Journal de Théorie des Nombres
de Bordeaux 00 (XXXX), 000–000

A classification of the extensions of degree p^2 over $\mathbb{Q}_p$ whose normal closure is a p-extension

par Luca CAPUTO

Résumé. Soit k une extension finie de $\mathbb{Q}_p$ et soit $\mathcal{E}_k$ l'ensemble des extensions de degré p^2 sur k dont la clôture normale est une p-extension. Pour chaque discriminant fixé, nous calculons le nombre des éléments de $\mathcal{E}_{\mathbb{Q}_p}$ qui ont un tel discriminant et nous donnons les discriminants et les groupes de Galois (avec leur filtrations des groupes de ramification) de leurs clôtures normales. Nous montrons aussi que l'on peut generalizer cette méthode pour obtenir une classification des extensions qui appartiennent à $\mathcal{E}_k$.

Abstract. Let k be a finite extension of $\mathbb{Q}_p$ and $\mathcal{E}_k$ be the set of the extensions of degree p^2 over k whose normal closure is a p-extension. For a fixed discriminant, we show how many extensions there are in $\mathcal{E}_{\mathbb{Q}_p}$ with such discriminant and we give the discriminant and the Galois group (together with its filtration of the ramification groups) of their normal closure. We show how this method can be generalized to get a classification of the extensions in $\mathcal{E}_k$.

1. Notation, preliminaries and results.

Throughout this paper, p is an odd prime and k will be a fixed p-adic field of degree d over $\mathbb{Q}_p$ which does not contain any primitive p-th root of unity. If E is a p-adic field and $L|E$ is a finite extension, then we say that $L|E$ is a p-extension if it is Galois and its degree is a power of p.
The aim of the present paper is to give a classification of the extensions of degree p^2 over $\mathbb{Q}_p$ whose normal closure is a p-extension. This classification is based on the discriminant of the extension and on the Galois group and the discriminant of its normal closure. Let $\mathcal{E}_k$ be the set of the extensions of degree p^2 over k whose normal closure is a p-extension. Then for every $L \in \mathcal{E}_k$, there exists a cyclic extension $K|k$ of degree p, $K \subseteq L$ and $L|K$ is cyclic (of degree p). Furthermore, the converse is true: if $K|k$ is a cyclic extension of degree p, then every cyclic extension L of degree p over K is an extension of degree p^2 over k whose normal closure is a p-extension (see Prop. 2.1). Therefore, if $K|k$ is a cyclic extension of degree p, we can

consider the subset $\mathcal{E}_k(K)$ of $\mathcal{E}_k$ made up by the extensions in $\mathcal{E}_k$ which contain K. The idea is to study the compositum $M_k(K)$ of the extensions in $\mathcal{E}_k(K)$. Clearly $M_k(K)$ is the maximal abelian p-elementary extension of K: it is easy to prove that $M_k(K)|k$ is Galois (see Prop. 2.2). We describe the structure of the Galois group $G_k(K) = Gal(M_k(K)|k)$ (see Prop. 3.1), using results both from classical group extensions theory (see [5]) and from [3]. $G_k(K)$ is a p-group of order p^{dp+2} which admits a presentation with $d+1$ generators.
Then we focus on the case $k = \mathbb{Q}_p$. We put $G_p(K) = G_{\mathbb{Q}_p}(K)$. Once one has a description of the normal subgroups of $G_p(K)$ (see Prop. 4.1), it is not difficult to describe the quotients of $G_p(K)$ (see Lemma 4.1). We are able as well to decide if a quotient of $G_p(K)$ is the Galois group of the normal closure of an extension in $\mathcal{E}_{\mathbb{Q}_p}(K)$ and, if this is the case, it is easy to give the number of extensions whose normal closure has that group as Galois group (see Section 5).
Finally using class field theory and [2], we determine the ramification groups of $G_p(K)$ (we distinguish the case when K is unramified from the case when K is totally ramified, see respectively Section 6 and Section 7). This allows us to determine, after some standard computations, the possible values for the discriminant of the extensions in $\mathcal{E}_{\mathbb{Q}_p}(K)$ as well as the possible values for the discriminant of their normal closures. We collect the results in a table (see Section 8).
It would not be difficult to generalize the results of Sections 4-7 to an arbitrary ground p-adic field k. Then the method used in the present paper could be generalized to give a classification, for example, of the extensions of degree p^3 over $\mathbb{Q}_p$ whose normal closure is a p-extension. In fact, if L is one of these extensions, then there exists a cyclic extension $K|\mathbb{Q}_p$ such that $K \subseteq L$ and $L|K$ is an extension of degree p^2 whose normal closure a p-extension (see Prop. 2.1).

Acknowledgements. The results presented here come from my master thesis which was made at the University of Pisa under the direction of Prof. Roberto Dvornicich. I would like to express my thanks to him for his supervision and his advice.

2. Some properties of the extensions of degree p^2 over k whose normal closure is a p-extension.

Proposition 2.1. *Let $L|k$ be an extension of degree p^s, $s \in \mathbb{N}$. We denote by $\overline{L}$ the normal closure of L over k. Then $\overline{L}|k$ is a p-extension if and only if there exists a tower of extensions of k, say*

$$k = L^{(0)} \subseteq L^{(1)} \subseteq \ldots \subseteq L^{(s-1)} \subseteq L^{(s)} = L,$$

such that, for each $i = 0, \ldots, s-1$, $L^{(i+1)}|L^{(i)}$ is cyclic of degree p.

Proof. We proceed by induction on s. Suppose $s = 1$, i.e. $[L : k] = p$. Assume first $[\overline{L} : k] = p^n$: then $Gal(\overline{L}|L)$ is a maximal subgroup of $Gal(\overline{L}|k)$. In particular $Gal(\overline{L}|L)$ is normal in $Gal(\overline{L}|k)$. Therefore $\overline{L} = L$ and we get what we want ($L|k$ is cyclic of degree p). The other implication is obvious.
Now suppose that the proposition is true for $s \in \mathbb{N}$. Assume first that $[L : k] = p^{s+1}$. If $[\overline{L} : k] = p^n$, there must exist $H < Gal(\overline{L}|k)$ maximal (and therefore normal) such that $Gal(\overline{L}|L) \subseteq H$. Put $k' = FixH$: then $k'|k$ is cyclic of degree p. Then $[L : k'] = p^s$ and, by induction, there exists

$$k' = L^{(1)} \subseteq L^{(2)} \subseteq \ldots \subseteq L^{(s-1)} \subseteq L^{(s)} = L$$

as in the claim. But then

$$k = L^{(0)} \subseteq k' = L^{(1)} \subseteq \ldots \subseteq L^{(s-1)} \subseteq L^{(s)} = L$$

is the sequence we are looking for. Conversely, assume that there exists a sequence with the properties of the claim, put $k' = L^{(1)}$ and let $\overline{L'}$ be the normal closure of L over k'. By induction, $\overline{L'}$ is a p-extension of k'. If $\overline{L'}|k$ is normal, there is nothing to show. Otherwise the normalizer of $Gal(\overline{L}|\overline{L'})$ in $Gal(\overline{L}|k)$ must be $Gal(\overline{L}|k')$ and the latter is normal in $Gal(\overline{L}|k)$. $\overline{L}$ is the compositum of the conjugates of $\overline{L'}$ over k: each of them contains k' and is a p-extension of k'. The compositum of p-extensions is again a p-extension and then $\overline{L}$ is a p-extension. □

Remark. We recover the well known result which says that an extension of degree p, whose normal closure is a p-extension, is cyclic (the highest power of p which divides $p!$ is p). We shall use Prop. 2.1 for $s = 2$: then for an extension L of degree p^2 over k the following are equivalent:

- the normal closure $\overline{L}$ of L over k is a p-extension;
- there exists a cyclic extension K of degree p over k such that $K \subseteq L$ and $L|K$ is Galois.

