A note on the discriminant and prime ramification of some real Kummer extensions

Andrea Lesavourey

A NOTE ON THE DISCRIMINANT AND PRIME RAMIFICATION OF SOME REAL KUMMER EXTENSIONS

ANDREA LESAVOUREY*

Abstract. In this note, we establish some facts about real Kummer extensions of the form $L = \mathbb{Q}(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_r})$, and $L = K(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_r})$ where $\mathbb{Q}(\sqrt[q]{n_1}, \ldots, \sqrt[q]{n_s})$. In particular, we study the splitting of primes in L and exhibit fairly canonical and simple $\mathbb{Q}$-bases of L and $d_L \in \mathbb{N}$ such that the order it generates contains $d_L\mathcal{O}_L$.

1. Introduction

The discriminant D_L of a number field L gives important information about the structure of the field. For example, a prime integer p ramifies in L if, and only if, it divides D_L, or the volume of the ring of integers $\mathcal{O}_L$ under Minkowski's embedding is equal to $\sqrt{|D_L|}$. Thus, knowing D_L can be particularly interesting. However, obtaining a closed formula can be difficult. Conversely, studying how primes ramify in L can help in determining a formula for D_L, notably through computing the different $\mathfrak{D}(L/\mathbb{Q})$ [3].

Computationally, computing the discriminant amounts to computing the ring of integers. The generic algorithms start with an order $\mathcal{O} = \mathbb{Z}[\theta]$ for some θ such that $L = \mathbb{Q}(\theta)$, and augment $\mathcal{O}$ in directions depending on the index $[\mathcal{O}_K : \mathcal{O}]$ [4]. They run in subexponential time as they require to factorise $[\mathcal{O}_K : \mathcal{O}]$. Hence, being able to identify an order $\mathcal{O}$ with a known factorisation of $[\mathcal{O}_L : \mathcal{O}]$ is interesting since it allows for the computation of $\mathcal{O}_L$ in polynomial time. In fact, knowing the set of primes dividing $[\mathcal{O}_L : \mathcal{O}]$ is sufficient.

Given $a \in \mathbb{Z}$ and $n \geqslant 3$ denote by $\sqrt[n]{a}$ the only *real* n-th root a. In this note, we will focus on Kummer extensions of the form $L = K(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_r})$ such that K is $\mathbb{Q}$ or $\mathbb{Q}(\sqrt[q]{n_1}, \ldots, \sqrt[q]{n_s})$, where $m_i, n_j \in \mathbb{Z}$ for any $i \in [\![1, r]\!], j \in [\![1, s]\!]$, and p, q are odd prime integers. Orders satisfying the aforementioned property have been identified for multiquadratic fields $\mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_r})$ by Schmal [9], together with the discriminant of these fields. Similar results have been obtained for bicubic fields [2] and multicubic fields [5]. Following these works, we study how primes ramify in the two types of Kummer extensions considered and identify similar orders, see Theorem 4 and

Theorem 6. Moreover, in the case where $K = \mathbb{Q}$, we study further the splitting of p in L an determine the exact factorisation of D_L in most cases, see Theorem 5.

2. Background and notation

First let us fix some notations and give some background required for the understanding. We refer the reader to [6, 8, 7] for anything related to number fields. Most of Subsections 2.1 and 2.3 is standard knowledge about discriminants and the splitting of primes in number field extensions. Therefore, an informed reader can easily skip those and go to Subsection 2.3 where we recall some facts and fix some notations connected to Kummer extensions.

Notations. Algebraic closures of number field extensions considered will be designated by Ω. Given a number field extension L/K we will denote by $\tilde{L}$ its Galois closure. We will write $\delta_{(\mathscr{P}(n))}$ for the indicator function of proposition $\mathscr{P}(\cdot)$, i.e. $\delta_{(\mathscr{P}(n))}$ is equal to 1 if $\mathscr{P}(n)$ is true and 0 otherwise. Finally, given two ordered sets A and B we will denote by $A \otimes B$ the tensor product of A and B (when it makes sense), i.e. $A \otimes B = \{ab, b \in B \mid a \in A\}$. If A and B are not ordered $A \otimes B$ will be the collection of all the products ab such that $a \in A$ and $b \in B$. Finally, we also use this notation for the tensor product of vectors and matrices.
If g is an element of a group G, we will write $o(g)$ its order in G.

2.1. Discriminants.

Definition 1 (Discriminant of a family)**.** Consider an extension of number fields L/K of degree n, $(x_1, \dots, x_n) \in L^n$, and write $\sigma_1, \dots, \sigma_n$ the elements of $\mathrm{Hom}(L/K, \Omega)$. Then the *discriminant of* $(x_1, \dots, x_n)$ *relative to* L/K, denoted by $D_K(x_1, \dots, x_n)$ is the element

$$D_{L/K}(x_1, \dots, x_n) = \det \left[\sigma_i(x_j)\right]_{\substack{i \in [\![1,n]\!] \\ j \in [\![1,n]\!]}}.$$

Proposition 1 ([8])**.** *Consider an extension of number fields L/K of degree n. The following properties are true.*

(1) For any $x \in \mathcal{O}_L$, $\mathrm{N}_{L/K}(x)$ are elements of $\mathcal{O}_K$.
(2) For any family $(x_1, \dots, x_n) \in \mathcal{O}_L^n$, the discriminant $D_{L/K}(x_1, \dots, x_n)$ is belongs to $\mathcal{O}_K$.

Moreover the norm map is transitive, i.e. if $M/L/K$ is a tower of number fields $\mathrm{N}_{M/K} = \mathrm{N}_{L/K}\mathrm{N}_{M/L}$.

Definition 2 (Discriminants)**.** (1) Let K be a number field. The *(absolute) discriminant* of an order $\mathcal{O}$ of K is the integer $D_{K/\mathbb{Q}}(b_1, \dots, b_n)$, where $(b_1, \dots, b_n)$ is any $\mathbb{Z}$-basis of $\mathcal{O}$. The *(absolute) discriminant* of K is the discriminant of its ring of integers $\mathcal{O}_K$.

(2) Given an extension of number fields L/K, its *relative discriminant* is defined to be the (well-defined) ideal of $\mathcal{O}_K$ generated by the discriminants of all basis of L/K which are contained in $\mathcal{O}_L$. It is denoted by $\mathfrak{d}(L/K)$.

Notation. The absolute discriminant of an order will be denoted by $D_K(\mathcal{O})$. The discriminant of K is simply denoted by D_K.

Proposition 2 ([4])**.** *Consider $\mathcal{O}_1$ and $\mathcal{O}_2$ two orders of a number field K. Then the following is true.*

$$\mathcal{O}_1 < \mathcal{O}_2 \iff \exists f \in \mathbb{Z}, D_K(\mathcal{O}_1) = D_K(\mathcal{O}_2)f^2.$$

Now let us consider part of the arithmetic of number fields and number fields extensions, by considering their ideals.

Definition 3 (Relative norm of ideals)**.** Let L/K be a number fields extension. The *norm* of an ideal I of L *relative* to L/K, denoted by $\mathrm{N}_{L/K}(I)$, is the fractional ideal of K generated by the norms of elements of I relative to L/K. In mathematical terms, one has $\mathrm{N}_{L/K}(I) = \langle \mathrm{N}_{L/K}(x) \mid x \in I \rangle_{\mathcal{O}_K}$.

