Annali di Matematica (2017) 196:457–477
DOI 10.1007/s10231-016-0581-8

Extensions of degree p^ℓ of a p-adic field

Maria Rosaria Pati[1]

Received: 8 September 2015 / Accepted: 17 May 2016 / Published online: 2 June 2016

Abstract Given a p-adic field K and a prime number ℓ, we count the total number of the isomorphism classes of p^ℓ-extensions of K having no intermediate fields. Moreover, for each group that can appear as Galois group of the normal closure of such an extension, we count the number of isomorphism classes that contain extensions whose normal closure has Galois group isomorphic to the given group. Finally, we determine the ramification groups and the discriminant of the composite of all p^ℓ-extensions of K with no intermediate fields. The principal tool is a result, proved at the beginning of the paper, which states that there is a one-to-one correspondence between the isomorphism classes of extensions of degree p^ℓ of K having no intermediate extensions and the irreducible H-submodules of dimension ℓ of F^*/F^{*p}, where F is the composite of certain fixed normal extensions of K and H is its Galois group over K.

Keywords p-adic fields · Isomorphism classes of extensions · Galois theory · Ramification theory

Mathematics Subject Classification 11S05 · 11S15

1 Introduction

It is well known that a p-adic field K has only a finite number of non-isomorphic algebraic extensions with given degree [8]. We want to classify these extensions up to K-isomorphism in the totally and wildly ramified case, which is the only one slightly difficult to treat.

In 1966, Krasner [8] obtained an explicit formula for the total number of extensions of K with given ramification index and inertial degree. Later, Serre [11] also computed the number of extensions using a different method in the proof of his famous "mass formula". In [10],

✉ Maria Rosaria Pati
pati@mail.dm.unipi.it

1 Dipartimento di Matematica, Università di Pisa, Largo Pontecorvo 5, 56127 Pisa, Italy

Pauli and Roblot, with a more computational approach, gave another proof for the formula counting the number of extensions of a given degree and discriminant. A new progress in the research was made in 2004, when Hou and Keating [6] considered the problem of determining the number of isomorphism classes of extensions of K with given ramification index e and inertial degree f; they found general formulas when $p^2 \nmid e$ and, under some additional assumptions on e and f, also when $p^2 \parallel e$. This question was definitively closed by Monge in 2011 [9].

In 2007, Dvornicich and Del Corso [3], looking at the isomorphism classes of extensions of K of degree p, gave a new way to attach the problem of counting extensions: their idea is to “shift” the p-extensions of K in a more easy environment, where they can be identified by the action of a certain group on a suitable space. This new method has been used also by Dalawat [2], who extended it to the case of local fields of characteristic p.

Recently in [4], Del Corso, Dvornicich and Monge, taking inspiration from [3], present a general and very useful way to study the extensions of degree p^k of a p-adic field having no intermediate extensions. Denoting by F the composite of all normal and tame extensions of K whose Galois group is a subgroup of $\mathrm{GL}(k, \mathbb{F}_p)$ and $H = \mathrm{Gal}(F/K)$, they show that there exists a one-to-one correspondence between the possible extensions $\tilde{L}/K$ that appear as normal closure of extensions L/K of degree p^k having no intermediate fields and the irreducible $\mathbb{F}_p[H]$-submodules of F^*/F^{*p} of dimension k.

This key result allows to classify the extensions of K of p-power degree only by studying the structure of the filtered $\mathbb{F}_p[H]$-module F^*/F^{*p}; in other words, our problem is reduced to find the irreducible representation of dimension k of a certain group H acting on a suitable module F^*/F^{*p}. This is practicable in the case in which k is a prime number ℓ, while in the general case this method is not indeed usable since the number of the possible representations increases with the number of divisors of k. The author intend to show the application of the same method to study the first non-prime case $k = 4$ in a forthcoming paper.

Specializing to the extensions of degree p^ℓ, we obtain an improvement of the general theorem on the correspondence between isomorphism classes and irreducible modules, showing that in this case we can substitute F with a smaller field, that is the composite of all normal extensions of K of degree prime to p whose Galois group is isomorphic to a subgroup of $\mathbb{F}_{p^\ell}^*$ or to a non-abelian subgroup of $\mathbb{F}_{p^\ell}^* \rtimes_\theta \mathrm{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p)$ where $\theta(\phi_p) =: \phi_{p|\mathbb{F}_{p^\ell}^*} \in \mathrm{Aut}(\mathbb{F}_{p^\ell}^*)$ (ϕ_p the Frobenius automorphism).

Using this result, we classify the p^ℓ-extensions of K having no intermediate field and count their total number up to K-isomorphism.

Finally, as a further application of the correspondence theorem, we determine the ramification groups and the discriminant of the composite of all extensions of degree p^ℓ of K having no intermediate fields.

2 Notation

Let p and ℓ be prime numbers. For a p-adic field K, we denote by e_K and f_K the ramification index and the inertial degree of $K/\mathbb{Q}_p$, respectively, and by $n_K = e_K f_K = [K : \mathbb{Q}_p]$ the absolute degree of K. We also denote by π_K a uniformizer of K, by κ_K its residue field and put $q_K = |\kappa_K|$.

If E/K is a finite extension, then $e_{E/K}$ and $f_{E/K}$ are the ramification index and the inertial degree of the extension; if E/K is Galois with $\mathrm{Gal}(E/K) = G$ then $G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots \supseteq \{1\}$ is, as usual, the lower numbering ramification filtration. In particular, G_0

is the inertia group and its fixed field E^{ur} is the maximal unramified subextension of E/K, while G_1 is the unique p-Sylow subgroup of G_0 and its fixed field is the maximal tame ramified subextension of E/K.

Finally, we shall denote by $\mathscr{C}_{p^\ell}$ the composite of all extensions of K of degree p^ℓ having no intermediate field.

3 The correspondence theorem

Let $F = F(K)$ be the composite of all normal extensions of K of degree prime to p whose Galois group is isomorphic to a subgroup of $\mathbb{F}^*_{p^\ell}$ or to a non-abelian subgroup of $\mathbb{F}^*_{p^\ell} \rtimes_\theta \mathrm{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p)$ where $\theta(\phi_p) = \phi_p|_{\mathbb{F}^*_{p^\ell}} \in \mathrm{Aut}(\mathbb{F}^*_{p^\ell})$ (ϕ_p the Frobenius automorphism), and let $H = \mathrm{Gal}(F/K)$. Then

Theorem 1 *There exists a one-to-one correspondence between the isomorphism classes of extensions of degree p^ℓ of K having no intermediate extensions and the irreducible H-submodules of dimension ℓ over $\mathbb{F}_p$ of F^*/F^{*p}.*

Remark 1 Since the degree of $K(\zeta_p)$ over K divides $p-1$, we have $K(\zeta_p) \subseteq F$.

Proof We first show that to an extension L/K of degree p^ℓ having no intermediate extensions, one can associate an irreducible H-submodule of dimension ℓ of F^*/F^{*p}. In order to obtain this, we will prove that LF/F is an elementary abelian extension of degree p^ℓ. It is easy to see that $[LF : F] = p^\ell$ since L and F are linearly disjoint over K. Observe that the extension L/K cannot be unramified, because otherwise it would be abelian and hence admit intermediate fields; in particular it is totally ramified, since otherwise it would have a proper subextension given by the maximal unramified subextension. Let $\tilde{L}$ be the normal closure of L/K and $G = \mathrm{Gal}(\tilde{L}/K)$. As usual, G has the lower numbering ramification filtration $G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots \supseteq \{1\}$, where for every i the subgroup G_i is normal in G and for every $i \geq 1$ the quotient G_i/G_{i+1} is an elementary abelian p-group.

Let $\tilde{H} \subseteq G$ be the subgroup fixing L. Since $\tilde{L}$ is the normal closure of L/K, no subgroup of $\tilde{H}$ is normal in G; it follows that the intersection of all its conjugates (which is normal if not trivial) is trivial. Moreover, since L/K has no intermediate extensions, $\tilde{H}$ is a maximal subgroup of G and hence there is a unique t such that $G_{t+1} \subseteq \tilde{H}$ and $G_t\tilde{H} = G$; observe that we must have $t \geq 1$ since L/K is a totally and wildly ramified extension.

Now, G_t is clearly a $\tilde{H}$-module (the action given by conjugation) and, since the centralizer $C_{\tilde{H}}(G_t)$ of G_t in $\tilde{H}$ is trivial (being contained in the intersection of all conjugates of $\tilde{H}$), it is a faithful $\tilde{H}$-module. Moreover, $G_{t+1} = \{1\}$ since $\tilde{H}$ has no subgroup normal in G, therefore G_t is an elementary abelian p-group, while from $C_{\tilde{H}}(G_t) = \{1\}$ we have $G_t \cap \tilde{H} = \{1\}$. It follows that $G \simeq G_t \rtimes \tilde{H}$ and $|G_t| = p^\ell$. This implies that G_t is also irreducible as $\tilde{H}$-module since otherwise there would exists a proper $\tilde{H}$-submodule A of G_t and then a proper subgroup $A \rtimes \tilde{H}$ of G containing $\tilde{H}$, which is a contradiction to the maximality of $\tilde{H}$.

Let L_1 be the subfield of $\tilde{L}$ fixed by G_t, so $\mathrm{Gal}(L_1/K) \simeq \tilde{H}$. We will show that the order of $\tilde{H}$ is prime to p. Since G_t is a faithful $\tilde{H}$-module, $\tilde{H}$ can be embedded in $\mathrm{Aut}(G_t) \simeq \mathrm{GL}(\ell, \mathbb{F}_p)$. Let $\tilde{H}_1$ be the ramification group of $\tilde{H}$, then either $\tilde{H}_1 = \{1\}$ or $\tilde{H}_1$ is the unique p-Sylow of $\tilde{H}_0$, and it is normal in $\tilde{H}$. But if $\tilde{H}$ has a non-trivial normal p-subgroup, then G_t would have a proper $\tilde{H}$-submodule, contradicting its irreducibility. So necessarily $p \nmid \mathrm{o}(\tilde{H})$.

Now we prove that L_1 is contained in F.

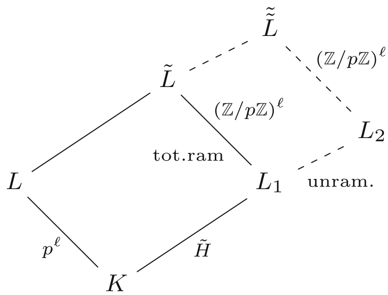
Since $p \nmid \mathrm{o}(\tilde{H})$, $\tilde{H} = \mathrm{Gal}(L_1/K)$ is the Galois group of a tame extension, therefore it is of the form

$$\langle v, \tau \mid v\tau v^{-1} = \tau^q, \tau^e = 1, v^f = \tau^r\rangle$$

where $e = e_{L_1/K}$, $f = f_{L_1/K}$, $q = p^{f_K}$ and r is the smallest positive integer such that $v^f = \tau^r$ (see [7]). Such an extension is not necessarily split, but it is always contained in a split one, say L_2/K, i.e. in a tame extension whose Galois group is a semidirect product of the inertia subgroup and its complement. In particular, we can take L_2 such that L_2/L_1 is the unramified extension of L_1 of degree $\frac{e}{(e,r)} = \mathrm{o}(v^f)$. Let $\tilde{\tilde{H}} = \mathrm{Gal}(L_2/K)$ and $\tilde{\tilde{L}} = \tilde{L}L_2$. Since $\tilde{\tilde{H}}$ is the Galois group of a split tame extension, we have

$$\tilde{\tilde{H}} = \langle\tilde{\tau}\rangle \rtimes \langle\tilde{v}\rangle$$

with $\mathrm{o}(\tilde{\tau}) = e_{L_2/K} = e_{L_1/K}$, $\mathrm{o}(\tilde{v}) = f_{L_2/K}$ and $\tilde{v}\tilde{\tau}\tilde{v}^{-1} = \tilde{\tau}^q$. The particular choice of L_2 implies that $\mathrm{Gal}(L_2/L_1) = \langle\tilde{v}^f\rangle$.