We define now some notation which will be used in what follows. Let $\mathcal{E}_k$ be the set of the extensions of degree p^2 over k whose normal closure is a p-extension. For any cyclic extension K of degree p of k, we define $\mathcal{E}_k(K)$ to be the set of the estensions in $\mathcal{E}_k$ which contain K. Then it is easily seen that $\mathcal{E}_k = \bigcup \mathcal{E}_k(K)$, the union being taken over the set of cyclic extensions K of degree p over k. Moreover $\mathcal{E}_k(K)$ is the set of the cyclic extensions of K of degree p.

Proposition 2.2. *Let K be a cyclic extension of degree p over k. Then there exists one and only one extension $M_k(K)$ of k such that*

(i) $K \subseteq M_k(K)$,

(ii) *$M_k(K)$ is Galois over K and $Gal(M_k(K)|K) \cong (\mathbb{Z}/p\mathbb{Z})^{pd+1}$.*

Moreover, $M_k(K)$ is Galois over k and, if K' is another Galois extension of degree p over k, we have

$$Gal(M_k(K)|k) \cong Gal(M_k(K')|k).$$

Proof. Since K has degree p over k (in particular it does not contain any primitive p-th root of unity), we know that $K^*/K^{*p} \cong (\mathbb{Z}/p\mathbb{Z})^{pd+1}$. Then we let $M_k(K)$ be the extension of K which corresponds by local class field theory to K^{*p}: $M_k(K)$ is the compositum of the cyclic extensions of degree p over K and $Gal(M_k(K)|K) \cong (\mathbb{Z}/p\mathbb{Z})^{pd+1}$. In particular $M_k(K)$ verifies (i) and (ii) and it is clearly unique.
Now, let $\overline{\mathbb{Q}_p}$ be an algebraic closure and we consider $M_k(K) \subseteq \overline{\mathbb{Q}_p}$. Let $\sigma : M_k(K) \to \overline{\mathbb{Q}_p}$ be an embedding over k. Since K is normal, we have $\sigma(K) = K$ then $\sigma(M_k(K))$ is an extension of degree p^{pd+1} of K. In fact it is Galois over K: for, if $\tau : \sigma(M_k(K)) \to \overline{\mathbb{Q}_p}$ is an embedding over K, denoting again with σ any extension of σ, we have $\sigma^{-1}\tau\sigma|_K = \mathrm{id}_K$. Using the normality of $M_k(K)$ over K, we obtain $\tau\sigma(M_k(K)) = \sigma(M_k(K))$, i.e. $\sigma(M_k(K))$ is Galois over K. At the same time, we obtain an isomorphism between the Galois groups of $\sigma(M_k(K))$ and $M_k(K)$ over K (which is $\tau \mapsto \sigma^{-1}\tau\sigma$); from the uniqueness, $\sigma(M_k(K)) = M_k(K)$.
Let K' be an other Galois extension of degree p over k. We denote by ρ the restriction homomorphism from $Gal(M_k(K')|k)$ to $Gal(K'|k) \cong \mathbb{Z}/p\mathbb{Z}$. Using [3], we see that there exists a Galois extension M' over k with Galois group isomorphic to $Gal(M_k(K')|k)$ which contains K and such that the restriction ρ' from $Gal(M'|k)$ to $Gal(K|k)$ coincides with ρ: then $\ker\rho \cong \ker\rho'$. From this it follows that M' is a Galois extension of K such that $Gal(M'|K) \cong (\mathbb{Z}/p\mathbb{Z})^{pd+1}$ and then $M' = M_k(K)$. In particular, $Gal(M_k(K')|k) \cong Gal(M'|k) = Gal(M_k(K)|k)$. □

We will denote $Gal(M_k(K)|k)$ by $G_k(K)$. Furthermore we put

$$M_{\mathbb{Q}_p}(K) = M_p(K), \quad G_{\mathbb{Q}_p}(K) = G_p(K), \quad \mathcal{E}_{\mathbb{Q}_p} = \mathcal{E}_p, \quad \mathcal{E}_{\mathbb{Q}_p}(K) = \mathcal{E}_p(K).$$

Remark. It is clear that the compositum of the extensions belonging to $\mathcal{E}_k(K)$ is equal to $M_k(K)$.

We end this section showing that every extension in $\mathcal{E}_k$ has no more than p conjugates (over k). Of course, the converse is not true, i.e. there exists an extension of degree p^2 over k which has p conjugates but does not belong to $\mathcal{E}_k$.

Proposition 2.3. *Let L be an extension of degree p^2 over k. If there exists a cyclic extension K of degree p over k such that $K \subseteq L$ and $L|K$ is Galois, then L has no more than p-conjugates (over k).*

Proof. Suppose that there exists a cyclic extension K of degree p over k such that $K \subseteq L$ and $L|K$ is Galois. Let $\overline{L}$ be the normal closure of L over k: then $Gal(\overline{L}|L) \subseteq Gal(\overline{L}|K)$ and $Gal(\overline{L}|L)$ is normal in $Gal(\overline{L}|K)$. Moreover $Gal(\overline{L}|K)$ has index p in $Gal(\overline{L}|k)$. We know that the number of conjugates of L is equal to the index of the normalizer of $Gal(\overline{L}|L)$ in $Gal(\overline{L}|k)$. Since the normalizer of $Gal(\overline{L}|L)$ must contain $Gal(\overline{L}|K)$, we see that L has 1 or p conjugates. □

3. Stucture of $G_k(K)$

Proposition 3.1. *A presentation for $G_k(K)$ on the set of generators*

$$\{X_1,\, X_{pd+2}\} \cup \{X_{l,\,i} \,|\, l = 1,\, \ldots,\, d,\, i = 2,\, \ldots,\, p+1\}$$

is given by the relations

$$X_{l,\,p+1}^p = X_{l,\,p}^p = \ldots = X_{l,\,2}^p = 1 \qquad l = 1,\, \ldots,\, d,$$
$$X_{pd+2}^p = X_1, \qquad X_1^p = 1,$$
$$[X_1,\, X_{l,\,i}] = [X_{l,\,i},\, X_{l,\,j}] = 1 \qquad i,\, j = 2,\, \ldots,\, p+1, \quad l = 1,\, \ldots,\, d,$$
$$[X_{l,\,2},\, X_{pd+2}] = [X_1,\, X_{pd+2}] = 1 \qquad l = 1,\, \ldots,\, d,$$
$$[X_{l,\,h},\, X_{pd+2}] = X_{l,\,h-1} \qquad h = 3,\, 4,\, \ldots,\, p+1, \quad l = 1,\, \ldots,\, d.$$

