, \mathbb{Q}_5)(X) = Irr(\alpha, \mathbb{Q})(X)$ and is still Eisenstein, then with respect to (Theorem 4.1. page 336 in [9]), $\mathbb{Q}_5(\alpha)/\mathbb{Q}_5$ is not normal. According thz study above the splitting field E of $Irr(\alpha, \mathbb{Q}_5)$ over $\mathbb{Q}_5$ is of degree dividing 20.
Now since none of the nonzero coefficients of f is divisible by 25 the principal coefficient of f is $a_1 = 5$ then thanks to corollary (3.8) and Theorem (3.11) the splitting field of f over $\mathbb{Q}_5$ is $\mathbb{Q}_5(\alpha, \sqrt[4]{-a_1}) = \mathbb{Q}_5(\alpha, \sqrt[4]{(-1)^{\frac{5(4)}{2}+1}\Delta(f)})$. Furthermore, the discriminant of $Irr(\alpha, \mathbb{Q}_5)$ is $\Delta(f) = 338000000 = 5^5.10816 = 5^5.16.26^2$. As $10816 \equiv 1$ modulo 5 it is then a 4-power in $\mathbb{Q}_5$, $\mathbb{Q}_5(\sqrt[4]{(-1)^{\frac{5(4)}{2}+1}\Delta(f)}) = \mathbb{Q}_5(\sqrt[4]{-5}) = \mathbb{Q}_5(\xi_5)$. That is $E = \mathbb{Q}_5(\alpha, \xi_5)$
2-nd case:
$K = \mathbb{Q}(i)$ (with $i^2 = -1$). The discriminant of $\mathbb{Q}(i)$ is -4, it is not divisible by 5, it does not ramify in $\mathbb{Q}(i)$, $Irr(\alpha, \mathbb{Q})$ is still Eisenstein in K. The splitting field M of $Irr(\alpha, \mathbb{Q})$, over $\mathbb{Q}$ has a solvable group of degree 20 (Software Pari), explicitly $< \sigma^5 = \tau^4 = 1, \tau^{-1}\sigma\tau = \sigma^2 >$. M is included in $\mathbb{Q}(r, \zeta_5)/\mathbb{Q}$ which is of degree at most 40 (r is a root of the polynomial $X^{10} - 10X^5 - 1$). Since, $r^5 = 5 + \sqrt{26}$ then $\mathbb{Q}(r^5) = \mathbb{Q}(\sqrt{26})$. $\mathbb{Q}(\alpha, \zeta_5, \sqrt{26}) = \mathbb{Q}(\alpha, \zeta_5, r^5)$ is included in $\mathbb{Q}(r, \zeta_5)$. Since $\mathbb{Q}(\alpha, \zeta_5, \sqrt{26})/\mathbb{Q}$ is of degree 40 then $\mathbb{Q}(\alpha, \zeta_5, \sqrt{26}) = \mathbb{Q}(r, \zeta_5)$, and the splitting field M is then included in it.
By degrees consideration $K(\sqrt[4]{-5}) \subset K(\sqrt{26}, \zeta_5)$. Ad absurdum assume that $\sqrt[4]{-5} \in K(\sqrt{26}, \zeta_5) = \mathbb{Q}(\sqrt{26}, \zeta_{20})$. $\mathbb{Q}(\sqrt{26}, \zeta_{20})/\mathbb{Q}$ being abelian cannot contain the non-normal extension $\mathbb{Q}(\sqrt[4]{-5})/\mathbb{Q}$, so $\sqrt[4]{-5}\sqrt{26}$ does not lay in $K(\alpha, \sqrt{26}, \zeta_5)$ neither to the splitting field of $Irr(\alpha, K) = Irr(\alpha, \mathbb{Q})$ over K that is included in it. Then the counter example.

References

[1] E. Artin, *Galois Theory*, Univ. of Notre Dame Press, Notre Dame, 1944, Second edition.

[2] M.Hazewinkel, *Local class field theory is easy*, Adv. in Math.18 (1975), 148–181.

[3] B. Huppert, *Endliche Gruppen I*, Grundlehren der mathematischen Wissenschaften Volume 134, 1967

[4] G. James and M. Liebeck, *Representations and characters of groups*, Cambridge University Press, New York, 2001.

[5] M.Krasner, *Sur la primitivite des corps p-adiques*, Mathematica Cluj t:13 (1937) pp. 72–191.

[6] M. Krasner, *Nombres des extensions de degre donne d'un corps p-adique, Les tendances geometriques en Algebre et en theorie des nombres*, Edition du centre national de la recherche scientifique Paris (1966) pp. 143–169.

[7] S. Lang, *Algebraic number theory, Addison-Wesley publishing company*, INC, 1968.

[8] A. Lbekkouri, *On the Ore-Krasner equation*, Scientiae Mathematicae Japonicae Vol. 74, No. 2 and 3 Whole Number 268 December 2011 pp. 121–134.

[9] A. Lbekkouri, *On the construction of normal wildly ramified extensions over* Q_p $p \neq 2$, Archiv der Math.Volume 93, Number 4 (2009), 331–344.

[10] A. Lbekkouri, *On the construction of normal wildly ramified extensions over* Q_2, Archiv der Mathematik Volume 93, Number 3 (2009), 235–243

[11] J. Neukirch, *Class Field Theory* (Grundlehren DerMathWissenschaften, 1986).

[12] P. Ribenboim, *L'Arithmetique des corps Volume 2*, Hermann Paris 1972.

[13] L. Ribes and P.Zalesskii, *Profinite groups*, A series of Modern surveys in Mathematics, Volume 40 Springer 2000.

[14] P. Rotman, *An introduction to group theory*, Springer Graduate texts in Mathematics, 2010.

[15] I.R. Safarevič, *On p-extensions*, Amer. Math. Soc. Transl. 4(2) (1954).

[16] J.P. Serre, *Une formule de masse pour les extensions totalement ramifiees de degre donne dun corps local*, Comptes Rendus 286, 1978, pp. 1031-1036.

[17] J.P. Serre, *Local fields*, Springer 1979.