JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Filippo VIVIANI

Ramification groups and Artin conductors of radical extensions of $\mathbb{Q}$

Tome 16, n° 3 (2004), p. 779-816.

<http://jtnb.cedram.org/item?id=JTNB_2004__16_3_779_0>

Journal de Théorie des Nombres
de Bordeaux **16** (2004), 779–816

Ramification groups and Artin conductors of radical extensions of $\mathbb{Q}$

par Filippo VIVIANI

Résumé. Nous étudions les propriétés de ramification des extensions $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}$ sous l'hypothèse que m est impair et si $p \mid m$, ou bien $p \nmid v_p(a)$ ou bien $p^{v_p(m)} \mid v_p(a)$ ($v_p(m)$ et $v_p(a)$ sont les exposants avec lesquels p divise a et m). En particulier, nous déterminons les groupes de ramification supérieurs des extensions complétées et les conducteurs d'Artin des caractères de leur groupe de Galois. A titre d'application, nous donnons des formules pour la valuation p-adique du discriminant des extensions globales considérées avec $m = p^r$.

Abstract. We study the ramification properties of the extensions $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}$ under the hypothesis that m is odd and if $p \mid m$ than either $p \nmid v_p(a)$ or $p^{v_p(m)} \mid v_p(a)$ ($v_p(a)$ and $v_p(m)$ are the exponents with which p divides a and m). In particular we determine the higher ramification groups of the completed extensions and the Artin conductors of the characters of their Galois group. As an application, we give formulas for the p-adique valuation of the discriminant of the studied global extensions with $m = p^r$.

1. Introduction

In this paper we study the ramification properties (ramification groups and Artin conductors) of the normal radical extensions of $\mathbb{Q}$, namely of the fields of the form $\mathbb{Q}(\zeta_m, \sqrt[m]{a})$ (ζ_m a primitive m-th rooot of unity, $a \in \mathbb{Z}$), under the hypothesis: (1) m odd; (2) if $p \mid m$ then either $p \nmid v_p(a)$ or $p^{v_p(m)} \mid v_p(a)$. While the first hypothesis is assumed for simplicity (many strange phenomenas appear when $2 \mid m$ as the examples of the second section show), the second hypothesis is a technical hypothesis that unfortunately we weren't able to overcome (we will explain in a moment why).

The interest in the radical extensions of the rationals is due to the fact that they are the simplest and the more explicit normal fields other than the abelian fields, so they are the "first" extensions not classified by the

Manuscrit reçu le 20 juin 2003.

class field theory. They have been studied under several point of view: Westlund ([16]) and Komatsu ([5]) determined integral bases for $\mathbb{Q}(\sqrt[p]{a})$ and $\mathbb{Q}(\zeta_p, \sqrt[p]{a})$, respectively. Velez and Mann (see [7], [13], [15]) studied the factorization of primes in $\mathbb{Q}(\sqrt[m]{a})$ and Jacobson and Velez ([4]) determined in complete generality the Galois group of $\mathbb{Q}(\zeta_m, \sqrt[m]{a})$ (many complications arise when $2 \mid m$, the case that we for simplicity avoid). Eventually, the algebraic properties of the radical extensions have been studied by Acosta and Velez [1], Mora and Velez [8] and Velez [14].

Our work is oriented in two new directions: the calculation of the ramification groups and the Artin conductor of the characters of the Galois group (for their definition and properties we refer to the chapter IV and VI of the Serre's book [10]). Let us now explain briefly what are the methods that we used to obtain these results.

To calculate the ramification groups we first complete our extensions with respect to p-adic valutation reducing in this way to study the ramification groups of $p \neq 2$ in the local extension $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^r]{a})$. Our original hypothesis on a splits in the two cases: (1) $p \nmid a$; (2) $p \mid\mid a$ (i.e. $p \mid a$ but $p^2 \nmid a$, or $v_p(a) = 1$).

Then the successive step is to calculate the ramification groups of the extensions $\mathbb{Q}_p(\zeta_p, \sqrt[p^{i-1}]{a}) < \mathbb{Q}_p(\zeta_p, \sqrt[p^i]{a})$ and we succeed in this by finding a uniformizer (i.e. an element of valuation 1) and letting the generator of the cyclic Galois group act on it (see Theorems 5.6 and 6.4).

The final step is a long and rather involved process of induction which uses the knowledge of the ramification groups of the cyclotomic fields (see [10, Chapter IV, section 4]) as well as the functorial properties of the inferior and superior ramification groups (see [10, Chapter IV, section 3]).

Let us make at this point three remarks about these results and the method used:
(1) the results obtained (Theorem 5.8 and 6.6) show that in the non-abelian case the break-numbers in the superior ramification groups are not necessarily integers (while the theorem of Hasse-Arf (see [10, Chapter V, section 7]) tells that this always happens in the abelian case).
(2) the original hypothesis on the power of p that divides a is necessary because only in this case we are able to find an uniformizer for the extension $\mathbb{Q}_p(\zeta_p, \sqrt[p^s]{a}) < \mathbb{Q}_p(\zeta_p, \sqrt[p^{s+1}]{a})$. If one finds a uniformizer also for the other cases than the same method will give the desired ramification groups in complete generality.
(3) a much more simple and short proof could be obtained if one finds directly a uniformizer for the whole extension $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^r]{a})$. Unfortunately we were unable to find this.

The other direction of our work is the calculation of the Artin conductor of the characters of the Galois group $G := Gal(\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q})$ (again we first reduce to the case $m = p^r$).

So our first result is the explicit determination of the characters of G (Theorem 3.7) and in order to do that we construct characters in two ways: (1) restricting characters of $(\mathbb{Z}/p^r\mathbb{Z})^*$ under the projection $G \twoheadrightarrow (\mathbb{Z}/p^r\mathbb{Z})^*$. (2) making Frobenius induction of characters of $\mathbb{Z}/p^r\mathbb{Z}$ under the inclusion $\mathbb{Z}/p^r\mathbb{Z} \hookrightarrow G$.

After this we determine the local Artin conductor of a character χ by looking at its restriction at the ramification groups (Theorems 5.13 and 6.12).

Now let us summarize the contents of the various sections of the paper.

In the second section we recall some known results on radical extensions and we prove, by applying a theorem of Schinzel (see [9]), that if k is a field that doesn't contain any non trivial m-root of unity then the polynomial $x^m - a$ remains irreducible over $k(\zeta_m)$ if it is irreducible over k (we shall apply this for $k = \mathbb{Q}, \mathbb{Q}_p$).

In the third section we calculate the characters of the group $Gal(\mathbb{Q}(\zeta_m, \sqrt[m]{a}))$ after having decomposed it according to the prime powers that divide m.

In the fourth section we treat the case of tamely ramified primes. In particular we show that if $p \mid a$ but $p \nmid m$ then p is tamely ramified and we calculate its ramification index (Theorem 4.3). Moreover in the case $p \mid m$ we show that the wild part of the ramification is concentrated in the p-part $\mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a})$ (Theorem 4.4).

The last two sections are devoted to study the ramification of p in $\mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a})$ in the two cases $p \nmid a$ and $p \mid a$. In particular we compute the ramification groups of p and the p-local Artin conductor of the characters found in the third section. Then, by applying the conductor-discriminat formula, we calculate the power of p which divides the discriminant.

The referee pointed out to me that in the article: H. Koch, E. de Shalit, *Metabelian local class field theory.* J. reine angew. Math. **478** (1996), 85-106, the authors studied the ramification groups of the maximal metabelian extension of a local field (of which the radical extensions considered here are particular examples) and asked about the compatibility between their and mine results. Actually to compare the results, one should compute the image of the metabelian norm map of our extensions and it's not at all clear to me how one can perform such a calculation (actually also in classical local class field theory, to determine the conductor of an abelian extension it's often simpler to calculate the ramification groups or the Artin conductors than the image of the norm map). The advantage

of my results is that they are explicit and permit to avoid this much more general and elaborated theory.

Aknowledgement: This work is the result of my master thesis which was made at the University of Pisa under the direction of prof. Roberto Dvornicich which we thank for his supervision and encouragements.

2. Some results on radical extensions

In this section we collect some known results on radical extensions that we shall need in the next sections. We shall always consider the equation $x^m - a$ defined over a field k such that $\mathrm{char}(k) \nmid m$ and we shall restrict ourselves to the case in which m is odd (when the prime 2 appears in the factorization of m, new strange phenomenas occur so that for semplicity we prefer to avoid these complications).

Theorem 2.1. *The equation $x^m - a$ (with m odd) is irreducible if and only if $a \notin k^p$ for every $p \mid m$.*

Proof. See [6, Chapter VI, Theorem 9.1]. □

Theorem 2.2. *Let $x^m - a$ irreducible over k with $2 \nmid m$. Then $k(\sqrt[m]{a})/k$ has the unique subfield property, i.e. for every divisor d of $[L : K]$ there exists a unique intermediate field M such that $[M : K] = d$.*
Precisely, if $d \mid m$, then the unique subextension L of degree d over k is $L = k(\sqrt[d]{a})$.

Proof. See [1, Theorem 2.1]. □

Theorem 2.3. *Let $x^m - a$ and $x^m - b$ irreducible over k, with m odd. If $k(\sqrt[m]{a}) = k(\sqrt[m]{b})$, then $\sqrt[m]{b} = c(\sqrt[m]{a})^t$ for some $c \in k$ and $t \in \mathbb{N}$ such that $(t, m) = 1$.*

Proof. It follows from the preceding theorem and from [12, Lemma 2.3]. □

Remark. *All these three results are false if m is divisible for 2 as the following examples show:*

(1) *$x^4 - (-4) = (x^2 + 2x + 2)(x^2 - 2x + 2)$ but $-4 \notin \mathbb{Q}^2$;*
(2) *$x^4 + 1$ is irreducible over $\mathbb{Q}$ but $\mathbb{Q}(\sqrt[4]{-1}) = \mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ has three subfields of degree 2: $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$;*
(3) *$\mathbb{Q}(\sqrt[8]{-1}) = \mathbb{Q}(\sqrt{2}, i, \sqrt{\sqrt{2} + 2}) = \mathbb{Q}(\sqrt[8]{-16})$ but $16 \notin \mathbb{Q}^8$.*

The last result we need is a theorem of Schinzel characterizing the abelian radical extensions, i.e. those radical extensions whose normal closure has abelian Galois group.

Theorem 2.4 (Schinzel)**.** *Let k be a field and let m be a natural such that $char(k) \nmid m$. Denote with ω_m the number of the m-roots of unity contained in k.*

Then the Galois group of $x^m - a$ over k is abelian (i.e. $Gal(k(\zeta_m, \sqrt[m]{a})/k)$ is abelian) if and only if $a^{\omega_m} = \gamma^m$ for some $\gamma \in k$.

Proof. See the original paper of Schinzel ([9, Theorem 2]). For other proofs see [12, Theorem 2.1] or [17, Lemma 7], while a nice generalization of this theorem is contained in [11]. □

Using the theorem of Schinzel we can prove the following proposition.

Proposition 2.5. *Let $1 \leq m \mid n$ and let k be a field such that $char(k) \nmid m$. If k doesn't contain any m-root of unity other than the identity then an element a of k is a m-power in $k(\zeta_n)$ if and only if it is a m-power in k.*

Proof. The "if" part is obvious. Conversely assume that $a \in k(\zeta_n)^m$. Then

$$k(\sqrt[m]{a}) \subset k(\zeta_n) \Rightarrow k(\sqrt[m]{a}, \zeta_m) \subset k(\sqrt[m]{a}, \zeta_n) \subset k(\zeta_n)$$

and so $x^m - a$ has abelian Galois group over k. But then the theorem of Schinzel implies $a \in k^m$, q.e.d. □

Remark. *The preceding result is false if the field contains some m-root of unity other than the identity as the following example shows:*

-1 is not a square in $\mathbb{Q}$ but it becomes a square in $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$ (the reason is that $\mathbb{Q}(i)$ contains the non trivial 2-root of unity -1).

We can now apply these results on radical extensions to the situation we are concerned with, i.e. the irreducibility of the polynomial $x^m - a$ defined over $\mathbb{Q}$ and with m odd.

Corollary 2.6. *If m is odd and $a \notin \mathbb{Q}^p$ for every $p \mid m$, then the polynomial $x^m - a$ is irreducible over $\mathbb{Q}$ and so the extension $\mathbb{Q}(\sqrt[m]{a})/\mathbb{Q}$ has degree m.*

Proof. It follows at once from Theorem 2.1. □

Moreover in the next sections we will consider the normal closure of $\mathbb{Q}(\sqrt[m]{a})$, i.e $\mathbb{Q}(\zeta_m, \sqrt[m]{a})$. The next result tells us what is the degree of this extension.

Corollary 2.7. *If m is odd and $a \notin \mathbb{Q}^p$ for every $p \mid m$, then $x^m - a$ is irreducible over $\mathbb{Q}(\zeta_m)$ and so $[\mathbb{Q}(\zeta_m, \sqrt[m]{a}) : \mathbb{Q}] = \phi(m)m$.*

Proof. It follows at once from Proposition 2.5 and Corollary 2.6 after observing that $\mathbb{Q}$ doesn't contain any m-root of unity other than 1 if m is odd. □

Remark. *Again the preceding result is false if $2 \mid m$ as the "usual" example shows:*

$x^4 + 1$ is irreducible over $\mathbb{Q}$ but over $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$ it splits as $x^4 + 1 = (x^2 + i)(x^2 - i)$ and hence $[\mathbb{Q}(\sqrt[4]{-1}, \zeta_4) : \mathbb{Q}] = 4 < \phi(4)4 = 8$.

For an analysis of the degree of the splitting field of the polynomial $x^{2^s} - a$ as well as of its Galois group see the paper [4].

We end this preliminary section with this useful splitting result.