Proof. $G_k(K)$ is a group extension of $(\mathbb{Z}/p\mathbb{Z})^{pd+1}$ by $\mathbb{Z}/p\mathbb{Z}$. We look for such an extension: let

$$\left\{X_{l,\,i} \,\middle|\, i = 2,\, \ldots,\, p+1;\;\; l = 1,\, \ldots,\, d\right\} \cup \{X_1\} \tag{3.1}$$

be a basis for $(\mathbb{Z}/p\mathbb{Z})^{pd+1}$ over $\mathbb{F}_p$. The relations above define an automorphism σ of $(\mathbb{Z}/p\mathbb{Z})^{pd+1}$ (the conjugation by X_{pd+2}). We have $\sigma^p(X) = X$ for every $X \in (\mathbb{Z}/p\mathbb{Z})^{pd+1}$ and $\sigma(X_1) = X_1$. Under these hypotheses, there exists one and only one extension G of $(\mathbb{Z}/p\mathbb{Z})^{pd+1}$ by $\mathbb{Z}/p\mathbb{Z}$ such that, for every $S \in G$ which represents a generator for the quotient, we have $S^{-1}XS = \sigma(X)$ for every $X \in (\mathbb{Z}/p\mathbb{Z})^{pd+1}$ and $S^p = X_1$ (see [5]). In other words in G the following relations hold:

$$X_{l,\,p+1}^p = X_{l,\,p}^p = \ldots = X_{l,\,2}^p = 1 \qquad l = 1,\, \ldots,\, d,$$
$$S^p = X_1, \qquad X_1^p = 1$$
$$[X_1,\, X_{l,\,i}] = [X_{l,\,i},\, X_{l,\,j}] = 1 \qquad i,\, j = 2,\, \ldots,\, p+1, \quad l = 1,\, \ldots,\, d,$$
$$[X_{l,\,2},\, S] = [X_1,\, S] = 1 \qquad l = 1,\, \ldots,\, d,$$
$$[X_{l,\,h},\, S] = X_{l,\,h-1} \qquad h = 3,\, 4,\, \ldots,\, p+1, \quad l = 1,\, \ldots,\, d.$$

where S is any of the elements which represent a generator for the quotient. Then the relations of the proposition really define a group G which is an extension $(\mathbb{Z}/p\mathbb{Z})^{pd+1}$ by $\mathbb{Z}/p\mathbb{Z}$; moreover G has $d+1$ generators (look at the Frattini subgroup). Then (see [3]) there exists a Galois extension E over k with group G and a Galois extension K of degree p over k such

that $E|K$ is Galois and $Gal(E|K) \cong (\mathbb{Z}/p\mathbb{Z})^{pd+1}$. Then $E = M_k(K)$ and $G = G_k(K)$. □

Let $H_k(K) = \langle X_1,\, X_{l,\,i} \,|\, i = 2,\, \ldots,\, p+1,\, l = 1,\, \ldots,\, d \rangle$.

Lemma 3.1.
- *Every element of order p in $G_k(K)$ belongs to $H_k(K)$: in particular, $G_k(K)$ cannot be written as a semidirect product between $H_k(K)$ and a subgroup of order p of $G_k(K)$;*
- $G_k(K)^p = \langle X_1,\, X_{l,\,2} \,|\, l = 1,\, \ldots,\, d \rangle$;
- $[G_k(K),\, G_k(K)] = \langle X_{l,\,i} \,|\, i = 2,\, \ldots,\, p,\, l = 1,\, \ldots,\, d \rangle$.

Proof. In what follows we consider $H_k(K)$ both as a group and as a vector space over $\mathbb{F}_p$ with basis as in (3.1). Let A denote the linear isomorphism of $H_k(K)$ which corresponds to the conjugation by X_{p+2} on $H_k(K)$. If we define $B = A - I$, we have

$$A^h - I = \sum_{i=1}^{h} \binom{h}{i} B^i$$

and then

$$\sum_{h=0}^{p-1} A^h = pI + \sum_{h=1}^{p-1} \sum_{i=1}^{h} \binom{h}{i} B^i = \sum_{i=1}^{p-1} (\sum_{h=i}^{p-1} \binom{h}{i}) B^i = B^{p-1}$$

(for the last equality argue by induction on h from $p-2$ to 1 using the well known properties of the binomial coefficient). Let ϕ the conjugation by X_{p+2} on $H_k(K)$ (so that A is a description of ϕ) and, for every $l = 1,\, \ldots,\, d$,

$$X_l(\underline{n}) = X_l(n_{l,\,2},\, n_{l,\,3}\, \ldots,\, n_{l,\,p+1}) = \sum_{i=2}^{p-1} n_{l,\,i} X_{l,\,i}.$$

Using the above computations, it is not difficult to see that, if

$$X = X_1^{n_1} + \sum_{l=1}^{d} X_l(\underline{n}),$$

then

$$(X_{p+2}^{n_{p+2}} X)^p = X_{p+2}^{n_{p+2} p} \left(\sum_{h=0}^{p-1} \phi^{n_{p+2} h} X \right) = n_{p+2} X_1 + \sum_{h=0}^{p-1} \sum_{l=1}^{d} \phi^{n_{p+2} h} X_l(\underline{n})$$

and, if $p \nmid n_{p+2}$, the last term is equal to

$$= n_{p+2} X_1 + \sum_{l=1}^{d} \left((\phi - \mathrm{Id})^{p-1} X_l(\underline{n}) \right) = n_{p+2} X_1 + \sum_{l=1}^{d} n_{l,\,p+1} X_{l,\,2}.$$

This concludes the proof of the first two claims. The last one follows from the structure of $G_k(K)$: in fact, if we take $Y_l \in \langle X_{l,\,2},\, X_{l,\,3},\, \ldots,\, X_{l,\,p+1} \rangle$ we

have $X_{p+2}^{-j} Y_l X_{p+2}^{j} \in \langle X_{l,2}, X_{l,3}, \ldots, X_{l,p} \rangle$. Since X_1 belongs to the center of $G_k(K)$, the last claim follows. □

In the case $k = \mathbb{Q}_p$, since $d = 1$, we omit the reference to l in the generators of $G_p(K)$: then we have

$$G_p(K) = \langle X_1, X_2, \ldots, X_{p+2} \rangle.$$

We put $H_{\mathbb{Q}_p}(K) = H_p(K) = \langle X_1, X_2, \ldots, X_{p+1} \rangle$.

Remark. It follows from the Lemma 3.1 that $H_k(K)$ is the only maximal subgroup $G_k(K)$ which is p-elementary abelian. Note that $H_k(K)$ is isomorphic as an $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$-module (the action being the conjugation) to the direct sum of a free $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$-module of rank d with the trivial $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$-module.

4. Normal subgroups and quotients of $G_p(K)$.

In what follows we shall focus on the case $d = 1$, i.e. $k = \mathbb{Q}_p$. We denote by $\mathcal{N}_n$ the number of normal subgroups of index p^n in $G_p(K)$ which are contained in $H_p(K)$.

Proposition 4.1. *Let A be as in the proof of Lemma 3.1. Then $\mathcal{N}_n$ ($0 < n \leq p+1$) is the number of vector subspaces of dimension $p+2-n$ in $H_p(K)$ invariant under the action of A. Moreover, if $1 < n \leq p+1$, then $\mathcal{N}_n = p+1$.*

Proof. In what follows we consider $H_p(K)$ both as subgroup and as vector space over $\mathbb{F}_p$ with basis $\{X_1, X_2, \ldots, X_{p+1}\}$. It is clear that the normal subgroups of $G_p(K)$ with index p^n ($0 < n \leq p+1$) which are contained in H are exactly the subspaces of $H_p(K)$ of dimension $p+2-n$ invariant under A. We claim that the proper subspaces of $H_p(K)$ invariant under A are exactly those of the form

$$W_i^{\lambda,\mu} = \{(x_1, x_2, \ldots, x_{p+1}) \in (\mathbb{Z}/p\mathbb{Z})^{p+1} \mid \lambda x_1 + \mu x_i = 0,\ x_j = 0 \text{ if } j > i\}$$

where $(\lambda, \mu) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \smallsetminus (0,0)$, $1 < i \leq p+1$ and we used the identification

$$(x_1, x_2, \ldots, x_{p+1}) = \sum_{i=1}^{p+1} x_i X_i.$$

First of all, observe that $\dim W_i^{\lambda,\mu} = i - 1$ and that, if $1 < i \leq p+1$ is fixed, there are exactly $p+1$ distinct $W_i^{\lambda,\mu}$. Then the statement of the proposition follows from the claim.