Proposition 3. *Let $M/L/K$ be a tower of number fields, and I be an ideal of M. Then $\mathrm{N}_{M/K} = \mathrm{N}_{L/K}\mathrm{N}_{M/L}$, and $\mathfrak{d}(M/K) = \mathfrak{d}(L/K)^{[M:L]}\mathrm{N}_{L/K}(\mathfrak{d}(M/L))$.*

2.2. **Splitting of an ideal in an extension.**

Lemma 1 ([8])**.** *Consider L/K an extension of number fields, $\mathfrak{p}$ an ideal of K, and $\mathfrak{P}$ an ideal of L. Then $\mathfrak{P}$ divides $\mathfrak{p}$ in L if, and only if, $\mathfrak{P} \cap K = \mathfrak{p}$.*

Definition 4. Given an extension of number fields L/K, $\mathfrak{p}$ an ideal of K and $\mathfrak{P}$ an ideal of L. Then we say that $\mathfrak{P}$ is *above* $\mathfrak{p}$ if $\mathfrak{P} \mid \mathfrak{p}$.

Theorem 1 ([8])**.** *Consider L/K an extension of number fields, $\mathfrak{p}$ an ideal of K, and $\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{P}_i^{v_{\mathfrak{P}_i}(\mathfrak{p})}$ its factorisation in L. Then the following propositions are true.*

(1) $\sum_{i=1}^{g} v_{\mathfrak{P}_i}(\mathfrak{p})[\frac{\mathcal{O}_L}{\mathfrak{P}_i} : \frac{\mathcal{O}_K}{\mathfrak{p}}] = [L : K]$.

(2) For all $i \in [\![1, g]\!]$, $\mathrm{N}_{L/K}(\mathfrak{P}_i) = \mathfrak{p}^{[\frac{\mathcal{O}_L}{\mathfrak{P}_i} : \frac{\mathcal{O}_K}{\mathfrak{p}}]}$.

Definition 5 (Residual degree and ramification index)**.** Consider L/K an extension of number fields, $\mathfrak{p}$ an ideal of K, and $\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{P}_i^{v_{\mathfrak{P}_i}(\mathfrak{p})}$ its factorisation in L. Moreover fix $j \in [\![1, g]\!]$.

(1) The *residual degree* or *inertial degree* of $\mathfrak{P}_j$ over $\mathfrak{p}$ is the index $[\frac{\mathcal{O}_L}{\mathfrak{P}_j} : \frac{\mathcal{O}_K}{\mathfrak{p}}]$. It is denoted by $f(\mathfrak{P}_j|\mathfrak{p})$.

(2) The exponent $v_{\mathfrak{P}_j}(\mathfrak{p})$ is called the *ramification index* of $\mathfrak{P}_j$ over $\mathfrak{p}$, and is denoted by $e(\mathfrak{P}_j|\mathfrak{p})$.

One can rewrite the formulae in Theorem 1 as $[L:K]=\sum_{i=1}^{g} e(\mathfrak{P}_i|\mathfrak{p})f(\mathfrak{P}_i|\mathfrak{p})$ and $\mathrm{N}_{L/K}(\mathfrak{P}_i)=\mathfrak{p}^{f(\mathfrak{P}_i|\mathfrak{p})}$. Moreover the factorisation is even simpler if the extension is Galois, as shown by Proposition 4.

Proposition 4 ([8])**.** *Consider L/K an extension of number field which is Galois, and $\mathfrak{p}$ a prime ideal of K. Then the maps $e(\cdot|\mathfrak{p})$ and $f(\cdot|\mathfrak{p})$ are constants over the primes of L dividing $\mathfrak{p}$. If e and f are the respective constant values and g the number of prime ideals of L above $\mathfrak{p}$, then $[L:K]=efg$.*

Definition 6 (Types of splitting [4])**.** Let L/K be an extension of number fields and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Let $\mathfrak{p}=\prod_{i=1}^{g}\mathfrak{P}_i^{e(\mathfrak{P}_i|\mathfrak{p})}$ the factorisation of $\mathfrak{p}$ in L.

(1) The ideal $\mathfrak{p}$ *ramifies* in L/K if there is $i\in[\![1,r]\!]$ with $e(\mathfrak{P}_i|\mathfrak{p})>1$.
(2) If $g=1$ and $f(\mathfrak{P}_1|\mathfrak{p})=1$, we say that $\mathfrak{p}$ *ramifies completely* in L.
(3) We say that $\mathfrak{p}$ is *completely split* or *totally split* (or splits completely) in L if for all $i\in[\![1,g]\!]$, $e(\mathfrak{P}_i|\mathfrak{p})=f(\mathfrak{P}_i|\mathfrak{p})=1$.
(4) If $g=1$ and $e(\mathfrak{P}_1|\mathfrak{p})=1$ then $\mathfrak{p}$ is said to be *inert* in L.

Now let us state how the discriminant ideal of an extension L/K is related to the splitting of prime ideals.

Theorem 2 ([3])**.** *Given L/K an extension of number fields, a prime ideal $\mathfrak{p}$ of K ramifies in L if, and only if, it divides the relative discriminant ideal $\mathfrak{d}(L/K)$.*

Another important object, related to the discriminant is the *different*.

Definition 7 (Different)**.** Consider an extension of number fields L/K. The *relative different* $\mathfrak{D}(L/K)$ is the ideal defined as follows,

$$\mathfrak{D}(L/K)^{-1}=\{x\in L\mid \mathrm{Tr}_{L/K}(x\mathcal{O}_L)\subset\mathcal{O}_K\}.$$

As it is the case for norm, the different is transitive.

Proposition 5. *Let $M/L/K$ be a tower of number field extensions. Then $\mathfrak{D}(M/K)=\mathfrak{D}(M/L)\mathfrak{D}(L/K)$.*

The different is useful because it can be used to compute the discriminant.

Proposition 6 ([3])**.** *Let L/K be an extension of number fields. Then the prime ideals of L dividing $\mathfrak{D}(L/K)$ are exactly the ones ramified in L/K. Moreover $\mathrm{N}_{L/K}(\mathfrak{D}(L/K))=\mathfrak{d}(L/K)$.*

Proposition 7 ([7])**.** *Consider L/K an extension of number fields, $\mathfrak{p}$ an ideal of K, $\mathfrak{P}$ and ideal of L above $\mathfrak{p}$ and p the characteristic of $\mathcal{O}_K/(\mathfrak{p})$. Then if p and $e(\mathfrak{P}\mid\mathfrak{p})$ are coprime, one has $v_{\mathfrak{P}}(\mathfrak{D}(L/K))=e(\mathfrak{P}\mid\mathfrak{p})-1$.*

Definition 8. Consider a Galois extension L/K, $\mathfrak{P}$ a prime ideal of L and $\mathfrak{p} = \mathfrak{P} \cap K$. Then the *decomposition group of* $\mathfrak{P}$, denoted by $\mathcal{D}(\mathfrak{P} \mid \mathfrak{p})$, is $\{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$.

Proposition 8. *Consider a Galois extension L/K, $\mathfrak{P}$ a prime ideal of L. Then one has $|\mathcal{D}(\mathfrak{P} \mid \mathfrak{p})| = e(\mathfrak{P} \mid \mathfrak{P} \cap K) f(\mathfrak{P} \mid \mathfrak{P} \cap K)$.*

2.3. **Kummer extensions.**

Notation. Given p a prime integer, we will denote by τ_p a generator of the Galois group of the cyclotomic field $\mathbb{Q}(\zeta_p)$.

Definition 9. A number field extension L/K is called a *Kummer extension of exponent n* if $\zeta_n \in K$ and there are elements $m_1, \ldots, m_r$ of K such that $L = K(\sqrt[n]{m_1}, \ldots, \sqrt[n]{m_r})$.