Proposition 2.8. *If $m = \prod_{i=1}^{s} p_i^{r_i}$ then the extension $k(\sqrt[m]{a})$ is the compositum of the extensions $k(\sqrt[p_i^{r_i}]{a})$ for $i = 1, \cdots, s$, i.e.*

$$k(\sqrt[m]{a}) = k(\sqrt[p_1^{r_1}]{a}) \cdots k(\sqrt[p_s^{r_s}]{a}).$$

Proof. It's enough to prove that if $m = m_1 m_2$ with m_1 and m_2 relatively prime, then $k(\sqrt[m]{a}) = k(\sqrt[m_1]{a})k(\sqrt[m_2]{a})$. The inclusion $k(\sqrt[m]{a}) \supset k(\sqrt[m_1]{a})k(\sqrt[m_2]{a})$ is obvious. On the other hand, since $(m_1, m_2) = 1$, there exist $s, t \in \mathbb{Z}$ such that $sm_1 + tm_2 = 1$. But this imply $(\sqrt[m_1]{a})^t(\sqrt[m_2]{a})^s = (\sqrt[m_1 m_2]{a})^{tm_2+sm_1} = \sqrt[m]{a}$, q.e.d. □

3. Characters of the Galois groups of $\mathbf{x^m - a}$

First of all we want to describe the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q})$.

Definition 3.1. *The holomorphic group of a finite group G (non necessarily abelian, although we use the addittive notation) is the semidirect product of G with $Aut(G)$ (indicated with $G \rtimes Aut(G)$), that is the set of pairs $\{(g, \sigma) : g \in G, \sigma \in Aut(G)\}$ with the multiplication given by*

$$(g, \sigma)(h, \tau) = (g + \sigma(h), \sigma \circ \tau). \tag{3.1}$$

Notation. *We shall denote by $C(m)$ the cyclic group of order m (identified with $\mathbb{Z}/m\mathbb{Z}$) and with $G(m)$ the group of its automorphisms (identified with $(\mathbb{Z}/m\mathbb{Z})^*$). We shall denote the holomorphic group of $C(m)$ with $K(m) := C(m) \rtimes G(m)$ (the letter K stands for Kummer who first studied this kind of extensions).*

Proposition 3.2. *Suppose that $x^m - a$ is irreducible over $\mathbb{Q}$. Then the Galois group of $x^m - a$ is isomorphic to the holomorphic group of the cyclic group of order m, i.e.*

$$Gal(\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}) \cong C(m) \rtimes G(m) = K(m).$$

Proof. Every element σ of $\mathrm{Gal}(\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q})$ is uniquely determined by its values on the generators of the extension and on these it must hold

$$\begin{array}{ll} \sigma(\sqrt[m]{a}) = \zeta_m^i \sqrt[m]{a} & i \in C(m), \\ \sigma(\zeta_m) = \zeta_m^k & k \in G(m). \end{array}$$

Then we can define an injective homomorphism

$$\Gamma : \mathrm{Gal}(\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}) \longrightarrow C(m) \rtimes G(m)$$
$$\sigma \overset{\Gamma}{\longmapsto} (i, k).$$

But this is an isomorphism since both groups have cardinality equal to $m\phi(m)$ (see Proposition 2.7). □

Next a useful splitting result.

Proposition 3.3. *If $m = \prod_i p_i^{r_i}$ then $K(m) \cong \prod_i K(p_i^{r_i})$.*

Proof. This follows easily from the analogue property of the groups $C(m)$ and $G(m)$. □

So we have reduced ourselves to study the characters of the Kummer group $K(p^r) = C(p^r) \rtimes G(p^r)$, for p odd prime.

Notation. *In what follows we shall adopt the following convention: the elements of $K(p^r)$ will be denoted with $z^i\sigma$, where the roman letters $i, j, k, \cdots$ will indicate elements of $C(p^r)$, the greek letters $\sigma, \tau, \cdots$ will indicate elements of $G(p^r)$ and the letter z is an auxiliary letter that will allow to transform the multiplicative notation for $K(p^r)$ into the additive notation for its subgroup $C(p^r)$.*

With this notation, the product in $K(p^r)$ is ruled by the following equation

$$z^i\sigma z^j\tau = z^{i+\sigma j}\sigma\tau. \tag{3.2}$$

Observe that $G(p^r)$ acts on the normal subgroup $C(p^r)$ by

$$\sigma z^i\sigma^{-1} = z^{\sigma i}. \tag{3.3}$$

Let us determine the conjugacy classes of $K(p^r)$.

Theorem 3.4. *Let $z^i\sigma$ be an element of $K(p^r)$ ($p \neq 2$) and let*

$$\begin{cases} \alpha = v_p(\sigma - 1) & 0 \leq \alpha \leq r, \\ \beta = v_p(i) & 0 \leq \beta \leq r. \end{cases}$$

Then the conjugacy class of $z^i\sigma$ is

$$[z^i\sigma] = \begin{cases} \{\, z^j\sigma \,:\, v_p(j) = v_p(i) = \beta \,\} & \text{if} \quad 0 \leq \beta < \alpha \\ \{\, z^j\sigma \,:\, v_p(j) \geq v_p(\sigma - 1) = \alpha \,\} & \text{if} \quad \alpha \leq \beta. \end{cases}$$

Proof. It's enough to consider the conjugates by elements of $C(p^r)$ and $G(p^r)$

$$z^{-k}z^i\sigma z^k = z^{i+k(\sigma-1)}\sigma, \tag{*}$$

$$\tau z^i\sigma\tau^{-1} = z^{i\tau}\sigma. \tag{**}$$

$\boxed{0 \leq \beta < \alpha}$ Let us prove the two inclusions in the statement of the theorem.

$\subseteq$ In (*) we have $v_p(i + k(\sigma - 1)) = v_p(i)$ since $v_p(i) < v_p(\sigma - 1) \leq v_p(k(\sigma - 1))$. In (**) $v_p(i\sigma) = v_p(i) + v_p(\sigma) = v_p(i)$.

$\supseteq$ Let $j \in C(p^r)$ be such that $v_p(j) = v_p(i)$. Then $\tau := ji^{-1}$ has p-adic valuation equal to 0 and so it belongs to $G(p^r)$. Then from (**) we see that

$z^j\sigma \in [z^i\sigma]$.

$\boxed{\alpha \leq \beta}$ Let us prove the two inclusions.

$\subseteq$ In (*) we have $v_p(i + k(\sigma - 1)) \geq \min\{v_p(i), v_p(k) + v_p(\sigma - 1)\} \geq \min\{\alpha, v_p(k) + \alpha\} = \alpha$. In (**) $v_p(i\tau) = v_p(i) = \beta \geq \alpha$.

$\supseteq$ Given $j \in C(p^r)$ such that $v_p(j) \geq v_p(\sigma - 1)$, the equation $j = i + k(\sigma - 1)$ is solvable for some $k \in C(p^r)$ and so from (*) we conclude $z^j\sigma \in [z^i\sigma]$. □

Recall that the group $G(p^r)$ has a filtration given by the subgroups $G(p^r)^\alpha = \{\, \sigma \in G(p^r) \,:\, v_p(\sigma - 1) \geq \alpha \,\}$.

Corollary 3.5. *Given $\sigma \in G(p^r)$ such that $v_p(\sigma - 1) = \alpha$ (which from now on we shall denote with σ_α), the set $\{\, z^i\sigma \,:\, i \in C(p^r)\}$ is invariant under conjugacy and splits in the $\alpha + 1$ classes*

$$\begin{aligned}
[z\sigma_\alpha] &= \{\, z^j\sigma_\alpha \,:\, v_p(j) = 0\} \\
&\cdots \qquad\qquad \cdots \\
[z^{p^i}\sigma_\alpha] &= \{\, z^j\sigma_\alpha \,:\, v_p(j) = i\} \\
&\cdots \qquad\qquad \cdots \\
[z^{p^{\alpha-1}}\sigma_\alpha] &= \{\, z^j\sigma_\alpha \,:\, v_p(j) = \alpha - 1\} \\
[z^{p^\alpha}\sigma_\alpha] &= \{\, z^j\sigma_\alpha \,:\, v_p(j) \geq \alpha\}.
\end{aligned}$$

Now we can count the number of conjugacy classes of $K(p^r)$.

Proposition 3.6. *The number of conjugacy classes of $K(p^r)$ (p odd prime) is equal to*

$$\#\{\textit{Conjugacy classes}\} = (p-1)p^{r-1} + \frac{p^r - 1}{p - 1}.$$

Proof. According to the preceding corollary we have

$$\begin{aligned}
&\#\{[z\sigma]\} = p^{r-1}(p-1) \\
&\#\{[z^p\sigma] \,:\, [z^p\sigma] \neq [z\sigma]\} = \#\{\sigma \,:\, v_p(\sigma - 1) \geq 1\} = |G(p^r)^1| = p^{r-1} \\
&\quad \cdots \\
&\#\{[z^{p^r}\sigma] \,:\, [z^{p^r}\sigma] \neq [z^{p^{r-1}}\sigma]\} = \#\{\sigma \,:\, v_p(\sigma - 1) \geq r\} = |G(p^r)^r| = 1.
\end{aligned}$$

So the number of conjugacy classes is

$$\#\{\text{Conjugacy classes}\} = p^{r-1}(p-1) + p^{r-1} + \cdots + p^{r-r} = p^{r-1}(p-1) + \frac{p^r - 1}{p - 1}.$$

□

Before we determine the characters of $K(p^r)$, we recall some facts about the characters of the group $G(p^r) = (\mathbb{Z}/p^r\mathbb{Z})^*$, with p odd prime. First of all we know that

$$G(p^r) = < g^{p^{r-1}} > \oplus < 1 + p > \cong C(p-1) \times C(p^{r-1})$$

with $0 < g < p$ a generator of the cyclic group $G(p)$.

Besides recall that $G(p^r)$ has a natural filtration

$$G(p^r) \supset G(p^r)^1 \supset \cdots \supset G(p^r)^{r-1} \supset G(p^r)^r = \{1\}$$

where $G(p^r)^k = \{\sigma \in G(p^r) : v_p(\sigma - 1) \geq k\} =< 1 + p^k > \cong C(p^{r-k})$, for $1 \leq k \leq r$, and moreover we have $G(p^r)/G(p^r)^k = G(p^k)$.

If we translate this information at the level of characters we obtain:

(1) $G(p^k)^* \subset G(p^r)^*$ through the projection $G(p^r) \twoheadrightarrow G(p^k)$;

(2) $G(p^r)^*/G(p^k)^* = (G(p^r)^k)^* \cong C(p^{r-k})$ through the inclusion

$$G(p^r)^k =< 1 + p^k > \hookrightarrow G(p^r).$$

Notation. *In what follows we shall denote the characters of $G(p^r)$ with ψ^r, and with ψ_k^r a fixed system of representatives for the lateral cosets of $G(p^k)^*$ in $G(p^r)^*$, in such a way that, when restricted, they give all the characters of $G(p^r)^k$.*

With these notation we can now determine all the characters of $K(p^r)$.

Theorem 3.7. *The irreducible characters of $K(p^r)$ (for p odd prime) are*

CHARACTERS	*Number*	*Degree*
ψ^r *with* $\psi^r \in G(p^r)^*$	$p^{r-1}(p-1)$	1
$\psi_r^r \otimes \chi_r^r$ *with* ψ_r^r *syst. of repr. for* $G(p^r)^*/G(p^r)^*$	1	$p^{r-1}(p-1)$
...	...	...
$\psi_k^r \otimes \chi_k^r$ *with* ψ_k^r *syst. of repr. for* $G(p^r)^*/G(p^k)^*$	p^{r-k}	$p^{k-1}(p-1)$
...	...	...
$\psi_1^r \otimes \chi_1^r$ *with* ψ_1^r *syst. of repr. for* $G(p^r)^*/G(p^1)^*$	p^{r-1}	$(p-1)$

where

(i) $\otimes$ means the tensorial product of representations which, at the level of characters, becomes pointwise product;

(ii) ψ^r is the character defined by

$$\psi^r(z^{p^\beta}\sigma_\alpha) = \psi^r(\sigma_\alpha)$$

that is the character induced on $K(p^r)$ from $G(p^r)$ through the projection $K(p^r) \twoheadrightarrow G(p^r)$. Analogously the ψ_k^r are seen as characters on $K(p^r)$.

(iii) χ_k^r, $1 \leq k \leq r$, is the character defined by

$$\chi_k^r([z^{p^\beta}\sigma_\alpha]) = \begin{cases} 0 & \text{if} \quad \alpha < k \quad \text{or} \quad \beta < k-1, \\ -p^{k-1} & \text{if} \quad k \leq \alpha \quad \text{and} \quad \beta = k-1, \\ p^{k-1}(p-1) & \text{if} \quad k \leq \alpha \quad \text{and} \quad k-1 < \beta. \end{cases}$$

(Recall that σ_α indicates an element of $K(p^r)$ such that $v_p(\sigma-1)=\alpha$).

Proof. First some remarks:

(1) All the functions in the above table (which are clearly class functions) are distinct. In fact for functions belonging to different rows, this follows from the fact that they have different degrees; for functions of the first rows it's obvious; finally for the functions $\psi_k^r \otimes \chi_k^r$ notice that

$$\psi_k^r \otimes \chi_k^r([z^{p^k}(1+p^k)]) = p^{k-1}(p-1)\psi_k^r(1+p^k)$$

and so the difference follows from having chosen the ψ_k^r among a rapresentative system of $G(p^r)^*/G(p^k)^* =< 1+p^k >^*$ in $G(p^r)^*$.

Hence, being all distinct, the number of these functions is

$$\#\{\text{Characters on the table}\} = p^{r-1}(p-1)+\sum_{k=1}^{r} p^{r-k} = p^{r-1}(p-1)+\frac{p^r-1}{p-1}$$

which, for the Proposition 3.6, is equal to the number of conjugacy classes of $K(p^r)$. So it's enough to show that they are indeed irreducible characters of $K(p^r)$.

(2) The functions ψ^r (hence also ψ_k^r) are irreducible characters as they are induced by irreducible characters of $G(p^r)$ through the projection $K(p^r) \twoheadrightarrow G(p^r)$.