Let us prove the claim. On one hand, it is clear that $W_i^{\lambda,\mu}$ is invariant under A. Conversely, let V be a subspace of $H_p(K)$ invariant under and let k be the maximum of the integers h such that there exists

$v = (v_1, v_2, \dots, v_{p+1}) \in V$ with $v_h \neq 0$ and $v_m = 0$ for $m > h$: in particular this means that $\dim V \leq k$ and, if $\dim V = k \leq p$, then $V =< X_1, X_2, \dots, X_k >= W_{k+1}^{0,1}$.
Suppose that $k > 2$. Let $B = A - I$: obviously V is invariant under B. In particular $(0, v_k, 0, \dots, 0) = B^{k-2}(v) \in V$ where $v = (v_1, v_2, \dots, v_{p+1}) \in V$ is such that $v_k \neq 0$. On the other hand

$$B^{k-3}(v) - \frac{v_{k-1}}{v_k} B^{k-2}(v) = (0, 0, v_k, 0, \dots, 0) \in V.$$

Inductively, this means that V contains $\{X_i\}_{i=2}^{k-1}$. If $\dim V = k-1$, then we can complete $\{X_i\}_{i=2}^{k-1}$ to form a basis for V adjoining the vector

$$(v_1, 0, \dots, 0, v_k, 0, \dots, 0).$$

In this case then $V = W_k^{\lambda,\mu}$ with $\lambda = 1$ and $\mu = -v_1/v_k$. If $\dim V = k \leq p$, we saw that $V = W_{k+1}^{0,1}$, while, if $\dim V = p+1$, we have $V = H_p(K)$.
Suppose now that $k = 2$: if $\dim V = 1$, then $V =< v >= W_2^{\lambda,\mu}$ with $\lambda = 1$ and $\mu = -v_1/v_2$, otherwise, if the dimension is 2, $V = W_3^{0,1}$.
Lastly, if $k = 1$, $v = (v_1, 0, \dots, 0)$ and $V =< v >= W_2^{0,1}$. □

In the following we shall denote with $W_j^{\lambda,\mu}$ the subgroups defined in the proof of Prop. 4.1, for $2 \leq j \leq p+1$ and $(\lambda, \mu) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \smallsetminus (0, 0)$. Observe that $W_j^{\lambda_1,\mu_1} = W_j^{\lambda_2,\mu_2}$ if and only if there exists $c \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $(\lambda_1, \mu_1) = c(\lambda_2, \mu_2)$.

Lemma 4.1. *Let $p \geq r \geq 3$ and $p \geq j \geq 2$. Then*

$$G_p(K)/W_j^{1,0} \ncong G_p(K)/W_j^{\lambda,1} \qquad \lambda \in \mathbb{Z}/p\mathbb{Z},$$

$$G_p(K)/W_r^{0,1} \ncong G_p(K)/W_r^{\lambda,1} \qquad \lambda \in (\mathbb{Z}/p\mathbb{Z})^*,$$

$$G_p(K)/W_j^{\lambda_1,1} \cong G_p(K)/W_j^{\lambda_2,1} \qquad \lambda_1, \lambda_2 \in (\mathbb{Z}/p\mathbb{Z})^*,$$

$$G_p(K)/W_2^{0,1} \cong G_p(K)/W_2^{1,\mu} \qquad \mu \in (\mathbb{Z}/p\mathbb{Z})^*.$$

Proof. In order to prove that $G_p(K)/W_j^{1,0} \ncong G_p(K)/W_j^{\lambda,1}$ ($\lambda \in \mathbb{Z}/p\mathbb{Z}$) it is sufficient to look at the cardinalities of the commutator subgroups of these two groups. We note that in particular $W_j^{1,0}$ is an invariant subgroups of $G_p(K)$.
For the second claim, observe that $G_p(K)/W_r^{0,1}$ is *regular* (it has order $p^{p-r+3} \leq p^p$, see [1]): in particular it has exponent p (because it admits a presentation with generators of order p) while $G_p(K)/W_r^{\lambda,1}$ has exponent p^2. This proves that $G_p(K)/W_r^{0,1} \ncong G_p(K)/W_r^{\lambda,1}$ ($\lambda \in (\mathbb{Z}/p\mathbb{Z})^*$).
Now, for every $\lambda_1, \lambda_2 \in (\mathbb{Z}/p\mathbb{Z})^*$, we construct an automorphism σ of

$G_p(K)$ such that $\sigma(W_j^{\lambda_1,1}) = W_j^{\lambda_2,1}$. Choose λ such that $<\lambda>=(\mathbb{Z}/p\mathbb{Z})^*$ and put

$$\sigma(X_{p+2}) = X_{p+2}, \quad \sigma(X_1) = X_1, \quad \sigma(X_k) = \lambda X_k \text{ for } 2 \leq k \leq p+1.$$

It is not difficult to verify that this choice defines an automorphism of $G_p(K)$. Moreover for every $2 \leq j \leq p$

$$\sigma(W_j^{1,0}) = (W_j^{1,0})$$

because $W_j^{1,0}$ is invariant. Then, if $p+1 \geq i \geq 3$,

$$\sigma(W_i^{\lambda^h,1}) = \sigma\left(W_{i-1}^{1,0} \oplus < X_1 - \lambda^h X_i >\right) =$$

$$= W_{i-1}^{1,0} \oplus < X_1 - \lambda^{h+1} X_i >= W_i^{\lambda^{h+1},1}$$

and we see that our choice of λ gives the result. This proves the third assertion.
Finally, for every $\mu \in (\mathbb{Z}/p\mathbb{Z})^*$, there exists an automorphism τ of $G_p(K)$ such that $\tau(W_2^{0,1}) = W_2^{1,\mu}$. In fact, it is easily seen that

$$X_{p+2} \mapsto X_{p+2} X_{p+1}^{\mu}, \qquad X_1 \mapsto X_1 X_2^{\mu}, \qquad X_i \mapsto X_i \quad \text{if } i > 1 \tag{4.1}$$

effectively defines an automorphism of $G_p(K)$ that satisfies the required properties. This proves the last assertion. □

5. Extensions of fields.

Observe that the cardinality of $\mathcal{E}_p(K)$ is equal to $\frac{(p^{p+1}-1)}{p-1}$. In fact it suffices to compute the number of the maximal subgroups of $H_p(K)$ whose number is precisely $\frac{(p^{p+1}-1)}{p-1}$.
Using class field theory, it is easily seen that the number of cyclic extensions of degree p^2 over $\mathbb{Q}_p$ which contain K is equal to p. Moreover, there is only one Galois extension of degree p^2 over $\mathbb{Q}_p$ whose Galois group is p-elementary abelian. So the normal extensions contained in $\mathcal{E}_p(K)$ are exactly $p+1$.
Now we want to compute the number of extensions in $\mathcal{E}_p(K)$ whose normal closure has a fixed group as Galois group. A group which appears as a Galois group of the normal closure of an extension in $\mathcal{E}_p(K)$ is a quotient of $G_p(K)$. The preceding discussion answers the question for the two groups of order p^2 (of course, both of them are quotients of $G_p(K)$). So we restrict ourselves to the quotients of order p^n with $3 \leq n \leq p+2$. In the following, we denote by $E_j^{\lambda,\mu}$ the subextension of $M_k(K)$ which correspond to $W_j^{\lambda,\mu}$ (in the notation for these extensions, we omit the reference to K).

