ON WILD EXTENSIONS OF A p-ADIC FIELD

ILARIA DEL CORSO, ROBERTO DVORNICICH, AND MAURIZIO MONGE

Abstract. In this paper we consider the problem of classifying the isomorphism classes of extensions of degree p^k of a p-adic field K, restricting to the case of extensions without intermediate fields.

We establish a correspondence between the isomorphism classes of these extensions and some Kummer extensions of a suitable field F containing K. We then describe such classes in terms of the representations of $\mathrm{Gal}(F/K)$.

Finally, for $k = 2$ and for each possible Galois group G, we count the number of isomorphism classes of the extensions whose normal closure has a Galois group isomorphic to G. As a byproduct, we get the total number of isomorphism classes.

1. Introduction

Let p be a prime number, and let K be a p-adic field. A natural problem is to describe the set $\mathcal{E}_K(e, f)$ of all extensions of K with fixed ramification index e and inertial degree f. In this setting one may consider several questions, such as finding enumerating formulas and, more generally, characterizing subfamilies of $\mathcal{E}_K(e, f)$ whose fields share some property: for example, the valuation of the discriminant, the Galois group of the normal closure, or, more finely, the full ramification filtration. These questions are elementary in the tame case ($p \nmid e$) and definitely more complicated in the wild case ($p|e$) and have been considered, over the years, by many authors.

In 1962 Krasner [Kra62], by examining all possible Eisenstein polynomials, obtained an explicit formula for the total number of elements of $\mathcal{E}_K(e, f)$. Later on, Serre [Ser78], with a similar method, was able to refine Krasner's result by counting the elements in $\mathcal{E}_K(e, f)$ with given discriminant for all possible discriminants; in the same paper, he also showed that the distribution of the extensions in $\mathcal{E}_K(e, f)$ according to their discriminant satisfies a "mass formula" of general type.

In 2004, Hou and Keating [HK04] considered the problem of determining the number of isomorphism classes of fields in $\mathcal{E}_K(e, f)$; they found general formulas when $p^2 \nmid e$ and, under some additional assumptions on e and f, also when $p^2||e$. In 2011 one of the authors was able to deduce a formula enumerating the isomorphism classes of extensions

Date: September 12, 2016.

2010 *Mathematics Subject Classification.* 11S05, 11S15.

Key words and phrases. p-adic fields, Kummer theory, ramification theory.

of a p-adic field K with given ramification e and inertia f, for each e and f [Mon11].

In the paper [DCD07], two of the authors present a complete description of the smallest degree case for which there is wild ramification, namely the case of extensions of degree p of a p-adic field K. They introduced a suitable extension F of K over which all extensions of degree p of K become "special" Kummer extensions, in the sense that they can be recognized, among all degree p extensions of F, in terms of Galois representations (see Theorem 1.1). This method allows them to get a very detailed information on each field of the family; in particular, they derive the formula for the number of the extensions of K of degree p and of their isomorphism classes according to their discriminant. In 2010, Dalawat [Dal10] revisited the method of [DCD07], introducing a different language, and extended the main result to local fields of characteristic p.

In this paper we consider the problem of classifying the isomorphism classes of the extensions of degree p^k of a p-adic field for all $k \geq 1$. We focus on the case of extensions with no intermediate field, since in this case we are able to adapt the same scheme of proof that was used for extensions of degree p in [DCD07] and [Dal10]. An extension of Theorem 1.1 and the study of the Galois representations allows us to obtain a classification of the extensions of degree p^k in this case. Moreover, for $k = 2$ we perform more explicit computations and we find formulas for the number of extensions whose normal closure has a given Galois group.

In the following we give an account of the methods and the results of this paper. The general case turns out to be substantially more involved than the degree p case; however, since the sequence of the main steps is the same, to describe the present paper we find it useful to give first a sketch of the proof of the case $k = 1$; for details one can refer to [DCD07] and [Dal10].

The basic idea. An extension L/K of degree p is either unramified and hence cyclic, or totally ramified. In the latter case, it is well known that the Galois group of the normal closure $\tilde{L}$ of L is isomorphic to $S \rtimes_\varphi H$, where $S \cong \mathbb{Z}/p\mathbb{Z}$ is the p-Sylow subgroup and H is the subgroup fixing L; moreover, the map $\varphi : H \to \mathrm{Aut}(S) \cong \mathbb{Z}/p\mathbb{Z}^\times$ is injective and H is cyclic of order d dividing $p-1$. It is easy to see that each subgroup of index p in $S \rtimes_\varphi H$ is generated by one element of order d, and these elements are exactly the generators of the conjugates of H. Hence $\tilde{L}$ can only be obtained as the normal closure of extensions of degree p that are in the same isomorphism class.

Let F be the compositum of all extensions of K of exponent dividing $p-1$; note that F contains the p-th roots of unity. If L/K is an arbitrary extension of degree p, then the composite extension

$L_F = FL$ is clearly Galois over K. The group $\mathrm{Gal}(L_F/K)$ has a p-Sylow subgroup $\hat{S} = \mathrm{Gal}(L_F/F)$ which is normal and cyclic, and $\hat{H} = \mathrm{Gal}(L_F/L) \cong \mathrm{Gal}(F/K)$ is a complement acting on $\hat{S}$ by conjugation. The subgroup of $\hat{H}$ fixing $\tilde{L}$ is the maximal subgroup of $\hat{H}$ which is normal in $\mathrm{Gal}(L_F/K) \cong \hat{S} \rtimes \hat{H}$, so it coincides with the subgroup of $\hat{H}$ acting trivially on $\hat{S}$. It follows that from L_F one can recover $\tilde{L}$ as the field fixed by the central elements of $\mathrm{Gal}(L_F/K)$ of order prime to p.

A key point is that the set of fields L_F obtained in this way coincides with the set Ω of all extensions of degree p of F that are Galois over K (see [DCD07, Lemma 4]). By Kummer theory, the extensions of degree p of F correspond to the subgroups of order p of $F^\times/(F^\times)^p$; moreover, the elements of Ω correspond to those subgroups that are invariant under the action of $\mathrm{Gal}(F/K)$.

Let $\rho : \mathrm{Gal}(F/K) \to \mathrm{Aut}(F^\times/(F^\times)^p)$ be the representation associated to conjugation. Then the elements of Ω correspond to the irreducible representations contained in ρ (which have all degree 1).

Summarizing, we obtain the following theorem.

Theorem 1.1. *Let K be a p-adic field, and F be the compositum of all cyclic extensions of exponent $p-1$. Then we have a natural one-to-one correspondence between the isomorphism classes of extensions of degree p of K and the irreducible subspaces of the* $\mathrm{Gal}(F/K)$*-module $F^\times/(F^\times)^p$.*

To enumerate the isomorphism classes it remains to study the Galois module structure of $F^\times/(F^\times)^p$, and in particular its irreducible subspaces and their multiplicity.

Finally, we remark that in this case the correspondence can be made very explicit, and makes it possible to recover easily additional invariants of the extensions.

To generalize the result to the higher dimensional case, the first task is to find a suitable field F for which an analogue of Theorem 1.1 holds. For each degree p^k, with $k \geq 2$, restricting to the case of fields with no intermediate extension, we are able to prove that in fact there are many possible choices for F (see Section 3) .

In Section 4 we describe the $\mathrm{Gal}(F/K)$-module structure of $F^\times/F^{\times p}$ for any tame and split extension F of K. We start with the classification of the irreducible representations of $\mathrm{Gal}(F/K)$ over $\mathbb{F}_p$, via the study of the irreducible representations over $\bar{\mathbb{F}}_p$. Next, we determine the decomposition of $F^\times/F^{\times p}$ as a $\bar{\mathbb{F}}_p[\mathrm{Gal}(F/K)]$-module and then we bring back this information to get the structure of $F^\times/F^{\times p}$ as a $\mathbb{F}_p[\mathrm{Gal}(F/K)]$-module. Again, the results of this section hold for every k.

In Section 5 we focus on $k = 2$: for each possible Galois group G, we count the number of isomorphism classes of the extensions whose normal closure has a Galois group isomorphic to G. As a byproduct, we get the total number of isomorphism classes and the total number of extensions of degree p^2 without intermediate extensions.

We remark that, in principle, the results of Section 4 would allow to perform the same classification for any value of k. However, the number of cases to be examined increases with k and therefore we restricted our analysis to the case $k = 2$. Recently, M. R. Pati [Pat15], following our method, extended the classification to the case when k is any prime number.

Finally, we observe that restricting to the case of extensions without intermediate fields, has made it possible to find a tame extension F of K for which the correspondence theorem holds; in turn this yields that the Galois module structure of $F^\times/F^{\times p}$ has a very nice form. One important feature is that all representations considered are induced by representations of groups of order coprime to p. Trying to adapt the same scheme of proof to the general case, one can not hope for a tame extension F of K playing the same role, and so one has to consider representations of groups of order divisible by p.

In the case $k = 2$ we can further subdivide the extensions not considered here, into two cases: those with just one intermediate field and those with more than one. The last case can be easily dealt using the results of [DCD07], since each extension is the compositum of two extensions of degree p. The case of extensions with just one intermediate field requires different methods and will be the object of a separate paper by one of the authors.

2. Notation and preliminaries

Throughout the paper we shall use the following notation. For a p-adic field K we denote by e_K and f_K the absolute ramification index and inertial degree of K, respectively, by π_K an uniformizing element, by κ_K its residue field and we put $q_K = |\kappa_K|$.

If E/K is a finite extension we denote by $e(E/K)$ and $f(E/K)$ the ramification index and the inertial degree of the extension; if E/K is Galois with $\mathrm{Gal}(E/K) = G$, then $G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \dots$ 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.