(3) As the ψ^r (and so ψ_k^r) have values in $\mathbb{S}^1 = \{z \in \mathbb{C} :\mid z \mid = 1\}$, in order to verify that $\psi_k^r \otimes \chi_k^r$ are irreducible characters, it's enough to verify that the χ_k^r are. In fact, by the remark (i) of the theorem, the tensorial product of two irreducible characters is again a character; as for the irreducibility we can calculate their norm (in the usual scalar product between characters) as follows

$$\begin{aligned}(\psi_k^r \otimes \chi_k^r, \psi_k^r \otimes \chi_k^r)_{K(p^r)} &= \frac{1}{|K(p^r)|}\sum_{g\in K(p^r)} \psi_k^r(g)\chi_k^r(g)\overline{\psi_k^r(g)\chi_k^r(g)} \\ &= \frac{1}{|K(p^r)|}\sum_{g\in K(p^r)} \chi_k^r(g)\overline{\chi_k^r(g)} = (\chi_k^r, \chi_k^r)_{K(p^r)}\end{aligned}$$

from which it follows that $\psi_k^r \otimes \chi_k^r$ is irreducible if and only if χ_k^r is irreducible.

So these remarks tell us that to prove the theorem it's enough to show that the functions χ_k^r are irreducible characters of $K(p^r)$. We will do this first for the "top" function χ_r^r and then for the others functions χ_k^r, $1 \leq k \leq r-1$, we will proceed by induction on r.

$\boxed{\chi_r^r}$

We will show first that it is a character and then that it is irreducible.

CHARACTER

Consider the primitive character χ of $C(p^r)$ which sends $[1]_{C(p^r)}$ in ζ_{p^r} and induct with respect to the inclusion $C(p^r) \hookrightarrow C(p^r) \rtimes G(p^r) = K(p^r)$. The formula for the induced character χ^* (see [6, Chapter XVIII, Section 6]) tells us

$$\chi^*(z^i\sigma) = \sum_{\substack{\tau \in G(p^r) \\ \tau z^i \sigma \tau^{-1} \in C(p^r)}} \chi(\tau z^i \sigma \tau^{-1})$$

$$= \begin{cases} 0 & \text{if } \sigma \neq 1, \\ \displaystyle\sum_{\tau \in G(p^r)} \chi(z^{i\tau}) = \sum_{\tau \in G(p^r)} (\zeta_{p^r}^i)^\tau & \text{if } \sigma = 1. \end{cases}$$

Let us calculate the last summation.

Lemma 3.8. *Given $0 \leq s \leq r$, we have*

$$\sum_{\tau \in G(p^r)} \zeta_{p^s}^\tau = \begin{cases} 0 & \text{if} \quad s \geq 2 \\ -p^{r-1} & \text{if} \quad s = 1 \\ p^{r-1}(p-1) & \text{if} \quad s = 0. \end{cases} \tag{3.4}$$

Proof. For $t \geq s$ we have

$$\sum_{x \in C(p^t)} \zeta_{p^s}^x = \begin{cases} 0 & \text{if} \quad s \geq 1 \\ p^t & \text{if} \quad s = 0 \end{cases} \tag{3.5}$$

where the last one is obvious since $\zeta_{p^0} = 1$ while the first equality follows from the fact that ζ_{p^s}, with $1 \leq s$, is a root of the polynomial $x^{p^s-1} + \cdots + 1$ and so

$$\sum_{x \in C(p^t)} \zeta_{p^s}^x = \sum_{\substack{y \in C(p^s) \\ z \in C(p^{t-s})}} \zeta_{p^s}^{zp^s+y} = p^{t-s} \sum_{y \in C(p^s)} \zeta_{p^s}^y = 0.$$

With the help of formula (3.5), we can write

$$\sum_{\tau \in G(p^r)} \zeta_{p^s}^\tau = \sum_{x \in C(p^r)} \zeta_{p^s}^x - \sum_{y \in C(p^{r-1})} \zeta_{p^s}^{py}$$

$$= \begin{cases} 0 & \text{if} \quad s \geq 2 \\ -p^{r-1} & \text{if} \quad s = 1 \\ p^r - p^{r-1} = p^{r-1}(p-1) & \text{if} \quad s = 0. \end{cases}$$

□

Hence for χ^* we obtain

$$\chi^*([z^{p^\beta}\sigma_\alpha]) = \begin{cases} 0 & \text{if} \quad \sigma_\alpha \neq 1 \quad \text{or} \quad r-\beta \geq 1 \\ -p^{r-1} & \text{if} \quad \sigma_\alpha = 1 \quad \text{and} \quad r-\beta = 1 \\ p^{r-1}(p-1) & \text{if} \quad \sigma_\alpha = 1 \quad \text{and} \quad r-\beta = 0 \end{cases}$$

which is precisely the definition of χ_r^r. So, being induced from a character of $C(p^r)$, χ_r^r is a character of $K(p^r)$.

IRREDUCIBILITY

Now we calculate the scalar product of χ_r^r with itself. Since $[z^{p^r}\sigma_r]$ contains only the identity and $[z^{p^{r-1}}\sigma_r]$ contains $p-1$ elements, we have

$$\begin{aligned} (\chi_r^r, \chi_r^r)_{K(p^r)} &= \frac{1}{|K(p^r)|} \sum_{g \in K(p^r)} \chi_r^r(g)\overline{\chi_r^r(g)} \\ &= \frac{1}{|K(p^r)|} \left\{ \left[p^{r-1}(p-1)\right]^2 + (p-1)\left[-p^{r-1}\right]^2 \right\} \\ &= \frac{p^{2(r-1)}(p-1)p}{|K(p^r)|} = 1 \end{aligned}$$

from which the irreducibility of χ_r^r.

$\boxed{\chi_k^r,\ 1 \leq k \leq r-1}$

Proceed by induction on r (for $r = 1$ we have only the function χ_1^1 which is an irreducible character for what proved before). So let us assume, by induction hypothesis, that χ_k^{r-1}, $1 \leq k \leq r-1$, are irreducible characters of $K(p^{r-1})$ and let us show that χ_k^r is an irreducible character of $K(p^r)$. In order to do this, consider the projection

$$\pi_r : K(p^r) \twoheadrightarrow K(p^{r-1})$$

obtained by reducing both $C(p^r)$ and $G(p^r)$ modulo p^{r-1}. Pull back the character χ_k^{r-1} to an irreducible character $(\chi_k^{r-1})'$ on $K(p^r)$. We will show

$$(\chi_k^{r-1})' = \chi_k^r \tag{3.6}$$

and this will conclude the proof. Since, by definition,

$$(\chi_k^{r-1})'([z^{p^\beta}\sigma_\alpha]) = \chi_k^{r-1}(\pi_r([z^{p^\beta}\sigma_\alpha]))$$

and on the other hand

$$\pi_r([z^{p^\beta}\sigma_\alpha]) = \begin{cases} \text{if} \quad \alpha \leq r-1 & = [z^{p^\beta}\sigma_\alpha] \\ \text{if} \quad \alpha = r & \begin{cases} \text{and if} \quad \beta \leq r-1 & = [z^{p^\beta} \cdot 1] \\ \text{and if} \quad \beta = r & = [1] \end{cases} \end{cases}$$

then we have

$$(\chi_k^{r-1})'([z^{p^\beta}\sigma_\alpha]) =$$

$$\begin{cases} \text{if} \quad \alpha \leq r-1 & \begin{cases} \text{and if} \quad \alpha < k \quad \text{or} \quad \beta < k-1 & = 0 \\ \text{and if} \quad k \leq \alpha \quad \text{and} \quad \beta = k-1 & = -p^{k-1} \\ \text{and if} \quad k \leq \alpha \quad \text{and} \quad k-1 < \beta & = p^{k-1}(p-1) \end{cases} \\ \text{if} \quad \alpha = r & \begin{cases} \text{and if} \quad \beta < k-1 & = 0 \\ \text{and if} \quad \beta = k-1 & = -p^{k-1} \\ \text{and if} \quad k-1 < \beta \leq r-1 & = p^{k-1}(p-1) \\ \text{and if} \quad \beta = r & = p^{k-1}(p-1) \end{cases} \end{cases}$$

from which it follows that $(\chi_k^{r-1})' = \chi_k^r$. □

In the next section we will consider also the group $C(p^s) \rtimes G(p^r)$ for some $0 \leq s \leq r$ where the semi-direct product is made with respect to the map $G(p^r) \twoheadrightarrow G(p^s) \cong \mathrm{Aut}(C(p^s))$. As a corollary of the preceding theorem, we now derive also explicit formulas for the characters of this group (we can suppose $1 \leq s \leq r$ because if $s = 0$ we obtain the group $G(p^r)$ of which already we know the characters). The notation used will be similar to that of the Theorem 3.7.

Corollary 3.9. *The irreducible characters of* $C(p^s) \rtimes G(p^r)$ *are*

CHARACTERS	*Number*	*Degree*
ψ^r *with* $\psi^r \in G(p^r)^*$	$p^{r-1}(p-1)$	1
$\psi_r^r \otimes \chi_r^r$ *with* ψ_r^r *syst. of repr. for* $G(p^r)^*/G(p^r)^*$	1	$p^{r-1}(p-1)$
$\cdots$	$\cdots$	$\cdots$
$\psi_k^r \otimes \chi_k^r$ *with* ψ_k^r *syst. of repr. for* $G(p^r)^*/G(p^k)^*$	p^{r-k}	$p^{k-1}(p-1)$
$\cdots$	$\cdots$	$\cdots$
$\psi_1^r \otimes \chi_1^r$ *with* ψ_1^r *syst. of repr. for* $G(p^r)^*/G(p^1)^*$	p^{r-1}	$(p-1)$

where χ_k^s, $1 \leq k \leq s$, *is the character so defined*

$$\chi_k^s([z^{p^\beta}\sigma_\alpha]) = \begin{cases} 0 & \text{if} \quad \alpha < k \quad \text{or} \quad \beta < k-1, \\ -p^{k-1} & \text{if} \quad k \leq \alpha \quad \text{and} \quad \beta = k-1, \\ p^{k-1}(p-1) & \text{if} \quad k \leq \alpha \quad \text{and} \quad k-1 < \beta. \end{cases}$$

Proof. Observe first of all that the number of conjugacy classes of $C(p^s) \rtimes G(p^r)$ is determined by the same rules of Theorem 2.4 except for the new

condition $\beta = v_p(i) \leq s$. Hence the number of the conjugacy classes can be calculated in this way

$$\begin{aligned}\#\{\text{Conjugacy classes}\} &= \#\{[z\sigma]\} + \#\{[z^p\sigma] \,:\, [z^p\sigma] \neq [z\sigma]\} \\ &\quad + \cdots + \#\{[z^{p^s}\sigma] \,:\, [z^{p^s}\sigma] \neq [z^{p^{s-1}}\sigma]\} \\ &= |G(p^r)| + |G(p^r)^1| + \cdots + |G(p^r)^s| \\ &= p^{r-1}(p-1) + p^{r-1} + \cdots + p^{r-s} \\ &= p^{r-1}(p-1) + p^{r-s}\frac{p^s-1}{p-1}. \qquad (3.7)\end{aligned}$$

Now consider the projection

$$\pi : C(p^r) \rtimes G(p^r) \twoheadrightarrow C(p^s) \rtimes G(p^r)$$

obtained by reducing $C(p^r)$ modulo p^s. From it, we deduce that the irreducible representations of $C(p^s) \rtimes G(p^r)$ are exactly the representations of $C(p^r) \rtimes G(p^r)$ which are the identity on $\ker \pi =< z^{p^s} >$. This implies that an irreducible character of $C(p^s) \rtimes G(p^r)$ induces, by composition with the projection π, an irreducible character χ of $C(p^r) \rtimes G(p^r)$ such that

$$\chi_{|<z^{p^s}>} = \chi(1) \cdot 1_{|<z^{p^s}>}.$$

The only characters of $C(p^r) \rtimes G(p^r)$ which satisfy this property are (with the notation of the Theorem 3.7):

(i) ψ^r, for which $\psi^r([z^{p^s}]) = 1 = \chi([1])$;

(ii) $\psi_k^r \otimes \chi_k^r$, with $1 \leq k \leq s$, for which

$$\psi_k^r \otimes \chi_k^r([z^{p^s}]1) = p^{k-1}(p-1) = \psi_k^r \otimes \chi_k^r([1]).$$

As their number is

$$p^{r-1}(p-1) + p^{r-1} + \cdots + p^{r-s} = p^{r-1}(p-1) + p^{r-s}\frac{p^s-1}{p-1}$$

which, for what observed at the beginning, is the number of the conjugacy classes of $C(p^s) \rtimes G(p^r)$, necessarily they are all the irreducible characters $C(p^s) \rtimes G(p^r)$. This proves the theorem after having renamed χ_k^r as χ_k^s. □

In the next sections, in order to calculate the Artin conductor, we will be interested in knowing if the restriction of a character to certain subgroups is trivial or not. So we end this section with a result in this direction. First some definitions.

Definition 3.10 (Level)**.** *We call level of a character of $C(p^s) \rtimes G(p^r)$ the number so determined:*

$$lev(\chi) = \begin{cases} 0 & \text{if } \chi = \psi^r \in G(p^r)^* \\ k & \text{if } \chi = \psi_k^r \otimes \chi_k^s. \end{cases}$$

Definition 3.11 (Primitive degree)**.** *It is called primitive degree (and indicated pr) of $\psi^r \in G(p^r)^*$ the smallest number $0 \leq \rho \leq r$ such that ψ^r is induced by a character of $G(p^\rho)$ through the projection $G(p^r) \twoheadrightarrow G(p^\rho)$.*

It is called primitive degree of $\psi_k^r \otimes \chi_k^s$ the smallest number $k \leq \rho \leq r$ such that ψ_k^r is induced by a character of $G(p^\rho)$ through the projection $G(p^r) \twoheadrightarrow G(p^\rho)$.

Definition 3.12 (Null subgroup)**.** *The null subgroup of a character χ of $C(p^s) \rtimes G(p^r)$ (indicated with $Gr(\chi)$) is the smallest subgroup of $C(p^s) \rtimes G(p^r)$ such that*

$$\chi_{|Gr(\chi)} = \chi(1)1_{|Gr(\chi)}$$

i.e. the corresponding representation is the identity.

Theorem 3.13. *The null subgroup of a character χ of $C(p^s) \rtimes G(p^r)$ is equal to*

$$Gr(\chi) = C(p^{s-lev(\chi)}) \rtimes G(p^r)^{pr(\chi)}.$$

Proof. Observe that:

(1) $\psi \in G(p^r)^*$ is equal to 1 on $G(p^r)^t$ if and only if $t \geq pr(\psi)$.