It easy to see that $\mathrm{Gal}(\tilde{\tilde{L}}/L_2) \simeq G_t \simeq (\mathbb{Z}/p\mathbb{Z})^\ell$, $\mathrm{Gal}(\tilde{\tilde{L}}/L) \simeq \tilde{\tilde{H}}$ and thus $\mathrm{Gal}(\tilde{\tilde{L}}/K) \simeq G_t \rtimes_\rho \tilde{\tilde{H}}$. This means that there exists a representation ρ of $\tilde{H}$ of dimension ℓ over $\mathbb{F}_p$ which factors through $\tilde{H} \simeq \tilde{\tilde{H}}/\langle\tilde{v}^f\rangle$ and the induced map $\bar{\rho}\colon \tilde{H} \to \mathrm{GL}(\ell, \mathbb{F}_p)$ must give the action of $\tilde{H}$ on G_t. ρ is irreducible, since otherwise G_t would have a proper $\tilde{H}$-submodule, but not necessarily faithful. Nevertheless, since the action of $\tilde{H}$ on G_t is faithful and being L_2/L_1 the unramified extension of L_1 degree $\frac{e}{(e,r)}$, ρ is still faithful in $\langle\tilde{\tau}\rangle$ and $\mathrm{Ker}\rho = \langle\tilde{v}^f\rangle$. In fact, since ρ factors through $\tilde{H}$, $\mathrm{Ker}\rho \supseteq \langle\tilde{v}^f\rangle$ and since $\bar{\rho}$ is injective being the action of $\tilde{H}$ faithful on G_t, $\mathrm{Ker}\rho = \langle\tilde{v}^f\rangle$.

The advantage of passing from $\tilde{H}$ to $\tilde{\tilde{H}}$ is explained by the following

Lemma 1 *Every irreducible representation V over $\mathbb{F}_p$ of $\langle\nu\rangle \rtimes_\mu \langle\eta\rangle$, where $\mu(\eta)$ is the elevation to p^{f_K} and which is faithful on $\langle\nu\rangle$, is the sum of the conjugates of an irreducible representation over $\overline{\mathbb{F}}_p$, which is induced from a 1-dimensional representation of $\langle\nu\rangle \rtimes \langle\eta_c\rangle$, where $\langle\eta_c\rangle = C_{\langle\eta\rangle}(\langle\nu\rangle)$ and ν and η_c act as multiplication by α and β, respectively.*

Moreover, the following equation holds

$$\dim_{\mathbb{F}_p} V = \mathrm{lcm}\left(\frac{rw}{(r, f_K)}, r\right) \tag{1}$$

where $r = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ and $w = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$.

Proof See for example [4]. □

By Lemma 1, there exist $\alpha, \beta \in \overline{\mathbb{F}}_p^*$ such that ρ is the sum of the conjugates of the representation obtained by induction from the 1-dimensional representation on which $\tilde{\tau}$ and $\tilde{v}_c$ (with $\langle \tilde{v}_c \rangle = C_{\langle \tilde{v} \rangle}(\langle \tilde{\tau} \rangle)$ act as multiplication by α and β, respectively. Moreover, by Eq. (1), α and β are such that

$$\ell = \text{lcm}\left(\frac{rw}{(r, f_K)}, r\right).$$

Therefore, we must have $r = 1$ or $r = \ell$ (and also $w = 1$ or $w = \ell$). This means that our representations over $\mathbb{F}_p$ are either the sum of the ℓ conjugates of a 1-dimensional representation defined over $\mathbb{F}_{p^\ell}$, or it is the only conjugate of an induced representation from a 1-dimensional one.

Since $\tilde{H}$ is isomorphic to $\tilde{\tilde{H}}/\ker\rho$, we are interested in the image of $\tilde{\tilde{H}}$ under ρ.

If $r = 1$ then $\alpha \in \mathbb{F}_p^*$, i.e. $e = \mathrm{o}(\tilde{\tau}) = \mathrm{o}(\alpha) \mid p - 1$, therefore $\tilde{\tau}^q = \tilde{\tau}$ so that $\tilde{\tilde{H}}$ is abelian. It follows that the image of $\tilde{\tilde{H}}$ under ρ is cyclic, isomorphic to the subgroup of $\mathbb{F}_{p^\ell}^*$ generated by α and β. Therefore, in this case $L_1 \subseteq F$.

If $r = \ell$, then we have to distinguish two cases: $\ell \mid f_K$ and $\ell \nmid f_K$. In the first case, we have again $\tilde{\tau}^q = \tilde{\tau}$ and hence $\tilde{\tilde{H}}$ abelian; since $r = \ell$, by the same argument of the previous case, $\tilde{H}$ is isomorphic to a subgroup of $\mathbb{F}_{p^\ell}^*$. If $\ell \nmid f_K$, then $\tilde{v}$ acts as elevation to p and $\tilde{\tilde{H}}$ is not abelian. But $\langle \tilde{\tau} \rangle \rtimes \langle \tilde{v}^\ell \rangle$ is abelian and its image under ρ is cyclic, isomorphic to the subgroup C of $\mathbb{F}_{p^\ell}^*$ generated by α and β. The group $\tilde{\tilde{H}}$ has a subgroup isomorphic to the quotient $\frac{\tilde{\tilde{H}}}{\langle \tilde{\tau} \rangle \rtimes \langle \tilde{v}^\ell \rangle} \simeq \frac{\langle \tilde{v} \rangle}{\langle \tilde{v}^\ell \rangle} \simeq \mathbb{Z}/\ell\mathbb{Z}$, which acts on $\langle \tilde{\tau} \rangle \rtimes \langle \tilde{v}^\ell \rangle$ as elevation to p so that the image of $\tilde{\tilde{H}}$ under ρ is isomorphic to a subgroup of

$$C \rtimes \mathrm{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p)$$

with $C < \mathbb{F}_{p^\ell}^*$. Therefore again, we find that L_1 is contained in F.

It follows that $\tilde{L} = LL_1 \subseteq LF$. $\tilde{L}/L_1$ is totally and wildly ramified since L/K is, therefore $\tilde{L} \cap F = L_1$ and $\mathrm{Gal}(LF/F) \simeq G_t$. This means that LF/F is an elementary abelian extension of degree p^ℓ. Thus, by Kummer theory, $LF = F(\sqrt[p]{\Xi})$ for some subgroup Ξ of F^*/F^{*p} of dimension ℓ as $\mathbb{F}_p$-vector space. Moreover, LF/K is Galois because $LF = \tilde{L}F$ and $\tilde{L}/K$ and F/K are Galois, so Ξ is a H-module (the action of H being that induced by the action on F^*) and it is irreducible because otherwise G_t would have a proper $\tilde{H}$-submodule.

Note that the conjugates of L over K are exactly the extensions which lead to the H-module Ξ with this construction. Thus we can define a map Ψ from the set of the isomorphism classes of p^ℓ-extensions of K having no intermediate fields to the set of the irreducible H-submodules of F^*/F^{*p} of dimension ℓ over $\mathbb{F}_p$.

Conversely, we show that each irreducible H-submodule of dimension ℓ of F^*/F^{*p} corresponds to the isomorphism class of an extension of degree p^ℓ of K having no subextensions. Note that $p \nmid \mathrm{o}(H)$ since F is the composite of normal extensions of degree prime to p.

Let Ξ be an irreducible H-submodule of F^*/F^{*p} which has dimension ℓ as vector space over $\mathbb{F}_p$. Put $M = F(\sqrt[p]{\Xi})$, then M/K is a Galois extension and $S = \mathrm{Gal}(M/F)$ is a H-module which is irreducible because Ξ is. Let $\mathfrak{G}$ be the Galois group of M/K. Since S is a normal subgroup of $\mathfrak{G}$ of order p^ℓ and $\mathfrak{G}/S \simeq H$ has order prime to p, by Schur-Zassenhaus theorem we have $\mathfrak{G} \simeq S \rtimes H$. Let L be the fixed field of H; the fields fixed by the conjugates of H in $\mathfrak{G}$ form the isomorphism class of the extension L/K. Each of these extensions has degree p^ℓ and has no intermediate extensions. In fact, let T be such that $K \subseteq T \subseteq L$; T is the field fixed by a subgroup C of $\mathfrak{G}$, and since $L \supseteq T$ we have $C \supseteq H$. Therefore, $C \simeq S_0 \rtimes H$ with $S_0 < S$, but S is irreducible as H-module so $S_0 = \{1\}$ or $S_0 = S$ i.e. $T = L$ or $T = K$.

It follows that we can define a map Φ from the set of the irreducible H-submodules of dimension ℓ of F^*/F^{*p} to the set of the isomorphism classes of p^ℓ-extensions of K having no intermediate fields.

Finally, it is easily seen that Ψ and Φ are inverse to each other.

3.1 Example

We now give a concrete example of the field F that appears in Theorem 1, in particular we determine F when $\ell = 2$. Let $F = F(K)$ be the composite of all normal extensions of K of degree prime to p whose Galois group is isomorphic to a subgroup of $\mathbb{F}^*_{p^2}$ or to a non-abelian subgroup of $\mathbb{F}^*_{p^2} \rtimes_\theta \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ where $\theta(\phi_p) = \phi_p|_{\mathbb{F}^*_{p^2}} \in \mathrm{Aut}(\mathbb{F}^*_{p^2})$ (ϕ_p the Frobenius automorphism), and let $H = \mathrm{Gal}(F/K)$ (note that if $p \neq 2$ the hypothesis about the degree is redundant). Then

Proposition 1 *If $p \neq 2$ or, $p = 2$ and $2 \mid f_K$, one has $F = K(\zeta_{q_K^{p^2-1}-1}, \pi)$ where $\pi^{p^2-1} = \pi_K$, $[F : K] = (p^2-1)^2$ and*

$$H \simeq \begin{cases} \mathbb{Z}/(p^2-1)\mathbb{Z} \times \mathbb{Z}/(p^2-1)\mathbb{Z} & if \quad 2 \mid f_K \\ \mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z} \times \mathbb{Z}/(p^2-1)\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} & if \quad 2 \nmid f_K \end{cases}$$

where in the case $2 \nmid f_K$, the nonzero element of $\mathbb{Z}/2\mathbb{Z}$ acts trivially on $\mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$ and as multiplication by p on $\mathbb{Z}/(p^2-1)\mathbb{Z}$.

If $p = 2$ and $2 \nmid f_K$, one has $F = K(\zeta_{q_K^3-1})$, $[F : K] = 3$ and $H \simeq \mathbb{Z}/3\mathbb{Z}$.

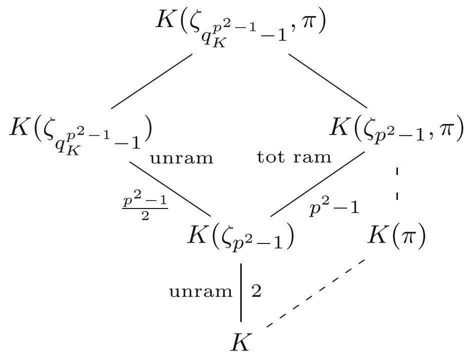
Proof The case $p = 2$ and $2 \nmid f_K$ is simple because $\mathbb{F}_4^* \rtimes \mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2) \simeq S_3$ has only one subgroup of odd order, that is the cyclic group of order 3, and since $\zeta_3 \notin K$ there is only one normal extension of degree 3 of K, that is the unique unramified one. The claim about the Galois group is then trivial.