Remark 1. In our work we relax this definition to allow ζ_n to not belong to L. We will also only consider extensions of prime exponents p. First let us recall some facts and fix some notations about the structure of Kummer extensions, and $\mathrm{Hom}(L/K, \Omega)$. We refer the reader interested in a more general and in-depth presentation of Kummer extensions to [3].

2.3.1. *Simple extensions:*

Definition 10. Consider L/K an extension of number fields, and prime number p. Then L/K is called a *simple Kummer extension of exponent p* if there is $m \in K$ such that $\sqrt[p]{m} \notin K$ and $L = K(\sqrt[p]{m})$.

Proposition 9. *Consider $L = K(\sqrt[p]{m})$ a simple Kummer extension. Then the following properties are true.*

1. *L/K is a field extension of degree p.*
2. *The elements of the set $\mathrm{Hom}(L/K, \Omega)$ can be fully described by their action on $\sqrt[p]{m}$ as $\sigma^{(i)} : \sqrt[p]{m} \longmapsto \zeta_p^i \sqrt[p]{m}, i \in [\![0, p-1]\!]$.*
3. *If $\zeta_p \in L$ then L/K is Galois. If $\zeta_p \notin K$ then the Galois closure of L/K is $\widetilde{L} = L(\zeta_p)$ and if p is odd then $\mathrm{Gal}(\widetilde{L}/K) = \langle \tau_p \rangle \ltimes \langle \sigma \rangle$ where σ is the extension of the embedding $\sigma^{(1)}$ which acts trivially on ζ_p. If p is 2 then L is Galois.*

Proposition 10. *Let $L = K(\sqrt[p]{m})$ be a simple Kummer extension of exponent p, and $n \in K$. Then $L = K(\sqrt[p]{n})$ if, and only if, there is $a \in K$ such that $n = ma^p$.*

2.3.2. *General extensions:* The properties described for simple Kummer extensions can be extended to general extensions.

Proposition 11. *Consider $L = K(\sqrt[p]{m_1}, \dots, \sqrt[p]{m_r})$ a Kummer extension. Then the following assertions are equivalent.*

(1) $[L : K] = p^r$;

(2) $(\forall \alpha \in \mathbb{Z}^r)$, $m_1^{\alpha_1} m_2^{\alpha_2} \cdots m_r^{\alpha_r} \in (K^*)^p \iff \forall i \in [\![1, r]\!], p \mid \alpha_i$.

Definition 11. Given a prime p, an integer $r \in \mathbb{N}^*$ and a sequence m of rational numbers $m_1, \dots, m_r$ we will say that m is *p-reduced for K* if it satisfies the condition of Proposition 11.

Proposition 12. *Consider p a prime number and $L = K(\sqrt[p]{m_1}, \dots, \sqrt[p]{m_r})$ a Kummer extension of exponent p. Then L can be described as $K(\sqrt[p]{n_1}, \dots, \sqrt[p]{n_s})$ with $n = (n_1, \dots, n_s)$ being a p-reduced sequence.*

From now on all Kummer extensions are considered to be generated by reduced sequences.

Notation. Consider $m = (m_1, \dots, m_r) \in K^r$ such that $L = K(\sqrt[p]{m_1}, \dots, \sqrt[p]{m_r})$ is an extension of degree p^r. For $i \in [\![1, r]\!]$ the field $L_{m_i} = K(\sqrt[p]{m_i})$ is a simple Kummer extension of K of exponent p. Given any $j \in [\![0, p-1]\!]$, write $\sigma_{m_i}^{(j)}$ the embeddings of L_{m_i} following the notation described previously and $\sigma_{m_i}^{j}$ the corresponding element of $\mathrm{Gal}(\widetilde{L_{m_i}}/K)$.

Proposition 13. *Consider L/K which satisfies the equivalent assertions of Proposition 11. Then the following assertions are true.*

(1) L/K has exactly $\frac{p^r-1}{2}$ simple subextensions of degree p over K and they are of the form $L_\alpha := L(\prod_{i=1}^r \sqrt[p]{m_i}^{\alpha_i})$ with $\alpha \in [\![0, p-1]\!]^r$. Moreover L_α and L_β are equal if, and only if, there is an integer λ such that $\alpha = \lambda \cdot \beta \pmod p$.

(2) Any subextension of L/K can be written as $K(\sqrt[p]{M_1}, \dots, \sqrt[p]{M_{r'}})$ where $0 \leqslant r' \leqslant r$ and $M_j = \prod_{i=1}^r \sqrt[p]{m_i}^{\alpha_i^{(j)}}$ with $\alpha^{(j)} \in [\![0, p-1]\!]^r$ for any $j \in [\![1, r']\!]$.

The Galois group of $\widetilde{L}/\mathbb{Q}$ can also be fully described with the ones of the subfields L_{m_i}.

Proposition 14. *Consider L/K which satisfies the equivalent assertions of Proposition 11. Then the following assertions are true.*

- $\mathrm{Hom}(L/K, \Omega) \cong \bigotimes_{i=1}^r \mathrm{Hom}(L_{m_i}/K, \Omega) = \{\otimes_{i=1}^r \sigma_{m_i}^{(\beta_i)} \mid \beta \in [\![0, p-1]\!]^r\}$.
- *$L(\zeta_p)/K(\zeta_p)$ is abelian with Galois group isomorphic to $\langle \sigma_{m_1} \rangle \times \cdots \times \langle \sigma_{m_r} \rangle$; if $\zeta_p \in K$ then the previous extension is L/K.*
- *If $\zeta_p \notin K$ then $L(\zeta_p)/K$ is Galois with Galois group isomorphic to $\langle \tau_p \rangle \ltimes \langle \sigma_{m_1} \rangle \times \cdots \times \langle \sigma_{m_r} \rangle$.*

Notation. Given a tuple β we will write $\sigma^{(\beta)}$ the embedding $\otimes_{i=1}^r \sigma_{m_i}^{(\beta_i)}$ and σ^β its extension in $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$. Given a subset S of $\mathrm{Hom}(K, \Omega)$ we will denote by $\widetilde{S}$ the subset of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ whose elements are the direct extension of elements of S.

3. Extensions with one exponent

First we will study fields of the form $K = \mathbb{Q}(\sqrt[p]{m_1}, \dots, \sqrt[p]{m_r})$.

Notation. Given a tuple $m = (m_1, \dots, m_r)$, we will write $\mathcal{P}(m)$ the set $\{p \in \mathcal{P}, p \mid \prod_{i=1}^r m_i\}$. Given $m \in \mathbb{Q}$ and an integer n we will denote by $PF(m, n)$ the rational number $\prod_{p\in\mathcal{P}} m^{v_p(m) \pmod n}$. Similarly if $m \in \mathbb{Q}^r$ then $PF(m, n) = (PF(m_1, n), \dots, PF(m_r, n))$. We extend $PF(\cdot, p)$ to elements in $\mathbb{Q}^{1/p}$ and sequences in $\mathbb{Q}^{1/p}$ with $PF(x, p) = PF(x^p, p)^{1/p}$. Finally, given a tuple $m \in \mathbb{Q}^r$ and $\alpha \in \mathbb{Z}^r$, we will write m^α to designate the product $\prod_{i\in[\![1,r]\!]} m_i^{\alpha_i}$.

3.1. A canonical $\mathbb{Q}-$basis of K.

One can define two fairly natural bases of K. One has already been mentioned earlier.