(2) $\chi_k^s([z^{p^\beta}\sigma]) = \chi_k^s(1) = p^{k-1}(p-1)$ if and only if $\beta \geq k$ and $v_p(\sigma - 1) \geq k$.

From these two remarks it follows that

$$\chi([z^{p^\beta}\sigma]) = \chi(1) \Rightarrow \begin{cases} \beta \geq lev(\chi) \\ \sigma \in G(p^r)^{pr(\chi)} \end{cases}$$

and hence the theorem. □

4. Reduction to the prime power case

In the section we begin to study the ramification of a prime p in the extension $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}$ with the hypothesis m odd and if $p \mid m$ then $p \nmid v_p(a)$ or $p^{v_p(m)} \mid v_p(a)$. The aim of this section is to show that the wild part of the ramification is concentrated on the subextension $\mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a})$, where $r = v_p(m)$, so that the higher ramification groups can be calculated considering only this subextension.

First we want to determine which primes ramify in $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}$.

Lemma 4.1. *Let K be a number field and $L = K(\sqrt[n]{a})$. If a prime $\mathfrak{p}$ of K doesn't divide na then it is not ramified in L.*

Proof. Consider the discriminant $d(L/K)$ of L/K. It holds:

$$d(L/K) \mid d_{L/K}(\sqrt[n]{a}) \Big| \left(N_{L/K}((x^n - a)'_{|x=\sqrt[n]{a}} \right) = n^n a^{n-1}.$$

Hence if $\mathfrak{p} \nmid (na)$, then $\mathfrak{p} \nmid d(L/K)$ and so it is not ramified. □

Corollary 4.2. *The primes ramified in the extension* $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}$ *are the divisor of* m *or* a.

Next we study the primes which divides a but not m.

Theorem 4.3. *If* $p \nmid m$ *then* $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}$ *has ramification index respect to* p *equal to*

$$e(\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}) = \frac{m}{(m, v_p(a))}.$$

In particular it is tamely ramified.

Proof. Consider the tower of extensions

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[m]{a}) \subset \mathbb{Q}(\zeta_m, \sqrt[m]{a}).$$

The last extension is obtained by adding $\sqrt[m]{1}$ to the preceding one so that, as $p \nmid m$, Lemma 4.1 implies that it is not ramified respect to p. So the ramification index of the total extension is equal to the ramification index of the extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[m]{a})$.

If we put $d = (v_p(a), m)$, then we can write

$$a = p^{d\alpha} a'$$
$$m = dm'$$

with $(\alpha, m') = 1$ and $p \nmid (dm'a')$. Now consider the tower of extensions

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[d]{a}) \subset \mathbb{Q}(\sqrt[m]{a}).$$

Since $\sqrt[d]{a} = p^{\alpha} \sqrt[d]{a'}$, again by Lemma 4.1 we deduce that $\mathbb{Q} \subset \mathbb{Q}(\sqrt[d]{a}) = \mathbb{Q}(\sqrt[d]{a'})$ is not ramified respect to p. Hence the total ramification index is equal to the ramification index of the extension

$$\mathbb{Q}\left(\sqrt[d]{a'}\right) \subset \mathbb{Q}\left(\sqrt[m']{p^{\alpha}\sqrt[d]{a'}}\right).$$

Since $(\alpha, m') = 1$, there exist $s, t \in \mathbb{Z}$ such that $s\alpha - tm' = 1$ with $(s, m') = 1$. Now according to Theorem 2.3 we can transform the extension as

$$\mathbb{Q}\left(\sqrt[m']{p^{\alpha}\sqrt[d]{a'}}\right) = \mathbb{Q}\left(\left(\sqrt[m']{p^{\alpha}\sqrt[d]{a'}}\right)^{s} p^{-t}\right) = \mathbb{Q}\left(\sqrt[m']{p\sqrt[d]{(a')^{s}}}\right)$$

and so, called $u = \sqrt[d]{(a')^s}$, we can complete with respect to the valuation $\mathfrak{p}$-adic ($\mathfrak{p}$ is one the primes of $\mathbb{Q}\left(\sqrt[d]{a'}\right)$ lying above p) reducing ourselves to determine the ramification index of the local extension

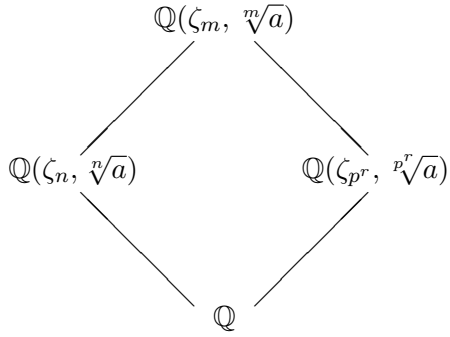
$$K \subset K(\sqrt[m']{pu}) = L$$

where K is a non ramified finite extension of $\mathbb{Q}_p$ and u is an invertible element of K. Look now to the valuation v_L-adic of the element $\sqrt[m']{pu}$:

$$v_L\left(\sqrt[m']{pu}\right) = \frac{v_L(pu)}{m'} = \frac{e(L/K)v_K(pu)}{m'} = \frac{e(L/K)}{m'}$$

from which it follows that $m' \mid e(L/K)$; but since $e(L/K) \leq [L:K] \leq m'$ then $e(L/K) = m'$. The theorem follows from the definition of $m' = m/d = m/(m, v_p(a))$. □

Now we come to the general case in which p divides m (and possibly also a). If we write $m = p^r n$ with $p \nmid n$, then we can split our extension as



Now we show how the determination of the ramification groups can be reduced to the study of the extension $\mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a})$ that will be done in next sections.

Theorem 4.4. *The ramification index of p in $\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}$ ($m = p^r n$, with $p \nmid n$) is equal to the following least common multiple*

$$e(\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}) = \left[\frac{n}{(n, v_p(a))}, e(\mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q})\right]$$

while for the higher ramification groups we have

$$G(\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q})^u = G(\mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q})^u \quad \textit{for } u > 0$$

Proof. For the second assertion, observe that, since $\mathbb{Q}(\zeta_n, \sqrt[n]{a})/\mathbb{Q}$ is tamely ramified, its ramification groups vanish for degree > 0. But this implies

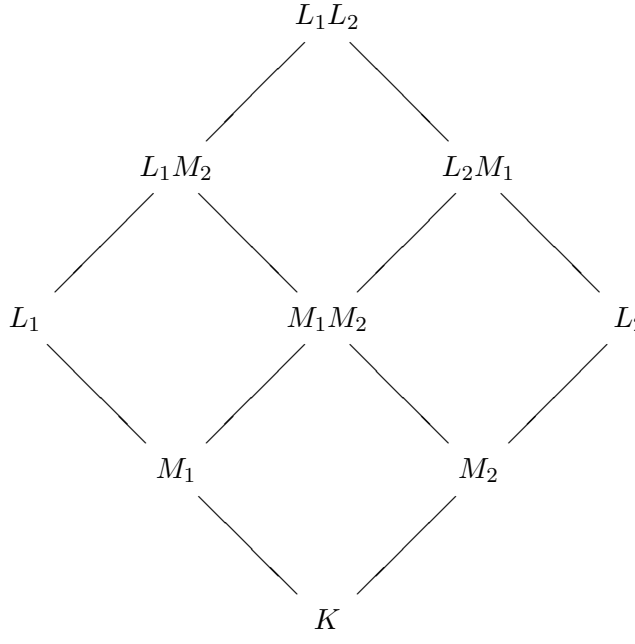
$$G(\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q})^u K(p^r)/K(p^r) = \{1\} \Rightarrow G(\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q})^u \subset K(p^r)$$

for $u > 0$ and hence we conclude by taking the quotient with respect to $K(n)$.

For the first assertion, observe that question is local (so that we can take the completion of all the fields involved respect to primes lying above p) and that the preceding theorem tells us that the extension $\mathbb{Q}(\zeta_n, \sqrt[n]{a})$ is tamely ramified with index of ramification equal to $n/(n, v_p(a))$. So the theorem descends from the following proposition.

Proposition 4.5. *Let L_1/K and L_2/K two disjoint finite extensions of p-local field with ramification index e_1 and e_2 respectively. If L_1/K is tamely ramified (that is $p \nmid e_1$) then the ramification e of the composition L_1L_2 is equal to the lest common multiple of e_1 and e_2: $e = [e_1, e_2]$.*

Proof. Consider the maximal unramified subextensions M_1 and M_2 of respectively L_1 and L_2 and look at the following diagram



From the property of stability of the unramified extensions ([2, Chapter 1, section 7]), it follows that M_1M_2/K is unramified while L_1M_2/M_1M_2 and L_2M_1/M_2M_1 are totally ramified with

$$e(L_1M_2/M_1M_2) = e(L_1/K),$$
$$e(L_2M_1/M_2M_1) = e(L_2/K).$$

So we can reduce precisely to the situation of the following lemma and that will conclude the proof.

Lemma 4.6. *Let M_1/M and M_2/M two disjoint finite extensions of p-local field totally and tamely ramified of degree e_1 and e_2. Then the composition M_1M_2 has ramification index over M equal to $[e_1, e_2]$.*

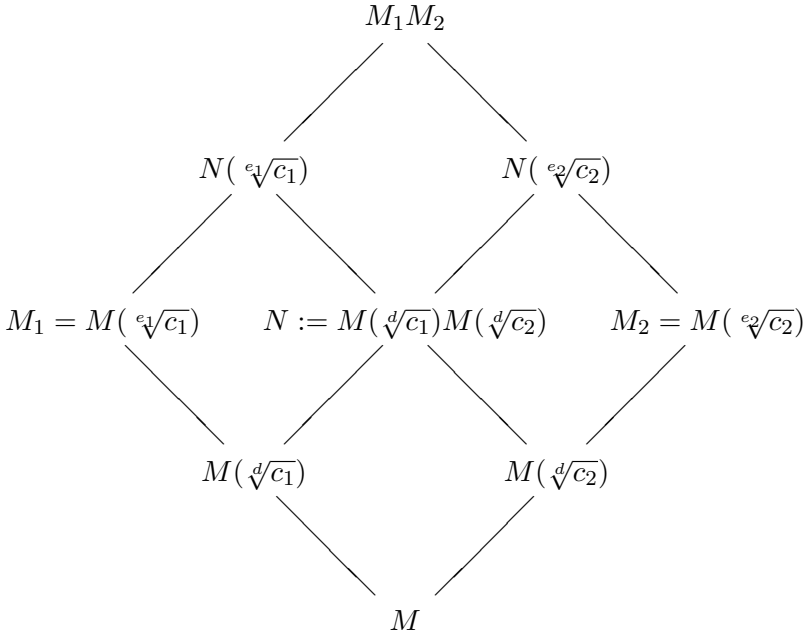
Proof. According to the structure theorem for tamely totally ramified extensions of local fields (see [2, Chapter 1, section 8]), there exist in M elements c_1 e c_2 of valuation 1 such that

$$M_1 = M(\sqrt[e_1]{c_1}),$$
$$M_2 = M(\sqrt[e_2]{c_2}).$$

If we put $d = (e_1, e_2)$ then we can write

$$e_1 = de_1',$$
$$e_2 = de_2'.$$

Consider the following diagram



We will show that $e(N/M) = d$ and $e(M_1M_2/N) = e_1'e_2'$, from which it will follow that $e(M_1M_2/M) = de_1'e_2' = [e_1, e_2]$ as requested.

$\underline{e(N/M) = d}$

Write N as

$$N = M(\sqrt[d]{c_1}, \sqrt[d]{c_2}) = M(\sqrt[d]{c_1})\left(\sqrt[d]{\frac{c_1}{c_2}}\right)$$

and since $v_M(c_1/c_2) = 0$ Lemma 4.1 implies that the extension $M(\sqrt[d]{c_1}) \subset M(\sqrt[d]{c_1})\left(\sqrt[d]{\frac{c_1}{c_2}}\right)$ is not ramified; hence $e(N/M) = e(M(\sqrt[d]{c_1})/M) = d$, q.e.d.

$\underline{e(M_1M_2/N) = e_1'e_2'}$

Observe that

$$\begin{cases} M_1/M(\sqrt[d]{c_1}) & \text{tot. ram. of deg. } e_1' \\ N/M(\sqrt[d]{c_1}) & \text{non ram.} \end{cases} \Rightarrow N(\sqrt[e_1]{c_1})/N \text{ tot. ram. of deg. } e_1'.$$

Analogously $N(\sqrt[e_2]{c_2})/N$ is totally ramified of degree e_2'. Then, as $(e_1', e_2') = 1$, the extension $M_1M_2 = N(\sqrt[e_1]{c_1})N(\sqrt[e_2]{c_2})$ is totally ramified over N of degree $e_1'e_2'$, q.e.d. . □

To summarize, we have shown in this section that we can concentrate on the study of the ramification of p in the extension $\mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a})$. Besides, the original hypothesis that $p^r \mid v_p(a)$ or $p \nmid v_p(a)$ splits into the conditions $p \nmid a$ or $p \,||\, a$.

In fact in the first case, we write $a = p^{p^s\alpha}a'$ with $p \nmid \alpha a'$ and $s \geq r$ and obtain

$$\sqrt[p^r]{a} = p^{p^{s-r}\alpha}\sqrt[p^r]{a'}$$

so that replacing a with a' we can assume $p \nmid a$.

In the second case we can write $a = p^{v_p(a)}a'$ with $p \nmid v_p(a)$. Hence there exist $s, t \in \mathbb{Z}$ such that $p^r s + v_p(a)t = 1$ and $p \nmid t$, which gives

$$a^t = \frac{pa'}{p^{p^r s}}$$

and by Theorem 2.3 we can replace a by pa'.

So in the next two sections we will study the extension $\mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a})$ distinguishing between these two cases.

5. $\mathbb{Q}(\zeta_{\mathbf{p^r}}, \sqrt[\mathbf{p^r}]{\mathbf{a}})/\mathbb{Q}$ when $\mathbf{p \nmid a}$

First of all we want to complete our extensions. We recall the following lemma of Kummer.