To prove the remaining part of the proposition it is useful to distinguish two cases: $2 \mid f_K$ and, $2 \nmid f_K$ and $p \neq 2$.

If $2 \mid f_K$ then K contains the (p^2-1)th roots of unity. Therefore, the unramified extension $K(\zeta_{q_K^{p^2-1}-1})/K$ and the totally ramified extension $K(\pi)/K$ are both cyclic of order p^2-1, so that $K(\zeta_{q_K^{p^2-1}-1}, \pi) \subseteq F$. We must show the inverse inclusion. Let L/K be a normal extension with Galois group isomorphic to a subgroup of $\mathbb{F}^*_{p^2}$ or to a non-abelian subgroup of $\mathbb{F}^*_{p^2} \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$, and let e and f be its ramification index and inertial degree, respectively. By basic theory, $L = K(\zeta_{q_K^f-1}, \pi_L)$ where π_L is a root of the polynomial $X^e - u\pi_K$, for some root of unity u in $K(\zeta_{q_K^f-1})$. The thesis follows if we show that $K(\zeta_{q_K^f-1}) \subseteq K(\zeta_{q_K^{p^2-1}-1})$ and that u is a eth power in $K(\zeta_{q_K^{p^2-1}-1})$, i.e. $K(\zeta_{q_K^{p^2-1}-1})$ contains the $e(q_K^f-1)$th roots of unity. This last is equivalent to show that $e(q_K^f-1) \mid q_K^{p^2-1}-1$. If L/K is cyclic, then $ef \mid p^2-1$, and in particular $e \mid p^2-1$ and $f \mid p^2-1$ therefore $K(\zeta_{q_K^f-1}) \subseteq K(\zeta_{q_K^{p^2-1}-1})$. Moreover, $q_K^{p^2-1}-1 = q_K^{eft}-1 = (q_K^f-1)((q_K^f)^{et-1}+\cdots+1)$ and the factor to the right is the sum of et addends, each of which is congruent to 1 modulo e because $q_K \equiv 1 (\mathrm{mod}\ e)$ since $2 \mid f_K$ and $p^2 \equiv 1 (\mathrm{mod}\ e)$. So we have proved that $L \subseteq K(\zeta_{q_K^{p^2-1}-1}, \pi)$. Now we show that if $2 \mid f_K$, then there exists no extension L/K such that $\mathrm{Gal}(L/K) \simeq D \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ with $D < \mathbb{F}_{p^2}^* \backslash \mathbb{F}_p^*$, thus proving that $F \subseteq K(\zeta_{q_K^{p^2-1}-1}, \pi)$. If $p = 2$, this is trivial since $\mathbb{F}_4^* \rtimes \mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2) \simeq S_3$ has no not cyclic subgroup of odd order. If $p \neq 2$, it suffices to observe that every quotient $\mathrm{Gal}(L/K)/G_0$ acts trivially on the inertia subgroup G_0. This is true because one can easily see that, since $D \nsubseteq \mathbb{F}_p^*$ the only normal and cyclic subgroups of $D \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ are the subgroups of $D \subseteq \mathbb{F}_{p^2}^*$, therefore G_0 can be embedded in $\mathbb{F}_{p^2}^*$ and the Frobenius $\phi_{q_K} = \phi_{p^{f_K}}$ acts trivially on it since f_K is even.

Thus $F = K(\zeta_{q_K^{p^2-1}-1}, \pi)$ and, since the extensions $K(\zeta_{q_K^{p^2-1}-1})/K$ and $K(\pi)/K$ are linearly disjoint, we have $[F : K] = (p^2 - 1)^2$ and $H \simeq (\mathbb{Z}/(p^2 - 1)\mathbb{Z})^2$.

If $2 \nmid f_K$ and $p \neq 2$ then K does not contain the $(p^2 - 1)$th roots of unity. The unramified extension $K(\zeta_{q_K^{p^2-1}-1})/K$ is again cyclic of order $p^2 - 1$, while the totally ramified extension $K(\pi)/K$ is not cyclic (it is not even Galois). Nevertheless, $K(\zeta_{q_K^{p^2-1}-1}, \pi)/K$ is the composite of $K(\zeta_{q_K^{p^2-1}-1})/K$ with the normal extension $K(\zeta_{p^2-1}, \pi)$, and this last is of the type asked because $\mathrm{Gal}(K(\zeta_{p^2-1}, \pi)/K) \simeq \mathbb{F}_{p^2}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$.



So again $K(\zeta_{q_K^{p^2-1}-1}, \pi) \subseteq F$, it remains to prove the inverse inclusion. Let L/K be a normal extension with $\mathrm{Gal}(L/K)$ isomorphic to a subgroup of $\mathbb{F}_{p^2}^*$ or to a non-abelian subgroup of $\mathbb{F}_{p^2}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$, e and f its ramification index and inertial degree, respectively. As usual we can write $L = K(\zeta_{q_K^f-1}, \pi_L)$ where π_L is a root of the polynomial $X^e - u\pi_K$, for some root of unity u in $K(\zeta_{q_K^f-1})$, thus we must show that $K(\zeta_{q_K^f-1}) \subseteq K(\zeta_{q_K^{p^2-1}-1})$ and that $K(\zeta_{q_K^{p^2-1}-1})$ contains the $e(q_K^f - 1)$th roots of unity. If L/K is cyclic, then $ef \mid p^2 - 1$, therefore $K(\zeta_{q_K^f-1}) \subseteq K(\zeta_{q_K^{p^2-1}-1})$ and, like the previous case, $q_K^{p^2-1} - 1 = q_K^{eft} - 1 = (q_K^f - 1)((q_K^f)^{et-1} + \cdots + 1)$ with the factor to the right divisible by e since it is the sum of et addends, each of which is congruent to 1 modulo e because $q_K^f \equiv 1 (\mathrm{mod}\, e)$ since $L/K(\zeta_{q_K^f-1})$ is cyclic and thus $K(\zeta_{q_K^f-1})$ contains the eth roots of unity. So $L \subseteq K(\zeta_{q_K^{p^2-1}-1}, \pi)$. Suppose now that $\mathrm{Gal}(L/K) \simeq D \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ with $D < \mathbb{F}_{p^2}^* \backslash \mathbb{F}_p^*$. Since the only normal and cyclic subgroup of $D \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ are those of D, the inertia subgroup G_0 is contained in $D \subseteq \mathbb{F}_{p^2}^*$ so $|G_0| = e \mid p^2 - 1$; moreover, $\mathrm{Gal}(L/K)/G_0$ is a cyclic group of order f, and therefore it is contained in the biggest abelian quotient of $D \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ whose order, as one can easily

see, divides p^2-1. It follows that necessarily $f \mid p^2-1$ and thus $K(\zeta_{q_K^f-1}) \subseteq K(\zeta_{q_K^{p^2-1}-1})$. From $e \mid p^2-1$, we also have $2 \mid f$; it follows that $K(\zeta_{q_K^f-1})$ (and hence L) contains the cyclic subextension $K(\zeta_{p^2-1})/K$ of order 2 and $\mathrm{Gal}(K(\zeta_{q_K^f-1}, \pi_L)/K(\zeta_{p^2-1})) \simeq D$; therefore, for the previous case $K(\zeta_{q_K^f-1}, \pi_L)$ is contained in $K(\zeta_{q_K^{p^2-1}-1}, \pi)$. This concludes the proof that $F \subseteq K(\zeta_{q_K^{p^2-1}-1}, \pi)$.
Finally, observe that F is the composite of the Galois extensions $K(\zeta_{q_K^{p^2-1}-1})/K$ and $K(\zeta_{p^2-1}, \pi)/K$ and that $K(\zeta_{q_K^{p^2-1}-1}) \cap K(\zeta_{p^2-1}, \pi) = K(\zeta_{p^2-1})$. We have that $K(\zeta_{q_K^{p^2-1}-1})/K(\zeta_{p^2-1})$ is cyclic of order $\frac{p^2-1}{2}$ and $K(\zeta_{p^2-1}, \pi)/K(\zeta_{p^2-1})$ is cyclic of order p^2-1, thus $[F:K] = \frac{p^2-1}{2}(p^2-1)2 = (p^2-1)^2$ and $\mathrm{Gal}(F/K) \simeq \mathrm{Gal}(\mathbb{F}_{q_K^{p^2-1}}/\mathbb{F}_{q_K^2}) \times \mathbb{F}_{p^2}^* \rtimes \mathrm{Gal}(\mathbb{F}_{q_K^2}/\mathbb{F}_{q_K})$; taking into account that $2 \nmid f_K$ it is easy to see that this group is isomorphic to that in the claim. □

4 Counting the isomorphism classes

We now return to the general case in which ℓ is an arbitrary prime number.

Theorem 1 says that to count the number of isomorphism classes of extensions of K of degree p^ℓ it suffices to count the number of irreducible representations of H of dimension ℓ in the $\mathbb{F}_p$-vector space F^*/F^{*p}. To do this, we need some information about H.

Note that H is the Galois group of a finite tame extension therefore, as observed in the proof of the Theorem 1, it has the following form

$$\langle v, \tau \mid v\tau v^{-1} = \tau^q, \tau^e = 1, v^f = \tau^r \rangle$$

where $e := e_{F/K}$, $f := f_{F/K}$, $q := p^{f_K}$ and r is the smallest positive integer such that $v^f = \tau^r$, and the extension F/K is always contained in a split one, i.e. in a tame extension whose Galois group is a semidirect product of the inertia subgroup and its complement. Since this tame split extension is of degree prime to p and unramified over F, the Theorem 1 still holds if we put it in place of F, as one can easily see by the proof of the same Theorem. With abuse of notation, we continue to denote by F this split tame extension of K and by H its Galois group over K.

So we can suppose that $H = H_0 \rtimes U$ where $H_0 = \langle \tau \rangle$ and $U = \langle v \rangle$ are cyclic of order e and f, respectively, $(e, p) = 1$, $e \mid q^f - 1$ and v acts on H_0 via the map $x \mapsto x^q$. This group satisfies the hypothesis of Lemma 1, which describes its representations over $\mathbb{F}_p$.

For convenience, we now describe in more details the irreducible representations of H over $\mathbb{F}_p$.

The irreducible representations of such a group over $\overline{\mathbb{F}}_p$ are easy to describe; using this description we determine that contained in the module obtained from F^*/F^{*p} by extension of scalar, and from these we recover the irreducible representation of H over $\mathbb{F}_p$ contained in F^*/F^{*p}.

First of all, we can observe that to study the irreducible representation ρ of $H_0 \rtimes U$ one can study the irreducible representation $\bar{\rho}$ of $\bar{H}_0 \rtimes U$, where $\bar{H}_0 = H_0/\ker(\rho_{|H_0})$.

As one can easily see for example in [4], all irreducible representations ρ of $H_0 \rtimes U$ in a $\overline{\mathbb{F}}_p$-vector space are induced from 1-dimensional representations of the abelian group $H_0 \rtimes \tilde{U}$, where $\tilde{U} = \langle \tilde{v} \rangle$ is the centralizer of $\bar{H}_0$ in U. In particular, if $\rho\colon H_0 \rtimes U \longrightarrow \mathrm{GL}(W)$

is an irreducible representation, then $\rho = \mathrm{Ind}_{H_0 \times \tilde{U}}^{H_0 \rtimes U}(W_\chi)$ where W_χ is a 1-dimensional $\overline{\mathbb{F}}_p$-subspace of W on which $H_0 \times \tilde{U}$ acts by the character χ. Moreover, if $\alpha = \chi(\tau)$ and $\beta = \chi(\tilde{v})$, then there is a basis of W with respect to τ and v act on W via the matrices

$$T_\alpha = \begin{pmatrix} \alpha & & & & \\ & \alpha^q & & & \\ & & \alpha^{q^2} & & \\ & & & \ddots & \\ & & & & \alpha^{q^{s-1}} \end{pmatrix}, \quad V_\beta = \begin{pmatrix} & & & \beta \\ 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

where s is the index of $\tilde{U}$ in U.