We now recall some basic facts about the structure of the Galois group of a tamely ramified normal extension E/K (see for instance [Iwa55]). Let $G = \mathrm{Gal}(E/K)$, then $G_0 = \langle\tau\rangle$ is a cyclic group and can be canonically embedded into $\kappa_E^\times$ via the map $\sigma \mapsto \overline{\sigma(\pi_E)/\pi_E}$, which is independent of the uniformizer π_E. Moreover, G/G_0 is isomorphic to $\mathrm{Gal}(\kappa_E/\kappa_K)$, so $G/G_0 \cong \langle\phi_q\rangle$, where $q = q_K$ and ϕ_q is the Frobenius of the extension, and it acts on G_0 via $\phi_q \tau \phi_q^{-1} = \tau^q$. Since $f = f(E/K) = |G/G_0|$, we obtain that $\tau^{q^f-1} = 1$.

Let υ be a representative of ϕ_q in G; then $\upsilon^f = \tau^r$ for some r. Taking into account that τ^r commutes with υ, we have that the order of τ^r divides $q-1$, whence the order of τ, $e = e(E/K)$, divides $r(q-1)$. In particular, the Galois group of a finite tame extension is of the form

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

where e divides $\left(q^f - 1, r(q-1)\right)$.

A Galois extension E/K such that $\mathrm{Gal}(E/K)$ is a semidirect product of G_0 and a subgroup isomorphic to G/G_0 will be called a split extension. In general, a tame extension E/K need not be split; however, there always exists an unramified extension M of E such that M/K is split. In fact, let M/E be the unramified extension of degree $s = e/(e,r) = \operatorname{ord} \tau^r$. Then $M = M^{\mathrm{ur}}E$ is Galois over K, and M^{ur} and E are linearly disjoint over E^{ur}. Denote by $\tilde{\tau}$ the lifting of τ to $\mathrm{Gal}(M/K)$ that fixes M^{ur}, and by $\tilde{\upsilon}$ any lifting of υ. We have that $\tilde{\tau}$ generates the inertia subgroup, and $\tilde{\upsilon}$ satisfies $\tilde{\upsilon}^{fs} = 1$. It follows that $\mathrm{Gal}(M/K)$ is generated by $\tilde{\upsilon}, \tilde{\tau}$ with relations $\tilde{\upsilon}\tilde{\tau}\tilde{\upsilon}^{-1} = \tilde{\tau}^q$, $\tilde{\tau}^e = \tilde{\upsilon}^{fs} = 1$, and its inertia subgroup is generated by $\tilde{\tau}$. Finally, we remark, for later use, that $[M : E] = s$ is coprime to p and so if the p-core of $\mathrm{Gal}(E/K)$ (i.e., the intersection of all p-Sylow subgroups of $\mathrm{Gal}(E/K)$) is trivial, then the same is true for the p-core of $\mathrm{Gal}(M/K)$.

3. The correspondence Theorem

In this section we will state and prove the key result for the classification of the extensions. It is a direct generalization of Theorem 1.1, and it describes, for any k, the isomorphism classes $[E/K]$ of extensions of E/K of degree p^k having no intermediate extensions.

Let F be the compositum of all normal and tame extensions of K whose Galois group is a subgroup of $GL_k(\mathbb{F}_p)$ and let $H = \mathrm{Gal}(F/K)$.

Remark 3.1. Let P be a p-Sylow subgroup of H and let U/K be the maximal unramified subextension of F/K. Since F/K is tame, the degree $[F : U]$ is coprime to p. Denote by U_0 the unramified extension of K such that $[U_0 : K] = |P|$. Then U_0 is the fixed field of a normal subgroup A of H of order coprime to p, and therefore H is isomorphic to a semidirect product $A \rtimes P$.

The main result of this section is the following.

Theorem 3.2. *There exists a natural one-to-one correspondence between the isomorphism classes of extensions of degree p^k ($k \geq 1$) having no intermediate extension and the irreducible H-submodules $\Xi \subset F^\times/(F^\times)^p$ of dimension k of the Galois module $F^\times/(F^\times)^p$. The isomorphism class $[L/K]$ corresponds to Ξ where $LF = F(\Xi^{1/p})$, and* $\mathrm{Gal}(LF/K)$ *is always a split extension of* $\mathrm{Gal}(F/K)$.

One sees that this case is very similar to the case of extensions of degree p. It follows easily that the Galois group of the normal closure of an extension L/K which corresponds to Ξ is isomorphic to the semidirect product of Ξ by the smallest quotient of H acting on it.

The following lemma will be useful in the proof of the theorem.

Lemma 3.3. *Let H be finite group, and let A be a normal subgroup of H such that $|A|$ is coprime to p and H/A is a p-group. Let S be a finite dimensional irreducible representation of H over $\mathbb{F}_p$ of dimension ≥ 2. Then any extension of H by S with the given action is isomorphic to the split extension $S \rtimes H$, and the complements to S in $S \rtimes H$ are exactly the conjugates of H.*

Proof. This is essentially the same argument used in the proof of [BDar, Thm. 6.1]. Since $|S|$ and $|A|$ are relatively prime we have $H^q(A, S) = 0$ for all $q \geq 1$ (see [Ser79, Cor. 1, §2, Chap. VIII]). Consequently, we have [Ser79, Prop. 5, §6, Chap. VII] that

$$0 \to H^2(H/A, S^A) \to H^2(H, S) \to H^2(A, S) = 0,$$

is an exact sequence, hence $H^2(H/A, S^A) \cong H^2(H, S)$. We shall now show that the module S^A of A-invariants is trivial. Suppose that this is not the case: since H/A is a p-group, by the class formula, the subspace of elements of S^A fixed by H/A is non-trivial, so there exists a H/A-invariant subspace of dimension 1, contradicting the irreducibility of S. Therefore $S^A = 0$ and $0 = H^2(H/A, S^A) = H^2(H, S)$, so all the extensions of H by S are split (see [Ser79, §3, Chap. VII] for the interpretation of $H^2(H, S)$).

In the same way we obtain that $H^1(H, S) = 0$. But $H^1(H, S)$ classifies all possible splittings $H \to S \rtimes H$ of the canonical projection up to conjugacy (see [Bro82, Prop. 2.3, §2, Chap. IV]), so the only possible complements of S are the conjugates of H. □

Proof of Theorem 3.2. We first show that the compositum $L_F = LF$ is an abelian elementary p-extension of degree p^k of F. The degree $[L_F : F]$ is p^k, since L and F are linearly disjoint over K. The extension L/K is totally ramified, since otherwise it would contain an unramified subextension of degree p and hence it would have a proper subextension. Let $G = \mathrm{Gal}(\tilde{L}/K)$ be the Galois group of the normal closure $\tilde{L}$ of L/K, and let

$$G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \dots$$

be its lower numbering ramification filtration. It is well-known that for every i the subgroup G_i is normal in G, and that for $i \geq 1$ the quotient G_i/G_{i+1} is an elementary abelian p-group.

Let $\tilde{H} \subseteq G$ be the subgroup fixing L. Since L/K has no intermediate extension, $\tilde{H}$ is a maximal subgroup of G and hence there is a unique index t such that $G_{t+1} \subseteq \tilde{H}$ and $G_t\tilde{H} = G$; observe that $t \geq 1$ since L/K is a totally ramified wild extension.

Moreover, since $\tilde{L}$ is the normal closure of L/K, no subgroup of $\tilde{H}$ is normal in G. It follows that G_{t+1} and $\mathrm{Core}_G(\tilde{H})$ (that is, the intersection of all conjugates $\bigcap_{\sigma\in G} \sigma\tilde{H}\sigma^{-1}$ of $\tilde{H}$) are trivial. The centralizer $C_{\tilde{H}}(G_t)$ is trivial too, since it is contained in all the conjugates of $\tilde{H}$. It follows that G_t is a faithful $\tilde{H}$-module.

Observe now that, since G_{t+1} is trivial, G_t is an elementary abelian p-group; from $C_{\tilde{H}}(G_t) = \{1\}$ we then obtain $G_t \cap \tilde{H} = \{1\}$ and therefore G is a semidirect product $G_t \rtimes \tilde{H}$ and $|G_t| = p^k$. This implies that the module G_t is irreducible: in fact, if there would exist a proper submodule A of G_t, then $A \rtimes \tilde{H}$ would be a proper subgroup of G containing $\tilde{H}$, contradicting the maximality of $\tilde{H}$.

We will next show that the p-core $O_p(\tilde{H})$ is trivial. Suppose $O_p(\tilde{H}) \neq 1$; since $O_p(\tilde{H}) \lhd \tilde{H}$, the subgroup $G_t \rtimes O_p(\tilde{H})$ is normal in G. Now, $O_p(\tilde{H})$ is a p-group and therefore the set A of the points of G_t which are fixed by the action of $O_p(\tilde{H})$ is a non-trivial subgroup of G_t, different from G_t because the action is faithful. However, it is immediate to see that the subgroup A is also invariant by $\tilde{H}$, contradicting the irreducibility of G_t.

Let L_1 be the subfield of $\tilde{L}$ fixed by G_t; we have that $\mathrm{Gal}(L_1/K) \cong \tilde{H}$ and L_1/K is a tame extension, since the p-core of $\tilde{H}$ is trivial. Clearly its Galois group embeds into $\mathrm{Aut}(G_t) \cong GL(k, \mathbb{F}_p)$, so we have $L_1 \subseteq F$ and $\tilde{L} \subseteq L_F$.

By construction, $\tilde{L}/L_1$ is totally ramified and hence $\tilde{L} \cap F = L_1$. It follows that $\mathrm{Gal}(L_F/F) \cong G_t$ and therefore L_F/F is abelian elementary of degree p^k. By Kummer theory, L_F can be written as $F(\Xi^{1/p})$ for some $\Xi \subset F^\times/(F^\times)^p$. This is naturally a H-module; this module is irreducible: in fact, a proper submodule of $\mathrm{Gal}(L_F/F)$ would fix a proper subextension E of L_F/F, normal over K; hence, $E \cap \tilde{L}$ would be a proper subextension of $\tilde{L}/L_1$ normal over K, corresponding to a proper $\tilde{H}$-submodule of the irreducible module $\mathrm{Gal}(\tilde{L}/L_1) \cong G_t$.