Lemma 5.1 (Kummer)**.** *Let L/K be an extension of number fields with rings of integer respectively R_K and R_L. Let $\theta \in R_L$ such that $L = K(\theta)$ and let $f(X) \in R_K[X]$ the minimal polynomial of θ over K. Let $K_\mathfrak{p}$ the completion of K respect to an ideal $\mathfrak{p}$ of R_K and let $R_\mathfrak{p}$ its ring of integers. If $f(X)$ factors on $R_\mathfrak{p}[X]$ as*

$$f(X) = \prod_{1 \leq i \leq g} g_i(X)$$

then over $\mathfrak{p}$ there are g ideals of R_L and the completions with respect to this ideals are $K_\mathfrak{p}(\theta_i)$ with θ_i root of $g_i(X)$.

Proof. See [2, Chapter 2, section 10]. □

If we apply this lemma to our situation we find the following result.

Theorem 5.2. *Let $0 \leq s \leq r$ such that $a \in \mathbb{Q}_p^{p^{r-s}}$ and, if $s \neq 0$, $a \notin \mathbb{Q}_p^{p^{r-s+1}}$. In the extension $\mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q}$, above p there are p^{r-s} prime ideals. Besides, if $b \in \mathbb{Q}_p$ is such that $b^{p^{r-s}} = a$, then the completion with respect to one of this ideals above p is $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})$.*

Proof. Consider the tower

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_{p^r}) \subset \mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a}).$$

We know that the cyclotomic extension $\mathbb{Q} \subset \mathbb{Q}(\zeta_{p^r})$ is totally ramified at p. Hence $\mathbb{Q}_p \subset \mathbb{Q}_p(\zeta_{p^r})$ is the completion with respect to p and to the unique ideal over p.

Now apply the Kummer lemma to the extension $\mathbb{Q}(\zeta_{p^r})(\sqrt[p^r]{a})$. From our hypothesis on s, we know that $a = b^{p^{r-s}}$ with $b \in \mathbb{Q}_p$ such that, if $s \neq 0$, $b \notin \mathbb{Q}_p^p$. The polynomial $X^{p^r} - a$ factorizes in $\mathbb{Q}_p(\zeta_{p^r})$ as

$$(*) \qquad X^{p^r} - a = (X^{p^s})^{p^{r-s}} - b^{p^{r-s}} = \prod_{i=1}^{p^{r-s}} (X^{p^s} - \zeta_{p^{r-s}}^i b).$$

Now if $s = 0$ then the polynomial splits into linear factors and so the number of ideals over p is $g = p^r$. Instead if $s > 0$ then we know that $b \notin \mathbb{Q}_p^p$ and the Theorem 2.4 of Schinzel implies:

$$b \notin \mathbb{Q}_p^p \Rightarrow b \notin \mathbb{Q}_p(\zeta_{p^r})^p$$

and so $\zeta_{p^{r-s}}^i b \notin \mathbb{Q}_p(\zeta_{p^r})^p$, for every $i = 1, \cdots, p^{r-s}$. But then the Theorem 2.1 gives us that $X^{p^s} - \zeta_{p^{r-s}}^i b$ is irreducible over $\mathbb{Q}_p(\zeta_{p^r})$ and so the (*) is an irreducible factorization on $\mathbb{Q}_p(\zeta_{p^r})$. Now the lemma of Kummer concludes the proof. □

Now we want to compute the number s of the preceding theorem. In order to achieve this, we need the following theorem on the structure of the units of $\mathbb{Z}_p$.

Lemma 5.3. *The group $U(\mathbb{Z}_p)$ of the invertible elements of $\mathbb{Z}_p$ admits the decomposition*

$$U(\mathbb{Z}_p) \cong (\mathbb{Z}/p\mathbb{Z})^* \times < 1 + p > .$$

Moreover the p^k-powers are

$$U(\mathbb{Z}_p)^{p^k} \cong (\mathbb{Z}/p\mathbb{Z})^* \times < 1 + p^{k+1} > .$$

Proof. See [3, p. 246-247]. □

Now the desired result.

Theorem 5.4. *Let $a \in \mathbb{Q}_p$ with $p \nmid a$. Then*

$$a \in \mathbb{Q}_p^{p^r} \Leftrightarrow p^{r+1} \mid \left(a^{p-1} - 1\right).$$

Instead for $0 < s \leq r$

$$a \in \mathbb{Q}_p^{p^{r-s}} \setminus \mathbb{Q}_p^{p^{r-s+1}} \Leftrightarrow p^{r-s+1} \mid\mid \left(a^{p-1} - 1\right).$$

Proof. It follows from the preceding lemma that

$$a \in \mathbb{Q}_p^{p^k} \Leftrightarrow p^{k+1} \mid \left(a^{p-1} - 1\right)$$

so that the conclusion is straightforward. □

So we can restrict ourselves to the study of the local extension $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})$ with $0 < s \leq r$, $p \nmid b$ and $b \in \mathbb{Q}_p \setminus \mathbb{Q}_p^p$ (in fact the case $s = 0$ reduces to the cyclotomic extension $\mathbb{Q}_p(\zeta_{p^r})/\mathbb{Q}_p$ of which all is known). Note that the fact that $b \notin \mathbb{Q}_p^p$ is equivalent to say that $p \,||\, (b^{p-1} - 1)$.

Now we want to determine the ramification degree of our extension.

Theorem 5.5. *The local extension $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p$ with $b \in \mathbb{Q}_p \setminus \mathbb{Q}_p^p$ is totally ramified.*

Proof. Since it is well known that $\mathbb{Q}_p(\zeta_{p^r})/\mathbb{Q}_p$ is totally ramified, it's enough to show that $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p(\zeta_{p^r})$ is totally ramified, too. Suppose, on the contrary, that the inertia degree f is greater than 1 and let

$$[\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})^{ur} : \mathbb{Q}_p(\zeta_{p^r})] = f$$

where $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})^{ur}$ is the maximal unramified subextension of $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})$ over $\mathbb{Q}_p(\zeta_{p^r})$. Then the unique subfield property (Theorem 2.2) gives

$$\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})^{ur} = \mathbb{Q}_p(\zeta_{p^r}, \sqrt[f]{b})$$

and in particular $\sqrt[p]{b} \in \mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})^{ur}$. Now the structure theorem for the unramified extensions of local fields (see [2, Chapter 1, section 7]) says that $\mathbb{Q}_p(\zeta_{p^r})^{ur}$ is obtained from $\mathbb{Q}_p(\zeta_{p^r})$ adding some roots of unity and so $\mathbb{Q}_p(\zeta_{p^r})^{ur}$is abelian over $\mathbb{Q}_p$. In particular, since $\sqrt[p]{b} \in \mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})^{ur}$, $x^p - b$ has abelian Galois group over $\mathbb{Q}_p$. Then the Theorem 2.4 of Schinzel gives $b = \gamma^p$ for some $\gamma \in \mathbb{Q}_p$ contrary to our hypothesis $b \notin \mathbb{Q}_p^p$. □

So our extension $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p$ is totally ramified of degree $\phi(p^r)p^s$ and, with the same proof of Theorem 3.2, one shows that its Galois group is $G = C(p^s) \rtimes G(p^r)$ where the semidirect product is made with respect to the map

$$G(p^r) \twoheadrightarrow G(p^s) \cong \mathrm{Aut}(C(p^s)).$$

Now we come to the heart of our work: the determination of the higher ramification groups. The fundamental trick is to consider the following filtration of subfields

$$\begin{array}{ccccccccc}
\mathbb{Q}_p & < & \mathbb{Q}_p(\sqrt[p]{b}) & < \cdots < & \mathbb{Q}_p(\sqrt[p^s]{b}) & < \cdots < & \mathbb{Q}_p(\sqrt[p^r]{b}) \\
\triangle & & \triangle & & \wedge & & \wedge \\
\mathbb{Q}_p(\zeta_p) & \lhd & \mathbb{Q}_p(\zeta_p, \sqrt[p]{b}) & < \cdots < & \mathbb{Q}_p(\zeta_p, \sqrt[p^s]{b}) & < \cdots < & \mathbb{Q}_p(\zeta_p, \sqrt[p^r]{b}) \\
\triangle & & \triangle & & \wedge & & \wedge \\
\mathbb{Q}_p(\zeta_{p^2}) & \lhd & \mathbb{Q}_p(\zeta_{p^2}, \sqrt[p]{b}) & \lhd \cdots < & \mathbb{Q}_p(\zeta_{p^2}, \sqrt[p^s]{b}) & < \cdots < & \mathbb{Q}_p(\zeta_{p^2}, \sqrt[p^r]{b}) \\
\triangle & & \triangle & & \wedge & & \wedge \\
\vdots & & \vdots & & \vdots & & \vdots \\
\triangle & & \triangle & & \triangle & & \triangle \\
\mathbb{Q}_p(\zeta_{p^r}) & \lhd & \mathbb{Q}_p(\zeta_{p^r}, \sqrt[p]{b}) & \lhd \cdots \lhd & \mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b}) & \lhd \cdots \lhd & \mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^r]{b})
\end{array}$$

where $\lhd$ means that the subfield on the right is normal over $\mathbb{Q}_p$, where $<$ means that it is not normal over $\mathbb{Q}_p$. But observe that in the second line every 1-step is normal, in the third line every 2-step is normal and so on; while along the column all the extensions are normal.

Our strategy will be as follows: we shall determine the ramification on every step of the second line and this, together with the knowledge of the ramification groups of the cyclotomic extension (the first column of the diagram), will allow us to calculate the total ramification groups of $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p$.

Theorem 5.6. *Consider the infinite tower of fields (in the hypothesis* $p \mid\mid (b^{p-1}-1)$*)*

$$K_0 = \mathbb{Q}_p(\zeta_p) < K_1 = \mathbb{Q}_p(\zeta_p, \sqrt[p]{b}) < \cdots < K_i = \mathbb{Q}_p(\zeta_p, \sqrt[p^i]{b}) < \cdots$$

in which every extension is normal respect to the preceding one with Galois group cyclic of order p*. The unique break-number* b_i *in the ramification groups of* K_i/K_{i-1} *is*

$$b_i = 1 + p(p^{i-1}-1).$$

Proof. We shall first construct a uniformizer (i.e. an element of valuation 1) for K_i/K_{i-1}.

Lemma 5.7. *A uniformizer for the extension* K_i/K_{i-1} *(with the hypothesis* $p \mid\mid (b^{p-1}-1)$*) is given by*

$$\pi_i = \frac{1-\zeta_p}{(b-\sqrt[p]{b})\cdots(\sqrt[p^{i-1}]{b}-\sqrt[p^i]{b})}.$$

Proof. Consider in K_i the element $(\sqrt[p^{i-1}]{b}-\sqrt[p^i]{b})$. For it we have

$$N_{K_i/K_{i-1}}(\sqrt[p^{i-1}]{b}-\sqrt[p^i]{b}) = \prod_{j=1}^{p}(\sqrt[p^{i-1}]{b}-\zeta_p^j\sqrt[p^i]{b}) = (\sqrt[p^{i-2}]{b}-\sqrt[p^{i-1}]{b}).$$

So inductively we have that

$$N_{K_i/K_0}(\sqrt[p^{i-1}]{b}-\sqrt[p^i]{b}) = b^p - b$$

and this implies

$$(*)\quad v_{K_i}(\sqrt[p^{i-1}]{b}-\sqrt[p^i]{b}) = \frac{v_{K_0}(b^p-b)}{f(K_i/K_0)} = v_{K_0}(b^p-b) = (p-1)v_p(b^p-b) = p-1$$

in view of the hypothesis $p \mid\mid (b^{p-1}-1)$. But this, together with the fact that $1-\zeta_p$ is a uniformizer for $K_0 = \mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$, allows to prove the theorem by induction on $i \geq 1$.

In fact:
$\underline{i=1}$

$$v_{K_1}\left(\frac{1-\zeta_p}{b-\sqrt[p]{b}}\right) = pv_{K_0}(1-\zeta_p) - v_{K_1}(b-\sqrt[p]{b}) = p-(p-1) = 1.$$

$\underline{i \Rightarrow i+1}$
From (*) and the inductive hypothesis, we have

$$v_{K_i}\left(\frac{\pi_{i-1}}{\sqrt[p^{i-1}]{b}-\sqrt[p^i]{b}}\right) = p\cdot v_{K_{i-1}}(\pi_{i-1}) - v_{K_i}(\sqrt[p^{i-1}]{b}-\sqrt[p^i]{b}) = p-(p-1) = 1.$$

□

Now that we have a uniformizer π_i, to calculate the break-number of K_i/K_{i-1} we can simply let act on it the generator of the group $\mathrm{Gal}(K_i/K_{i-1}) \cong C(p)$ which sends $\sqrt[p^i]{b}$ in $\zeta_p\sqrt[p^i]{b}$ (see [10, Chapter IV, section 1, lemma 1]). We obtain

$$\begin{aligned}
1+b_i &= v_{K_i}(s(\pi_i)-\pi_i)\\
&= v_{K_i}\left(\frac{\pi_{i-1}}{\sqrt[p^{i-1}]{b}-\zeta_p\sqrt[p^i]{b}} - \frac{\pi_{i-1}}{\sqrt[p^{i-1}]{b}-\sqrt[p^i]{b}}\right)\\
&= v_{K_i}(\pi_{i-1}) + v_{K_i}\left(\frac{\sqrt[p^i]{b}\cdot(\zeta_p-1)}{(\sqrt[p^{i-1}]{b}-\zeta_p\sqrt[p^i]{b})(\sqrt[p^{i-1}]{b}-\sqrt[p^i]{b})}\right)\\
&= p\cdot v_{K_{i-1}}(\pi_{i-1}) + v_{K_i}(\sqrt[p^i]{b}) + p^i\cdot v_{K_0}(\zeta_p-1) - 2\cdot v_{K_i}(\sqrt[p^{i-1}]{b}-\sqrt[p^i]{b})\\
&= p + v_{K_i}(\sqrt[p^i]{b}) + p^i - 2(p-1)\\
&= p + p^i - 2(p-1)
\end{aligned}$$

where in the last equality we have used that $p \nmid b$. □

Now we can turn to the determination of the ramification groups of our extension $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p$.

Notation. *In the next theorem we shall use the following notation*

(i) for $i, s \leq r$, $C(p^s) \rtimes G(p^r)^i$ will indicate the semidirect product made respect to the map $G(p^r)^i \hookrightarrow G(p^r) \twoheadrightarrow G(p^s) \cong Aut(C(p^s))$.