It easy to see that conjugate characters lead to the same representation on W.

Now, the second step is to pass from the irreducible representations over $\overline{\mathbb{F}}_p$ to the irreducible representations over $\mathbb{F}_p$. These last are sums of the conjugates of irreducible representations over $\overline{\mathbb{F}}_p$. If φ is an irreducible representation of $H_0 \rtimes U$ over an $\mathbb{F}_p$-vector space V, then it is the sum of the conjugates of an irreducible representation over $\overline{\mathbb{F}}_p$ which, as written above, is induced from a 1-dimensional one, and one has

$$\dim_{\mathbb{F}_p} V = \mathrm{lcm}\left(\frac{rw}{(r, f_K)}, r\right) \tag{2}$$

where $r = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ and $w = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$.

Finally, it remains to identify the irreducible representations of $H_0 \rtimes U$ over the $\mathbb{F}_p$-vector space F^*/F^{*p}. For what we have said above, we first identify those over the $\overline{\mathbb{F}}_p$-vector space $F^*/F^{*p} \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$ obtained from F^*/F^{*p} by extension of scalar and then recover from these the irreducible representations over F^*/F^{*p}.

4.1 The structure of F^*/F^{*p} as $\mathbb{F}_p[H]$-module

This section is due to the work of Del Corso et al. [4], so for more details one can see their paper.

We describe the irreducible representations of H of any dimension $k \geq 2$ contained in F^*/F^{*p}, while in the next section we specialize to $k = \ell$ prime.

Recall that we are interested in representations of $H = H_0 \rtimes U = \langle\tau\rangle \rtimes \langle v\rangle$ in a subspace of dimension k of F^*/F^{*p}, that is to say in the $\mathbb{F}_p[H]$-submodules of F^*/F^{*p} of dimension k.

If π is a uniformizer of F and U_1 denotes the group of principal units of F, it is well known that

$$F^* \simeq \langle\pi\rangle \times \kappa_F^* \times U_1$$

as H- modules, and that U_1 has a filtration $\{U_i\}_{i\geq 1}$, where $U_i = \{u \in F^* | u \equiv 1 (\mathrm{mod}\ \pi^i)\}$. It follows that

$$F^*/F^{*p} \simeq \langle\pi\rangle/\langle\pi\rangle^p \times U_1/U_1^p$$

as $\mathbb{F}_p[H]$-modules. The filtration $\{U_i\}_{i\geq 1}$ of U_1 induces the filtration $\{U_i U_1^p/U_1^p\}_{i\geq 1}$ of U_1/U_1^p and, as U_{i+1} is complemented in U_i as H-module, also $U_{i+1}U_1^p/U_1^p$ is complemented in $U_i U_1^p/U_1^p$ as $\mathbb{F}_p[H]$-module. So one has

$$F^*/F^{*p} \simeq \langle\pi\rangle/\langle\pi\rangle^p \oplus \bigoplus_{i=1}^{\infty} U_i U_1^p/U_{i+1}U_1^p.$$

The nonzero terms in the right-hand side are those with $i = pe_F/(p-1)$ and, $0 < i < pe_F/(p-1)$ with $(i, p) = 1$ (see for example [5]). Then the above relation can be written as

$$F^*/F^{*p} \simeq \langle\pi\rangle/\langle\pi\rangle^p \oplus \bigoplus_{i\in[\![0,I_F]\!]} U_iU_1^p/U_{i+1}U_1^p \oplus U_{I_F}U_1^p/U_1^p.$$

where $I_F = pe_F/(p-1)$ and $[\![0, I_F]\!]$ is the set of integers prime with p in the interval $]0, I_F[$.

We want to describe the representations of H contained in F^*/F^{*p}. To do this, observe that the action of H on $\langle\pi\rangle/\langle\pi\rangle^p \simeq \mathbb{F}_p$ is clearly trivial and that $U_{I_F}U_1^p/U_1^p$ corresponds via Kummer theory to the Galois unramified extension of degree p, so the action of H on this submodule of dimension 1 of F^*/F^{*p} is given by the cyclotomic character ω. Since we are interesting in the irreducible subrepresentations of dimension $k \geq 2$, we can reduce to consider those contained in $\bigoplus_{i\in[\![0,I_F]\!]} U_iU_1^p/U_{i+1}U_1^p$.

We need to study the structure of $U_iU_1^p/U_{i+1}U_1^p$ as $\mathbb{F}_p[H]$-module. Since F/K is a tamely ramified extension, we can choose as a uniformizer π of F an eth root of a uniformizer of K, where clearly $e = e_{F/K}$. Then for $i \geq 1$, each element of U_i/U_{i+1} can be written as $1 + \epsilon\pi^i$ with $\epsilon \in U_0$ ($U_0 = \mathcal{O}_F^*$ is the multiplicative subgroup of the ring of the integers of F). The action of H on it is given by

$$\tau(1+\epsilon\pi^i) = 1 + \zeta^i\epsilon\pi^i + \cdots, \qquad \upsilon(1+\epsilon\pi^i) = 1 + \epsilon^q\pi^i + \cdots,$$

where $\zeta = \tau(\pi)/\pi$ is a primitive eth root of 1. As usual, one can identify U_i/U_{i+1} with κ_F via the map

$$1 + \epsilon\pi^i \mapsto \bar{\epsilon}$$

and this induces on κ_F the following action of H

$$\tau(\bar{\epsilon}) = \bar{\zeta}^i\bar{\epsilon}, \qquad \upsilon(\bar{\epsilon}) = \bar{\epsilon}^q.$$

Denote by M_i the $\mathbb{F}_p[H]$-module formed by the $\mathbb{F}_p$-module κ_F with the above action of H. It is clear that

$$U_iU_1^p/U_{i+1}U_1^p \simeq M_i$$

as $\mathbb{F}_p[H]$-modules. So we search the irreducible $\mathbb{F}_p[H]$-submodules of $\bigoplus_{i\in[\![0,I_F]\!]} M_i$ or, equivalently, the irreducible representations of H over $\mathbb{F}_p$ contained in $\bigoplus_{i\in[\![0,I]\!]} M_i$ (viewed as $\mathbb{F}_p$-vector space). To do this, we first extend the $\mathbb{F}_p$-representation M_i of H to an $\overline{\mathbb{F}}_p$-representation, identify its $\overline{\mathbb{F}}_p$ subrepresentations and from each of these find the $\mathbb{F}_p$ subrepresentations via the sum of its conjugates.

Let $\overline{M}_i = M_i \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$ be the extension of M_i to the algebraic closure of $\mathbb{F}_p$.

It can be shown that

$$\overline{M}_i \simeq \bigoplus_{\substack{\beta\in\overline{\mathbb{F}}_p \\ \beta^{f/s}=1}} J_{(\alpha,\beta)}{}^{f_K} \tag{3}$$

where $f = f_{F/K}, s = [U : \tilde{U}]$ and $J_{(\alpha,\beta)} = \mathrm{Ind}_{H_0\times\tilde{U}}^H(V_{(\alpha,\beta)})$ is the irreducible s-dimensional representation over $\overline{\mathbb{F}}_p$ induced from the 1-dimensional representation on which τ and $\tilde{\upsilon}$ act via multiplication by $\alpha = \zeta^i$ and β, respectively.

Let $Y = \bigoplus_{i \in [\![0, I_F]\!]} \overline{M}_i$, then $J_{(\alpha,\beta)}$ appears $n_K = [K : \mathbb{Q}_p]$ times in Y. In fact, the i's such that $\zeta^i = \alpha$ have equal remainder modulo e; being $(e, p) = 1$ those in $]0, I_F[$ and prime with p are exactly e_K. Multiplying by the exponent of $J_{(\alpha,\beta)}$ that appears in (3) we have the claim.

Moreover, as observed in the previous section, the s conjugated pairs (α^{q^i}, β) yield the same representation, therefore the multiplicity of $J_{(\alpha,\beta)}$ in Y is sn_K.

It is easy to see that the representation $J_{(\alpha,\beta)}$ has

$$d = \operatorname{lcm}(w, (r, f_K))$$

conjugates over $\mathbb{F}_p$, where $r = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ and $w = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$ as above, and so it is defined over $D = \mathbb{F}_{p^d}$. Moreover, a short reflection leads to observe that $s = [U : \tilde{U}]$ is equal to $\frac{r}{(r, f_K)}$ since U acts on H_0 as elevation to q and therefore s is the smallest power of q such that $e \mid q^s - 1$.

Let X be an irreducible subrepresentation of Y defined over $\mathbb{F}_p$ and containing a unique copy of $J_{(\alpha,\beta)}$. From each copy of $J_{(\alpha,\beta)}$ contained in Y and defined over D, we obtain a representation isomorphic to X. Consequently, to count the subrepresentations isomorphic to X and defined over $\mathbb{F}_p$ is the same as to count the subrepresentations that are isomorphic to $J_{(\alpha,\beta)}$ and defined over D. This can be made counting the subrepresentations contained in $(J_{(\alpha,\beta)})^{sn_K}$ and working over D. Let us consider the immersions

$$J_{(\alpha,\beta)} \longrightarrow (J_{(\alpha,\beta)})^{sn_K}$$

which are defined over D. Using Schur lemma, we find that the number of immersions is $|D|^{sn_K} - 1$ and this number must be divided by $|D| - 1$ when taking into account that two immersions have the same image if and only if they differ by multiplication by a constant. It follows that the number of representations defined over $\mathbb{F}_p$ and containing a representation isomorphic to $J_{(\alpha,\beta)}$ is $\frac{p^{dsn_K}-1}{p^d-1}$.

4.2 The total number of isomorphism classes of extensions of degree p^ℓ of K

Let V be an irreducible $\mathbb{F}_p[H]$-submodule of F^*/F^{*p} of dimension ℓ. From what we have said above, viewing V as irreducible representation of H over $\mathbb{F}_p$, it is isomorphic to the sum of the conjugates over $\mathbb{F}_p$ of an irreducible representation of H over $\overline{\mathbb{F}}_p$, which we have denoted by $J_{(\alpha,\beta)}$. If $r = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ and $w = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$, by Eq. (2), we have

$$\dim_{\mathbb{F}_p} V = \operatorname{lcm}\left(\frac{rw}{(r, f_K)}, r\right) = \ell, \tag{4}$$

therefore $r = 1$ or $r = \ell$. It follows that $s = \frac{r}{(r, f_K)} = 1$ or $s = \ell$. We must distinguish two cases: $\ell \mid f_K$ and $\ell \nmid f_K$.

If $\ell \mid f_K$, then r and w must be equal to 1 or ℓ and at least one of them must be equal to ℓ. It follows that we have exactly $(p^\ell - 1)^2 - (p - 1)^2$ possible pairs (α, β); moreover, since $s = \frac{r}{(r, f_K)} = 1$, for each of them there are $\frac{p^{\ell n_K}-1}{p^\ell-1}$ representations over $\mathbb{F}_p$ containing a representation isomorphic to $J_{(\alpha,\beta)}$. Finally, we have to take in account that the pairs $(\alpha, \beta), (\alpha^p, \beta^p), \ldots, (\alpha^{p^{\ell-1}}, \beta^{p^{\ell-1}})$ lead to the same representation over $\mathbb{F}_p$.