Proposition 5.1. *Let $2 \leq j \leq p$. Then $E_j^{1,0}$ is not the splitting field of any of the extensions in $\mathcal{E}_p(K)$.*

Proof. The result will follow if we prove that every subgroup of order p^{p-j+1} contained in the image of $H_p(K)$ in $G_p(K)/W_j^{1,0}$ contains an element of the center of $G/W_j^{1,0}$. In fact, a subgroup of these corresponds to an extension in $\mathcal{E}_p(K)$ ($E_j^{1,0}$ has degree p^{p-j+3} over $\mathbb{Q}_p$) and the condition implies that this extension is contained in a Galois extension of degree strictly less than p^{p-j+3}. These subgroups correspond to the subgroups of $H_p(K)$ which contain $W_j^{1,0}$ and whose order is p^p. Let H' be such a subgroup: suppose that $< X_1, X_{j+1} > \cap H' = \{1\}$. Then H' cannot have order p^p. Now we conclude observing that the image of $< X_1, X_{j+1} >$ is contained in the center of $G/W_j^{1,0}$. □

Proposition 5.2. *Let $2 \leq j \leq p$ and $\lambda \in \mathbb{Z}/p\mathbb{Z}$. Then $E_j^{\lambda,1}$ is the splitting field of exactly p^{p-j+1} extensions in $\mathcal{E}_p(K)$.*

Proof. First of all, observe that the center of $G_p(K)/W_j^{\lambda,1}$ is generated by the image of X_j. In fact, look at the centralizer of the image of X_{p+2}: it is easy to see that it is generated by $\overline{X_j}$ (the bar denotes the images under the projection) and then it must be equal to $< \overline{X_j} >$ (the center of a p-group cannot be trivial). Since in a p-group the intersection between a normal subgroup and the center is not trivial, we deduce that the center of $G_p(K)/W_j^{\lambda,1}$ is contained in each of his normal subgroups. Now we look at the subgroups of $H_p(K)$ whose order is p^p, which contain $W_j^{\lambda,1}$ and do not contain X_j. These subgroups are in one-to-one correspondence with the hyperplanes of $< X_1, X_j, X_{j+1} \ldots, X_{p+1} >$ which contain the one dimensional subspace $\{y_1 X_1 + y_j X_j \,|\, \lambda y_1 + y_j = 0\}$ and do not contain X_j. These hyperplanes are exactly the hyperplanes defined by the equations

$$\lambda y_1 + y_j + c_{j+1} y_{j+1} + \ldots + c_{p+1} y_{p+1} = 0.$$

with $c_{j+1}, \ldots, c_{p+1} \in \mathbb{F}_p$. Then the subgroups of $G_p(K)/W_j^{\lambda,1}$ of order p^{p-j+1} which do not contain $\overline{X_j}$ are of the form

(5.1)
$$H_{c_{j+1},\ldots,c_{p+1}} = \{\overline{X_j}^{z_j} \cdots \overline{X_{p+1}}^{z_{p+1}} \,|\, z_j + c_{i+1} z_{j+1} + \ldots + c_{p+1} z_{p+1} = 0\}.$$

Observe that these subgroups cannot contain any normal subgroup otherwise they would contain the center. So it suffices to count the $(p-j+1)$-tuples of elements of $\mathbb{Z}/p\mathbb{Z}$ to count all the extensions of degree p^2 over $\mathbb{Q}_p$ whose splitting field is $E_j^{\lambda,1}$. □

We may reinterpret these results in the following way. We have $p+1$ Galois extensions and $\sum_{i=2}^{p} p(p^{p-i+1}) = \sum_{j=2}^{p} p^j$ non-normal extensions in $\mathcal{E}_p(K)$. The sum of these two numbers really gives the number of elements of $\mathcal{E}_p(K)$,

that is

$$1 + p + \sum_{j=2}^{p} p^j = \sum_{j=0}^{p} p^j = \frac{(p^{p+1} - 1)}{p - 1}.$$

6. Ramification groups of $M_p(K)$ when K is unramified.

In the next two sections we are going to use results from local class field theory and ramification theory. We prefer not to report every time the reference: the definitions and the proof of every result concerning those theories can be found in [4].
Let K_0 be the unramified extension of degree p over $\mathbb{Q}_p$: for this section, as a matter of notation, we put $M_p(K_0) = M_0$. Let F_0 be the unramified extension of degree p^2 of $\mathbb{Q}_p$: we have $F_0 \subset M_0$. Moreover $M_0|F_0$ is a totally ramified abelian p-extension (of degree p^p). Let $\psi_{F_0}^{M_0}$ denotes the Hasse-Arf function relative to the extension $M_0|F_0$ and let $\varphi_{F_0}^{M_0}$ be its inverse. We denote by $\{G_i\}$ and $\{G^i\}$ respectively the lower numbering and the upper numbering filtrations relative to the extension $M_0|F_0$.

Remark. We have

$$Gal(M_0|F_0) = \langle X_1^a X_{p+1},\, X_2,\, X_3,\, \ldots,\, X_p \rangle$$

for some $a \in \mathbb{Z}/p\mathbb{Z}$ since the subgroup $\langle X_1,\, X_2,\, \ldots,\, X_p \rangle$ has non cyclic quotient. Therefore up to an automoprhism of G (more precisely the automorphism which fixes every generator except X_{p+1} which maps to $X_1^{-a} X_{p+1}$) we can suppose

$$Gal(M_0|F_0) = \langle X_2,\, X_3,\, \ldots,\, X_p,\, X_{p+1} \rangle.$$

Proposition 6.1. *The following holds: $Gal(M_0|F_0) = G_0 = G_1$ and $G_i = \{1\}$ for every $i > 1$.*

Proof. We denote as usual for a p-adic field F by U_F^i the subgroup of units of F which are congruent to 1 modulo the i-th power of the prime ideal of F.
First of all, we observe that $U_{F_0}^2 = (U_{F_0}^1)^p$ since F_0 is (absolutely) unramified. Now, in the isomorphism

$$F_0^* \cong \langle \pi_{F_0} \rangle \times \mathbb{F}_{p^2}^* \times U_{F_0}^1,$$

the subgroup $N_{F_0}^{M_0}(M_0^*)$ corresponds to

$$N_{F_0}^{M_0}(M_0^*) \cong \langle \pi_{F_0} \rangle \times \mathbb{F}_{p^2}^* \times N_{F_0}^{M_0}(U_{M_0}^1).$$

Since we have $F_0^{*p} \subseteq N_{F_0}^{M_0}(M_0^*)$ (both are normic subgroups and the abelian extension corresponding to F_0^{*p} contains M_0) and we get $U_{F_0}^2 = (U_{F_0}^1)^p \subset$

$N_{F_0}^{M_0}(U_{M_0}^1)$.
One has $G_0 = G_1$ as $M_0|F_0$ is widly ramified. It follows $\varphi_{F_0}^{M_0}(1) = 1 = \psi_{F_0}^{M_0}(1)$. Then from class field theory, we get

$$U_{F_0}^1/U_{F_0}^2 N_{F_0}^{M_0}(U_{M_0}^1) \cong G_1/G_2.$$

Now, the first term is equal to $U_{F_0}^1/N_{F_0}^{M_0}(U_{M_0}^1)$ which is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^p$. Then $G_2 = \{1\}$. □