Definition 12. Let $K = \mathbb{Q}(\sqrt[p]{m_1}, \dots, \sqrt[p]{m_r})$ be a real Kummer field. Then the *naive basis of K relative to m* is $(\prod_{i=1}^r m_i^{\alpha_i/p})_{\alpha\in[\![0,p-1]\!]^r}$. It will be denoted by $\mathfrak{B}(p, m)$. The *power-free basis of K relative to m* is $PF(\mathfrak{B}(p, m), p)$. It will be denoted by $\mathfrak{IB}(p, m)$.

Remark 2. Both bases were considered in several work on Kummer fields such as [9, 1, 10].

The first property that can be proven is that $\mathfrak{IB}(p, m)$ is somehow independent of the choice of m.

Lemma 2. *Let K be a real Kummer field. Consider m and n two sequences defining K. Then $\mathfrak{IB}(p, m)$ and $\mathfrak{IB}(p, n)$ are equal as sets.*

Proof. Consider $q \in \mathcal{P}(m)$. First let us prove that if $q \notin \mathcal{P}(n)$ then $v_q(m^\alpha) \equiv 0 \pmod p$ for all $\alpha \in [\![0, p-1]\!]^r$. Let us fix such α. Since m and n define the same field K, one can use the simple subfields and conclude that $\mathbb{Q}(\sqrt[p]{m^\alpha}) = \mathbb{Q}(\sqrt[p]{n^\beta})$ for some β. This is equivalent to $m^\alpha = n^{j\beta}a^p$ for some $j \in [\![0, p-1]\!]$ and $a \in \mathbb{Q}$. Then we obtain the equality

$$v_q(m^\alpha) = \sum_{i=1}^r \alpha_i v_q(m_i) = \sum_{i=1}^r j\beta_i v_q(n_i) + pv_q(a) \tag{1}$$

and taking it modulo p gives $\sum_{i=1}^r \alpha_i v_q(m_i) = 0 \pmod p$, since $v_q(n_i) = 0$, for all $i \in [\![1, r]\!]$. This is true for all α. Thus we obtain that none of $q \in \mathcal{P}(m) \cup \mathcal{P}(n) \setminus (\mathcal{P}(m) \cap \mathcal{P}(n))$ can be found in $\mathfrak{IB}(p, m)$ nor $\mathfrak{IB}(p, m)$.

Now let us consider only $q \in \mathcal{P}(m) \cap \mathcal{P}(n)$. Let $\alpha \in \mathbb{F}_p^r \setminus \{0\}$. Then for all $q \in \mathcal{P}(m) \cap \mathcal{P}(n)$ and all $j \in [\![1, p-1]\!]$, $(v_q(m^{j\alpha})) = jv_q(m^\alpha) \pmod p$. Following Equation (1), if β is such that n^β defines the same simple field as m^α, then $(v_q(m^\alpha))_q = j(v_q(n^\beta))_q$ for some $j \in [\![1, p-1]\!]$. Therefore the sets $\{(v_q(m^{j\alpha}))_q \mid j \in [\![1, p-1]\!]\}$ and $\{(v_q(n^{j\beta}))_q \mid j \in [\![1, p-1]\!]\}$ are identical.

Finally, if α and α' define distinct simple subfields of K then they are not colinear in $\mathbb{F}_p^r$, thus $\{j\alpha \mid j \in [\![1, p-1]\!]\} \cap \{j\alpha' \mid j \in [\![1, p-1]\!]\} = \emptyset$. □

The equality given by Lemma 2 shows that the set of power-free basis of a real Kummer field is a canonical choice of a $\mathbb{Q}$-basis of K.

Definition 13. Let K be a real Kummer field with one exponent p defined by a sequence m. *The power-free basis* of K is the unordered sequence set $\mathfrak{IB}(p, m)$. It will be denoted $\mathfrak{IB}(K)$.

Now let us prove another simple result on defining sequences, that will be used later.

Lemma 3. *Let $m \in \mathbb{Q}^r$ be a sequence defining a real Kummer extension K with one exponent p, and $i_0 \in [\![1, r]\!]$. Consider $q \in \mathcal{P}(m)$ such that $\exists i \in [\![1, r]\!], v_q(m_i) \not\equiv 0 \pmod p$. Then there is $m' \in \mathbb{Q}^r$ defining K such that*

$$\forall i \in [\![1, r]\!], q \mid m'_i \iff i = i_0.$$

Proof. One can always assume $v_q(m_{i_0}) \not\equiv 0 \pmod 0$, modulo a permutation on m. Then fix $m'_{i_0} = PF(m_{i_0}, p)$, and $m'_i = PF(m_i, p)$ for all $i \in [\![1, r]\!]$ such that $q \nmid m_i$. Finally consider $i \in [\![1, r]\!]$ such that $q \mid m_i$. Let $e_i \geqslant 0$ such that $e_i \equiv -v_q(m_i)v_q(m_{i_0})^{-1} \pmod p$. Then fix $m'_i = PF(m_i m_{i_0}^{e_i}, p)$. □

We will now determine the discriminant of $\mathfrak{IB}(K)$.

Theorem 3. *Let $K = \mathbb{Q}(\sqrt[p]{m_1}, \dots, \sqrt[p]{m_r})$ be a real Kummer field, and q a prime integer. Moreover write $b = \delta_{(p \in \mathcal{P}(m))}$. Then the discriminant $D_K(\mathfrak{IB}(K))$ satisfies the following:*

$$v_q(D_K(\mathfrak{IB}(K))) = \begin{cases} p^{r-1}(p-1), & \text{if } q \in \mathcal{P}(m) \setminus \{p\}, \\ p^{r-1}(p-1) \times b + rp^r, & \text{if } q = p. \end{cases} \tag{2}$$

Proof. Given a sequence m such that $K = \mathbb{Q}(\sqrt[p]{m_1}, \dots, \sqrt[p]{m_r})$, let us denote by M_m the matrix $(\sigma^{(\beta)}(\mathfrak{IB}(p, m)_j))_{\beta, j}$, where as usual $\sigma^{(\beta)} : \sqrt[p]{m_i} \longmapsto \zeta_p^{\beta_i} \sqrt[p]{m_i}$. Moreover we will write M_B the matrix $[\sigma^{(\beta)}(b_j)]_{\beta, j}$ for any $\mathbb{Q}-$basis $B = (b_1, \dots, b_{p^r})$.

First remark that $D_K(\mathfrak{IB}(K)) = D_K(\mathfrak{IB}(p, m))$ for any sequence m defining K. Indeed, considering different sequences amounts to applying permutations on the rows and columns of a fixed matrix M_m. Moreover, if $m' = (m_1, \dots, m_{r-1})$ then $\mathfrak{B}(p, m) = \mathfrak{B}(m_r) \otimes \mathfrak{B}(m')$ and $\mathfrak{IB}(p, m) = PF(\mathfrak{IB}(p,m_r) \otimes \mathfrak{IB}(p,m'), p)$. Let us denote by $\mathfrak{B}$ the basis $\mathfrak{IB}(p,m_r) \otimes \mathfrak{IB}(p,m')$.