Collecting all the information, we find that if $\ell \mid f_k$, there are exactly

$$\frac{1}{\ell} \frac{p^{\ell n_K} - 1}{p^\ell - 1}((p^\ell - 1)^2 - (p - 1)^2)$$

isomorphism classes of extensions of degree p^ℓ of K having no intermediate fields.

If $\ell \nmid f_K$ then Eq. (4) says that one of r and w must be 1 and the other ℓ.

For $r = 1$ and $w = \ell$, we have again $s = \dim J_{(\alpha,\beta)} = 1$ and $d = \ell$ therefore, for each of the $(p-1)(p^\ell-1)-(p-1)^2$ possible choices of (α, β), there are $\frac{p^{\ell n_K}-1}{p^\ell-1}$ $\mathbb{F}_p$-representations containing a representation isomorphic to $J_{(\alpha,\beta)}$, and for the same reason as above this number must be divided by ℓ. So for $\alpha \in \mathbb{F}_p^*$ and $\beta \in \mathbb{F}_{p^\ell}^*$ we have $\frac{1}{\ell}\frac{p^{\ell n_K}-1}{p^\ell-1}(p-1)(p^\ell-p)$ irreducible representations of H of dimension ℓ over the $\mathbb{F}_p$-vector space F^*/F^{*p}.

To these, we have to add that obtained from $r = \ell$ and $w = 1$. In this case, $s = \ell$ and $d = 1$ i.e. $J_{(\alpha,\beta)}$ is already defined over $\mathbb{F}_p$, therefore for each of the $(p^\ell - 1)(p - 1) - (p - 1)^2$ possible pairs (α, β) there are $\frac{p^{\ell n_K}-1}{p-1}$ representations isomorphic to $J_{(\alpha,\beta)}$. This value needs to be divided by ℓ because from the definition of $J_{(\alpha,\beta)}$ one has $J_{(\alpha,\beta)} = J_{(\alpha^p,\beta)} = \cdots = J_{(\alpha^{p^{\ell-1}},\beta)}$. It follows that for $\alpha \in \mathbb{F}_{p^\ell}^*$ and $\beta \in \mathbb{F}_p^*$ there are $\frac{1}{\ell}(p^{\ell n_K} - 1)(p^\ell - p)$ irreducible representations of H of dimension ℓ over F^*/F^{*p}.

Adding the two contributions one finds

$$\frac{1}{\ell}(p^{\ell n_K} - 1)(p^\ell - p) + \frac{1}{\ell}\frac{p^{\ell n_K} - 1}{p^\ell - 1}[(p - 1)(p^\ell - 1) - (p - 1)^2]$$
$$= \frac{1}{\ell}\frac{p^{\ell n_K} - 1}{p^\ell - 1}[(p^\ell - 1)^2 - (p - 1)^2]$$

isomorphism classes of extensions of degree p^ℓ of K having no intermediate fields.

Note that we have obtained the same number of isomorphism classes of extensions as in the case $\ell \mid f_K$.

Examples Using the above formula, we find that there are 16 classes of extensions of degree $2^3 = 8$ of the field $\mathbb{Q}_2$ with no intermediate extensions, and 224 classes of extensions of degree $3^3 = 27$ of the field $\mathbb{Q}_3$ with no intermediate extensions.

4.3 The number of isomorphism classes of extensions whose normal closure has a prescribed Galois group

In the previous section, we have counted all the isomorphism classes of extensions of degree p^ℓ of K having no intermediate fields. To each of them, we can associate a group, that is the Galois group of the normal closure of the extensions over K. It turns that some isomorphism classes are associated with the same group, i.e. non-isomorphic p^ℓ-extensions of K can have normal closure with the same Galois group.

In this section, we identify all possible groups that can appear as the Galois group of the normal closure of a p^ℓ-extension of K having no intermediate fields, and for each of them we count the number of isomorphism classes of extensions which are associated with it.

First of all observe that if L/K is a p^ℓ-extension having no intermediate fields and $\tilde{L}$ is its normal closure then, by Theorem 1,

$$\mathrm{Gal}(\tilde{L}/K) \simeq V \rtimes_{\bar{\rho}} \bar{H}$$

where $\bar{\rho}$ is the map induced on the quotient $\bar{H} = H/\ker\rho$ and the pair (V, ρ) is the representation of dimension ℓ of H in F^*/F^{*p}, which correspond to the class of L/K under the correspondence of Theorem 1. In other words, $\mathrm{Gal}(\tilde{L}/K)$ is the semidirect product of V with the biggest quotient of H acting faithfully on it.

Fixing a basis of the $\mathbb{F}_p$-vector space V, we can identify the image of ρ with a subgroup of $\mathrm{GL}(\ell, \mathbb{F}_p)$, so that $\mathrm{Gal}(\tilde{L}/K) \simeq (\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_\rho$ where $\mathcal{H}_\rho$ represents the action of $\bar{H}$ on V given by $\bar{\rho}$, expressed with respect to the fixed basis.

Now observe that for what we have said above, our representations are sums of the conjugates of s-dimensional representations $J_{(\alpha,\beta)}$, where $s = 1$ or $s = \ell$ and $\alpha, \beta \in \mathbb{F}_{p^\ell}^*$: if $s = 1$ then $J_{(\alpha,\beta)}$ is defined over $\mathbb{F}_{p^\ell}$ and $\bar{H}$ is abelian, so $\mathcal{H}_\rho = \mathcal{H}_{(\alpha,\beta)}$ is cyclic since it is isomorphic to the homomorphic image of a finite group in $\mathrm{GL}(1, \mathbb{F}_{p^\ell}) = \mathbb{F}_{p^\ell}^*$; if $s = \ell$, then $J_{(\alpha,\beta)}$ is already defined over $\mathbb{F}_p$, but the group $\mathcal{H}_{(\alpha,\beta)}$ of the matrices which describes the action of $\bar{H}$ is not abelian.

The normal closures of two isomorphism classes have the same Galois group if and only if

$$(\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_{(\alpha,\beta)} \simeq (\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_{(\alpha',\beta')}$$

and this happens if and only if the two subgroups $\mathcal{H}_{(\alpha,\beta)}, \mathcal{H}_{(\alpha',\beta')}$ of $\mathrm{GL}(\ell, \mathbb{F}_p)$ are conjugated over $\mathrm{GL}(\ell, \mathbb{F}_p)$. In fact, if $\sigma : (\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_{(\alpha,\beta)} \longrightarrow (\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_{(\alpha',\beta')}$ is an isomorphism then for every $A \in \mathcal{H}_{(\alpha,\beta)}$ the following diagram must be commutative

$$\begin{array}{ccc} \mathbb{F}_p^\ell & \xrightarrow{A} & \mathbb{F}_p^\ell \\ {\scriptstyle \sigma|_{\mathbb{F}_p^\ell}}\downarrow & & \downarrow{\scriptstyle \sigma|_{\mathbb{F}_p^\ell}} \\ \mathbb{F}_p^\ell & \xrightarrow[\sigma(A)]{} & \mathbb{F}_p^\ell \end{array}$$

where $\sigma|_{\mathbb{F}_p^\ell} \in \mathrm{Aut}(\mathbb{F}_p^\ell)$ and thus can be expressed as an invertible matrix in $\mathrm{GL}(\ell, \mathbb{F}_p)$.

To classify the various case depending on the value of $s = r/(r, f_K)$, we must distinguish two different situations: $\ell \mid f_K$ and $\ell \nmid f_K$.

For what will follow, it is convenient to introduce the function $\psi(a, b)$ that maps $(a, b) \in \mathbb{N} \times \mathbb{N}$ to the number of elements of order a in the group $C_a \times C_b$. It can be expressed as

$$\psi(a, b) = a \cdot (a, b) \cdot \prod_{\substack{l \text{ prime} \\ l \mid (a,b)}} \left(1 - \frac{1}{l^2}\right) \cdot \prod_{\substack{l \text{ prime} \\ l \mid a \\ l \nmid (a,b)}} \left(1 - \frac{1}{l}\right).$$

Moreover, for every c dividing $p^\ell - 1$ we define the function $\lambda(c, p)$ as

$$\lambda(c, p) = \begin{cases} 1 & \text{if} \quad p \equiv 2, \ldots, \ell - 1 \pmod{\ell} or \\ & \mathrm{p} \equiv 1 \pmod{\ell} \text{and, } v_\ell(c) = 0 \text{ or } v_\ell(c) = v_\ell(p^\ell - 1) \\ \frac{1}{\ell} & \text{if} \quad p \equiv 1 \pmod{\ell} \text{and} v_\ell(p-1) < v_\ell(c) < v_\ell(p^\ell - 1) \\ \frac{1}{\ell+1} & \text{if} \quad p \equiv 1 \pmod{\ell} \text{and} v_\ell(c) \le v_\ell(p-1) \end{cases} \tag{5}$$

CASE $\ell \mid f_K$.

Theorem 2 *Let K be a p-adic field, f_K its inertial degree over $\mathbb{Q}_p$ and n_K its absolute degree. Let ℓ be a prime number and suppose that $\ell \mid f_K$. Then the Galois group of the normal closure of a p^ℓ-extension of K having no intermediate fields is of type $\mathbb{F}_{p^\ell}^+ \rtimes C$, where C is a subgroup of $\mathbb{F}_{p^\ell}^*$ not contained in $\mathbb{F}_p^*$ with the natural action on $\mathbb{F}_{p^\ell}^+$.*

Moreover, for every integer c dividing $p^\ell - 1$ but not $p - 1$, if C is the cyclic subgroup of $\mathbb{F}_{p^\ell}^*$ of order c, then there are

$$n(c) = \frac{1}{\ell}\psi(c, p^\ell - 1)\frac{p^{\ell n_K} - 1}{p^\ell - 1}$$

classes of isomorphic p^ℓ-extensions of K having no intermediate fields whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^\ell}^+ \rtimes C$.

Proof Since ℓ is a prime number, from (2) it follows that in this case for the dimension to be ℓ we need r, w equal to 1 or ℓ and at least one to be equal to ℓ. Moreover, for every α and β satisfying this condition, we always have $\dim J_{(\alpha,\beta)} = s = \frac{r}{(r, f_K)} = 1$. It follows that $\mathcal{H}_{(\alpha,\beta)}$ is generated by the diagonal matrices

$$\begin{pmatrix} \alpha & & & \\ & \alpha^p & & \\ & & \ddots & \\ & & & \alpha^{p^{\ell-1}} \end{pmatrix}, \quad \begin{pmatrix} \beta & & & \\ & \beta^p & & \\ & & \ddots & \\ & & & \beta^{p^{\ell-1}} \end{pmatrix}$$

and therefore it is isomorphic to the cyclic subgroup of $\mathbb{F}_{p^\ell}^*$ generated by α and β. Therefore, the only case in which $(\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_{(\alpha,\beta)} \simeq (\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_{(\alpha',\beta')}$ is when $\{\alpha, \beta\}$ and $\{\alpha', \beta'\}$ generate groups of the same order.

Note that if α and β generate the cyclic subgroup C of $\mathbb{F}_{p^\ell}^*$ then $(\mathbb{F}_p^+)^\ell \rtimes \mathcal{H}_{(\alpha,\beta)} \simeq \mathbb{F}_{p^\ell}^+ \rtimes C$, where C acts in the natural way on $\mathbb{F}_{p^\ell}^+$.