Next we consider the extension $M_0|\mathbb{Q}_p$. We denote by $\{G_i\}$ and $\{G^i\}$ respectively the lower numbering and the upper numbering filtrations relative to the extension $M_0|\mathbb{Q}_p$. This notation is consistent with the preceding one if we restrict ourselves to $i \geq 0$, as we will do in the following.
Let W be a normal subgroup of $G_p(K_0)$ which is contained in $H_p(K_0)$. We put

$$\overline{G}_i = (G_p(K_0)/W)_i\,, \qquad \overline{G}^i = (G_p(K_0)/W)^i\,.$$

We are going to determine the ramification groups of the extension corresponding to W using the well known formulas for the ramification groups of a quotient. As we are interested in W as long as $G_p(K_0)/W$ is the Galois group the normal closure of an extension in $\mathcal{E}_p(K_0)$, we can suppose $W \neq W_j^{1,0}$.
We know that W is not contained in $Gal(M_0|F_0)$ because W is one of the $W_j^{\lambda,1}$'s with $2 \leq j \leq p+1$ and $\lambda \in \mathbb{Z}/p\mathbb{Z}$. In particular $W \cdot Gal(M_0|F_0) = H_p(K_0)$. Then $\overline{G}_i = \overline{G}^i = H_p(K_0)/W$ if $0 \leq i \leq 1$ and $\overline{G}_i = \overline{G}^i = \{1\}$ for every $i > 1$.
Let E be the extension corresponding to W: we have $p^n = [E : \mathbb{Q}_p]$ form some n. We denote by $\mathfrak{d}_E$ the discriminant of the extension $E|\mathbb{Q}_p$ and put $d_E = v(\mathfrak{d}_E)$, where v is the valuation on $\mathbb{Q}_p$ such that $v(p) = 1$. Observe that $W \nsubseteq Gal(M_0|F_0)$ implies $F_0 \nsubseteq E$. Then we have

$$d_E = 2p(p^{n-1} - 1)$$

(for this computation we use the Hilbert formula for the different which involves the cardinalities of the ramification groups). Note that the factor p comes from the inertia index of $E|\mathbb{Q}_p$.

7. Ramification groups of $M_p(K)$ when K is totally ramified.

Let K be a totally ramified cyclic extension of degree p over $\mathbb{Q}_p$ and let F be the unramified extension of degree p of K: F is the maximal abelian extension of exponent p over $\mathbb{Q}_p$. For this section, as a matter of notation, we put

$$M_p(K) = M, \quad G_p(K) = G, \quad H_p(K) = H,$$

every statement of this section being independent of the particular choice of K within the set of cyclic totally ramified extensions of degree p of $\mathbb{Q}_p$. Observe that $F \subset M$ and $L|M$ is a totally ramified abelian p-extension (of degree p^p). Let ψ_K^M denotes the Hasse-Arf function relative to the extension $M|K$ and let φ_K^M be its inverse. We denote by $\{G_u\}$ and $\{G^v\}$ respectively the lower numbering and the upper numbering filtrations relative to the extension $M|\mathbb{Q}_p$. Similarly, we denote by $\{H_u\}$ and $\{H^v\}$ respectively the lower numbering and the upper numbering filtrations relative to the extension $M|K$. Put finally, for every u and v,

$$h_u = |H_u|, \quad h^v = |H^v|, \quad g_u = |G_u|, \quad g^v = |G^v|.$$

Proposition 7.1. *The following holds:*

$$H^v \cong (\mathbb{Z}/p\mathbb{Z})^{p-i+1} \quad \textit{if} \quad i-1 < v \leq i, \quad 1 \leq i \leq p-1,$$
$$H^v \cong \mathbb{Z}/p\mathbb{Z} \quad \textit{if} \quad p-1 < v \leq p+1$$

and $H^v = \{1\}$ *if* $v > p+1$.

Proof. We apply the results of [2] to the extension $M|K$: M is the maximal abelian extension of exponent p over K and K is totally ramified of degree p over $\mathbb{Q}_p$. Then we know that the jumps of ψ_K^M are 1, 2, ..., $p-1$, $p+1$, since

$$p+1 < \frac{p^2}{p-1} < p+2.$$

We have $f(M|K) = p$ and $e(M|K) = p^p$, then $h^0 = h^1 = p^p$. Since there are p jumps, the ratio between the right and the left derivatives of ψ_K^M at every jump must be equal to p. This proves what we want. □

Now observe that for every $i \geq -1$ one has

$$H_i = G_i \cap H. \tag{7.1}$$

Furthermore

$$\varphi_{M|\mathbb{Q}_p} = \varphi_{K|\mathbb{Q}_p} \circ \varphi_{M|K}. \tag{7.2}$$

Using (7.2) it is easy to compute $\varphi_{M|\mathbb{Q}_p}$ and the g_i's. Then we get

$$g_0 = g_1 = p^{p+1},$$
$$g_{2+p+\ldots+p^{j-1}} = \ldots = g_{1+p+\ldots+p^j} = p^{p-j} \qquad \text{if} \quad 1 \leq j \leq p-2,$$
$$g_{2+p+\ldots+p^{p-2}} = \ldots = g_{1+p+\ldots+p^{p-2}+2p^{p-1}} = p.$$

Using (7.1), we can deduce that $H_i = G_i$, if $i \geq 2$: in particular the subgroups H_i are normal in G. Observe that the jumps in the filtration $\{G^v\}$ are *not* integers: more precisely one has

$$g^v = p^{p+1} \quad \text{if} \quad 0 \leq v \leq 1,$$
$$g^v = p^{p-i} \quad \text{if} \quad 1 + \frac{i-1}{p} < v \leq 1 + \frac{i}{p}, \quad i = 1, \ldots, p-2,$$

$$g^v = p \quad \text{if} \quad 1 + \frac{p-2}{p} < v \leq 2,$$
$$g^v = 1 \quad \text{if} \quad v > 2.$$

In the following we shall call v_m the m-th jump in the filtration $\{G^v\}$. For example $v_1 = 1$, $v_2 = 1 + \frac{1}{p}$ and $v_p = 2$.

Remark. Up to an automorphism of G (more precisely an automorphism such that $X_{p+2}X_{p+1}^h \mapsto X_{p+2}$, see (4.1)), we can suppose

$$Gal(L|K_0) = \langle X_2, X_3, \ldots, X_p, X_{p+2} \rangle$$

where we still denote by K_0 the unramified extension of degree p of $\mathbb{Q}_p$, as in the preceding section.

Lemma 7.1. *$M|K_0$ has precisely p cyclic subextensions of degree p^2: they corresponds to the subgroups*

$$\langle X_1^h X_p, X_2, X_3, \ldots, X_{p-1} \rangle \subseteq Gal(L|K_0)$$

as h runs in $\{0, 1, \ldots, p-1\}$. Moreover, if E one of these subextensions of $M|K_0$ and $\{Gal(E|K_0)^v\}$ is the upper numbering filtration on $Gal(E|K_0)$, one has

$$Gal(E|K_0)^v \cong \mathbb{Z}/p^2\mathbb{Z} \quad \textit{if} \quad 0 \leq v \leq 1$$
$$Gal(E|K_0)^v \cong \mathbb{Z}/p\mathbb{Z} \quad \textit{if} \quad 1 < v \leq 2$$

and $Gal(E|K_0)^v = \{1\}$ if $v > 2$.

Proof. Clear. □

If $h = 0, 1, \ldots, p-1$, we denote with E_h the cyclic extension of degree p^2 over K_0 corresponding to $\langle X_1^h X_p, X_2, X_3, \ldots, X_{p-1} \rangle$. Observe that

$$(G/Gal(M|E_h))^v = G^v Gal(M|E_h)/Gal(M|E_h). \tag{7.3}$$

Proposition 7.2. *There exists $m \in \mathbb{Z}/p\mathbb{Z}$ such that the following holds*

$$G^v = \langle X_2, X_3, \ldots, X_p, X_{p+2} \rangle \quad \textit{if} \quad 0 \leq v \leq v_1$$
$$G^v = \langle X_1, X_2, \ldots, X_{p-i} \rangle \quad \textit{if} \quad v_i < v \leq v_{i+1}, \quad i = 1, \ldots, p-2$$
$$G^v = \langle X_1 X_2^m \rangle \quad \textit{if} \quad v_{p-1} < v \leq v_p$$

and $G^v = \{1\}$ for $v > v_p$.