Conversely, we show that each irreducible Ξ of dimension k corresponds to one isomorphism class $[L/K]$. Let $M = F(\Xi^{1/p})$, then $S = \mathrm{Gal}(M/F)$ is an irreducible H-module by Kummer theory. Let $\mathcal{G} = \mathrm{Gal}(M/K)$; then $\mathcal{G}$ is an extension of H by S.

By Remark 3.1, if $k \geq 2$ then the group H satisfies the hypothesis of Lemma 3.3; if $k = 1$ we have $(|H|, |S|) = 1$. In any case it follows that the exact sequence

$$1 \to S \to \mathcal{G} \to H \to 1$$

splits, namely, there exists a complement B to S in $\mathcal{G}$ and $\mathcal{G} \cong S \rtimes B$; moreover, the complements to S in $\mathcal{G}$ are exactly the conjugates of B.

If L is the fixed field of B, then the fixed fields of the conjugates of B form an isomorphism class of extensions of K of degree p^k. The field L, as well as its conjugates, has no proper subextension. In fact, let $K \subseteq L_0 \subseteq L$ and let $C = \mathrm{Gal}(M/L_0)$; then $B \subseteq C$ and $C \cong S_0 \rtimes B$ where $S_0 = S \cap C$, by the formula $|S_0| \cdot |B| = |C|$. But this means that S_0 is H-invariant, and therefore either $S_0 = \{1\}$ or $S_0 = S$.

It is now immediate to check that the two maps are inverse to each other. □

Looking carefully at the proof of the theorem, one can see that it works also for many other choices of the field F. For instance, we have the following corollary.

Corollary 3.4. *Suppose that Theorem 3.2 holds replacing F with a field $\mathcal{F}$. Then it holds also for the field $\tilde{\mathcal{F}}$ in the following cases:*
i) $[\tilde{\mathcal{F}} : \mathcal{F}]$ is finite and coprime to p;
ii) $\tilde{\mathcal{F}}$ is the subfield of $\mathcal{F}$ fixed by the p-core of $\mathrm{Gal}(\mathcal{F}/K)$.

Remark 3.5. The last corollary and the argument given at the end of Section 2 show that there exists a field F for which Theorem 3.2 holds with the additional properties that F is a split extension of K and the p-core of $H = \mathrm{Gal}(F/K)$ is trivial.

Unless otherwise specified, in the following F will denote an extension of K with the properties just mentioned.

4. The Galois structure of $F^\times/F^{\times p}$

In this section we will describe the H-module structure of $F^\times/F^{\times p}$. We start with the classification of the irreducible representations of H over $\mathbb{F}_p$, via the study of the irreducible representations over $\bar{\mathbb{F}}_p$ (Section 4.1); our results are quite similar to those of [CMR10]. Next, we determine the decomposition of $F^\times/F^{\times p}$ as a $\mathbb{F}_p[H]$-module; we first obtain the decomposition of the $\bar{\mathbb{F}}_p[H]$-module obtained from $F^\times/F^{\times p}$ by extension of scalars and then we bring back this information to get the structure of $F^\times/F^{\times p}$.

4.1. **The irreducible representations of a tame Galois group.**

We shall consider groups of type $\mathfrak{H} = T \rtimes U$, where $T = \langle \tau \rangle$ and $U = \langle \upsilon \rangle$ are cyclic groups of orders e and f, respectively, with $(e,p) = 1$ and $e \mid q^f - 1$, and where υ acts on T via the map $x \mapsto x^q$, and q is a power of p, that in view of our applications we will denote by p^{f_K}. Note that he group $H = \mathrm{Gal}(F/K)$ belongs to this type of groups with $T = H_0$.

Let V be an $\bar{\mathbb{F}}_p$-vector space and let $\rho : \mathfrak{H} \to GL(V)$ be a representation of $\mathfrak{H}$ irreducible over $\bar{\mathbb{F}}_p$. Let $T_0 = \ker(\rho_{|T})$, $\bar{T} = \bar{T}(\rho) = T/T_0$; to study the irreducible representation ρ we can study the irreducible representation $\bar{\rho} : \bar{T} \rtimes U \to GL(V)$ which is faithful on $\bar{T}$.

Denote by $\tilde{U}$ the kernel of $U \to \mathrm{Aut}(\bar{T})$, *i.e.*, $\tilde{U} = C_U(\bar{T})$. Let $t = t(\rho) = |\bar{T}|$, $r = r(\rho) = \mathrm{ord}_t^\times p$ (that is, the smallest power of p such that $t | p^r - 1$). Let $s = s(\rho) = \mathrm{ord}_t^\times q$; hence $s = r/(r, f_K)$ and q^s is the smallest power of q such that $t | q^s - 1$. Then $\tilde{U}$ is generated by υ^s, that we denote by $\tilde{\upsilon}$.

The group $\bar{T} \times \tilde{U}$ is abelian, so its p-core is equal to its p-Sylow subgroup. With the same argument as in the proof of Theorem 3.2, we get that this subgroup acts trivially on V, because otherwise the representation would have a proper invariant subspace. It follows that the representation of $\bar{T} \times \tilde{U}$ can be factored by the p-Sylow, hence it defines a representation of an abelian group of order coprime to p; so there exists a subspace of dimension 1 invariant for $\bar{T} \times \tilde{U}$ and therefore also for $T \rtimes \tilde{U}$.

Let V_χ be a 1-dimensional invariant subspace, where $\chi : T \rtimes \tilde{U} \to \bar{\mathbb{F}}_p^\times$ is the character of the representation in V_χ. Let $\alpha = \chi(\tau)$ and $\beta = \chi(\tilde{\upsilon})$; then υ^i maps V_χ to a space where τ acts via a conjugate α^{q^i} of α, and the orbit under υ generates the whole V. Moreover, α has order t, because the representation is faithful on $\bar{T}$. Hence for $0 \le i < s$ the $\upsilon^i V_\chi$ are all distinct, and ρ is equal to $\mathrm{Ind}_{T \rtimes \tilde{U}}^{T \rtimes U}(V_\chi)$.

If $x \in V_\chi$ is a generator, then the elements $x, \upsilon x, \dots, \upsilon^{s-1} x$ are a basis of V on which τ and υ act via the matrices:

$$\mathcal{T}_\alpha = \begin{pmatrix} \alpha & & & & \\ & \alpha^q & & & \\ & & \alpha^{q^2} & & \\ & & & \ddots & \\ & & & & \alpha^{q^{s-1}} \end{pmatrix}, \qquad \mathcal{U}_\beta = \begin{pmatrix} & & & & \beta \\ 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \end{pmatrix}.$$

The representations obtained in this way starting from V_χ or $\upsilon^i V_\chi$ are equal for all i, and on $\upsilon^i V_\chi$ the action is described via the character χ^{q^i} (the character obtained from χ by conjugation with υ^i).

On the other hand, given any subgroup T_0 of T and any character χ of $T \rtimes \tilde{U}$, where $\tilde{U} = C_U(\bar{T})$ ($\bar{T} = T/T_0$) and $\ker(\chi_{|T}) = T_0$, all representations of the type $\mathrm{Ind}_{T \rtimes \tilde{U}}^{T \rtimes U}(V_\chi)$ are irreducible, because clearly the matrices $\mathcal{T}_\alpha$ and $\mathcal{U}_\beta$ do not have common proper invariant subspaces.

The results just proven can be summarized in the following proposition.

Proposition 4.1. *Let T_0 be any subgroup of T and let $\bar{T} = T/T_0$. All irreducible representations ρ of $T \rtimes U$ in a $\bar{\mathbb{F}}_p$-vector space V such that* $\ker(\rho_{|T}) = T_0$ *are obtained as* $\mathrm{Ind}_{T \rtimes \tilde{U}}^{T \rtimes U}(V_\chi)$, *where $\tilde{U} = C_U(\bar{T})$, χ is a character of $T \rtimes \tilde{U}$ such that* $\ker(\chi_{|T}) = T_0$ *and V_χ is the representation given by χ.*

Moreover, $\mathrm{Ind}_{T \rtimes \tilde{U}}^{T \rtimes U}(V_\chi) = \mathrm{Ind}_{T \rtimes \tilde{U}}^{T \rtimes U}(V_{\chi'})$ *if and only if χ and χ' are conjugate.*

The p-core of $T \rtimes U$ is contained in the kernel of all irreducible representations.

Our next step is to show how to deduce the irreducible representations over $\mathbb{F}_p$ from those over $\bar{\mathbb{F}}_p$. More generally, if Ω/Ω_0 is a Galois extension of fields, we deduce the irreducible representations of a group G over Ω_0, from the irreducible representations of G over Ω.

Let $\rho : G \to GL(V)$ be an irreducible representation of G in $V = \Omega^n$ over Ω. The irreducible representation over Ω_0 which contains ρ is the sum of the conjugates of ρ under the action $\mathrm{Gal}(\Omega/\Omega_0)$. In fact, a representation containing ρ, defined over Ω_0, must contain all the conjugates of ρ under the action of $\mathrm{Gal}(\Omega/\Omega_0)$ and it is easy to verify that the sum over all distinct conjugates is defined and it is irreducible over Ω_0. It follows that the dimension of this representation is the product of the dimension of ρ by the number of its conjugates.