Now let us start with the proof per se. Let m be a defining sequence of K. One can assume it is p-reduced and composed of integers. Let $q \in \mathcal{P}(m) \setminus \{p\}$. Following Lemma 2 and Lemma 3, one can also assume that $q \mid m_r$ and for all $i < r, q \nmid m_i$. We mentioned that $\mathfrak{IB}(p,m) = PF(\mathfrak{IB}(m_r) \otimes \mathfrak{IB}(m'), p)$. The action of PF amounts to dividing elements of the basis by an integer. Let us denote by $c_1, \ldots, c_{p^r}$ these integers. Since q divides only m_r and $\mathfrak{IB}(m_r)$ is already reduced, none of said coefficients is divided by q. Now remark that $M_m = M_{\mathfrak{IB}(p,m)} = [\frac{C_1(M_{\mathfrak{B}})}{c_1} | \ldots | \frac{C_{p^r}(M_{\mathfrak{B}})}{c_{p^r}}]$, where $C_j(M_{\mathfrak{B}})$ is the j-th column of $M_{\mathfrak{B}}$. Therefore we have $\det M_m = \frac{\det M_{\mathfrak{B}}}{c_1 c_2 \ldots c_{p^r}}$. Consequently we obtain $v_q(\det M_m) = v_q(\det M_{\mathfrak{B}})$, and we can consider the discriminant of the basis $\mathfrak{B}$. Now let us denote by $b_1, \ldots, b_p$ the elements of $\mathfrak{IB}(m_r)$. Then we have $\mathfrak{B} = [\mathfrak{IB}(m')b_1 | \mathfrak{IB}(m')b_2 | \ldots | \mathfrak{IB}(m')b_p]$ and for $\beta \in [\![0, p-1]\!]^r$, $\sigma^{(\beta)} = \sigma_1^{(\beta_1)} \otimes \cdots \otimes \sigma_r^{(\beta_r)}$ acts on $\mathfrak{IB}(m')b_i$ as

$$\sigma_1^{(\beta_1)} \otimes \cdots \otimes \sigma_{r-1}^{(\beta_{r-1})} \left(\mathfrak{IB}(m')\right) \sigma_r^{(\beta_r)}(b_i).$$

Thus we obtain that $M_{\mathfrak{B}}$ is equal to

$$\left[\begin{array}{c|c|c|c} b_1 M_{\mathfrak{IB}(m')} & b_2 M_{\mathfrak{IB}(m')} & \ldots & b_p M_{\mathfrak{IB}(m')} \\ \hline \sigma_r^{(1)}(b_1) M_{\mathfrak{IB}(m')} & \sigma_r^{(1)}(b_2) M_{\mathfrak{IB}(m')} & \ldots & \sigma_r^{(1)}(b_p) M_{\mathfrak{IB}(m')} \\ \hline \vdots & \vdots & & \vdots \\ \hline \sigma_r^{(p-1)}(b_1) M_{\mathfrak{IB}(m')} & \sigma_r^{(p-1)}(b_2) M_{\mathfrak{IB}(m')} & \ldots & \sigma_r^{(p-1)}(b_p) M_{\mathfrak{IB}(m')} \end{array}\right],$$

which is $M_{m_r} \otimes M_{m'}$. Therefore, we have $\det M_{\mathfrak{B}} = \det M_{m_r}^{p^{r-1}} \det M_{m'}^p$, and

$$v_q(D_K(\mathfrak{IB}(K))) = p^{r-1} v_q(\det M_{m_r}^2) + p v_q(\det M_{m'}^2).$$

Westlund showed that $v_q(\det M_{m_r}^2) = p-1$ and since $q \nmid m_i$ for all $i \in [\![1, r-1]\!]$ one has $v_q(\det M_{m'}^2) = 0$, by induction and remarking that $v_q(\det M'_m) = v_q(\det M_{m_1} \otimes \cdots \otimes M_{m_{r-1}})$ [10]. Finally we obtain $v_q(D_K(\mathfrak{IB}(K))) = (p-1)p^{r-1}$.

Now consider $q = p$. As before we have $v_p(\det M_m^2) = v_p(\det M_{m_1}^2 \otimes \cdots \otimes \det M_{m_r}^2)$, and $\det M_1^2 \otimes \det M_r^2 = \prod_{i=1}^r (\det M_{m_i}^2)^{p^{r-1}}$. If $p \notin \mathcal{P}(m)$ then $v_p(\det M_{m_i}^2) = p$ for all $i \in [\![1, r]\!]$ [10], so $v_p(D_K(\mathfrak{IB}(K))) = \sum_{i=1}^r p^{r-1} v_p(\det M_{m_i}^2) = rp^r$. If $p \in \mathcal{P}(m)$ then $v_p(\det M_{m_i}^2) = p$ for all $i \in [\![1, r-1]\!]$ and $v_p(\det M_{m_r}^2) = 2p-1$ [10]. Therefore we have $v_p(D_K(\mathfrak{IB}(K))) = \sum_{i=1}^{r-1} p^{r-1} v_p(\det M_i^2) + p^{r-1}(2p-1) = rp^r + p^{r-1}(p-1)$. □

We established that $\mathfrak{IB}(K)$ is a fairly canonical basis for a real Kummer field K, and determined its discriminant. We will show that the order it generates contains $[K : \mathbb{Q}]\mathcal{O}_K$. For this we will

study the discriminant of K. Indeed recall that we have the following result. Given $\mathcal{O}_1$ and $\mathcal{O}_2$ two orders of a number field, then $\mathcal{O}_1 < \mathcal{O}_2 \iff D_K(O_2) \mid D_K(O_1)$.

Lemma 4. *Let $K \in \mathbb{Q}(\sqrt[p]{m_1}, \dots, \sqrt[p]{m_r})$ be a real Kummer extension defined by a p-reduced sequence m. Then q ramifies in $K/\mathbb{Q}$ if, and only if, $q \in \mathcal{P}(m) \cup \{p\}$.*

Proof. We know that $K = \otimes_{i=1}^r \mathbb{Q}(\sqrt[p]{m_i})$, and given two linearly disjoints fields K_1 and K_2, the discriminant of their compositum $D_{K_1K_2}$ divides $D_{K_1}^{[K_2:\mathbb{Q}]} D_{K_2}^{[K_1:\mathbb{Q}]}$. Therefore we have $D_K \mid \prod_{i=1}^r D(\mathbb{Q}(\sqrt[p]{m_i}))^{p^{r-1}}$. Following Westlund [10], $q \mid D(\mathbb{Q}(\sqrt[p]{m_i}))$ if, and only if, $q \in \mathcal{P}(m_i) \cup \{p\}$. □

In order to study the $q-$valuation of D_K, we will study the splitting of q in $K/\mathbb{Q}$. A similar approach has been done over multiquadratic fields [9] and bicubic fields [2]. We will use some results over dihedral groups, which are stated and proved in Appendix B.

3.1.1. *Splitting of primes in K.* To study the splitting of primes we will use the different of the extensions. Westlund established the splitting for simple fields.

Proposition 15 (Westlund [10])**.** *Let $K = \mathbb{Q}(\sqrt[p]{m})$ be a simple Kummer extension and q a prime integer. Then one has the following possibilities:*

(1) $q \neq p$ and $q \mid m \implies (q) = \mathfrak{q}^p$;
(2) $p \mid m \implies (p) = \mathfrak{p}^p$;
(3) $p \nmid m$ and $m^{p-1} \equiv 1 \bmod p^2 \implies (p) = \mathfrak{p}^{p-1}\mathfrak{q}$;
(4) $p \nmid m$ and $m^{p-1} \not\equiv 1 \bmod p^2 \implies (p) = \mathfrak{p}^p$.

One can see that for simple Kummer field, the splitting of p depends on a condition satisfied by m: whether $m^{p-1} \equiv 1 \bmod p$ or not. The splitting of primes in a general number field K will then be influenced by their splitting in the simple subfields of K. We can identify different types of Kummer fields.