(ii) with the numbers d we shall indicate the difference of the break-numbers in the ramification groups. Precisely d_i will be the difference between the $(i+1)$-th inferior break-number and the i-th inferior break-number. Analogous meaning for d^i respect to the superior ramification groups.

Theorem 5.8. *The ramification groups of* $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p$ *(*$p \mid\mid (b^{p-1}-1)$*) are:*

$$\begin{cases} G^0 & = C(p^s) & \rtimes\ G(p^r) & = G_0 \\ G^{(i-1)+\frac{1}{p-1}} & = C(p^{s-i+1}) & \rtimes\ G(p^r)^i & = G_{\frac{2p^{2i-1}-p+1}{p+1}} \\ G^i & = C(p^{s-i}) & \rtimes\ G(p^r)^i & = G_{\frac{(p-1)(p^{2i}-1)}{p+1}} \\ G^{s+j} & = & G(p^r)^{s+j} & = G_{\frac{(p-1)(p^{2s}-1)}{p+1}+p^{2s}(p^j-1)} \end{cases}$$

with $1 \le i \le s$ *and* $1 \le j \le r-1-s$*. The difference of the break-numbers are:*

$$\begin{cases} d^0 = 0 \\ d^{2i-1} = 1/(p-1) \\ d^{2i} = (p-2)/(p-1) \\ d^{2s+j} = 1 \end{cases} \quad \textit{and} \quad \begin{cases} d_0 = 0 \\ d_{2i-1} = p^{2(i-1)} \\ d_{2i} = p^{2i-1}(p-2) \\ d_{2s+j} = p^{2s-1+j}(p-1). \end{cases}$$

The proof is by induction on s. For $s = 0$ we reduce to a cyclotomic extension and so the theorem follows from the known ramification groups of the cyclotomic extensions of $\mathbb{Q}_p$. (see [10, Chapter IV, section 4]). So we assume by induction that the theorem is true for $s < r$ and we will prove it for $s+1$.

Lemma 5.9. *The ramification groups of* $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p(\zeta_p, \sqrt[p^s]{b})$ *are (call* $\widetilde{G} = G(p^r)^1$ *its Galois group):*

$$\begin{cases} \widetilde{G}^{(p-1)(p^i-1)} & = G(p^r)^i & = \widetilde{G}_{\frac{(p-1)(p^{2i}-1)}{p+1}} \\ \widetilde{G}^{(p-1)[(j+1)p^s-1]} & = G(p^r)^{j+s} & = \widetilde{G}_{\frac{(p-1)(p^{2s-1}-1)}{p+1}+p^{2s}(p^j-1)} \end{cases}$$

with $1 \le i \le s$ *and* $1 \le j \le r-1-s$*. The differences of the break-numbers are*

$$\begin{cases} \widetilde{d}^{i-1} = p^{i-1}(p-1)^2 \\ \widetilde{d}^{s+j-1} = p^s(p-1) \end{cases} \quad \textit{and} \quad \begin{cases} \widetilde{d}_{i-1} = p^{2i-2}(p-1)^2 \\ \widetilde{d}_{s+j-1} = p^{2s+j-1}(p-1). \end{cases}$$

Proof. We know, by induction hypothesis, the ramification groups of $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p$ and so, to find the inferior ramification groups of $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p(\zeta_p, \sqrt[p^s]{b})$, it's enough to intersect with $G(p^r)^1$. In particular for the inferior d we obtain

$$\begin{cases} \widetilde{d}_{i-1} = d_{2i-1} + d_{2i} = p^{2(i-1)} + p^{2i-1}(p-2) = p^{2i-2}(p-1)^2 \\ \widetilde{d}_{s+j-1} = d_{2s+j} = p^{2s+j-1}(p-1). \end{cases}$$

Now we can pass to the superior d:

$$\begin{cases} \widetilde{d}^{i-1} = \frac{\widetilde{d}_{i-1}}{p^{i-1}} = p^{i-1}(p-1)^2 \\ \widetilde{d}^{s+j-1} = \frac{\widetilde{d}_{s+j-1}}{p^{s+j-1}} = p^s(p-1). \end{cases}$$

And now from the d_i and d^i it's easy to calculate the inferior and superior ramification groups. □

Now using Theorem 5.6 we can move to the field $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^{s+1}]{b})$ leaving fixed the base $\mathbb{Q}_p(\zeta_p, \sqrt[p^s]{b})$.

Lemma 5.10. *The ramification groups of* $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^{s+1}]{b})/\mathbb{Q}_p(\zeta_p, \sqrt[p^s]{b})$ *are (call* ${}^sG = C(p) \rtimes G(p^r)^1$ *its Galois group):*

$$\begin{cases} {}^sG^{(p-1)(p^i-1)} & = C(p) \rtimes G(p^r)^i & = {}^sG_{\frac{(p-1)(p^{2i}-1)}{p+1}} \\ {}^sG^{1+p(p^s-1)} & = C(p) \rtimes G(p^r)^{s+1} & = {}^sG_{\frac{p^{2s+1}-p+1}{p+1}} \\ {}^sG^{(p-1)[(j+1)p^s-1]} & = G(p^r)^{s+j} & = {}^sG_{\frac{(p-1)(p^{2s+2}-1)}{p+1}+p^{2s+2}(p^{j-1}-1)} \end{cases}$$

with $1 \le i \le s$ *and* $1 \le j \le r-s-1$. *The differences of the break-numbers are:*

$$\begin{cases} {}^sd^{i-1} = p^{i-1}(p-1)^2 \\ {}^sd^s = p^s \\ {}^sd^{s+1} = p^s(p-2) \\ {}^sd^{s+j} = p^s(p-1) \end{cases} \quad \textit{and} \quad \begin{cases} {}^sd_{i-1} = p^{2i-2}(p-1)^2 \\ {}^sd_s = p^{2s} \\ {}^sd_{s+1} = p^{2s+1}(p-2) \\ {}^sd_{s+j} = p^{2s+j}(p-1) \quad \textit{for } 2 \le j. \end{cases}$$

Proof. Consider the diagram

$$\begin{array}{ccccc} \mathbb{Q}_p(\zeta_p, \sqrt[p^s]{b}) & \lhd & \mathbb{Q}_p(\zeta_p, \sqrt[p^{s+1}]{b}) & & \\ \triangle & & \triangle & & G(p^r)^1 \\ \mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b}) & \lhd & \mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^{s+1}]{b}) & & \\ & C(p) & & & \end{array}$$

where the fixed fields of the subgroups $C(p)$ and $G(p^r)^1$ are respectively $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})$ and $\mathbb{Q}_p(\zeta_p, \sqrt[p^{s+1}]{b})$. From Theorem 5.6 and Lemma 5.9, we see that the unique break-numbers in the quotients are:

$${}^sG^{1+p(p^s-1)}/G(p^r)^1 = C(p) \quad \text{and} \quad \begin{cases} {}^sG^{(p-1)(p^i-1)}/C(p) & = G(p^r)^i \\ {}^sG^{(p-1)[(j+1)p^s-1]}/C(p) & = G(p^r)^{s+j}. \end{cases}$$

Since $(p-1)(p^s-1) < 1+p(p^s-1) < (p-1)(2p^s-1)$, we conclude that

(1) The superior ramification groups of order $> 1+p(p^s+1)$ are contained in $G(p^r)^1$ and so ${}^sG^{(p-1)[(j+1)p^s-1]} = G(p^r)^{s+j}$.

(2) ${}^sG^{1+p(p^s-1)} = C(p) \rtimes G(p^r)^{s+1}$.

(3) For the ramification groups of order $< 1+p(p^s+1)$ we have

$${}^sG^{(p-1)(p^i-1)} = C(p) \rtimes G(p^r)^i.$$

Next, with easily calculations (similar to that of the preceeding lemma), one can pass to superior d, inferior d and finally to inferior ramification groups. □

Now, always using Theorem 5.6, we can go down with the base field.

Lemma 5.11. *The ramification groups of* $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^{s+1}]{b})/\mathbb{Q}_p(\zeta_p, \sqrt[p^{s-t}]{b})$ *with* $0 \leq t \leq s$ *are (call* ${}^{s-t}G = C(p^{t+1}) \rtimes G(p^r)^1$*):*

$$\begin{cases} {}^{s-t}G^{(p-1)(p^i-1)} & = C(p^{t+1}) \rtimes G(p^r)^i \\ {}^{s-t}G^{p^{s-t+1}+(p-1)[kp^{s-t}-1]} & = C(p^{t+1-k}) \rtimes G(p^r)^{s-t+1+k} \\ {}^{s-t}G^{(p-1)[(k+2)p^{s-t}-1]} & = C(p^{t-k}) \rtimes G(p^r)^{s-t+1+k} \\ {}^{s-t}G^{(p-1)[(r+j+1)p^{s-t}-1]} & = G(p^r)^{s+j} \end{cases}$$

with $1 \leq i \leq s-t$, $0 \leq k \leq t$ *and* $2 \leq j \leq r-s-1$. *The differences of the break-numbers are:*

$$\begin{cases} {}^{s-t}d^{i-1} & = p^{i-1}(p-1)^2 \\ {}^{s-t}d^{s-t+2k} & = p^{s-t} \\ {}^{s-t}d^{s-t+1+2k} & = p^{s-t}(p-2) \\ {}^{s-t}d^{s+t+j} & = p^{s-t}(p-1) \end{cases} \quad \textit{and} \quad \begin{cases} {}^{s-t}d_{i-1} & = p^{2i-2}(p-1)^2 \\ {}^{s-t}d_{s-t+2k} & = p^{2(s-t)+2k} \\ {}^{s-t}d_{s-t+1+2k} & = p^{2(s-t)+2k+1}(p-2) \\ {}^{s-t}d_{s+t+j} & = p^{2s+j}(p-1). \end{cases}$$

Proof. The proof is by induction on t. For $t = 0$ it reduces to Lemma 5.10. So let us assume the theorem true for $t < s$ and prove it for $t+1$. Consider the tower of subfields

$$\mathbb{Q}_p(\zeta_p, \sqrt[p^{s-t-1}]{b}) \lhd \mathbb{Q}_p(\zeta_p, \sqrt[p^{s-t}]{b}) \lhd \mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^{s+1}]{b}).$$

Theorem 5.6 tells us that the break-number of $\mathbb{Q}_p(\zeta_p, \sqrt[p^{s-t}]{b})/\mathbb{Q}_p(\zeta_p, \sqrt[p^{s-t-1}]{b})$ is

$$d_{s-t} = 1 + p(p^{s-t-1} - 1).$$

and since $(p-1)(p^{s-t-1}-1) < 1 + p(p^{s-t-1}-1) < (p-1)(p^{s-t}-1)$, we must distinguish for the differences of break-numbers the following cases:

(1) The first $(s-t-1)$ break-number remains the same as the initial case t and the corresponding ramification groups have an increase of the first factor from $C(p^{t+1})$ to $C(p^{t+2})$, i.e.

$$1 \leq i \leq s-t \Rightarrow \begin{cases} {}^{s-t-1}d^{i-1} & = {}^{s-t}d^{i-1} = p^{i-1}(p-1)^2 \\ {}^{s-t-1}d_{i-1} & = {}^{s-t}d_{i-1} = p^{2i-2}(p-1)^2 \\ {}^{s-t-1}G^{(p-1)(p^i-1)} & = C(p^{t+2}) \rtimes G(p^r)^i. \end{cases}$$

(2) It appears a new break-number for which one has

$$\begin{cases} {}^{s-t-1}G^{1+p(p^{s-t-1}-1)} & = {}^{s-t-1}G^{p^{s-t}+(p-1)[0p^{s-t-1}-1]} \\ & = C(p^{t+2}) \rtimes G(p^r)^{s-t+1} \\ {}^{s-t-1}d^{s-t-1} & = 1 + p(p^{s-t-1}-1) - (p-1)(p^{s-t-1}-1) = p^{s-t-1} \\ {}^{s-t-1}d_{s-t+1} & = p^{2(s-t-1)}. \end{cases}$$

(3) For the successive break-number it holds

$$\begin{cases} {}^{s-t-1}d_{s-t+2} = {}^{s-t}d_{s-t-1} - {}^{s-t-1}d_{s-t-1} = p^{2(s-t-1)+1}(p-2) \\ {}^{s-t-1}d^{s-t+2} = \frac{{}^{s-t-1}d_{s-t+2}}{p^{s-t+2}} = p^{s-t-1}(p-2) \\ {}^{s-t-1}G^{2(p-1)p^{s-t-1}-(p-1)} = C(p^{t+1}) \rtimes G(p^r)^{s-t-1}. \end{cases}$$

(4) For the remaining break-number one has (for $1 \leq k+1 \leq t+1$ and $2 \leq j \leq r-1-s$):

$$\begin{cases} {}^{s-t}d_{s-t+2k} = {}^{s-t-1}d_{s-t+2k+1} = {}^{s-t-1}d_{s-(t+1)+2(k+1)} \\ {}^{s-t}d_{s-t+1+2k} = {}^{s-t-1}d_{s-t+1+2k+1} = {}^{s-t-1}d_{s-(t+1)+1+2(k+1)} \\ {}^{s-t}d_{s+j+t} = {}^{s-t-1}d_{s+j+(t+1)} \end{cases}$$

because of the appearance of the new ramification group. And for the same reason one has that for every $h \geq 2(s-t)$

$${}^{s-t-1}d^{h+1} = \frac{{}^{s-t}d^h}{p}$$

from which we conclude that

$$\begin{cases} {}^{s-t-1}d^{s-(t+1)+2(k+1)} = p^{s-(t+1)} \\ {}^{s-t-1}d^{s-(t+1)+1+2(k+1)} = p^{s-(t+1)}(p-2) \\ {}^{s-t-1}d^{s+(t+1)+j} = p^{s-(t-1)}(p-1). \end{cases}$$

Now it's easy to compute the superior ramification groups

$$\begin{cases} {}^{s-t-1}G^{p^{s-t}+(p-1)[(k+1)p^{s-t}-1]} = C(p^{t+2-(k+1)}) \rtimes G(p^r)^{s-(t+1)+1+(k+1)} \\ {}^{s-t-1}G^{(p-1)[(k+3)p^{s-t-1}-1]} = C(p^{t+1-(k+1)}) \rtimes G(p^r)^{s-(t+1)+1+(k+1)} \\ {}^{s-t-1}G^{(p-1)[(t+1+j+1)p^{s-t-1}-1]} = G(p^r)^{s+j}. \end{cases}$$