Proof. The first claim is clear because

$$G^1 = G^0 = Gal(M|K_0)$$

Now observe that $Gal(M|K_0)^v = G^v$ if $v \geq 0$. Using (7.3) we get, if $1 < v \leq 2$, for every $0 \leq h \leq p-1$,

$$\begin{aligned} \mathbb{Z}/p\mathbb{Z} &\cong (Gal(M|K_0)/Gal(E_h|K_0))^v \\ &= G^v \langle X_1^h X_p, X_2, \ldots, X_{p-1} \rangle / \langle X_1^h X_p, X_2, \ldots, X_{p-1} \rangle \end{aligned} \tag{7.4}$$

Now, G^v is p-elementary abelian (since we showed that $G_i = H_i$ if $i \geq 2$) and it is contained in G^1. Then, since $g^v = p^{p-1}$ if $1 < v \leq v_2$,

$$G^v = \langle X_1, X_2, \ldots, X_{p-1} \rangle \quad \text{if} \quad 1 < v \leq v_2$$

(one can also use the fact that G^1/G^{v_1} has to be a p-elementary abelian group). Observe that $g^{v_3} = p^{p-2}$; furthermore $G^{v_3} \neq \langle X_2, \ldots, X_{p-1} \rangle$ because of (7.4). Then $G^{v_3} = \langle X_1 X_{p-1}^l X_2, \ldots, X_{p-2} \rangle$ for some $l \in \mathbb{Z}/p\mathbb{Z}$. We have

$$\langle X_{p-2}^l, X_2, \ldots, X_{p-3} \rangle = [G^1, G^{v_3}] \subseteq G^{v_4} \tag{7.5}$$

If $l \neq 0$, $\langle X_{p-2}^l, X_2, \ldots, X_{p-3} \rangle$ has order $p^{p-3} = g^{v_4}$: then in (7.5), we would have equality. But this is impossible because $G^{v_4} \nsubseteq \langle X_2, \ldots, X_{p-1} \rangle$ since (7.4) holds. Then $G^{v_3} = \langle X_1, X_2, \ldots, X_{p-2} \rangle$.
In a similar way one proves that

$$G^v = \langle X_1, X_2, \ldots, X_{p-i} \rangle$$

if $v_i < v \leq v_{i+1}$ and $i = 1, \ldots, p-2$. Then $G^{v_{p-1}} = \langle X_1, X_2 \rangle$ but we cannot use the commutator argument again because both X_1 and X_2 belong to the center of G. Still, thanks to (7.4), we have $G^{v_p} \neq \langle X_2 \rangle$. This concludes the proof. □

For every $W_j^{\lambda,\mu}$ we put

$$(\overline{G_j^{\lambda,\mu}})^v = \left(G/W_j^{\lambda,\mu}\right)^v.$$

As in the preceding section we are going to determine the ramification groups of the extension $E_j^{\lambda,\mu}$ over $\mathbb{Q}_p$ corresponding to $W_j^{\lambda,\mu}$. We denote by $\mathfrak{d}_{E_j^{\lambda,\mu}|\mathbb{Q}_p}$ the discriminant of the extension $E_j^{\lambda,\mu}|\mathbb{Q}_p$ and put $d_{E_j^{\lambda,\mu}|\mathbb{Q}_p} = v(\mathfrak{d}_{E_j^{\lambda,\mu}})$, where v is the valuation on $\mathbb{Q}_p$ such that $v(p) = 1$. We suppose $2 \leq j \leq p$, because $\{E_{p+1}^{\lambda,\mu}|\mathbb{Q}_p\}$ is the set of Galois extensions of degree p^2 over $\mathbb{Q}_p$, whose discriminants are well known. Furthermore, as we are interested in the $E_j^{\lambda,\mu}$ as long as they are the normal closure of extensions of degree p^2 over $\mathbb{Q}_p$, we are going to omit the computations for the case $\mu = 0$ and $\lambda = 1$ (see Prop. 5.1).
Suppose first $\mu = 1$, $\lambda = 0$ and $3 \leq j \leq p$. Then we have

$$|(\overline{G_j^{\lambda,\mu}})^v| = p^{p-j+2} \quad \text{if} \quad 0 \leq v \leq v_1,$$

$$|(\overline{G_j^{\lambda,\mu}})^v| = p^{p-j-i+1} \quad \text{if} \quad v_i < v \leq v_{i+1}, \quad 1 \leq i \leq p-j,$$

and $|(\overline{G_j^{\lambda,\mu}})^v| = 1$ if $v > v_{p-j+1}$. Then

$$d_{E_j^{0,1}|\mathbb{Q}_p} = p\left(2(p^{p-j+2}-1) + \sum_{i=1}^{p-j} p^i(p^{p-j-i+1}-1)\right).$$

Now suppose $\mu = 1$, $\lambda \neq 0$ and $3 \leq j \leq p-1$. Then we have

$$|(\overline{G_j^{\lambda,\mu}})^v| = p^{p-j+2} \quad \text{if} \quad 0 \leq v \leq v_1,$$

$$|(\overline{G_j^{\lambda,\mu}})^v| = p^{p-j-i+1} \quad \text{if} \quad v_i < v \leq v_{i+1}, \quad 1 \leq i \leq p-j-1,$$

$$|(\overline{G_j^{\lambda,\mu}})^v| = p \quad \text{if} \quad v_{p-j} < v \leq v_p,$$

and $|(\overline{G_j^{\lambda,\mu}})^v| = 1$ if $v > v_p$. Then

$$\begin{aligned} d_{E_j^{\lambda,1}|\mathbb{Q}_p} \quad = \quad & p\Big(2(p^{p-j+2}-1) + \sum_{i=1}^{p-j-1} p^i(p^{p-j-i+1}-1) + \\ & + p^{p-j}(v_p - v_{p-j})(p-1)\Big). \end{aligned}$$

If $\mu = 1$, $\lambda \neq 0$ and $j = p$, then we have

$$|(\overline{G_j^{\lambda,\mu}})^v| = p^2 \quad \text{if} \quad 0 \leq v \leq v_1,$$

$$|(\overline{G_j^{\lambda,\mu}})^v| = p \quad \text{if} \quad v_1 < v \leq v_p$$

and $|(\overline{G_j^{\lambda,\mu}})^v| = 1$ if $v > v_p$. Then

$$d_{E_p^{\lambda,1}|\mathbb{Q}_p} = p\left(2(p^2-1) + p(p-1)\right).$$

Now suppose $j = 2$. Observe that we have $G/W_2^{0,1} \cong G/W_2^{1,\mu}$ for every $\mu \in (\mathbb{Z}/p\mathbb{Z})^*$ (see Lemma 4.1). We have two cases which must be considered separately. Suppose first that $W_2^{\lambda,\mu} = G^{v_p} = \langle X_1 X_2^m \rangle$: then, denoting with d_e the valuation of the discriminant of $E_2^{\lambda,\mu}|\mathbb{Q}_p$ in this case, we have

$$d_e = p\left(2(p^p-1) + \sum_{i=1}^{p-2} p^i(p^{p-i-1}-1)\right).$$

Conversely suppose that $W_2^{\lambda,\mu} \neq G^{v_p}$: then, denoting with d_u the valuation of the discriminant of $E_2^{\lambda,\mu}|\mathbb{Q}_p$ in this case, we have

$$d_u = p\left(2(p^p-1) + \sum_{i=1}^{p-3} p^i(p^{p-i-1}-1) + (v_p - v_{p-2})p^{p-1}(p-1)\right).$$