Let $c \mid p^\ell - 1$ but $c \nmid p - 1$, then the number of pairs (α, β) in $\mathbb{F}_{p^\ell}^* \times \mathbb{F}_{p^\ell}^*$ having order c is equal to $\psi(c, p^\ell - 1)$. Since $s = 1$ for each of them, the number of representations in F^*/F^{*p} defined over $\mathbb{F}_p$ and containing a representation isomorphic to $J_{(\alpha,\beta)}$ is $(p^{\ell n_K} - 1)/(p^\ell - 1)$. Observe that we need to count together (α, β), (α^p, β^p) $\ldots$ $(\alpha^{p^{\ell-1}}, \beta^{p^{\ell-1}})$ since they lead to the same representation over $\mathbb{F}_p$, so we must divide by ℓ.

It follows that if C is the cyclic group of order c in $\mathbb{F}_{p^\ell}^*$, the number of classes of extensions whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^\ell}^+ \rtimes C$ (where C acts naturally on $\mathbb{F}_{p^\ell}^+$) is exactly

$$\frac{1}{\ell}\psi(c, p^\ell - 1)\frac{p^{\ell n_K} - 1}{p^\ell - 1}.$$

The groups of type $\mathbb{F}_{p^\ell}^+ \rtimes C$ with $C < \mathbb{F}_{p^\ell}^*$ are the only groups that can appear as Galois group of the normal closure of a p^ℓ-extension of K having no intermediate fields when $\ell \mid f_K$. □

CASE $\ell \nmid f_K$.

Theorem 3 *Let K be a p-adic field, f_K its inertial degree over $\mathbb{Q}_p$ and n_K its absolute degree. Let ℓ be a prime number and suppose that $\ell \nmid f_K$. Then the Galois group of the normal closure of a p^ℓ-extension of K having no intermediate fields is either of type $\mathbb{F}_{p^\ell}^+ \rtimes C$, where C is a subgroup of $\mathbb{F}_{p^\ell}^*$ not contained in $\mathbb{F}_p^*$ (with the natural action on $\mathbb{F}_{p^\ell}^+$), or of type $\left(\mathbb{F}_p\right)^\ell \rtimes \mathcal{H}$, where $\mathcal{H} \subseteq \mathrm{GL}(\ell, \mathbb{F}_p)$ is isomorphic to a non-abelian subgroup of $\mathbb{F}_{p^\ell}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p)$.*

Moreover,

- *for every integer c dividing $p^\ell - 1$ but not $p - 1$, if C is the cyclic subgroup of $\mathbb{F}_{p^\ell}^*$ of order c, then there are*

$$n(c) = \frac{1}{\ell}\psi(c, p - 1)\frac{p^{\ell n_K} - 1}{p^\ell - 1}$$

classes of isomorphic p^ℓ-extensions of K having no intermediate fields whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^\ell}^+ \rtimes C$;

– *for every non-abelian subgroup $\mathcal{H} \subseteq \mathrm{GL}(\ell, \mathbb{F}_p)$ isomorphic to a subgroup Z of $\mathbb{F}_{p^\ell}^* \rtimes \mathrm{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p)$, if $C = Z \cap \mathbb{F}_{p^\ell}^*$ has order c then there are*

$$n(\mathcal{H}) = \begin{cases} \lambda(c, p)\psi(c, p-1)\frac{1}{\ell}\frac{p^{\ell n_K}-1}{p-1} & if\ C \to Z\, splits \\ \frac{1-\lambda(c,p)}{\ell-1}\psi(c, p-1)\frac{1}{\ell}\frac{p^{\ell n_K}-1}{p-1} & if\ C \to Z\, doesnotsplit \end{cases}$$

classes of isomorphic p^ℓ-extensions of K having no intermediate fields whose normal closure has Galois group isomorphic to $\left(\mathbb{F}_p\right)^\ell \rtimes \mathcal{H}$.

Proof Since $\ell \nmid f_K$ from (2), the dimension of a representation of a quotient $\bar{H}$ over $\mathbb{F}_p$ is ℓ when one of r, w is 1 and the other ℓ.

For $r = 1$ and $w = \ell$, i.e. for the pairs α, β with $\alpha \in \mathbb{F}_p^*$ and $\beta \in \mathbb{F}_{p^\ell}^*$, it turns out again $\dim J_{(\alpha,\beta)} = s = 1$ so, as above, the group $\mathcal{H}_{(\alpha,\beta)}$ acting in the representation is cyclic of order equal to the order of (α, β) in $(\mathbb{F}_p^* \times \mathbb{F}_{p^\ell}^*)\backslash(\mathbb{F}_p^* \times \mathbb{F}_p^*)$ and for each pair (α, β) there are $(p^{\ell n_K} - 1)/(p^\ell - 1)$ representations over $\mathbb{F}_p$ containing a unique copy of $J_{(\alpha,\beta)}$.

Let $c \mid p^\ell - 1$ but $c \nmid p-1$, the possible pairs (α, β) in $\mathbb{F}_p^* \times \mathbb{F}_{p^\ell}^*$ of order c are $\psi(c, p-1)$. Thus, similarly to above, if C is the cyclic group of order c in $\mathbb{F}_{p^\ell}^*$, then the number of classes of extensions whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^\ell}^+ \rtimes C$ is

$$\frac{1}{\ell}\psi(c, p-1)\frac{p^{\ell n_K} - 1}{p^\ell - 1}.$$

For $r = \ell$ and $w = 1$, we have $\dim J_{(\alpha,\beta)} = s = \frac{r}{(r, f_K)} = \ell$ and $J_{(\alpha,\beta)}$ is already defined over $\mathbb{F}_p$. It follows that the group $\mathcal{H}_{(\alpha,\beta)}$ coincides with the group of matrices which describe the action on $J_{(\alpha,\beta)}$.

Recalling that $q = p^{f_K}$ and $\ell \nmid f_K$, from the study of the representations of H, we have made at the beginning of Sect. 4, we find that the action on $J_{(\alpha,\beta)}$ is described by the matrices

$$T_\alpha = \begin{pmatrix} \alpha & & & \\ & \alpha^p & & \\ & & \ddots & \\ & & & \alpha^{p^{\ell-1}} \end{pmatrix}, \quad V_\beta = \begin{pmatrix} & & \beta \\ 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}.$$

So $\mathcal{H}_{(\alpha,\beta)} = \langle T_\alpha, V_\beta \rangle$ is a non-abelian group. Moreover, the number of representations contained in F^*/F^{*p} isomorphic to $J_{(\alpha,\beta)}$ is exactly $(p^{\ell n_K} - 1)/(p-1)$. This number must be divided by ℓ when taking into account that the pairs $(\alpha, \beta), (\alpha^p, \beta) \ldots (\alpha^{p^{\ell-1}}, \beta)$ in $\mathbb{F}_{p^\ell}^* \times \mathbb{F}_p^*$ give the same representation.

It remains to multiply by the number of pairs (α', β') such that $(\mathbb{F}_p^+)^\ell \rtimes \langle T_{\alpha'}, V_{\beta'} \rangle \simeq (\mathbb{F}_p^+)^\ell \rtimes \langle T_\alpha, V_\beta \rangle$. For what we have remarked above, this means that we have to count the number of pairs $(\alpha', \beta') \in \mathbb{F}_{p^\ell}^* \times \mathbb{F}_p^*$ such that $\langle T_{\alpha'}, V_{\beta'} \rangle$ and $\langle T_\alpha, V_\beta \rangle$ are conjugated in $\mathrm{GL}(\ell, \mathbb{F}_p)$ (note that this is equivalent to require that they are conjugated in $\mathrm{GL}(\ell, \mathbb{F}_{p^\ell})$).

It turns out that $\mathcal{H}_{(\alpha,\beta)}$ is conjugated to $\mathcal{H}_{(\alpha',\beta')}$ if only if there exists a matrix $M \in \mathrm{GL}(\ell, \mathbb{F}_p)$ such that $M^{-1}\mathcal{H}_{(\alpha,\beta)}M = \mathcal{H}_{(\alpha',\beta')}$ and diagonal matrices are sent in diagonal matrices.

In fact, the subgroup of the diagonal matrices of $\mathcal{H}_{(\alpha,\beta)}$ is generated by T_α and V_β^ℓ, and it is a maximal cyclic subgroup $\langle T_\gamma \rangle$ of $\mathcal{H}_{(\alpha,\beta)}$ of order equal to $\mathrm{o}(\gamma) = \mathrm{lcm}(\mathrm{o}(\alpha), \mathrm{o}(\beta))$ and index

ℓ. Suppose that $\mathcal{H}_{(\alpha,\beta)}$ and $\mathcal{H}_{(\alpha',\beta')}$ are conjugated, and then the maximal cyclic subgroups of the diagonal matrices have the same order, and in particular they are equal since they are isomorphic to the same subgroup of $\mathbb{F}^*_{p^\ell}$ via the same map. Therefore, $\mathcal{H}_{(\alpha,\beta)} = \langle T_\gamma, V_\beta\rangle$ and $\mathcal{H}_{(\alpha',\beta')} = \langle T_\gamma, V_{\beta'}\rangle$.

Now, $\mathcal{H}_{(\alpha,\beta)}$ and $\mathcal{H}_{(\alpha',\beta')}$ have either only one maximal cyclic subgroup, that is the subgroup of the diagonal matrices, or $\ell + 1$ maximal cyclic subgroups (one of which is that of the diagonal matrices). In the first case, there is nothing to prove since clearly all the conjugations send diagonal matrices in diagonal matrices. For the second case, observe that by the proof of Theorem 1, $\mathcal{H}_{(\alpha,\beta)}$ is isomorphic to $\langle(\gamma, \mathrm{id}), (\gamma, \phi_p)\rangle \subseteq \mathbb{F}^*_{p^\ell} \rtimes \mathrm{Gal}(\mathbb{F}_{p^\ell}/\mathbb{F}_p)$, i.e. it is isomorphic to a subgroup of the normalizer of a Cartan subgroup of $\mathrm{GL}(\ell, \mathbb{F}_p)$.

The key point is to observe that there always exists a basis under which (γ, id) and (γ, ϕ_p) are represented by the generators of any two cyclic subgroups of index ℓ of $\mathcal{H}_{(\alpha,\beta)}$ and every pairs of these matrices generate the whole group $\mathcal{H}_{(\alpha,\beta)}$. This is enough to prove that we can suppose not only $\langle T_\gamma\rangle$ is sent in $\langle T_\gamma\rangle$ but also that $\langle T_{\alpha^\ell}, V_\beta\rangle$ goes in $\langle T_{\alpha'^\ell}, V_{\beta'}\rangle$.

Therefore, there exists a diagonal matrix $D = T^i_\alpha V^{\ell j}_\beta \in \mathcal{H}_{(\alpha,\beta)}$ such that $M^{-1}(DV_\beta)M = V_{\beta'}$. This leads to

$$\beta' = \gamma^{p^{\ell-1}+\cdots+p+1}\beta,$$

where recall that $\gamma \in \mathbb{F}^*_{p^\ell}$ has order $\mathrm{lcm}(\mathrm{o}(\alpha), \mathrm{o}(\beta)) = \mathrm{lcm}(\mathrm{o}(\alpha'), \mathrm{o}(\beta'))$.

Consequently, the Galois group is identified by the order of the cyclic group $C = \langle\gamma\rangle \subseteq \mathbb{F}^*_{p^\ell}$ and the class of β in $(C \cap \mathbb{F}^*_p)/C^{p^{\ell-1}+\cdots+p+1}$.