We apply this argument to the representations described in Proposition 4.1: consider $\mathrm{Ind}_{T\rtimes\tilde{U}}^{T\rtimes U}(V_\chi)$, and set $\alpha = \chi(\tau)$ and $\beta = \chi(\tilde{\upsilon})$ as above. Clearly this representation is stabilized by $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p(\alpha, \beta))$ and by the powers of the Frobenius ϕ_q fixing β, since χ and χ^{q^i} correspond to the same representation. In $\mathrm{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$ the group generated by ϕ_q is equal to the group generated by $\phi_{p^{(r,f_K)}}$. Putting $w = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$, we obtain that the smallest power of $\phi_{p^{(r,f_K)}}$ fixing $\mathbb{F}_p(\beta)$ is $\phi_{p^{\mathrm{lcm}(w,(r,f_K))}}$, which generates also the stabilizer of the representation. Hence the number of conjugates of ρ is $\mathrm{lcm}(w, (r, f_K))$. We can now prove the following proposition.

Proposition 4.2. *Let $\rho : T \rtimes U \to GL(V)$ be an irreducible representation over $\mathbb{F}_p$. Consider the restriction of the representation to $T \rtimes \tilde{U}$ over the algebraic closure, where, setting $\ker(\rho_{|T}) = T_0$ and $\bar{T} = T/T_0$, $\tilde{U} = C_U(\bar{T})$. Let χ be the character of an invariant subspace of dimension 1. Then*

$$\dim_{\mathbb{F}_p} V = \mathrm{lcm}({}^{rw}/_{(r,f_K)}, r)$$

where $r = \mathrm{ord}_t^\times(p)$, and $w = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$ where $\beta = \chi(\tilde{\upsilon})$.

Proof. Indeed, $\mathrm{Ind}_{T\rtimes\tilde{U}}^{T\rtimes U}(V_\chi)$ has dimension s so we obtain

$$\dim_{\mathbb{F}_p} V = s \cdot \mathrm{lcm}(w, (r, f_K)),$$

and the proposition follows because $s = {}^{r}/_{(r,f_K)}$. □

4.2. **The structure of $F^\times/(F^\times)^p$.** In this section F/K will be a normal tamely ramified extension, and H will denote the group $\mathrm{Gal}(F/K)$. We also assume that $\zeta_p \in F$ and that the extension is split. Let $H_0 = T = \langle\tau\rangle$, and let υ be a lifting of the Frobenius ϕ_q generating a complement U, so that $H = T \rtimes U$. Let F' be the field fixed by U; then the extension F/F' is unramified. Let π be a uniformizer of F', that we choose as an e-th root of a uniformizer of K, where

$e = e(F/K)$ (recall that in this case $e|q-1$). We observe that π is also a uniformizer of F. Denote by U_F the group of units of F and by $U_{1,F}$ the subgroup of principal units of F. It is well-known that

$$F^\times \cong \left(\langle\pi\rangle \times \kappa_F^\times\right) \oplus U_{1,F} \tag{1}$$

as H-modules.

We now consider the filtration $\{U_{i,F}\}_{i\geq 1}$ of $U_{1,F}$, where $U_{i,F} = \{u \in U_F \mid u \equiv 1 \pmod{\pi^i}\}$. We want to describe the structure of $U_{i,F}$ as H-module.

For $i \geq 1$, the action of τ and υ on $U_{i,F}/U_{i+1,F}$ is described by

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

for each $\alpha \in U_F$, where $\zeta = \tau(\pi)/\pi$ is a primitive e-th root of 1.

We can identify $U_{i,F}/U_{i+1,F}$ with κ_F via the map

$$(1+\alpha\pi^i) \mapsto \bar{\alpha}$$

and this induces on κ_F the action given by

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

Proposition 4.3. *For $i \geq 1$, let M_i be the $\kappa_K[H]$-module formed by κ_F as set, and with the above action. Then M_i is projective both as a $\kappa_K[H]$-module and as a $\mathbb{F}_p[H]$-module.*

Proof. Consider the sum $M = \oplus_{i=1}^e M_i$. We shall prove that M is a free $\kappa_K[H]$-module. Let $\bar{\eta}$ be normal basis generator for κ_F over κ_K; we claim that the vector $w = (\bar{\eta})_{1\leq i\leq e}$, with all components equal to $\bar{\eta}$, is a generator for M. Indeed, under the action of $\kappa_K[U]$ we obtain all elements of the form $(\bar{\alpha})_{1\leq i\leq e}$; now the vector

$$\frac{1}{e}\sum_{j=1}^{e}\tau^j\left((\bar{\zeta}^{-jk}\bar{\alpha})_{1\leq i\leq e}\right)$$

has the k-th component equal to $\bar{\alpha}$ (recall that $e|q-1$), and the other components equal to 0. This proves the claim, namely $M = \kappa_K[H]w$. Hence M is a quotient of the free module $\kappa_K[H]$, and in fact $M = \kappa_K[H]$ since they have the same dimension. It follows that, for $1 \leq i \leq e$, the module M_i is projective, being a direct summand of a free module. On the other hand, $M_{e+i} = M_i$ and thus M_i is projective for all $i \geq 1$. Clearly, this implies that M_i is projective also as a $\mathbb{F}_p[H]$-module. □

The proposition just proved shows that $U_{i+1,F}$ has a complement in $U_{i,F}$ as a $\mathbb{F}_p[H]$-module, namely, $U_{i,F} \cong M_i \oplus U_{i+1,F}$. By induction

$$U_{1,F} \cong \bigoplus_{i=1}^{\frac{pe_F}{p-1}} M_i \oplus U_{\frac{pe_F}{p-1}+1,F}. \tag{2}$$

Proposition 4.4. *Let $I_F = {}^{pe_F}/_{(p-1)}$, and let $[\![0, I_F]\!]$ be the set of integers prime to p in the interval $[0, I_F]$. Denote by $\mathbb{F}_p$ and M_ω the $\mathbb{F}_p[H]$-module $\mathbb{F}_p$ with the trivial action and the action given by the cyclotomic character ω, respectively. Then we have the $\mathbb{F}_p[H]$-module isomorphism*

$$F^\times/(F^\times)^p \cong \mathbb{F}_p \oplus \big(\bigoplus_{i \in [\![0,I_F]\!]} M_i \big) \oplus M_\omega.$$

Proof. By equation (1) we get

$$F^\times/(F^\times)^p \cong \big(\langle\pi\rangle \times \kappa_F^\times\big) \,/\, \big(\langle\pi\rangle \times \kappa_F^\times\big)^p \oplus U_{1_F}/U_{1,F}^p \cong \mathbb{F}_p \oplus U_{1_F}/U_{1,F}^p,$$

since clearly the action on $\big(\langle\pi\rangle \times \kappa_F^\times\big) \,/\, \big(\langle\pi\rangle \times \kappa_F^\times\big)^p$ is trivial.

Consider now $U_{1_F}/U_{1,F}^p$. By equation (2),

$$U_{1,F}^p \cong \bigoplus_{i=1}^{\frac{pe_F}{p-1}} M_i^p \oplus U^p_{\frac{pe_F}{p-1}+1,F}$$

and, applying [FV02, (5.7) and (5.8)], we get

$$U_{1,F}^p \cong \bigoplus_{i=1}^{\frac{e_F}{p-1}-1} M_{ip} \oplus N \oplus U_{\frac{pe_F}{p-1}+1,F},$$

where N is a subspace of $M_{\frac{pe_F}{p-1}}$ of codimension 1.

It follows that

$$U_{1_F}/U_{1,F}^p = \bigoplus_{i \in [\![0,I_F]\!]} M_i \oplus M_{\frac{pe_F}{p-1}}/N.$$

Finally, the submodule $M_{\frac{pe_F}{p-1}}/N$ corresponds via Kummer theory to the unramified extension of degree p, and the action of H on this submodule is given by the cyclotomic character (see for instance [DCD07, Prop.7]). $\square$

By the last proposition we are left to decompose each M_i (for $i \in [\![0, I_F]\!]$), and hence $Y := \oplus_{i\in[\![0,I_F]\!]} M_i$, into a sum of irreducible representations. We begin by studying the decomposition of $M_i \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p$; using Proposition 4.2 we shall then obtain the decomposition of M_i.

Proposition 4.5. *Let V_i be the $\bar{\mathbb{F}}_p[T]$ module of dimension 1 where τ acts via multiplication by $\bar{\zeta}^i$. Then*

$$M_i \otimes_{\kappa_K} \bar{\mathbb{F}}_p \cong \mathrm{Ind}_T^H(V_i) \quad \text{and} \quad M_i \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p \cong \big(\mathrm{Ind}_T^H(V_i)\big)^{f_K}$$

as $\bar{\mathbb{F}}_p[H]$-modules.

Proof. Consider the $\kappa_F[H]$-module $M_i \otimes_{\mathbb{F}_p} \kappa_F$ with the action $h(\alpha \otimes \beta) = h\alpha \otimes \beta$. Denote by M_i' the $\kappa_F[T]$-module obtained from M_i by restrictions of the scalars and consider the $\kappa_F[H]$-module $\kappa_F[H] \otimes_{\kappa_F[T]} M_i'$.