□

Putting $t = s$ in the preceding lemma, we obtain the following corollary

Corollary 5.12. *The ramification groups of* $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^{s+1}]{b})/\mathbb{Q}_p(\zeta_p)$ *are (call* ${}^0G = C(p^{s+1}) \rtimes G(p^r)^1$ *its Galois group):*

$$\begin{cases} {}^0G^{1+k(p-1)} = C(p^{s+1-k}) \rtimes G(p^r)^{k+1} \\ {}^0G^{(k+1)(p-1)} = C(p^{s-k}) \rtimes G(p^r)^{k+1} \\ {}^0G^{(s+j)(p-1)} = G(p^r)^{s+j} \end{cases}$$

where $0 \leq k \leq s$ *and* $2 \leq j \leq r-s-1$. *The differences of the break-numbers are*

$$\begin{cases} {}^0d^{2k} = 1 \\ {}^od^{1+2k} = p-2 \\ {}^0d^{2s+j} = p-1 \end{cases} \quad \textit{and} \quad \begin{cases} {}^0d_{2k} = p^{2k} \\ {}^0d_{1+2k} = p^{1+2k}(p-2) \\ {}^0d_{2s+j} = p^{2s+j}(p-1). \end{cases}$$

Proof. [of the Theorem 5.8] Now we can conclude our proof by induction showing that the theorem is true for $s+1$. Consider the composition

$$\mathbb{Q}_p \lhd \mathbb{Q}_p(\zeta_p) \lhd \mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^{s+1}]{b}).$$

Since $\mathbb{Q}_p(\zeta_p)$ is the maximal subextensions tamely ramified, the inferior and superior ramification groups $\mathbb{Q}_p \lhd \mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^{s+1}]{b})$ differ from those of $\mathbb{Q}_p(\zeta_p) \lhd \mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^{s+1}]{b})$ only for the 0-th group which now is $G_0 = C(p^{s+1}) \rtimes G(p^r)$. Hence for the inferior d it holds

$$\begin{cases} d_0 & = 0 \\ d_{2k+1} & = {}^0d_{2k} = p^{2k} \\ d_{2k+1} & = {}^0d_{2k+1} = p^{2k+1}(p-2) \\ d_{2s+j+1} & = {}^0d_{2s+j} = p^{2s+j}(p-1) \end{cases}$$

with $0 \leq k \leq s$ and $2 \leq j \leq r-s-1$. Analogously for the superior d one has

$$\begin{cases} d^0 & = 0 \\ d^{2k+1} & = \frac{1}{p-1} \\ d^{2k+1} & = \frac{p-2}{p-1} \\ d^{2s+j+1} & = 1. \end{cases}$$

Now we calculate the superior ramification groups:

$$\begin{cases} G^0 & = C(p^{s+1}) & \rtimes\ G(p^r) \\ G^{k+\frac{1}{p-1}} & = C(p^{s+1-k}) & \rtimes\ G(p^r)^{k+1} \\ G^{k+1} & = C(p^{s-k}) & \rtimes\ G(p^r)^{k+1} \\ G^{s+j} & = & G(p^r)^{s+j} \end{cases}$$

which, after putting $i = k+1$ and $j' = j-1$, gives us the desired groups. Now its easy to calculate the inferior ramification groups. □

Now that we know the ramification groups of our extension $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p$, we can calculate the local Artin conductor of the characters of $C(p^s) \rtimes G(p^r)$. For this we shall use the formula ([10, Chapter VI, section 2, exercise 2])

$$f(\chi) = \chi(1)(1 + c^\chi)$$

where c^χ is the biggest real u such that $\chi_{|G^u} \neq \chi(1) \cdot id_{|G^u}$ (if $\chi = id$ we put $c^{id} = -1$).

Theorem 5.13. *For a character χ of $C(p^s) \rtimes G(p^r)$, we have*

$$c^\chi = \begin{cases} pr(\chi) - 1 & \text{if } lev(\chi) < pr(\chi) \text{ or } 0 = lev\chi, \\ pr(\chi) - 1 + \dfrac{1}{p-1} & \text{if } 0 < lev(\chi) = pr(\chi), \end{cases}$$

(here $lev(\chi)$ has the meaning of Def. 3.10).

Proof. From the definition 3.12 of the null subgroup of a character, we have that c^χ (with $\chi \neq id$) is the biggest real number such that $G^{c^\chi} \not\subset Gr(\chi)$. Now from Theorem 5.8 it follows that

$$G^u \not\subset Gr(\chi) = C(p^{s-lev(\chi)}) \rtimes G(p^r)^{pr(\chi)}$$

$$\Leftrightarrow \begin{cases} u \leq lev(\chi) - 1 + \dfrac{1}{p-1} & \text{if } 0 < lev(\chi), \\ \text{or} & \\ u \leq pr(\chi) - 1 & \text{if } 0 < pr(\chi), \end{cases}$$

and hence if $0 < lev(\chi)$

$$c^\chi = \max\left\{lev(\chi) - 1 + \frac{1}{p-1}, pr(\chi) - 1\right\}$$

$$= \begin{cases} pr(\chi) - 1 & \text{if } 0 < lev(\chi) < pr(\chi), \\ pr(\chi) - 1 + \dfrac{1}{p-1} & \text{if } 0 < lev(\chi) = pr(\chi). \end{cases}$$

□

Corollary 5.14. *The local Artin conductor of χ is*

$$f(\chi) = \begin{cases} p^{lev(\chi)-1}(p-1)pr(\chi) & \text{if } 0 < lev(\chi) < pr(\chi), \\ p^{lev(\chi)-1}(p-1)\left[pr(\chi) + \dfrac{1}{p-1}\right] & \text{if } 0 < pr(\chi) = lev(\chi), \\ pr(\chi) & \text{if } lev(\chi) = 0. \end{cases}$$

Proof. It follows at once from the preceding theorem and from the formula

$$f(\chi) = \chi(1)(1 + c^\chi).$$

□

As an application of the formula for the local Artin conductor, we now calculate the p-component of the discriminant of the extension $\mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q}$. First of all, since above p there are p^{r-s} prime ideals, we can complete our extension and apply the formula

$$v_p\left[d(\mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q})\right] = p^{r-s} v_p\left[d(\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p)\right]. \tag{5.1}$$

For the discriminant of the extension $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p$, we use the local conductor-discriminant formula ([10, Chapter 6, section 3])

$$v_p(d) = \sum_{\chi \in G^*} \chi(1) f(\chi). \tag{5.2}$$

Theorem 5.15. *For the extension* $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p$ *with* $p \nmid b$ *we have*

$$v_p\left[d(\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{b})/\mathbb{Q}_p)\right] = p^s\left[rp^r - (r+1)p^{r-1}\right] + 2\frac{p^{2s}-1}{p+1}.$$

First of all we need the following lemma.

Lemma 5.16. *If* $G = C(p^s) \rtimes G(p^r)$ *then we have for its characters the two formulas*

$$\text{Card}\,\{\chi \in G^* : lev(\chi) = 0 \ \textit{and}\ 0 \le pr(\chi) = t \le r\} = \begin{cases} 1 & \textit{if } t = 0, \\ p-2 & \textit{if } t = 1, \\ p^{t-2}(p-1)^2 & \textit{if } t \ge 2; \end{cases}$$

$$\text{Card}\,\{\chi \in G^* : lev(\chi) = k > 0 \ \textit{and}\ k \le pr(\chi) = t \le r\} = \begin{cases} 1 & \textit{if } t = k, \\ (p-1)p^{t-k-1} & \textit{if } t > k. \end{cases}$$

Proof. The first formula follows from:

$$\text{Card}\,\{\chi \in G^* : lev(\chi) = 0 \text{ and } 0 \le pr(\chi) = t \le r\} = |G(p^t)| - |G(p^{t-1})|$$

while the second follows from (remember that we take only a system of representatives for $G(p^r)/G(p^k)$):

$$\text{Card}\,\{\chi \in G^* : lev(\chi) = k > 0 \text{ and } k \le pr(\chi) = t \le r\} = \frac{|G(p^t)| - |G(p^{t-1})|}{|G(p^k)|}.$$

□

Proof. [of the Theorem 5.15] According to Corollary 5.14 we can split the sum in the formula (5.2) as

$$\begin{aligned} v_p(d) = &\sum_{lev(\chi)=0} pr(\chi) + \sum_{0<lev(\chi)} p^{2(lev(\chi)-1)}(p-1)^2 pr(\chi) \\ &+ \sum_{0<lev(\chi)=pr(\chi)} p^{2(lev(\chi)-1)}(p-1)^2\left[\frac{1}{p-1}\right] \end{aligned} \tag{5.3}$$

and with the help of the preceding lemma we can calculate these three sums. Let us begin with the first sum:

$$\sum_{lev(\chi)=0} pr(\chi) = (p-2)\cdot 1 + \sum_{t=2}^{r} p^{t-2}(p-1)^2 t = rp^r - (r+1)p^{r-1}. \tag{5.4}$$

For the second sum:

$$\sum_{0<lev(\chi)} p^{2(lev(\chi)-1)}(p-1)^2 pr(\chi) = \sum_{k=1}^{s} p^{2(k-1)}(p-1)^2 k + \sum_{k=1}^{s}\sum_{t=k+1}^{r} p^{2(k-1)}(p-1)^2 t(p-1)p^{t-k-1}$$

$$= (p^s-1)\left[rp^r-(r+1)p^{r-1}\right] + \frac{p^{2s}-1}{p+1}. \tag{5.5}$$

Finally for the third sum we have:

$$\sum_{0<lev(\chi)=pr(\chi)} p^{2(lev(\chi)-1)}(p-1)^2\left[\frac{1}{p-1}\right] = \sum_{k=1}^{s} p^{2(k-1)}(p-1) = \frac{p^{2s}-1}{p-1}. \tag{5.6}$$

Now adding the formulas (5.4), (5.5) and (5.6) we obtain what asserted. □

So for the global extension we have:

Corollary 5.17. *The p-adic valuation of the discriminant of $\mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q}$ with $p \nmid a$ is equal to*

$$p^r\left[rp^r-(r+1)p^{r-1}\right] + 2\frac{p^{r+s}-p^{r-s}}{p+1}.$$

6. $\mathbb{Q}_{\mathbf{p}}(\zeta_{\mathbf{p^r}}, \sqrt[p^r]{a})/\mathbb{Q}_{\mathbf{p}}$ in the case $\mathbf{p} \,||\, \mathbf{a}$

The other case of our interest is the extension $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q}_p$ in the case $p \,||\, a$. First we want to complete this extension.

Lemma 6.1. *In the extension $\mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q}$ with $p \,||\, a$, above p there is only one prime ideal. So the completion of our extension with respect to p is $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q}_p$.*

Proof. It follows from Theorem 5.2 since if $p \,||\, a$ then $a \notin \mathbb{Q}_p^p$. □

Corollary 6.2. *The local extension $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q}_p$ with $p \,||\, a$ is totally ramified.*

Proof. It follows from the preceding lemma together with Theorem 5.5. □

Now we come to the determination of the higher ramification groups. We begin with an analogue of Theorem 5.6.

Theorem 6.3. *Consider the tower of extensions (in the hypothesis $p \,||\, a$)*

$$K_0 = \mathbb{Q}_p(\zeta_p) < K_1 = \mathbb{Q}_p(\zeta_p, \sqrt[p]{a}) < \cdots < K_i = \mathbb{Q}_p(\zeta_p, \sqrt[p^i]{a}) < \cdots$$

in which every extension is normal respect to the preceding one with Galois group cyclic of order p. The unique break-number b_i in the ramification groups of K_i/K_{i-1} is

$$b_i = p^i.$$

Proof. We shall first construct a uniformizer for K_i/K_{i-1}.

Lemma 6.4. *A uniformizer for the extension K_i/K_{i-1} (with the hypothesis $p \,||\, a$) is given by*

$$\pi_i = \frac{1-\zeta_p}{\sqrt[p]{a}\cdots\sqrt[p^i]{a}}.$$

Proof. Consider in K_i the element $\sqrt[p^i]{a}$. Thanks to the hypothesis $p \,||\, a$

$$(*) \qquad v_{K_i}(\sqrt[p^i]{a}) = \frac{v_{K_i}(a)}{p^i} = \frac{p^i v_{K_0}(a)}{p^i} = p-1.$$

But this, together with the fact that $1-\zeta_p$ is a uniformizer for $K_0 = \mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$, allows to prove the theorem by induction on $i \geq 1$. In fact:
$\underline{i=1}$

$$v_{K_1}\left(\frac{1-\zeta_p}{\sqrt[p]{a}}\right) = p v_{K_0}(1-\zeta_p) - v_{K_1}(\sqrt[p]{a}) = p-(p-1) = 1.$$

$\underline{i \Rightarrow i+1}$
From (*) and the inductive hypothesis, we have

$$v_{K_i}\left(\frac{\pi_{i-1}}{\sqrt[p^i]{a}}\right) = p\cdot v_{K_{i-1}}(\pi_{i-1}) - v_{K_i}(\sqrt[p^i]{a}) = p-(p-1) = 1.$$

□

Now that we have a uniformizer π_i, to calculate the break-number b_i of K_i/K_{i-1} we can simply let act on it the generator of the group $\mathrm{Gal}(K_i/K_{i-1}) \cong C(p)$ which sends $\sqrt[p^i]{a}$ in $\zeta_p\sqrt[p^i]{a}$ (see [10, Chapter IV, section 1, lemma 1]). We obtain

$$\begin{aligned} 1+b_i = v_{K_i}(s(\pi_i)-\pi_i) &= v_{K_i}\left(\frac{\pi_{i-1}}{\zeta_p\sqrt[p^i]{a}} - \frac{\pi_{i-1}}{\sqrt[p^i]{a}}\right) \\ &= v_{K_i}(\pi_i) + v_{K_i}\left(\frac{1-\zeta_p}{\zeta_p}\right) = 1 + p^i v_{K_0}(1-\zeta_p) = 1+p^i. \end{aligned}$$

□

Now that we have an analogue of the Theorem 5.6 we can calculate the higher ramification groups of our extension with the same inductive method that we used in the preceding section. So, even if we are now interested only in the extension $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q}_p$, we must consider also the intermediate extensions $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{a})/\mathbb{Q}_p$ with $0 \leq s \leq r$.