Lemma 5. *Let $K = \mathbb{Q}(\sqrt[p]{m_1}, \sqrt[p]{m_2})$ be a Kummer extension of degree p^2 such that $m_i \not\equiv 0 \bmod p$ and $m_i \not\equiv 1 \bmod p^2$, for $i \in \{1, 2\}$. Then one can find m' a sequence defining K such that $m'_2 \equiv 1 \bmod p^2$.*

Proof. For $i \in \{1, 2\}$, since $m_i \not\equiv 0 \bmod p$ then m_i can be seen as an element of $G = (\frac{\mathbb{Z}}{p^2\mathbb{Z}})^\times$. Moreover the order of m_i in G is p or $p(p-1)$, and we want to prove that we can find a defining sequence m' such that $o(m'_2) \mid p-1$. The group G is isomorphic to $\frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}$. Let us denote by $\phi = (\phi_1, \phi_2)$ this isomorphism. Then $\phi(m_i) = (\phi_1(m_i), \phi_2(m_2))$ with $\phi_2(m_i) \neq 0$. Let m' defined by $m'_1 = m_1$ and $m'_2 = m_1 m_2^k$ with $k \in [\![1, p-1]\!]$ such that $k\phi_2(m_2) = -\phi_2(m_1)$. Then one has $\phi_2(m'_2) = 0$ so $o(m'_2) \mid p-1$ in G. Clearly m' also defines K. □

Using Lemma 5, we obtain only a few possibilities for general real Kummer extensions.

Proposition 16. *Let K be a real Kummer extension of degree p^r for an integer $r \geqslant 1$. Then one can find a sequence $m = (m_1, \dots, m_r)$ defining K and satisfying one of the following properties.*

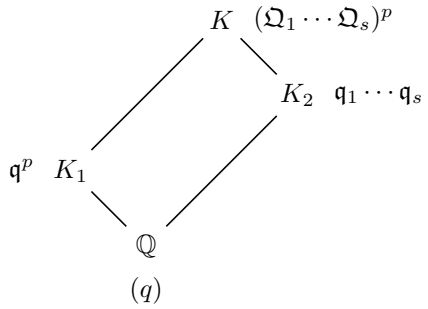
(1) $p \notin \mathcal{P}(m)$ *and* $\forall i \in [\![1, r]\!], m_i^{p-1} \equiv 1 \bmod p^2$.
(2) $p \notin \mathcal{P}(m)$, $m_1^{p-1} \not\equiv 1 \bmod p^2$ *and* $\forall i \in [\![2, r]\!], m_i^{p-1} \equiv 1 \bmod p^2$.
(3) $p \mid m_1$ *and* $\forall i \in [\![2, r]\!], m_i^{p-1} \equiv 1 \bmod p^2$.
(4) $p \mid m_1$, $m_2^{p-1} \not\equiv 1 \bmod p^2$ *and* $\forall i \in [\![3, r]\!], m_i^{p-1} \equiv 1 \bmod p^2$.

Proof. This is just an application of Lemma 3 and Lemma 5. □

Now we can express how primes split in K depending on which type of Kummer field it is. However remark than only the splitting of p will be influenced by the types identified in Proposition 16. Therefore, let us start by $q \neq p$.

Proposition 17. *Consider $K = \mathbb{Q}(\sqrt[p]{m_1}, \dots, \sqrt[p]{m_r})$ a real Kummer extension with one exponent, and $q \in \mathcal{P}(m)$. Then q splits in K as $\mathfrak{Q}_1^p \dots \mathfrak{Q}_s^p$ for $s \geqslant 1$, and $v_q(D_K) = (p-1)p^{r-1}$.*

Proof. By Lemma 3, one can suppose that $\forall i \in [\![2, r]\!], q \mid m_i \iff i = 1$. Let us fix $K_1 = \mathbb{Q}(\sqrt[p]{m_1})$ and $K_2 = \mathbb{Q}(\sqrt[p]{m_2}, \dots, \sqrt[p]{m_r})$. By [10] the prime q ramifies in K_1 as $\mathfrak{q}^p$. Moreover q is unramified in K_2 so $q\mathcal{O}_{K_2} = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ with $s \geqslant 1$. By multiplicativity of the ramification index, for all $i \in [\![1, s]\!]$, the ideal $\mathfrak{q}_i$ ramifies completely in K as $\mathfrak{Q}_i^p$. Therefore $q\mathcal{O}_K = (\mathfrak{Q}_1 \cdots \mathfrak{Q}_s)^p$.



Now recall that the different of $K/\mathbb{Q}$ satisfies $\mathfrak{D}(K/\mathbb{Q}) = \prod_{\mathfrak{Q}} \mathfrak{Q}^{s_{\mathfrak{Q}}}$ where the product is over the prime ideals of $\mathcal{O}_K$ which are ramified over $\mathbb{Q}$. Thus the part of $\mathfrak{D}(K/\mathbb{Q})$ above q is $\prod_{i=1}^{s} \mathfrak{Q}_i^{s_i}$ for some integers s_i. For all $i \in [\![1, s]\!]$ we know that $e(\mathfrak{Q}_i|q) = p$ and q are coprime. Therefore s_i is equal to $e(\mathfrak{Q}_i|q) - 1 = p - 1$. Thus one has for the discriminant

$$v_q(D_K) = v_q(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{D}(K/\mathbb{Q}))) = v_q(\mathrm{N}_{K_2/\mathbb{Q}}(\mathrm{N}_{K/K_2}(\prod_{i=1}^{s} \mathfrak{q}_i^{p-1}))).$$

Finally since $\mathrm{N}_{K/K_2}(\mathfrak{Q}_i) = \mathfrak{q}_i$ we obtain

$$v_q(D_K) = v_q(\mathrm{N}_{K_2/\mathbb{Q}}(\prod_{i=1}^{s} \mathfrak{q}_i^{p-1})) = v_q(\mathrm{N}_{K_2/\mathbb{Q}}(q\mathcal{O}_{K_2})^{p-1}) = (p-1)p^{r-1}.$$

□

With Proposition 17 one is able to prove the result we were looking for.

Theorem 4. *Let $K = \mathbb{Q}(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_r})$ be a real Kummer extension, and denote by $\mathcal{O}$ the order $\mathbb{Z}[\mathfrak{IB}(K)]$. Then the following propositions are true:*

- *$\forall q \in \mathcal{P}(m) \setminus \{p\}$, $\mathcal{O}$ is $q-$maximal;*
- *$[K:\mathbb{Q}]\mathcal{O}_K < \mathcal{O}$.*

Proof. Proposition 17 and Theorem 3 show that $v_q(\mathcal{O}) = v_q(\mathcal{O}_K)$ for all $q \in \mathcal{P}(m) \setminus \{p\}$, so $\mathcal{O}$ is indeed $q-$maximal. Concerning p one has

$$v_p(D_K([K:\mathbb{Q}]\mathcal{O}_K)) \geqslant 2[K:\mathbb{Q}]v_q([K:\mathbb{Q}]) = 2rp^r \geqslant rp^r + p^{r-1}(p-1)$$

so the second property is also true. □

3.2. **Splitting of the exponent.** Despite the fact that Theorem 4 shows that $\mathfrak{IB}(K)$ is a basis satisfying the properties we were looking for, we can still study further the splitting of p in K in each of the four types of real Kummer fields established in Proposition 16. It allows us to have a finer knowledge of D_K. First let us establish a result concerning extensions of number fields such that the Galois group of their Galois closure is dihedral.