Let c be the order of C. Since

$$(p-1, p^{\ell-1} + \cdots + p + 1) = \begin{cases} \ell & \text{if} \quad p \equiv 1 \pmod{\ell} \\ 1 & \text{if} \quad p \equiv 2, \ldots, \ell-1 \pmod{\ell} \text{ or } p = \ell \end{cases}$$

we have

$$\left|\frac{C \cap \mathbb{F}^*_p}{C^{p^{\ell-1}+\cdots+p+1}}\right| = \begin{cases} \ell & \text{if } p \equiv 1 \pmod{\ell} \text{ and } 0 < v_\ell(c) < v_\ell(p^\ell - 1) \\ 1 & \text{otherwise.} \end{cases}$$

Clearly, if $|(C \cap \mathbb{F}^*_p)/C^{p^{\ell-1}+\cdots+p+1}| = 1$, then there is only one class mod $C^{p^{\ell-1}+\cdots+p+1}$, therefore every pairs (α, β) such that α and β generate C give (class of) extensions with isomorphic Galois groups.

We now consider the case $|(C \cap \mathbb{F}^*_p)/C^{p^{\ell-1}+\cdots+p+1}| = \ell$.

Suppose $\ell^k \parallel c$, then $\beta \in C^{p^{\ell-1}+\cdots+p+1}$ if and only if its order is not divisible by a power of ℓ greater than $\ell^k/(\ell^k, p^{\ell-1} + \cdots + p + 1)$.

On the other hand, we have that $\beta \in C^{p^{\ell-1}+\cdots+p+1}$ if and only if the map $C \hookrightarrow \langle T_\alpha, V_\beta\rangle$ splits (with abuse of notation, we have identified C we its image in $\langle T_\alpha, V_\beta\rangle$). In fact, this map splits if and only if β has an ℓ-root in C, i.e. there exists $t \in C$ such that $t^\ell = \beta$. This is equivalent to say that there exists $r \in C$ such that $r^{p^{\ell-1}+\cdots+p+1} = \beta$ since $C^{p^{\ell-1}+\cdots+p+1} = (C \cap \mathbb{F}^*_p)^{p^{\ell-1}+\cdots+p+1} = (C \cap \mathbb{F}^*_p)^\ell$.

We write $\mathbb{F}^*_{p^\ell} \times \mathbb{F}^*_p$ as direct sum of l-groups for each prime l and chose the components of (α, β) in this sum among the elements of the correct order. For what we have said above, for $l \neq \ell$ the choice of the l-component of (α, β) has no effect on the condition $\beta \in C^{p^{\ell-1}+\cdots+p+1}$.

For $l = \ell$, the ℓ-part of $\mathbb{F}_{p^\ell}^* \times \mathbb{F}_p^*$ is $C_{\ell^{m+z}} \times C_{\ell^z}$ where $\ell^m \parallel p^{\ell-1} + \cdots + p + 1$ and $\ell^z \parallel p - 1$. Recall that $\ell^k \parallel c$ for some $1 \le k < m + z$. Since we are in the case $(p-1, p^{\ell-1} + \cdots + p + 1) = \ell$, we have $z = 1$ or $m = 1$.

If $z = 1$, then $C^{p^{\ell-1}+\cdots+p+1}$ is trivial, therefore $\beta \in C^{p^{\ell-1}+\cdots+p+1}$ when the ℓ-component of (α, β) is of type $(x, 1)$, and this happens for $\frac{\phi(\ell^k)}{\ell\phi(\ell^k)} = \frac{1}{\ell}$ of the possible ℓ-components when $k > 1$ and for $\frac{\ell-1}{\ell^2-1} = \frac{1}{\ell+1}$ of the possible ℓ-components when $k = 1$.

If $m = 1$, then $\beta \in C^{p^{\ell-1}+\cdots+p+1}$ if its order is not divisible by a power of ℓ greater than ℓ^{k-1}, therefore the ℓ-component of (α, β) must be of type (x, y) with the order of x greater than the order of y; this is true for $\frac{\phi(\ell^k)\ell^{k-1}}{2\phi(\ell^k)\ell^k - \phi(\ell^k)^2} = \frac{1}{\ell+1}$ of the elements with correct order.

Recollecting all the information achieved, we have that if λ is the function defined in (5), then $\lambda(c, p)\psi(c, p-1)$ is the number of pairs (α, β) such that the group C generated by α and β has order c and $\beta \in C^{p^{\ell-1}+\cdots+p+1}$, while $(1 - \lambda(c, p))\psi(c, p-1)$ counts the same pairs but with $\beta \notin C^{p^{\ell-1}+\cdots+p+1}$.

Finally, to conclude the proof it remains to observe that the β's not contained in $C^{p^{\ell-1}+\cdots+p+1}$ are equally distributed in each of the $\ell - 1$ non-trivial class mod $C^{p^{\ell-1}+\cdots+p+1}$. □

5 Ramification groups and discriminant of the composite of all p^ℓ-extensions of K

We know that there is a one-to-one correspondence between the isomorphism classes of extensions of degree p^ℓ of K having no intermediate extensions and the irreducible H-submodules of dimension ℓ of F^*/F^{*p}, or equivalently, the abelian p^ℓ-extensions of F of exponent p, Galois over K, having no intermediate subextensions that are Galois over K.

Denote by $\mathscr{C}_{p^\ell}$ the composite of all extensions of degree p^ℓ of K having no intermediate fields. Clearly $\mathscr{C}_{p^\ell}/K$ is Galois, we want to determine the ramification groups of its Galois group.

Let $\mathscr{G} = \mathrm{Gal}(\mathscr{C}_{p^\ell}/K)$, as usual for $i \ge -1$ we denote by $\mathscr{G}_i$ the ith ramification group of $\mathscr{G}$.

Lemma 2 *One has*

$$\mathscr{C}_{p^\ell} = \mathscr{A}_F^{(p^\ell)}$$

where $\mathscr{A}_F^{(p^\ell)}$ is the composite of all abelian p^ℓ extensions of F of exponent p having no other subextensions that are Galois over K.

Proof If L/K is a p^ℓ-extension having no intermediate fields, then LF is contained in $\mathscr{A}_F^{(p^\ell)}$ (see proof of Theorem 1), therefore $\mathscr{C}_{p^\ell} \subseteq \mathscr{A}_F^{(p^\ell)}$.

Conversely, let E be an abelian p^ℓ-extension of F of exponent p, Galois over K but having no subextensions that are Galois over K. As seen in the proof of Theorem 1, $\mathrm{Gal}(E/K) \simeq \Xi \rtimes H$ where Ξ is the $\mathbb{F}_p[H]$-submodule of F^*/F^{*p} of dimension ℓ which corresponds to E/K, E^H is contained in $\mathscr{C}_{p^\ell}$ and $E^H F = E$.

The Galois closure of E^H over K is also contained in $\mathscr{C}_{p^\ell}$ (being $\mathscr{C}_{p^\ell}/K$ Galois), and it is the composite of E^H with a suitable subextension of F/K, which is then contained in

$\mathscr{C}_{p^\ell}$. Since as E varies through the elements of $\mathscr{A}_F^{(p^\ell)}$ with E/K Galois these subextensions generate F, we have $F \subseteq \mathscr{C}_{p^\ell}$ and hence $E \subseteq \mathscr{C}_{p^\ell}$.

Finally, observe that these extensions E are sufficient to generate $\mathscr{A}_F^{(p^\ell)}$, thus we have $\mathscr{A}_F^{(p^\ell)} \subseteq \mathscr{C}_{p^\ell}$. □

Lemma 2 implies that $\mathscr{C}_{p^\ell}/F$ is a subextension of $\mathscr{A}_F/F$, where $\mathscr{A}_F$ is the maximal abelian extension of F of exponent p. Thus $[\mathscr{C}_{p^\ell} : F] = p^t$ for some $t \leq n_F + 2$ (see [3]). By Kummer theory, we know that $\mathscr{C}_{p^\ell}$ corresponds to a subgroup of F^*/F^{*p} and $[\mathscr{C}_{p^\ell} : F]$ is equal to the order of this subgroup (clearly F contains the pth roots of 1).

Proposition 2 *One has*

$$[\mathscr{C}_{p^\ell} : F] = \begin{cases} p^{((p^\ell-1)^2-(p-1)^2)n_K} & \text{if } \ell \mid f_K \\ p^{(\ell+1)(p^\ell-p)(p-1)n_K} & \text{if } \ell \nmid f_K \end{cases}.$$

Proof By Lemma 2, $[\mathscr{C}_{p^\ell} : F] = [\mathscr{A}_F^{(p^\ell)} : F]$ and $\mathscr{A}_F^{(p^\ell)} = F(\sqrt[p]{\Delta})$, where Δ is the $\mathbb{F}_p[H]$-submodule of F^*/F^{*p} generated by the irreducible submodules of dimension ℓ. It follows that $[\mathscr{C}_{p^\ell} : F]$ is the order of Δ.

Δ can be generated by a finite number of disjoint irreducible $\mathbb{F}_p[H]$-submodules of dimension ℓ, clearly if m is this number then $[\mathscr{C}_{p^\ell} : F] = p^{\ell m}$.

We know that

$$F^*/F^{*p} \simeq \mathbb{F}_p \oplus \bigoplus_{i\in[\![0,I_F]\!]} M_i \oplus M_\omega$$

as $\mathbb{F}_p[H]$-modules; the $\mathbb{F}_p[H]$-modules of dimension ℓ are contained in $\bigoplus_{i\in[\![0,I_F]\!]} M_i$. Moreover, we know that a similar module V is the sum of the conjugates of a certain $J_{(\alpha,\beta)}$ which is an $\overline{\mathbb{F}}_p[H]$-submodule of $\overline{M}_i = M_i \oplus_{\mathbb{F}_p} \overline{\mathbb{F}}_p$; as α and β vary in $\mathbb{F}_{p^\ell}^*$ we find all the irreducible representation of dimension ℓ contained in F^*/F^{*p}. The multiplicity of V in $\bigoplus_{i\in[\![0,I_F]\!]} M_i$ is equal to that of $J_{(\alpha,\beta)}$ in $Y = \bigoplus_{i\in[\![0,I_F]\!]} \overline{M}_i$, it counts the number of disjoint $\mathbb{F}_p$-vector space (resp. $\overline{\mathbb{F}}_p$-vector space) in F/F^{*p} on which H acts as on V (resp. $J_{(\alpha,\beta)}$).

In particular, if $\ell \mid f_K$, then to achieve $\mathbb{F}_p$-representation of dimension ℓ we must have $(\alpha,\beta) \in (\mathbb{F}_{p^\ell}^* \times \mathbb{F}_{p^\ell}^*)\backslash(\mathbb{F}_p^* \times \mathbb{F}_p^*)$ and for each of these pairs $J_{(\alpha,\beta)}$ has dimension 1 and multiplicity n_K. As usual observe that the $\mathbb{F}_p$-representation containing $J_{(\alpha,\beta)}$ is equal to that containing its other $\ell-1$ conjugates that is $J_{(\alpha^p,\beta^p)}, \ldots, J_{(\alpha^{p^{\ell-1}},\beta^{p^{\ell-1}})}$. Therefore, we have

$$m = \frac{1}{\ell}[(p^\ell-1)^2 - (p-1)^2]n_K.$$

If $\ell \nmid f_K$, then only one between α and β is in $\mathbb{F}_{p^\ell}^*\backslash\mathbb{F}_p^*$ and the other in $\mathbb{F}_p^*$. The $J_{(\alpha,\beta)}$'s with $\alpha \in \mathbb{F}_{p^\ell}^*$ and $\beta \in \mathbb{F}_p^*$ have no conjugates different from itself and multiplicity ℓn_K, but $J_{(\alpha,\beta)} = J_{(\alpha^p,\beta)} = \cdots = J_{(\alpha^{p^{\ell-1}},\beta)}$. While the $J_{(\alpha,\beta)}$'s with $\alpha \in \mathbb{F}_p^*$ and $\beta \in \mathbb{F}_{p^\ell}^*$ have multiplicity n_K and ℓ conjugates like the previous case. Thus we have

$$m = (p^\ell - p)(p-1)n_K + \frac{1}{\ell}(p-1)(p^\ell - p)n_K.$$

Substituting in $[\mathscr{C}_{p^\ell} : F] = p^{\ell m}$, we obtain the thesis. □

Observe that by the Theorem 1 $\mathscr{G} \simeq G \rtimes H$, where G is the Galois group of $\mathscr{C}_{p^\ell}$ over F. It is well known that $\mathscr{G}_{-1} = \mathscr{G}$, $\mathscr{G}_0$ is the inertia subgroup of $\mathscr{G}$ and $\mathscr{G}_1$ is the p-Sylow subgroup

of $\mathcal{G}_0$. Since $\mathcal{C}_{p^\ell}/F$ has no unramified subextensions being the composite of totally ramified extensions, $\mathcal{G}_0$ is isomorphic to $G \rtimes H_0$ where H_0 is the inertia subgroup of H, while $\mathcal{G}_i \simeq G_i$ for all $i \geq 1$ since F/K is tame.
It is suitable to search the upper numbering ramification groups because, if L is a Galois extension of F contained in $\mathcal{C}_{p^\ell}$ and $G_L = \mathrm{Gal}(\mathcal{C}_{p^\ell}/L)$, then for all v one has $(G/G_L)^v \simeq G^v G_L/G_L$ (see [12], Ch. IV, §3, Prop. 14) and, in our case, if also L has degree p^ℓ over F and is Galois over K the groups $(G/G_L)^v$ are easy to describe.