It is easy to check that the map

$$M_i \otimes_{\kappa_K} \kappa_F \xrightarrow{\sim} \kappa_F[H] \otimes_{\kappa_F[T]} M_i'$$
$$\alpha \otimes \beta \mapsto \sum_{i=0}^{f-1} \upsilon^{-i} \otimes \upsilon^i(\alpha)\beta$$

is an isomorphism of $\kappa_F[H]$-modules. We now tensor both sides with $\bar{\mathbb{F}}_p$; taking into account that $M_i' \otimes_{\kappa_F} \bar{\mathbb{F}}_p = V_i$ and that $\kappa_F[H] \otimes_{\kappa_F[T]} V_i \cong \mathrm{Ind}_T^H(V_i)$ we get the first formula; the second one follows immediately. □

Let T_0 be the kernel of the action of $\rho_{|T}$, let $\bar{T} = T/T_0$ and let $\tilde{U}$ be the centralizer of $\bar{T}$ in U. Assume that $\tilde{U}$ is generated by $\tilde{\upsilon}$ of order $\tilde{u}$. Then

$$\mathrm{Ind}_T^{T\rtimes\tilde{U}}(V_i) \cong \bar{\mathbb{F}}_p[\tilde{U}] \otimes_{\bar{\mathbb{F}}_p} V_i = \bigoplus_{\{\beta|\beta^{\tilde{u}}=1\}} V_{(i,\beta)},$$

where $V_{(i,\beta)}$ is the representation of dimension 1 such that τ, $\tilde{\upsilon}$ act by multiplication by ζ^i and β. Consequently we have

$$\mathrm{Ind}_T^H(V_i) = \bigoplus_{\{\beta|\beta^{\tilde{u}}=1\}} \mathrm{Ind}_{T\rtimes\tilde{U}}^H(V_{(i,\beta)})$$

and, by Proposition 4.1, this is a decomposition into irreducible representations. Denoting by $\bar{M}_i := M_i \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p$, by Proposition 4.5 we have $\bar{M}_i \cong \left(\mathrm{Ind}_T^H(V_i)\right)^{f_K}$ and hence

$$\bar{Y} := \bigoplus_{i\in[\![0,I_F]\!]} \bar{M}_i = \bigoplus_{i\in[\![0,I_F]\!]} \bigoplus_{\{\beta|\beta^{\tilde{u}}=1\}} (\mathrm{Ind}_{T\rtimes\tilde{U}}^H(V_{(i,\beta)}))^{f_K}.$$

We now compute the multiplicity of each irreducible representation contained in $\bar{Y}$.

Observe that if $\zeta^i = \zeta^j$ then $V_{(i,\beta)} = V_{(j,\beta)}$; let $V_{(\alpha,\beta)}$ denote any $V_{(i,\beta)}$ such that $\zeta^i = \alpha$ and set $J_{(\alpha,\beta)} = \mathrm{Ind}_{T\rtimes\tilde{U}}^H(V_{(\alpha,\beta)})$.

For any e-th root of unity $\alpha \in \bar{\mathbb{F}}_p^\times$, the indices i such that $\zeta^i = \alpha$ are a congruence class modulo e and, among these, there are exactly $p-1$ classes modulo ep which are coprime to p. Hence, in the set $[\![0, I_F]\!]$ there are $\frac{p-1}{ep}\frac{e_F p}{p-1} = e_K$ such indices. It follows that the representation $J_{(\alpha,\beta)}$ appears $e_K f_K = [K : \mathbb{Q}_p]$ times. Finally, since the conjugate pairs (α^{q^i}, β) yield the same representation, the multiplicity of $J_{(\alpha,\beta)}$ in $\bar{Y}$ is $se_K f_K$, where $s = [U : \tilde{U}]$.

Summarizing, we obtain the following proposition.

Proposition 4.6. *Let $\alpha, \beta \in \bar{\mathbb{F}}_p$. Suppose that $\alpha^e = 1$ where $e = e(F/K)$, and that* $\mathrm{ord}(\alpha) = t$. *Let $s = \mathrm{ord}_q^\times(t)$, $f = f(F/K)$, and $\tilde{u} = f/s$ and suppose that $\beta^{\tilde{u}} = 1$. Then the multiplicity of $J_{(\alpha,\beta)}$ in $\bar{Y}$ is equal to $s \cdot [K : \mathbb{Q}_p]$.*

Corollary 4.7. *The H-module $\bar{Y}$ is isomorphic to $\bar{\mathbb{F}}_p[H]^{[K:\mathbb{Q}_p]}$.*

Proof. The H-module $\bar{\mathbb{F}}_p[H]$ corresponds to the regular representation of H, and hence each irreducible representation occurs in $\bar{\mathbb{F}}_p[H]$ with a multiplicity equal to its degree. The corollary follows by noticing that the multiplicities of all irreducible representations in $\bar{Y}$ are equal to their degrees multiplied by $[K : \mathbb{Q}_p]$. □

Remark 4.8. Let $D = D_{(\alpha,\beta)}$ be the field of definition of $J_{(\alpha,\beta)}$; by Proposition 4.2 its degree over $\mathbb{F}_p$ is equal to $d = \mathrm{lcm}(w, (r, f_K))$. Let V be the irreducible sub-representation of Y defined over $\mathbb{F}_p$, obtained by summing all the conjugates of $J_{(\alpha,\beta)}$ over $\mathbb{F}_p$; then its multiplicity in Y is $s \cdot [K : \mathbb{Q}_p]$, while its degree is $s \cdot \mathrm{lcm}(w, (r, f_K))$. In particular, the H-module Y is not isomorphic, in general, to $\mathbb{F}_p[H]^{[K:\mathbb{Q}_p]}$ whereas this was true in the case of extensions of degree p, considered in [DCD07] and [Dal10].

For each irreducible $\mathbb{F}_p[H]$-module V contained in Y, we now count the number n_V of submodules isomorphic to V contained in Y. As before, V is the sum of the conjugates of $J_{(\alpha,\beta)}$ for some α, β; let D be the field of definition of $J_{(\alpha,\beta)}$, let $[D : \mathbb{F}_p] = d$, and call m the common multiplicity of $J_{(\alpha,\beta)}$ in $\bar{Y}$ and of V in Y. Then, all $\mathbb{F}_p$-irreducible modules isomorphic to V are contained in V^m and n_V is equal to the number of $\mathbb{F}_p[H]$-embeddings of V into V^m divided by the number of embeddings with the same image. Now, the $\mathbb{F}_p[H]$-embeddings of V into V^m are in one to one correspondence with the $D[H]$-embeddings of $J_{(\alpha,\beta)}$ into $(J_{(\alpha,\beta)})^m$, associating to $\varphi : V \to V^m$ the restriction to $J_{(\alpha,\beta)}$ of the extension of φ to $V \otimes_{\mathbb{F}_p} D$. Moreover, two embeddings of V have the same image if and only if the same is true for the corresponding embeddings of $J_{(\alpha,\beta)}$. Therefore, we count the $D[H]$-embeddings

$$\psi : J_{(\alpha,\beta)} \to (J_{(\alpha,\beta)})^m.$$

By Schur Lemma the projection of each component of ψ is the multiplication by an element $d_i \in D$, and ψ is injective if and only if the d_i are not all zero. Moreover, two embeddings have the same image if and only if they differ by multiplication by a constant. It follows that the total number of $D[H]$-embeddings is $|D|^m - 1$, while the possible constants are $|D| - 1$. As a conclusion, we have proved the following proposition:

Proposition 4.9. *Assume that the irreducible representation $J_{(\alpha,\beta)}$ has multiplicity m in $\bar{Y}$. Assume that the field of definition of $J_{(\alpha,\beta)}$ is D, and let $d = [D : \mathbb{F}_p]$. Then the number of representations defined over $\mathbb{F}_p$ and containing a representation isomorphic to $J_{(\alpha,\beta)}$ is $(p^{dm} - 1)/(p^d - 1)$.*

5. Extensions with a prescribed Galois group

In this section we classify the isomorphism classes of the extensions of degree p^2 of K without intermediate extensions. Actually, we give a more precise result, namely, for each possible Galois group G, we count the number of isomorphism classes of the extensions whose normal closure has a Galois group isomorphic to G.

We start by recalling some relevant facts proved above.

By Theorem 3.2, the isomorphism classes correspond to the irreducible H-submodules of dimension 2 of $F^\times/(F^\times)^p$, where F is as in Remark 3.5 and $H = \mathrm{Gal}(F/K)$. An irreducible submodule $X \subset F^\times/(F^\times)^p$ corresponds to an isomorphism class $[L]$ of extensions of K and, denoting by $\tilde{L}$ the normal closure of L/K, we have

$$\mathrm{Gal}(\tilde{L}/K) \cong X \rtimes (H/\ker(\rho)),$$

where $\rho : H \to \mathrm{Aut}(X)$ is the restriction of the Galois action to X. We shall see that the isomorphism class of the Galois group depends only on the group $H/\ker(\rho)$; more precisely, we have the following lemma.

Lemma 5.1. *Let X and X' be irreducible submodules of $F^\times/(F^\times)^p$ of dimension 2. Let ρ and ρ' be the restrictions of the Galois action of H to X and X', respectively. Then*

$$X \rtimes (H/\ker(\rho)) \cong X' \rtimes (H/\ker(\rho')) \iff H/\ker(\rho) \cong H/\ker(\rho').$$

Proof. The *if* part is obvious. To prove the converse it is enough to show that if $H/\ker(\rho) \cong H/\ker(\rho')$ then, by identifying the two groups with their images in $GL_2(\mathbb{F}_p)$, they are conjugate. Let ρ_0 (resp. ρ'_0) be an irreducible component of ρ (resp. ρ') over $\mathbb{F}_{p^2}$. With a case by case analysis we will show below that $H/\ker(\rho_0)$ and $H/\ker(\rho'_0)$ are conjugate over $\mathbb{F}_{p^2}$. Clearly, this implies that $H/\ker(\rho)$ and $H/\ker(\rho')$ are conjugate over $\mathbb{F}_{p^2}$; now, since $H/\ker(\rho)$ and $H/\ker(\rho')$ are realizable over $\mathbb{F}_p$, they are conjugate over $\mathbb{F}_p$. □

As before, we shall write $H = T \rtimes U$, where $T = \langle\tau\rangle$ is the inertia subgroup and $U = \langle\upsilon\rangle$.