Now we look at the extensions $E_j^{\lambda,\mu}|L$ where $L \in \mathcal{E}_p(K)$, $\mu \neq 0$ and $2 \leq j \leq p$: we have described the $Gal(E_j^{\lambda,\mu}|L)$'s in Prop. 5.2 (see 5.1). They are subgroups of $\overline{G_j^{\lambda,\mu}}$ and then, for every i,

$$\Big(Gal(E_j^{\lambda,\mu}|L)\Big)_i = \Big(\overline{G_j^{\lambda,\mu}}\Big)_i \cap Gal(E_j^{\lambda,\mu}|L).$$

We denote by $\mathfrak{d}_{E_j^{\lambda,\mu}|L}$ the discriminant of $E_j^{\lambda,\mu}|L$ and we put $d_{E_j^{\lambda,\mu}|\mathbb{Q}_p} = w(\mathfrak{d}_{E_j^{\lambda,\mu}|\mathbb{Q}_p})$, where w is the valuation on L such that $w|v$ and $w(p) = p^2$. Suppose first $\mu = 1$, $\lambda = 0$ and $3 \leq j \leq p$. Then we get

$$d_{E_j^{0,1}|L} = p\left(2(p^{p-j}-1) + \sum_{i=1}^{p-j} p^i(p^{p-j-i}-1)\right).$$

Now suppose $\mu = 1$, $\lambda \neq 0$ and $3 \leq j \leq p$. Then we get

$$d_{E_j^{\lambda,1}|L} = p\left(2(p^{p-j}-1) + \sum_{i=1}^{p-j} p^i(p^{p-j-i}-1)\right).$$

Finally, we analyze the case $j = 2$: it easily seen that $d_{E_2^{\lambda,\mu}|L}$ does not depend on whether $W_2^{\lambda,\mu} = G^{v_p}$ or not. Furthermore we have

$$d_{2|L} = d_{E_2^{\lambda,\mu}|L} = p\left(2(p^{p-2}-1) + \sum_{i=1}^{p-3} p^i(p^{p-i-2}-1)\right).$$

We denote by $\mathfrak{d}_{L|\mathbb{Q}_p}$ the discriminant of $L|\mathbb{Q}_p$ and we put $d_{L|\mathbb{Q}_p} = v(\mathfrak{d}_{L|\mathbb{Q}_p})$. Using the formula for the discriminants in towers of extensions, we get if $3 \leq j \leq p$,

$$d_{E_j^{\lambda,\mu}|\mathbb{Q}_p} = p^{p-j+1} d_{L|\mathbb{Q}_p} + d_{E_j^{\lambda,\mu}|L}$$

and analogous formulas in the case $j = 2$.

8. Classification table

We collect our results in a table which describes the classification of the extensions of degree p^2 over $\mathbb{Q}_p$ whose normal closure is a p-extension. We recall some notations. Let λ be a fixed element in $(\mathbb{Z}/p\mathbb{Z})^*$ and let j run in $\{3, 4, \ldots, p\}$. In the following table, the first four lines list the Galois extensions of degree p^2 over $\mathbb{Q}_p$. Lines from the fifth to the seventh list the non-normal extension of $\mathcal{E}_{\mathbb{Q}_p}(K_0)$. The remaining lines describe the non normal totally ramified extensions of degree p^2 over $\mathbb{Q}_p$. When j appears in a line, it simply means that there is a set of lines obtained by replacing $3, 4, \ldots, p$ to j. For an extension $L \in \mathcal{E}_{\mathbb{Q}_p}$, $e = e(L|\mathbb{Q}_p)$ is the ramification index of L, $d = d_{L|\mathbb{Q}_p} = v(\mathfrak{d}_{L|\mathbb{Q}_p})$ is the valuation of the discriminant of L, $G = Gal(\overline{L}|\mathbb{Q}_p)$ where $\overline{L}$ is the normal closure of L over $\mathbb{Q}_p$ and we

put $\overline{e} = e(\overline{L}|\mathbb{Q}_p)$ for the ramification index of $\overline{L}$ and $\overline{f} = f(\overline{L}|\mathbb{Q}_p)$ for the inertia degree of $\overline{L}$. Finally $\overline{d} = d_{\overline{L}|\mathbb{Q}_p} = v(\mathfrak{d}_{\overline{L}|\mathbb{Q}_p})$ is the valuation of the discriminant of $\overline{L}$.

TABLE 1. *Extensions of degree p^2 over $\mathbb{Q}_p$ whose normal closure is a p-extension.*

Number	e	d	G	$\overline{e}$	$\overline{f}$	$\overline{d}$
1	1	0	$\mathbb{Z}/p^2\mathbb{Z}$	1	p^2	0
$p-1$	p	$2p(p-1)$	$\mathbb{Z}/p^2\mathbb{Z}$	p	p	$2p(p-1)$
p^2	p^2	$2(p^2-1)+p(p-1)$	$\mathbb{Z}/p^2\mathbb{Z}$	p^2	1	$2(p^2-1)+p(p-1)$
1	p	$2p(p-1)$	$(\mathbb{Z}/p\mathbb{Z})^2$	p	p	$2p(p-1)$
p^{p-j+1}	p	$2p(p-1)$	$G_p/W_j^{0,1}$	p^{p-j+2}	p	$2p(p^{p-j+1}-1)$
$(p-1)p^{p-j+1}$	p	$2p(p-1)$	$G_p/W_j^{\lambda,1}$	p^{p-j+2}	p	$2p(p^{p-j+1}-1)$
p^p	p	$2p(p-1)$	$G_p/W_2^{0,1}$	p^p	p	$2p(p^{p-1}-1)$
p^{p-j+2}	p^2	$(d_{E_j^{0,1}\|\mathbb{Q}_p} - d_{E_j^{0,1}\|L})/p^{p-j+1}$	$G_p/W_j^{0,1}$	p^{p-j+2}	p	$d_{E_j^{0,1}\|\mathbb{Q}_p}$
$(p-1)p^{p-j+2}$	p^2	$(d_{E_j^{\lambda,1}\|\mathbb{Q}_p} - d_{E_j^{\lambda,1}\|L})/p^{p-j+1}$	$G_p/W_j^{\lambda,1}$	p^{p-j+2}	p	$d_{E_j^{\lambda,1}\|\mathbb{Q}_p}$
p^p	p^2	$(d_e - d_{2\|L})/p^{p-1}$	$G_p/W_2^{0,1}$	p^p	p	d_e
$(p-1)p^p$	p^2	$(d_u - d_{2\|L})/p^{p-1}$	$G_p/W_2^{0,1}$	p^p	p	d_u

References

[1] C. R. LEEDHAM-GREEN AND S. MCKAY, *The structure of groups of prime power order*, London Mathematical Society Monographs, New Series **27**, 2002

[2] E. MAUS, *On the jumps in the series of ramifications groups*, Colloque de Thorie des Nombres (Bordeaux, 1969), Bull. Soc. Math. France, Mem. No. *25* (1971), 127-133

[3] I. R. ŠAFAREVIČ, *On p-extensions*, Mat. Sb. **20** (**62**) (1947), 351-363 (Russian); English translation, Amer. Math. Soc. Transl. Ser. 2 **4** (1956), 59-72

[4] J. P. SERRE, *Local fields*, GTM **7**, Springer-Verlag, 1979

[5] H. ZASSENHAUS, *The theory of groups*, Chelsea, 1958

Luca CAPUTO
Università di Pisa
Largo Bruno Pontecorvo, 5
56127 Pisa, Italy
Université de Bordeaux 1
351, cours de la Libration
33405 Talence cedex, France
E-mail : caputo@mail.dm.unipi.it