Lemma 3 *Let*

$$d = \begin{cases} ((p^\ell - 1)^2 - (p-1)^2)n_K & \text{if } \ell \mid f_K \\ (\ell+1)(p^\ell - p)(p-1)n_K & \text{if } \ell \nmid f_K \end{cases}$$

One has

$$\dim_{\mathbb{F}_p} G^v = \begin{cases} d & \text{if } -1 \leq v \leq 1 \\ d - \left(\lceil v \rceil - \left\lceil \frac{v}{p} \right\rceil\right) f_F & \text{if } 1 < v \leq \frac{pe_F}{p-1} - 1 \\ 0 & \text{if } v > \frac{pe_F}{p-1} - 1 \end{cases}$$

Proof First of all observe that $\mathcal{C}_{p^\ell}/F$ is a totally and wildly ramified extension, therefore $G_{-1} = G_0 = G_1 = G$; moreover, a simple calculation of the Herbrand's function (see [12], Ch. IV, §3) yields to $G^1 = G_1$ so that for $-1 \leq v \leq 1$ one has $G^v = G = \mathrm{Gal}(\mathcal{C}_{p^\ell}/F)$ and $\dim_{\mathbb{F}_p} G^v = d$. Moreover, since $\mathcal{C}_{p^\ell}/F$ is an elementary abelian p-extension, by Theorem 12 of [1], for every $v > pe_F/p - 1$ we have $G^v = 1$, i.e. $\dim_{\mathbb{F}_p} G^v = 0$. It remains to determine $\dim_{\mathbb{F}_p} G^v$ when $1 < v \leq pe_F/p - 1$.

Let L be an abelian p^ℓ-extension of F of exponent p having no subextensions that are Galois over K and let $G_L = \mathrm{Gal}(\mathcal{C}_{p^\ell}/L)$.

As remarked before, we know that for all v one has $(G/G_L)^v \simeq G^v G_L/G_L$, hence

$$G^v = \bigcap_{(G/G_L)^v = 1} G_L.$$

Via Galois theory, this group corresponds to $\mathcal{C}_{p^\ell}^{G^v} = \prod L$, with the composite taken over the abelian p^ℓ-extensions L/F satisfying the previous condition, i.e. such that $(G/G_L)^v = 1$. It follows that $\dim_{\mathbb{F}_p} G^v$ is equal to d minus the dimension of the $\mathbb{F}_p$-vector space associated to $\prod L$ by Kummer theory.

Since $G/G_L \simeq \mathrm{Gal}(L/F) \simeq (\mathbb{Z}/p\mathbb{Z})^\ell$, by Proposition 7 in [1] L/F has an upper ramification jump in t if and only if there exists a subextension N/F of degree p with upper ramification jump equal to t; moreover, the jumps can only appear in the integers t such that $1 \leq t \leq pe_F/p - 1$ and $(t, p) = 1$. Therefore, for all $v > pe_F/p - 1$, $(G/G_L)^v = 1$ for every abelian p^ℓ-extension L/F.

Let v be a real number such that $1 < v \leq pe_F/p - 1$, then $G^v = G^{\lceil v \rceil}$ and $G^{\lceil v \rceil}$ is the subgroup of G fixing the composite of all the abelian p^ℓ-extensions L/F which have a jump in $\mathcal{J} = \{1, \ldots, \lceil v \rceil - 1\}$. Using Proposition 14 of [1] and the analysis of the possible representation associated to L, we have made in Sect. 4.1, we find that there are f_F disjoint extensions L/F which has a jump in a fixed $t \in \mathcal{J}$ and $(t, p) = 1$. Since the possible t are $\lceil v \rceil - \left\lceil \frac{v}{p} \right\rceil$, we have the thesis. □

Note that our results are in agreement with Lemma 9 of [3].

We can now prove the following

Proposition 3 *Let d be as in previous Lemma 3. The ramification groups $\mathscr{G}_i$ of $\mathscr{C}_{p^\ell}/K$ are:*

$$\begin{aligned}
\mathscr{G}_{-1} &= \mathscr{G} = G \rtimes H \\
\mathscr{G}_0 &= G \rtimes H_0 \\
\mathscr{G}_i &= (\mathbb{Z}/p\mathbb{Z})^{d-kf_F} && if \quad t(k-1) < i \le t(k) \\
\mathscr{G}_i &= \{e\} && if \quad i > t(e_F - 1)
\end{aligned}$$

where $t(-1) = 0, t(0) = 1$ and for every $1 \le k \le e_F - 1$,

$$t(k) = \begin{cases} t(k-1) + p^{kf_F} & if\ k \not\equiv 0 \pmod{p-1} \\ t(k-1) + 2p^{kf_F} & if\ k \equiv 0 \pmod{p-1} \end{cases}$$

Therefore, there are $e_F + 2$ jumps in the lower ramification groups.

Proof The claim for $\mathscr{G}_{-1}$ and $\mathscr{G}_0$ is clear by the considerations we have made before, $\mathscr{G}_1 = G_1$ since $\mathscr{C}_{p^\ell}/F$ is wildly ramified and so F/K is the maximal tame subextension. The rest of the Proposition follows by Lemma 3 with simple calculations, recalling that $\mathscr{G}_i = G_i$ for all $i \ge 1$ and the Herbrand's function (see [12], Ch. IV, §3)

$$G^v = G_{\psi(v)} \quad \text{with} \quad \psi(v) = \int_0^v (G^0 : G^w)\mathrm{d}w$$

which relates the upper and the lower ramification filtrations.

Lemma 3 says that G has jumps in the upper ramification in every integers of $[\![0, \frac{pe_F}{p-1}]\!]$, i.e. in the integers of the set $\{1 \le v \le \frac{pe_F}{p-1} - 1 \mid v \not\equiv 0 \pmod{p}\}$; every such jump of G gives a jump in the lower ramification of $\mathscr{G}$, and these together with -1 and 0 are exactly the $e_F + 2$ jumps of $\mathscr{G}$. □

Finally, we determine the discriminant $\mathfrak{d}_{\mathscr{C}_{p^\ell}/K}$ of $\mathscr{C}_{p^\ell}/K$.

Proposition 4 *If π_K is a uniformizer of K and $d = [\mathscr{C}_{p^\ell} : F]$ as in the previous Lemma 3 then*

$$\mathfrak{d}_{\mathscr{C}_{p^\ell}/K} = (\pi_K)^\alpha$$

where

$$\alpha = f_{F/K}\left(\left([F:K] - 1 + \frac{p(e_F+1)-1}{p-1}\right)p^d - 1 - \frac{p^{n_F}-1}{p^{f_F}-1} - \frac{p^{n_F}-1}{p^{(p-1)f_F}-1}\right).$$

Proof Using the well known formula

$$v_{\mathscr{C}_{p^\ell}}(\mathfrak{D}_{\mathscr{C}_{p^\ell}/K}) = \sum_{i=0}^{\infty}(|\mathscr{G}_i| - 1)$$

where $\mathfrak{D}_{\mathscr{C}_{p^\ell}/K}$ is the different of $\mathscr{C}_{p^\ell}/K$, one gets

$$v_{\mathscr{C}_{p^\ell}}(\mathfrak{D}_{\mathscr{C}_{p^\ell}/K}) = [F:K]p^d - 1 + \sum_{k=0}^{e_F-1}(p^{d-kf_F} - 1)p^{kf_F}$$
$$+ \sum_{\substack{k=1 \\ k\equiv 0 \pmod{p-1}}}^{e_F-1} (p^{d-kf_F} - 1)p^{kf_F}.$$

The conclusion follows by a simple calculation, recalling that $\mathfrak{d}_{\mathscr{C}_{p^\ell}/K} = N_{\mathscr{C}_{p^\ell}/K}(\mathfrak{D}_{\mathscr{C}_{p^\ell}/K})$ where $N_{\mathscr{C}_{p^\ell}/K}$ is the norm map and observing that, since $\mathscr{C}_{p^\ell}/F$ is totally ramified, $N_{\mathscr{C}_{p^\ell}/K}(\pi_{\mathscr{C}_{p^\ell}}) = (\pi_K)^{f_{F/K}}$ ($\pi_{\mathscr{C}_{p^\ell}}$ a uniformizer of $\mathscr{C}_{p^\ell}$). □

References

1. Capuano, L., Del Corso, I.: A note on upper ramification jumps in Abelian extensions of exponent *p*. Riv. Math. Univ. Parma (N.S.) **6**(2), 317–329 (2015)
2. Dalawat, C.: Serre's formule de masse in prime degree. Monatshefte für Mathematik **166**, 73–92 (2012)
3. Del Corso, I., Dvornicich, R.: The compositum of wild extensions of local fields of prime degree. Monatshefte für Mathematik **150**, 271–288 (2007)
4. Del Corso, I., Dvornicich, R., Monge, M.: On wild extension of *p*-adic field. J. Number Theory **174**, 322–342 (2017)
5. Fesenko, I., Vostokov, S.: Local Fields and Their Extensions, Translations of Mathematical Monographs, vol. 121, 2nd edn. American Mathematical Society, Providence (2002)
6. Hou, X., Keating, K.: Enumeration of isomorphism classes of extensions of *p*-adic fields. J. Number Theory **104**, 14–61 (2004)
7. Iwasawa, K.: On galois groups of local fields. Trans. Am. Math. Soc. **80**, 448–469 (1955)
8. Krasner, M.: Nombres des extensions d'un degré donné d'un corps *p*-adic. In: Les Tendances Géom. en Algèbre et Théorie des Nombres, pp. 143–169. Editions du Centre national de la Recherche Scientifique, Paris (1966)
9. Monge, M.: Determination of the number of isomorphism classes of extensions of a *p*-adic field. J. Number Theory **131**, 1429–1434 (2011)
10. Pauli, S., Roblot, X.: On the computation of all extensions of a *p*-adic field of a given degree. Math. Comput. **70**, 1641–1659 (2001)
11. Serre, J.: Une formule de masse pour les extensions totalement ramifiées de degré donné d'un corps local. C. R. Acad. Sci. Paris Sér. A B **286**, A1031–A1036 (1978)
12. Serre, J.: Local Fields, Graduate Texts in Mathematics, vol. 67. Springer, New York (1979)