Each irreducible representation ρ of H is described by two matrices $\rho(\tau) = \mathcal{T}_\alpha$, $\rho(\upsilon) = \mathcal{U}_\beta$ for some $\alpha, \beta \in \bar{\mathbb{F}}_p^\times$. Moreover, α and β must satisfy the following conditions: let t be the order of α, $r = \mathrm{ord}_t^\times(p) = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$, $s = \mathrm{ord}_t^\times(q)$ and $w = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$; then

$$t \mid e \quad \text{and} \quad \mathrm{ord}(\beta) \mid \frac{f}{s}. \tag{3}$$

According to Proposition 4.2, the degree of the representation given by the matrices $\mathcal{T}_\alpha$ and $\mathcal{U}_\beta$ is $\mathrm{lcm}(rw/(r,f_K), r)$. If follows that, if the degree of ρ is 2, then necessarily $\alpha, \beta \in \mathbb{F}_{p^2}^\times$; moreover, $s = r/(r,f_K) = 1, 2$, and the case $s = 2$ can occur only if $w = 1$, i.e., $\beta \in \mathbb{F}_p^\times$. Now, our construction of the field F is such that both e and f are divisible by

p^2-1 (in fact, it is immediate to check that F contains the unramified extension of K of degree p^2-1 and the splitting field of $X^{p^2-1}-\pi_k$); hence every pair (α,β) satisfying the condition $\operatorname{lcm}(rw/(r,f_K),r) = 2$ satisfies (3) as well.

The representations of degree 2 do not occur in the submodules $\mathbb{F}_p$ and M_ω of Proposition 4.4; hence, by Proposition 4.6, their multiplicity in $F^\times/(F^\times)^p$ is $s\cdot[K:\mathbb{Q}_p]$.

In the sequel we will use the following simple lemma.

Lemma 5.2. *For any ordered pair (a,b) of natural numbers, let $\psi(a,b)$ be the number of elements of order a in the group $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$. Then*

$$\psi(a,b) = a\cdot(a,b)\cdot \prod_{\substack{\ell \text{ prime} \\ \ell | a/(a,b)}} \left(1-\frac{1}{\ell}\right)\cdot \prod_{\substack{\ell \text{ prime} \\ \ell|a,\ \ell\nmid a/(a,b)}} \left(1-\frac{1}{\ell^2}\right). \qquad (4)$$

Proof. Clearly, the problem is equivalent to counting the elements (x,y) of order a in $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/(a,b)\mathbb{Z}$.

Let $a=\prod_{\ell\text{ prime}}\ell^{\mu_\ell}$ and $(a,b)=\prod_{\ell\text{ prime}}\ell^{\nu_\ell}$. Then, (x,y) is not of order a if:

- $\mu_\ell>\nu_\ell$ and $(x,y)\in\ell\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/(a,b)\mathbb{Z}$;
- $\mu_\ell=\nu_\ell$ and $(x,y)\in\ell\mathbb{Z}/a\mathbb{Z}\times\ell\mathbb{Z}/(a,b)\mathbb{Z}$.

The result follows using the inclusion-exclusion principle.

□

We are now ready to count the extensions of degree p^2 without intermediate extensions whose normal closure has a prescribed Galois group. We distinguish two cases.

Case $2\mid f_K$. In this case the degree is 2 if and only if $\max\{r,w\}=2$, and necessarily we have $s=1$. The group $H/\ker(\rho_0)$ is cyclic of order equal to the order c of (α,β) in $\mathbb{F}_{p^2}^\times\times\mathbb{F}_{p^2}^\times$. It follows that $\langle\mathcal{T}_\alpha,\mathcal{U}_\beta\rangle\cong H/\ker(\rho_0)$ is the unique subgroup N_c of $\mathbb{F}_{p^2}^\times$ of order c, which acts on $\mathbb{F}_{p^2}^+$ by multiplication, and the condition required in the proof of Lemma 5.1 is verified.

The number of elements in $\mathbb{F}_{p^2}^\times\times\mathbb{F}_{p^2}^\times$ having order c with $c\mid p^2-1$ but $c\nmid p-1$ is equal to $\psi(c,p^2-1)$. On the other hand, for a fixed (α,β) of order c, the representation $J_{(\alpha,\beta)}=V_{(\alpha,\beta)}$ has multiplicity $n=[K:\mathbb{Q}_p]$, and, by Proposition 4.9, the number of sub-representations X which contain $J_{(\alpha,\beta)}$ is $(p^{2n}-1)/(p^2-1)$, since the representation is defined over $\mathbb{F}_{p^2}$. Now, $X=J_{(\alpha,\beta)}\oplus J_{(\alpha^p,\beta^p)}$, hence if we sum over all pairs (α,β) of order c, each module X is counted twice. So, we obtain that the number of classes of extensions whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^2}^+\rtimes N_c$ is exactly

$$\frac{p^{2n}-1}{p^2-1}\cdot\frac{1}{2}\psi(c,p^2-1).$$

Summing over all pairs (α,β) in $\mathbb{F}_{p^2}^\times \times \mathbb{F}_{p^2}^\times$ but not in $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$ we obtain the total number of classes of extensions with degree p^2 having no intermediate extensions

$$\frac{p^{2n}-1}{p^2-1}\cdot\frac{1}{2}\left[(p^2-1)^2-(p-1)^2\right] = \frac{p(p^2+p-2)(p^{2n}-1)}{2(p+1)}.$$

Case $2\nmid f_K$. In this case the representations of dimension 2 over $\mathbb{F}_p$ are obtained when one between r,w is 1 and the other is 2.

For $r=1$ and $w=2$ we have again $s=1$ and the group $H/\ker(\rho_0)$ is cyclic of order equal to the order c of (α,β) in $\mathbb{F}_p^\times \times \mathbb{F}_{p^2}^\times$. As before, $\langle \mathcal{T}_\alpha, \mathcal{U}_\beta\rangle \cong H/\ker(\rho_0)$ is the unique subgroup of $\mathbb{F}_{p^2}^\times$ of order c, and again the condition required in the proof of Lemma 5.1 is verified. The pairs (α,β) of order c corresponding to this case are those of the set $(\mathbb{F}_p^\times \times \mathbb{F}_{p^2}^\times)\setminus(\mathbb{F}_p^\times \times \mathbb{F}_p^\times)$. Since $c \mid p^2-1$ but $c\nmid p-1$, the possible pairs are $\psi(c,p-1)$ and, similarly to above, the number of extensions with Galois group $\mathbb{F}_{p^2}^+ \rtimes N_c$ is

$$\frac{p^{2n}-1}{p^2-1}\cdot\frac{1}{2}\psi(c,p-1).$$

Finally, the total number of extensions obtained in this way is

$$\frac{p^{2n}-1}{p^2-1}\cdot\frac{1}{2}\left[(p-1)(p^2-1)-(p-1)^2\right] = \frac{p(p-1)(p^{2n}-1)}{2(p+1)}.$$

Assume now $r=2$, $w=1$ and in this case $s=2$. The group H acts on $J_{(\alpha,\beta)}$ (where $\alpha\in\mathbb{F}_{p^2}^\times\setminus\mathbb{F}_p^\times$ and $\beta\in\mathbb{F}_p^\times$) and the action is described by the matrices

$$\mathcal{T}_\alpha = \begin{pmatrix}\alpha & \\ & \alpha^p\end{pmatrix}, \qquad \mathcal{U}_\beta = \begin{pmatrix} & \beta \\ 1 & \end{pmatrix}.$$

Observe that the group $H/\ker(\rho)\cong\langle \mathcal{T}_\alpha, \mathcal{U}_\beta\rangle$ is non-abelian. The multiplicity of the representation is equal to $2n$ and $J_{(\alpha,\beta)}$ is defined over $\mathbb{F}_p$; by Proposition 4.9, the number of representations isomorphic to $J_{(\alpha,\beta)}$ are $(p^{2n}-1)/(p-1)$.

We now want to classify the isomorphism classes of groups generated by $\mathcal{T}_\alpha$ and $\mathcal{U}_\beta$, as α and β vary.

Let γ be a generator of the subgroup of $\mathbb{F}_{p^2}^\times$ generated by α and β and put $c=\mathrm{ord}(\gamma)=|\langle\alpha,\beta\rangle|$; with the notation already introduced we have $\langle\mathcal{T}_\gamma\rangle\cong\langle\gamma\rangle=N_c$.

Proposition 5.3. *The isomorphism class of the group $\mathcal{H}=\langle \mathcal{T}_\alpha, \mathcal{U}_\beta\rangle$, is identified by c and the class of β in $\langle\gamma\rangle/\langle\gamma\rangle^{p+1}$.*

Proof. First observe that the matrices $\mathcal{T}_\alpha$ and $\mathcal{U}_\beta^2=\mathcal{T}_\beta$ commute and they generate the cyclic group $\langle\mathcal{T}_\gamma\rangle$, of order c. This subgroup has index 2 in $\mathcal{H}$ and it is a maximal cyclic subgroup. It follows that $\mathcal{H}=\langle\mathcal{T}_\gamma,\mathcal{U}_\beta\rangle$.

Multiplying $\mathcal{U}_\beta$ by a diagonal matrix in the group, we obtain

$$\begin{pmatrix} \gamma^i & \\ & \gamma^{ip} \end{pmatrix} \cdot \begin{pmatrix} & \beta \\ 1 & \end{pmatrix} = \begin{pmatrix} & \gamma^i\beta \\ \gamma^{ip} & \end{pmatrix},$$

which scaling the second vector of the basis by γ^{ip} becomes

$$\begin{pmatrix} & \gamma^i\gamma^{ip}\beta \\ 1 & \end{pmatrix} = \begin{pmatrix} & \gamma^{i(p+1)}\beta \\ 1 & \end{pmatrix} = \mathcal{U}_{\gamma^{i(p+1)}\beta}$$

(note that this scaling is a conjugation of $\mathcal{H}$ by a diagonal matrix so it fixes $\mathcal{T}_\gamma$). In particular, β is defined up to elements of $\langle\gamma\rangle^{p+1}$. It follows that if $\langle \mathcal{T}_\alpha, \mathcal{U}_\beta\rangle$ and $\langle \mathcal{T}_{\alpha'}, \mathcal{U}_{\beta'}\rangle$ are such that $|\langle\alpha,\beta\rangle| = |\langle\alpha',\beta'\rangle|$ and $\beta' = \beta\gamma^{i(p+1)}$, then the two groups are isomorphic.