Theorem 6.5. *The ramification groups of* $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{a})/\mathbb{Q}_p$ *are:*

$$\begin{cases} G^0 & = C(p^s) & \rtimes\ G(p^r) \\ G^1 & = C(p^s) & \rtimes\ G(p^r)^1 \\ G^{i+\frac{1}{p-1}} & = C(p^{s-i+1}) & \rtimes\ G(p^r)^{i+1} \\ G^{i+1} & = C(p^{s-i}) & \rtimes\ G(p^r)^{i+1} \\ G^{s+j+1} & = & G(p^r)^{s+j+1} \end{cases}$$

with $1 \leq i \leq s$ *and* $1 \leq j \leq r-2-s$ *(with the convention that if* $r-2 \leq s$ *the last row doesn't appear).*

As the proof follows identically the same steps of that of Theorem 5.8, we give only the statement of the various lemmas involved without any proof (they are in fact conceptually identical to those relative to Theorem 5.8). By induction, we assume the theorem true for a certain $s < r$ and prove it for $s+1$ (the base of induction is as always the cyclotomic extension).

Lemma 6.6. *The ramification groups of* $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^s]{a})/\mathbb{Q}_p(\zeta_p, \sqrt[p^s]{a})$ *are (call* $\widetilde{G} = G(p^r)^1$ *its Galois group):*

$$\begin{cases} \widetilde{G}^{p-1} & = G(p^r)^1 \\ \widetilde{G}^{(p-1)p^i} & = G(p^r)^{i+1} \\ \widetilde{G}^{(j+1)(p-1)p^s} & = G(p^r)^{j+s+1} \end{cases}$$

with $1 \leq i \leq s$ *and* $1 \leq j \leq r-2-s$.

Now using Theorem 6.3 we can move to the field $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^{s+1}]{a})$ leaving fixed the base $\mathbb{Q}_p(\zeta_p, \sqrt[p^s]{a})$.

Lemma 6.7. *The ramification groups of* $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^{s+1}]{a})/\mathbb{Q}_p(\zeta_p, \sqrt[p^s]{a})$ *are (call* ${}^sG = C(p) \rtimes G(p^r)^1$ *its Galois group):*

$$\begin{cases} {}^sG^{p-1} & = C(p) \rtimes G(p^r)^1 \\ {}^sG^{(p-1)p^i} & = C(p) \rtimes G(p^r)^{i+1} \\ {}^sG^{p^{s+1}} & = C(p) \rtimes G(p^r)^{s+2} \\ {}^sG^{(j+1)(p-1)p^s} & = G(p^r)^{s+j+1} \end{cases}$$

with $1 \leq i \leq s$ *and* $1 \leq j \leq r-s-2$.

Now again using Theorem 6.3 we can go down with the base field.

Lemma 6.8. *The ramification groups of* $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^{s+1}]{a})/\mathbb{Q}_p(\zeta_p, \sqrt[p^{s-t}]{a})$ *with* $0 \le t \le s$ *are (call* ${}^{s-t}G = C(p^{t+1}) \rtimes G(p^r)^1$ *its Galois group):*

$$\begin{cases} {}^{s-t}G^{p-1} & = C(p^{t+1}) & \rtimes\ G(p^r)^1 \\ {}^{s-t}G^{(p-1)p^i} & = C(p^{t+1}) & \rtimes\ G(p^r)^{i+1} \\ {}^{s-t}G^{p^{s-t}[(2k+1)p-2k]} & = C(p^{t+1-k}) & \rtimes\ G(p^r)^{s-t+2+k} \\ {}^{s-t}G^{(k+2)(p-1)p^{s-t}} & = C(p^{t-k}) & \rtimes\ G(p^r)^{s-t+2+k} \\ {}^{s-t}G^{(j+t+1)(p-1)p^{s-t}} & = & G(p^r)^{s+j+1} \end{cases}$$

with $1 \le i \le s-t$, $0 \le k \le t$ *and* $2 \le j \le r-s-2$.

When $t = s$ the preceding lemma gives the following corollary.

Corollary 6.9. *The ramification groups of* $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^{s+1}]{a})/\mathbb{Q}_p(\zeta_p)$ *are (call* ${}^0G = C(p^{s+1}) \rtimes G(p^r)^1$ *its Galois group):*

$$\begin{cases} {}^0G^{p-1} & = C(p^{s+1}) & \rtimes\ G(p^r)^1 \\ {}^0G^{p+2k(p-1)} & = C(p^{s+1-k}) & \rtimes\ G(p^r)^{k+2} \\ {}^0G^{(k+2)(p-1)} & = C(p^{s-k}) & \rtimes\ G(p^r)^{k+2} \\ {}^0G^{(s+j+1)(p-1)} & = & G(p^r)^{s+j+1} \end{cases}$$

with $0 \le k \le s$ *and* $2 \le j \le r-s-2$.

Proof. [of Theorem 6.5] Now the theorem follows by observing that the inferior ramification groups of $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^{s+1}]{a})/\mathbb{Q}_p$ differ from those of $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^{s+1}]{a})/\mathbb{Q}_p(\zeta_p)$ only in degree 0 where we must substitute $G(p^r)^1$ with $G(p^r)$. □

We include in a corollary the case $s = r$ that interests us.

Corollary 6.10. *The ramification groups of* $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q}_p$ *are:*

$$\begin{cases} G^0 & = C(p^r) & \rtimes\ G(p^r) & = G_0 \\ G^1 & = C(p^r) & \rtimes\ G(p^r)^1 & = G_{(p-1)} \\ G^{i+\frac{1}{p-1}} & = C(p^{r-i+1}) & \rtimes\ G(p^r)^{i+1} & = G_{\frac{2p^{2i}+p-1}{p+1}} \\ G^{i+1} & = C(p^{r-i}) & \rtimes\ G(p^r)^{i+1} & = G_{(p-1)\frac{p^{2i}+1}{p+1}} \\ G^{r-1+\frac{1}{p-1}} & = C(p^2) & & = G_{\frac{2p^{2r-2}+p-1}{p+1}} \\ G^{r+\frac{1}{p-1}} & = C(p) & & = G_{\frac{p^{2r}+p^{2r-2}+p-1}{p+1}} \end{cases}$$

with $1 \le i \le r-2$.

Now that we have the higher ramification groups, we can calculate the local Artin conductor of the characters of $C(p^r) \rtimes G(p^r)$ using again the formula ([10, Chapter VI, section 2, exercise 2])

$$f(\chi) = \chi(1)(1 + c^\chi)$$

where c^χ is the biggest ramification group such that

$$\chi_{|G^{c^\chi}} \neq \chi(1)1_{|G^{c^\chi}}.$$

Theorem 6.11. *For a charcter χ of $C(p^r) \rtimes G(p^r)$ we have*

$$c^\chi = \begin{cases} pr(\chi) - 1 & \text{if } lev(\chi) + 2 \leq pr(\chi) \text{ or } 0 = lev\chi, \\ lev(\chi) + \dfrac{1}{p-1} & \text{if } 0 < lev(\chi) \leq pr(\chi) \leq lev(\chi) + 1. \end{cases}$$

Proof. From the definition of the null subgroup of a character (see definition 4.12), we deduce that c^χ is the biggest real number such that $G^{c^\chi} \not\subset Gr(\chi)$. So from Corollary 6.10 we deduce

$$G^u \not\subset Gr(\chi) = C(p^{r-lev(\chi)}) \rtimes G(p^r)^{pr(\chi)}$$
$$\Leftrightarrow \begin{cases} u \leq k + \dfrac{1}{p-1} & \text{if } 0 < lev(\chi) \\ \text{or} & \\ u \leq pr(\chi) - 1 & \text{if } 0 < pr(\chi). \end{cases}$$

Hence if $0 < lev(\chi)$ we have

$$c^\chi = \max\left\{lev(\chi) + \frac{1}{p-1}, pr(\chi) - 1\right\}$$
$$= \begin{cases} pr(\chi) - 1 & \text{if } lev + 2 \leq pr(\chi), \\ lev(\chi) + \dfrac{1}{p-1} & \text{if } pr(\chi) \leq lev(\chi) + 1. \end{cases}$$

□

Corollary 6.12. *The local Artin conductor $f(\chi)$ of χ is*

$$\begin{cases} pr(\chi) & \text{if } lev(\chi) = 0, \\ p^{lev(\chi)-1}(p-1)pr(\chi) & \text{if } 2 < lev(\chi) + 2 \leq pr(\chi), \\ p^{lev(\chi)-1}(p-1)[lev(\chi) + 1 + \frac{1}{p-1}] & \text{if } 0 < lev(\chi) \leq pr(\chi) \leq lev(\chi) + 1. \end{cases}$$

Proof. It follows from the preceding theorem and the formula $f(\chi) = \chi(1)(1 + c^\chi)$. □

Let us now calculate the p-component of the discriminant of the extension $\mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q}$ with $p \mid\mid a$. As it is a totally ramified extension we have

$$v_p(d(\mathbb{Q}(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q})) = v_p(d(\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q}_p))$$

so that we can focus ourselves on the local extension $\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q}_p$.

Theorem 6.13. *If $p \,||\, a$ then we have*

$$v_p\left(d(\mathbb{Q}_p(\zeta_{p^r}, \sqrt[p^r]{a})/\mathbb{Q}_p)\right) = rp^{2r-1}(p-1) + p\frac{p^{2r}-1}{p+1} - p\frac{p^{2r-3}+1}{p+1}.$$

Proof. Using the local conductor-discriminant formula and Corollary 6.12 we have:

$$\begin{aligned} v_p(d) &= \sum_{\chi \in G^*} \chi(1) f(\chi) \\ &= \sum_{lev(\chi)=0} pr(\chi) + \sum_{lev(\chi)>0} p^{2(lev(\chi)-1)}(p-1)^2 pr(\chi) \\ &\quad + \sum_{0<lev(\chi)=pr(\chi)-1} p^{2(lev(\chi)-1)}(p-1)^2 \frac{1}{p-1} \\ &\quad + \sum_{0<lev(\chi)=pr(\chi)} p^{2(lev(\chi)-1)}(p-1)^2 \left[1 + \frac{1}{p-1}\right]. \end{aligned}$$

The first two sums are identical to those in the formulas (5.4) and (5.5) of the fourth section. For the third sum we have:

$$\begin{aligned} &\sum_{0<lev(\chi)=pr(\chi)-1} p^{2(lev(\chi)-1)}(p-1)^2 \frac{1}{p-1} \\ &\qquad = \sum_{k=1}^{r-1} p^{2(lev(\chi)-1)}(p-1)^2 (p-1)\frac{1}{p-1} \\ &\qquad = (p-1)\frac{p^{2r-2}-1}{p+1}. \end{aligned} \tag{6.1}$$

Finally the fourth sum is equal to

$$\begin{aligned} &\sum_{0<lev(\chi)=pr(\chi)} p^{2(lev(\chi)-1)} \left[1 + \frac{1}{p-1}\right] \\ &\qquad = \sum_{k=1}^{r} p^{2(k-1)}(p-1)^2 \left(1 + \frac{1}{p-1}\right) \\ &\qquad = p\frac{p^{2r}-1}{p+1}. \end{aligned} \tag{6.2}$$

Adding together the formulas (5.4), (5.5), (6.1) and (6.2) we have the desired result. □

References

[1] M. ACOSTA, W. Y. VELEZ, *The lattice of subfields of radicals extensions*. Journal of Number theory **15** (1982), 388–405.

[2] J.W.S. CASSELS, A. FRÖHLICH, *Algebraic number theory*. Academic press: London, 1967.

[3] H. HASSE, *Number theory*. Springer-Verlag: New York, 1980.

[4] E.T. JACOBSON, W. Y. VELEZ, *The Galois group of a radical extension of the rationals*. Manuscripta Math. **67 no. 3** (1990), 271–284.

[5] K. KOMATSU, *An integral bases of the algebraic number field* $\mathbb{Q}(\sqrt[l]{a}, \sqrt[l]{1})$. J. Reine Angew. Math. **288** (1976), 152–153.

[6] S. LANG, *Algebra*, revised third edition. Springer-Verlag: New York, 2002.

[7] H. B. MANN, W. Y. VELEZ, *Prime ideal decomposition in* $F(\sqrt[n]{\mu})$. Monatsh. Math. **81** (1976), 131–139.

[8] B. MORA, W. Y. VELEZ, *Some results on radical extensions*. J. of Algebra **162** (1993), 295–301.

[9] A. SCHINZEL, *Abelian binomials, power residues and exponential congruences*. Acta Arith. f32 (1977), 245–274.

[10] J.P. SERRE, *Local fields*. Springer-Verlag: New York, 1979.

[11] W. Y. VELEZ, *A generalization of Schinzel's theorem on radical extensions of fields and an application*. Acta Arith. **51 no. 2** (1988), 119–130.

[12] W.Y. VELEZ, *On normal binomials*. Acta Arith. **36** (1980), 113–124.

[13] W. Y. VELEZ, *Prime ideal decomposition in* $F(\sqrt[p]{\mu})$. Pacific Journal of mathematics **75 no. 2** (1978), 589–600.

[14] W. Y. VELEZ, *Several results on radical extensions*. Arch. Math. (Basel) **45 no. 4** (1985), 342–349.

[15] W. Y. VELEZ, *The factorization of p in* $\mathbb{Q}(\sqrt[p^k]{a})$ *and the genus field of* $\mathbb{Q}(\sqrt[n]{a})$. Tokyo J. Math. **11 no. 1** (1988), 1–19.

[16] J. WESTLUND, *On the fundamental number of the algebraic number field* $K(\sqrt[p]{m})$. Trans. Amer. Math. Soc. **11** (1910), 388–392.

[17] J. WÓJCIK, *Contributions to the theory of Kummer extensions*. Acta Arith. **40** (1982), 155–174.

Filippo VIVIANI
Universita' degli studi di Roma Tor Vergata
Dipartimento dimatematica
via della ricerca scientifica 1
00133 Roma, Italy
E-mail : viviani@mat.uniroma2.it