On the other hand, let $\mathcal{H} = \langle \mathcal{T}_\alpha, \mathcal{U}_\beta\rangle$, $\mathcal{H}' = \langle \mathcal{T}'_\alpha, \mathcal{U}'_\beta\rangle$ and $\phi : \mathcal{H} \to \mathcal{H}'$ be an isomorphism. Then the maximal cyclic subgroups $\langle \mathcal{T}_\gamma\rangle$ and $\langle \mathcal{T}_{\gamma'}\rangle$ have the same order c, hence they are equal since $\langle\gamma\rangle = \langle\gamma'\rangle$; so $\mathcal{H} = \langle \mathcal{T}_\gamma, \mathcal{U}_\beta\rangle$ and $\mathcal{H}' = \langle \mathcal{T}_\gamma, \mathcal{U}_{\beta'}\rangle$.

Lemma 5.4. *Let $\phi : \mathcal{H} \to \mathcal{H}'$ be an isomorphism. Then $\phi(\langle \mathcal{T}_{\gamma^2}\rangle) = \langle \mathcal{T}_{\gamma^2}\rangle$. Moreover, one of the following holds:*

- i) $\phi(\langle \mathcal{T}_\gamma\rangle) = \langle \mathcal{T}_\gamma\rangle$;
- ii) $\gamma^2 \in \mathbb{F}_p^*$ *and* $\beta, \beta' \in \langle\gamma^2\rangle$.

Proof. If $p = 2$ the group $\langle \mathcal{T}_\alpha, \mathcal{U}_\beta\rangle$ is isomorphic to $\mathcal{S}_3$ and the result is trivial.

Now, let $p \neq 2$. In the case when $\phi(\langle \mathcal{T}_\gamma\rangle) = \langle \mathcal{T}_\gamma\rangle$ the result is clear. Otherwise, $\phi(\mathcal{T}_\gamma) = \mathcal{T}_{\gamma^i}\mathcal{U}_{\beta'}$ for some i, whence $\phi(\mathcal{T}_{\gamma^2}) = \mathcal{T}_{\gamma^{i(p+1)}\beta'}$. Now, $\gamma^{i(p+1)}, \beta' \in \mathbb{F}_p^*$ so $\gamma^2 \in \mathbb{F}_p^*$ and $\beta, \beta' \in \langle\gamma\rangle \cap \mathbb{F}_p^* = \langle\gamma^2\rangle$. It follows that $\phi(\langle \mathcal{T}_{\gamma^2}\rangle) \subseteq \langle \mathcal{T}_{\gamma^2}\rangle$ and, having the same order, they must be equal. □

Lemma 5.5. $\phi(\mathcal{T}_\beta\langle \mathcal{T}_{\gamma^{p+1}}\rangle) = \mathcal{T}'_\beta\langle \mathcal{T}_{\gamma^{p+1}}\rangle$.

Proof. Consider the sets of squares $\mathcal{H}^2$, $\mathcal{H}'^2$ of $\mathcal{H}$ and $\mathcal{H}'$, respectively. We have $\mathcal{H}^2 = \langle \mathcal{T}_{\gamma^2}\rangle \cup \mathcal{T}_\beta\langle \mathcal{T}_{\gamma^{p+1}}\rangle$ and $\mathcal{H}'^2 = \langle \mathcal{T}_{\gamma^2}\rangle \cup \mathcal{T}_{\beta'}\langle \mathcal{T}_{\gamma^{p+1}}\rangle$. Clearly $\phi(\mathcal{H}^2) = \mathcal{H}'^2$ whence, by Lemma 5.4, $\phi(\mathcal{H}^2 \setminus \langle \mathcal{T}_{\gamma^2}\rangle) = \mathcal{H}'^2 \setminus \langle \mathcal{T}_{\gamma^2}\rangle$.

If $\mathcal{T}_\beta \notin \langle \mathcal{T}_{\gamma^2}\rangle$, then $\mathcal{H}^2 \setminus \langle \mathcal{T}_{\gamma^2}\rangle = \mathcal{T}_\beta\langle \mathcal{T}_{\gamma^{p+1}}\rangle$ and $\phi(\mathcal{T}_\beta\langle \mathcal{T}_{\gamma^{p+1}}\rangle) = \mathcal{T}_{\beta'}\langle \mathcal{T}_{\gamma^{p+1}}\rangle$.

If $\mathcal{T}_\beta \in \langle \mathcal{T}_{\gamma^2}\rangle$, then in fact $\mathcal{T}_\beta\langle \mathcal{T}_{\gamma^{p+1}}\rangle \subseteq \langle \mathcal{T}_{\gamma^2}\rangle$, and the elements of $\mathcal{T}_\beta\langle \mathcal{T}_{\gamma^{p+1}}\rangle$ are characterised as the elements of $\mathcal{H}$ having more than 2 square roots and the same holds in $\mathcal{H}'$, so they correspond to each other under the isomorphism ϕ.

□

The map ϕ induces an automorphism $\bar\phi$ of the cyclic group $\langle \mathcal{T}_{\gamma^\varepsilon}\rangle/\langle \mathcal{T}_{\gamma^{p+1}}\rangle$, where $\varepsilon = 1, 2$ according to the cases (i) and (ii) of Lemma 5.4. Clearly $\mathcal{T}_\beta, \mathcal{T}_{\beta'} \in \langle \mathcal{T}_{\gamma^\varepsilon}\rangle$, and, by Lemma 5.5, $\bar\phi(\overline{\mathcal{T}_\beta}) = \overline{\mathcal{T}_{\beta'}}$, where $\bar x$ denotes the class of x in $\langle \mathcal{T}_{\gamma^\varepsilon}\rangle/\langle \mathcal{T}_{\gamma^{p+1}}\rangle$; in particular, $\overline{\mathcal{T}_\beta}$ and $\overline{\mathcal{T}_{\beta'}}$ have the same order. We now note that this order is either 1 or 2 (in fact,

$\beta^{p-1} = 1, \beta^{p+1} \in \langle\gamma\rangle^{p+1}$, so $\beta^2 \in \langle\gamma\rangle^{p+1}$, i.e., $\overline{\mathcal{T}_\beta}^2 = \bar{1}$). Since in the cyclic group $\langle\mathcal{T}_{\gamma^\varepsilon}\rangle/\langle\mathcal{T}_{\gamma^{p+1}}\rangle$ there is at most an element of order 2 and an element of order 1, then $\overline{\mathcal{T}_\beta} = \overline{\mathcal{T}_{\beta'}}$, so $\beta\langle\gamma\rangle^{p+1} = \beta'\langle\gamma\rangle^{p+1}$ thus proving the proposition. □

We now show that each group $\mathcal{H} = \langle\mathcal{T}_\gamma, \mathcal{U}_\beta\rangle$ is conjugate (via a diagonal matrix) to a subgroup of $\mathcal{H}_0 = \langle\mathcal{T}_{\gamma_0}, \mathcal{U}_1\rangle$, where γ_0 is a generator of $\mathbb{F}_{p^2}^\times$. Observe that $\mathcal{H}_0 = \{T_{\gamma_0^i}, V_i \mid i = 0, \dots, p^2-1\}$, where

$$V_i = \begin{pmatrix} & \gamma_0^i \\ \gamma_0^{ip} & \end{pmatrix}.$$

Let m and b be integers such that $\gamma = \gamma_0^m$ and $\beta = \gamma^b = \gamma_0^{mb}$. Since $\beta \in \mathbb{F}_p^\times$, then $p+1|mb$ and we may write $\beta = \gamma_0^{(p+1)j}$ where $j \equiv \frac{mb}{p+1} \pmod{p-1}$. Let also

$$M_j = \begin{pmatrix} 1 & \\ & \gamma_0^{jp} \end{pmatrix}.$$

It is easy to check that $M_j\mathcal{T}_\gamma M_j^{-1} = \mathcal{T}_\gamma$ and $M_j\mathcal{U}_\beta M_j^{-1} = V_j$. It follows that the group $\mathcal{H}$ is conjugate to the subgroup $\langle\mathcal{T}_\gamma, V_j\rangle = \{T_{\gamma^i}, V_{j+mi} \mid i = 0, \dots, \frac{p^2-1}{(m,p^2-1)} - 1\}$ of $\mathcal{H}_0$; we note that this subgroup depends only on the class of j modulo m, and since j is determined modulo $p-1$, the subgroup is determined by the class of j modulo $(m, p-1)$.

Now, if $\mathcal{H}'$ is isomorphic to $\mathcal{H}$ then, by Proposition 5.3, $\mathcal{H}' = \langle\mathcal{T}_\gamma, \mathcal{U}_{\beta'}\rangle$ with $\beta'\langle\gamma^{p+1}\rangle = \beta\langle\gamma^{p+1}\rangle$, namely

$$\frac{mb'}{p+1} \equiv \frac{mb}{p+1} \pmod{(m, p-1)},$$

hence the subgroups of $\mathcal{H}_0$ conjugate to $\mathcal{H}$ and $\mathcal{H}'$ with this construction are the same. In particular, $\mathcal{H}$ and $\mathcal{H}'$ are conjugate subgroups of $GL_2(\mathbb{F}_{p^2})$, as required in the proof of Lemma 5.1.

We are now ready to count the isomorphism classes of extensions in the case $2 \nmid f_K$ with a fixed Galois group.

Our first step will be to count the pairs (α, β) for which $c = \operatorname{ord}(\alpha, \beta)$ and the class of β modulo $\langle\gamma^{p+1}\rangle$ are fixed. The number of pairs (α, β) of order c is $\psi(c, p-1)$ and we must distinguish these pairs according to the class of β.

Lemma 5.6. *For $c \in \mathbb{N}$ with $c|p^2-1$ and $c \nmid p-1$ let*

$$\lambda(c, p-1) = \begin{cases} 1 & \text{if } v_2(c) = 0 \text{ or } v_2(c) = v_2(p^2-1), \\ 1/2 & \text{if } v_2(p-1) < v_2(c) < v_2(p^2-1), \\ 1/3 & \text{if } 0 < v_2(c) \le v_2(p-1). \end{cases}$$

Then the number of pairs $(\alpha, \beta) \in \mathbb{F}_{p^2}^\times \times \mathbb{F}_p^\times$ of order c such that $\beta \in \langle\gamma^{p+1}\rangle$ is $\lambda(c, p-1)\psi(c, p-1)$, while the number of pairs such that $\beta \notin \langle\gamma^{p+1}\rangle$ is $(1 - \lambda(c, p-1))\psi(c, p-1)$.

Proof. Let $\mathcal{H} = \langle \mathcal{T}_\alpha, \mathcal{U}_\beta \rangle = \langle \mathcal{T}_\gamma, \mathcal{U}_\beta \rangle$ with $\mathrm{ord}(\gamma) = c$. Since $(p-1, p+1) = 2$ (or 1 for $p = 2$) we have that $(\langle \gamma \rangle \cap \mathbb{F}_p^\times)/\langle \gamma^{p+1} \rangle$ has order 1 or 2, so it is the quotient of the 2-Sylow subgroups of $\langle \gamma \rangle \cap \mathbb{F}_p^\times$ and $\langle \gamma^{p+1} \rangle$. It is easy to check that the order of this quotient is 2 when $0 < v_2(c) < v_2(p^2-1)$ and it is 1 otherwise, namely if $v_2(c) = 0$ or $v_2(c) = v_2(p^2-1)$.

When this order is 1, necessarily $\beta \in \langle \gamma^{p+1} \rangle$.

Consider now the case when the order is 2 (in this case necessarily $p \neq 2$): we have that $\beta \in \langle \gamma^{p+1} \rangle$ if and only if $v_2(\mathrm{ord}(\beta)) \leq v_2(\mathrm{ord}(\gamma^{p+1})) = v_2\left(\frac{c}{(c,p+1)}\right)$, so the condition $\beta \in \langle \gamma^{p+1} \rangle$ depends only on the 2-component (x, y) of (α, β) in the decomposition of $\mathbb{F}_{p^2}^\times \times \mathbb{F}_p^\times$ as a direct sum of its ℓ-Sylow subgroups.

The 2-Sylow of $\mathbb{F}_{p^2}^\times \times \mathbb{F}_p^\times$ is isomorphic to $\mathbb{Z}/2^{w+z}\mathbb{Z} \times \mathbb{Z}/2^z\mathbb{Z}$, where $2^w \| (p+1)$ and $2^z \| (p-1)$. Note that either $z = 1$ or $w = 1$. Assume $2^k \| c$ for some $1 \leq k < w + z$. If $z = 1$ and $k = 1$, the possible pairs (x, y) are $(1, -1), (-1, -1), (-1, 1)$ and the only one with $\beta \in \langle \gamma^{p+1} \rangle$ is $(-1, 1)$, giving $\frac{1}{3}$ of the cases. If $z = 1$ and $k > 1$ the possible pairs (x, y) are $(x, \pm 1)$ where $\mathrm{ord}(x) = 2^k$, and $\beta \in \langle \gamma^{p+1} \rangle$ if and only if $y = 1$, giving $\frac{1}{2}$ of the cases. If $w = 1$, then $\beta \in \langle \gamma^{p+1} \rangle$ precisely when (x, y) is such that x has order bigger than y, and it is easy to verify that this happens $1/3$ of the times. With our definition of $\lambda(c, p-1)$ the lemma follows. □

Remark 5.7. A perhaps more intrinsic characterization of the property $\beta \in \langle \gamma^{p+1} \rangle$ is that it holds if and only if the sequence $1 \to \langle \gamma \rangle \to \mathcal{H} \to \frac{\mathcal{H}}{\langle \gamma \rangle} \to 1$ splits.

To count the isomorphism classes we have to take into account that the pairs (α, β) and (α^p, β) give the same representation, so the number of pairs just counted must be divided by 2. By Proposition 4.9 multiplying by $(p^{2n}-1)/(p-1)$ we obtain the number of isomorphism classes of extensions having a particular group.

The total number of classes of extensions for $r = 2$, $w = 1$ is obtained as

$$\frac{p^{2n}-1}{p-1}\frac{1}{2}\left[(p-1)(p^2-1) - (p-1)^2\right] = \frac{1}{2}p(p-1)(p^{2n}-1),$$

and the total number of classes of extension having no intermediate extension is again

$$\frac{1}{2}p(p-1)(p^{2n}-1) + \frac{p(p-1)(p^{2n}-1)}{2(p+1)} = \frac{p(p^2+p-2)(p^{2n}-1)}{2(p+1)}.$$

We collect all the results obtained in the following theorem.

Theorem 5.8. *Let K be an extension of $\mathbb{Q}_p$ of degree n. Let c be an integer dividing (p^2-1) but not $(p-1)$, and let N_c be the cyclic* *subgroup of* $\mathbb{F}_{p^2}^\times$ *of order* c. *Let* $\mathcal{G}(N_c)$ *be the number of isomorphism classes of extensions of degree* p^2 *such that the normal closure has group isomorphic to* $\mathbb{F}_{p^2}^+ \rtimes N_c$. *Then*

$$\mathcal{G}(N_c) = \frac{p^{2n}-1}{p^2-1} \cdot \frac{1}{2}\psi(c, p^{(f_k,2)}-1).$$

Let $\mathcal{H}$ *be a non-abelian subgroup of* $\mathbb{F}_{p^2}^\times \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ *not contained in* $\mathbb{F}_{p^2}^\times$. *Let* $\mathcal{G}(\mathcal{H})$ *be the number of isomorphism classes of extensions of degree* p^2 *such that the normal closure has Galois group isomorphic to* $\mathbb{F}_{p^2}^+ \rtimes \mathcal{H}$. *Put* $N_c = \mathcal{H} \cap \mathbb{F}_{p^2}^\times$ *and* $c = |N_c|$. *If* $2 \mid f_K$ *then* $\mathcal{G}(\mathcal{H}) = 0$, *while if* $2 \nmid f_K$ *we have*

$$\mathcal{G}(\mathcal{H}) = \begin{cases} \lambda(c,p-1)\cdot \frac{p^{2n}-1}{2(p-1)} \cdot \psi(c,p-1) & \text{if } N_c \to \mathcal{H} \text{ splits,} \\ (1-\lambda(c,p-1))\cdot \frac{p^{2n}-1}{2(p-1)} \cdot \psi(c,p-1) & \text{if } N_c \to \mathcal{H} \text{ does not split.} \end{cases}$$

The above groups exhaust the Galois groups of normal closures of isomorphism classes of extensions of degree p^2 *having no intermediate extension. The total number* $\mathcal{K}_K$ *of isomorphism classes of extensions of degree* p^2 *with no intermediate extension is*

$$\mathcal{K}_K = \frac{p(p^2+p-2)(p^{2n}-1)}{2(p+1)}.$$

In accordance with the data in [JR06], we obtain 4 classes of extensions of degree 4 over $\mathbb{Q}_2$ with no intermediate extension, and 30 of degree 9 over $\mathbb{Q}_3$. Finally, we note that each isomorphism class $[L]$ contains exactly p^2 extensions; in fact, the subgroup of $\mathrm{Gal}(\tilde{L}/K)$ fixing L coincides with its normalizer (because L/K has no intermediate extension) and therefore this normaliser has index p^2. It follows that the total number of extensions of degree p^2 with no intermediate extension is

$$\frac{p^3(p^2+p-2)(p^{2n}-1)}{2(p+1)}.$$

References

[BDar] A. Bartel and T. Dokchitser, *Brauer relations in finite groups*, J. Eur. Math. Soc. (to appear). arXiv:1103.2047

[Bro82] K. S. Brown, *Cohomology of groups*, vol. 87, Springer, 1982.

[CMR10] S. Chebolu, J. Mináč, and C. Reis, *Reciprocity laws for representations of finite groups*, Ann. Sci. Math. Québec **34** (2010), no. 1, 37–61.

[Dal10] C. S. Dalawat, *Serre's formule de masse in prime degree*, Monatshefte für Mathematik (2010), 1–20.

[DCD07] I. Del Corso and R. Dvornicich, *The Compositum of Wild Extensions of Local Fields of Prime Degree*, Monatshefte für Mathematik **150** (2007), no. 4, 271–288.

[FV02] I. Fesenko and S. Vostokov, *Local Fields and Their Extensions*, 2nd Edition, American Mathematical Society, 2002.

[HK04] X.-D. Hou and K. Keating, *Enumeration of isomorphism classes of extensions of p-adic fields*, Journal of Number Theory **104** (2004), no. 1, 14–61.

[Iwa55] K. Iwasawa, *On Galois groups of local fields*, Trans. Amer. Math. Soc **80** (1955), 448–469.

[JR06] J. W. Jones and D. P. Roberts, *A database of local fields*, Journal of Symbolic Computation **41** (2006), no. 1, 80–97.

[Kra62] M. Krasner, *Nombre des extensions d'un degré donné d'un corps $\mathfrak{p}$-adique*, C. R. Acad. Sc. Paris **254** (1962), 3470–3472, *ibidem* **255** (1962), 224–226, 1682–1684, 2342–2344, 3095–3097.

[Mon11] M. Monge, *Determination of the number of isomorphism classes of extensions of $\mathfrak{p}$-adic field*, Journal of Number Theory **131** (2011), no. 8, 1429–1434.

[Pat15] M. R. Pati, *Extensions of degree p^l of a p-adic field*, 2015. arXiv:arXiv:1511.02040

[Ser78] J.-P. Serre, *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** (1978), 1031–1036.

[Ser79] ———, *Local fields*, Springer, 1979.

E-mail address: ilaria.delcorso@unipi.it
E-mail address: roberto.dvornicich@unipi.it
E-mail address: maurizio.monge@gmail.com