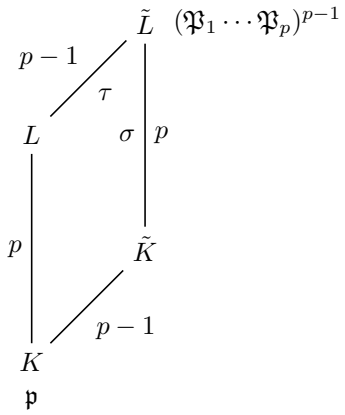
Lemma 6. *Let L/K be an extension of number fields. Suppose additionally that $\mathrm{Gal}(\tilde{L}/K)$ is isomorphic to $\langle\tau\rangle \ltimes \langle\sigma\rangle$, with $\langle\tau\rangle \cong \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$ and $\langle\sigma\rangle \cong \frac{\mathbb{Z}}{p\mathbb{Z}}$ for some prime integer p. Any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ satisfies*

$$\mathfrak{p}\mathcal{O}_{\tilde{L}} = (\mathfrak{P}_1 \ldots \mathfrak{P}_p)^{p-1} \implies \mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2^{p-1},$$

where each $\mathfrak{P}_i$ is a prime ideal of $\tilde{L}$ and each $\mathfrak{p}_i$ is a prime ideal of L.

It is similar to part of the proof for Proposition 10.1.26 of Cohen's book [3]. In fact several facts and their proofs that we will establish are generalisations of this Proposition.

Proof. Let $G = \mathrm{Gal}(\tilde{L}/K)$. By hypothesis we are in the following situation :



The group G acts transitively on the $\mathfrak{P}_i$ and by conjugation on the inertia groups $I(\mathfrak{P}_i \mid \mathfrak{p})$ for $i \in [\![1, p]\!]$. Clearly one has $|I(\mathfrak{P}_i/\mathfrak{p})| = p-1$. By Lemma 9 there are p distinct subgroups of G of order $p-1$. Moreover they are of the form $\langle \tau\sigma^b \rangle$ with $b \in [\![0, p-1]\!]$. Therefore the action of G on the set of such subgroups is transitive. Thus there is a unique $i_0 \in [\![1, p]\!]$ such that $I(\mathfrak{P}_{i_0} \mid \mathfrak{p}) = \langle \tau \rangle$, and $I(\mathfrak{P}_{i_0} \mid \mathfrak{P}_{i_0} \cap \mathcal{O}_L) = I(\mathfrak{P}_{i_0} \mid \mathfrak{p}) \cap \mathrm{Gal}(\tilde{L}/L) = \langle \tau \rangle$. Therefore $e(\mathfrak{P}_{i_0} \mid \mathfrak{P}_{i_0} \cap \mathcal{O}_L) = p-1$ so by multiplicativity $e(\mathfrak{P}_{i_0} \cap \mathcal{O}_L \mid \mathfrak{p}) = 1$. Now consider $i \neq i_0$. Then $I(\mathfrak{P}_i \mid \mathfrak{p}) = \langle \tau\sigma^b \rangle$ for some $b \in [\![1, p-1]\!]$, and $I(\mathfrak{P}_i \mid \mathfrak{P}_{i_0} \cap \mathcal{O}_L) = I(\mathfrak{P}_{i_0} \mid \mathfrak{p}) \cap \mathrm{Gal}(\tilde{L}/L) = \langle 1 \rangle$. Therefore again by multiplicativity of the ramification index, $e(\mathfrak{P}_i \cap \mathcal{O}_L \mid \mathfrak{p}) = p-1$. □

Theorem 5. *Consider $K = \mathbb{Q}(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_r})$ a real Kummer extension with exponent p. Then depending on the type of field as described in Proposition 16 the splitting of p in K and $v_p(D_K)$ are as follows :*

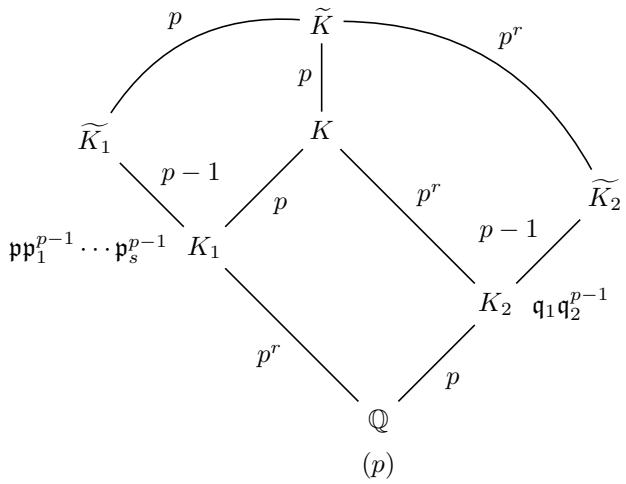
(1) $(p) = \mathfrak{p}(\mathfrak{p}_1 \ldots \mathfrak{p}_s)^{p-1}$ *for* $s = \frac{p^r-1}{p-1}$, *and* $v_p(D_K) = \frac{p^r-1}{p-1}(p-2)$;
(2) $(p) = \mathfrak{p}^p(\mathfrak{p}_1 \ldots \mathfrak{p}_s)^{p(p-1)}$ *for* $s = \frac{p^{r-1}-1}{p-1}$, *and* $v_p(D_K) = p^r + \frac{p^{r-1}-1}{p-1}(p-2)$;
(3) $(p) = \mathfrak{p}^p(\mathfrak{p}_1 \ldots \mathfrak{p}_s)^{p(p-1)}$ *for* $s = \frac{p^{r-1}-1}{p-1}$, *and* $v_p(D_K) = p^{r-1}(2p-1) + \frac{p^{r-1}-1}{p-1}(p-2)$.

Remark 3. We were not able to prove similar results for the fourth type of field for a general exponent p. However we did so for $p = 3$ in [5].

Proof. We will prove the results one type of fields after another.

Fields of the first type. We will prove the factorisation by induction. For $r = 1$, K is a simple Kummer extension. Then the splitting is correct, following Westlund [10]. Now consider $r \geqslant 1$ and assume the result is true for r. Let $K = \mathbb{Q}(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_{r+1}})$ a real Kummer field such that for all $i \in [\![1, r+1]\!], m_i^{p-1} \equiv 1 \bmod p^2$. Let us fix $K_1 = \mathbb{Q}(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_r})$ and $K_2 = \mathbb{Q}(\sqrt[p]{m_{r+1}})$. If one

denotes $\frac{p^r-1}{p-1}$ by s, one has the following decompositions by using the induction hypothesis, where the numbers are the dimensions of the respective extensions.



Moreover p is totally ramified as $\mathfrak{a}^{p-1}$ in $k=\mathbb{Q}(\zeta_p)$. First we consider the splitting of p in the Galois closure $\widetilde{K_1}$ and $\widetilde{K_2}$. We focus on $\widetilde{K_2}$, and the situation in $\widetilde{K_1}$ is similar. First remark that $\widetilde{K_2}/\mathbb{Q}$ is Galois with dimension $[\widetilde{K_2}:\mathbb{Q}]=p(p-1)$ so the decomposition of p satisfies $efg=p(p-1)$ with the functions $e(\cdot|p)$ and $f(\cdot|p)$ being constant – equal to e and f respectively – over prime ideals $\widetilde{\mathfrak{q}}$ of $\tilde{K_2}$ such that $\widetilde{\mathfrak{q}}\mid(p)$. Considering the factorisation $p\mathcal{O}_{K_2}=\mathfrak{q}_1\mathfrak{q}_2^{p-1}$ we obtain $p-1\mid e(\widetilde{\mathfrak{q}}|p)$. Moreover for the decomposition of $\mathfrak{q}_\mathfrak{i}$ in $\widetilde{K_2}$, since $\widetilde{K_2}/K_2$ is Galois, we have $e_if_ig_i=p-1$. Since $p-1\mid e$ and $e=e_1$ we have $e_1=p-1$, $f_1=1$ and $g_1=1$. Therefore $\mathfrak{q}_1\mathcal{O}_{\widetilde{K_2}}=\widetilde{\mathfrak{q}}^{p-1}$. Moreover $f=f_1=f_2$ and $e=(p-1)e_2$ so $e_2=1$ and $g_2=p-1$. Thus $\mathfrak{q}_2$ splits completely in $\widetilde{K_2}$ as $\widetilde{\mathfrak{q}_1}\widetilde{\mathfrak{q}_2}\dots\widetilde{\mathfrak{q}_{p-1}}$. Finally we obtain the factorisation $(p)=\widetilde{\mathfrak{q}}^{p-1}\widetilde{\mathfrak{q}_1}^{p-1}\widetilde{\mathfrak{q}_2}^{p-1}\dots\widetilde{\mathfrak{q}_{p-1}}^{p-1}$ in $\widetilde{K_2}$. Similarly we have $\mathfrak{p}\mathcal{O}_{\widetilde{K_1}}=\widetilde{\mathfrak{p}}^{p-1}$ and $\mathfrak{p}_i$ splits completely in $\widetilde{K_1}$ for all $i\in[\![1,s]\!]$. Therefore the factorisations of (p) in $\widetilde{K_1}$ and $\widetilde{K_2}$ are as follows:

$$(p)=\begin{cases}\widetilde{\mathfrak{q}}^{p-1}(\widetilde{\mathfrak{q}_1}\widetilde{\mathfrak{q}_2}\dots\widetilde{\mathfrak{q}_{p-1}})^{p-1}, & \text{in } \widetilde{K}_2/\mathbb{Q},\\ \widetilde{\mathfrak{p}}^{p-1}(\widetilde{\mathfrak{p}_1}\widetilde{\mathfrak{p}_2}\dots\widetilde{\mathfrak{p}_s})^{p-1}, & \text{in } \widetilde{K}_1/\mathbb{Q}.\end{cases}$$

Consequently the splitting of $\mathfrak{a}$ in the same two fields is

$$(\mathfrak{a})=\begin{cases}\widetilde{\mathfrak{q}}\widetilde{\mathfrak{q}_1}\widetilde{\mathfrak{q}_2}\dots\widetilde{\mathfrak{q}_{p-1}}, & \text{in } \widetilde{K}_2/\mathbb{Q},\\ \widetilde{\mathfrak{p}}\widetilde{\mathfrak{p}_1}\widetilde{\mathfrak{p}_2}\dots\widetilde{\mathfrak{p}_s}, & \text{in } \widetilde{K}_1/\mathbb{Q}.\end{cases}$$

Remark that the residual degree is 1 everywhere. We will now consider the decomposition of p in $\tilde{K}$. We will in fact look at the decomposition of $\mathfrak{a}$. Consider $\tilde{\mathfrak{P}}$ a prime ideal of $\widetilde{K}$ above p. Remark it is

also above $\mathfrak{a}$ in $\widetilde{K}/k$. For $i \in \{1,2\}$, denote by $\mathcal{D}_i$ the decomposition group $\mathcal{D}(\tilde{\mathfrak{P}} \mid \tilde{\mathfrak{P}} \cap \mathcal{O}_{\widetilde{K}_i})$. Let us write $G = \mathrm{Gal}(\widetilde{K}/k)$, $G_1 = \mathrm{Gal}(\widetilde{K}/\widetilde{K}_1)$ and $G_2 = \mathrm{Gal}(\widetilde{K}/\widetilde{K}_2)$. Each $\mathcal{D}_i$ is a subgroup of $G_i < G$. Moreover recall that $G_1 \cong \langle \sigma_{r+1} \rangle$, $G_2 \cong \langle \sigma_1 \rangle \times \cdots \times \langle \sigma_r \rangle$ and $G \cong G_1 \times G_2$. Remark also that $|\mathcal{D}_1| = |\mathcal{D}_2|$. Since $|G_1| = p$ then one has $\mathcal{D}_1 = \langle 1 \rangle$ or $\mathcal{D}_1 = G_1$. Let us show that $\mathcal{D}_1 = \langle 1 \rangle$. Suppose that we have $\mathcal{D}_1 = \langle \sigma_{r+1} \rangle$. Then $|\mathcal{D}_2| = p$ so there is $\sigma \in G_2$ such that $o(\sigma) = p$ and $\mathcal{D}_2 = \langle \sigma \rangle$. Now, since for $i \in \{1,2\}$ we have $\mathcal{D}_i = \mathcal{D}(\tilde{\mathfrak{P}} \mid \mathfrak{a}) \cap G$, we obtain $\langle \sigma_{r+1} \rangle < \mathcal{D}(\tilde{\mathfrak{P}} \mid \mathfrak{a})$ and $\langle \sigma \rangle < \mathcal{D}(\tilde{\mathfrak{P}} \mid \mathfrak{a})$. Therefore, $\langle \sigma_{r+1} \rangle \times \langle \sigma \rangle < \mathcal{D}(\tilde{\mathfrak{P}} \mid \mathfrak{a})$ which implies that $ef = |\mathcal{D}(\tilde{\mathfrak{P}} \mid \mathfrak{a})| \geqslant p^2$. However if we consider the splitting of $\mathfrak{a}$ in $\widetilde{K}_1$ and $\widetilde{K}$, we have $e_1 = f_1 = 1$ in $\widetilde{K}_1/k$ and $[\widetilde{K} : \widetilde{K}_1] = p$, so $ef \leqslant p$ in $\widetilde{K}/k$. Thus we have an absurdity so $\mathcal{D}_1$ is trivial as announced, $\mathcal{D}_1 = \mathcal{D}_2 = \langle 1 \rangle$ and $\mathfrak{a}$ splits completely in $\widetilde{K}/k$. Finally $\mathfrak{p}$ splits in $\widetilde{K}/K_1$ as

$$(\widetilde{\mathfrak{P}}\widetilde{\mathfrak{P}} \dots \widetilde{\mathfrak{P}_p})^{p-1},$$

and

$$\mathrm{Gal}(\widetilde{K}/K_1) \cong \langle \tau_p \rangle \ltimes \langle \sigma_{r+1} \rangle \cong \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \ltimes \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

We see that $\mathfrak{p}$ and $\tilde{K}/K_1$ satisfy the hypothesis of Lemma 6, so $\mathfrak{p}$ splits in K/K_1 as

$$\widetilde{\mathfrak{P}}\widetilde{\mathfrak{P}}_1^{p-1}.$$

Moreover, for each $i \in [\![1, s]\!]$, the ideal $\mathfrak{p}_i$ splits completely in $\widetilde{K}$ so it splits completely in K. We obtain the final decomposition for p in $K/\mathbb{Q}$ as

$$(p) = \mathfrak{P}(\mathfrak{P}_1 \dots \mathfrak{P}_t)^{p-1}$$

with $t = 1 + sp = 1 + \frac{p^r-1}{p-1}p = \frac{p^{r+1}-1}{p-1}$. Thus the decomposition is correct for $r+1$, which ends the proof by induction. Let us now fix $K = \mathbb{Q}(\sqrt[p]{m_1}, \dots, \sqrt[p]{m_r})$ and look at the p-valuation of D_K. Remark that $\gcd(1,p) = \gcd(p-1,p) = 1$, and that for any prime ideal $\mathfrak{Q}$ of K above p we have $e(\mathfrak{Q} \mid p) = 1$ or $e(\mathfrak{Q} \mid p) = p-1$. Therefore the part of $\mathfrak{D}(K/\mathbb{Q})$ above p is

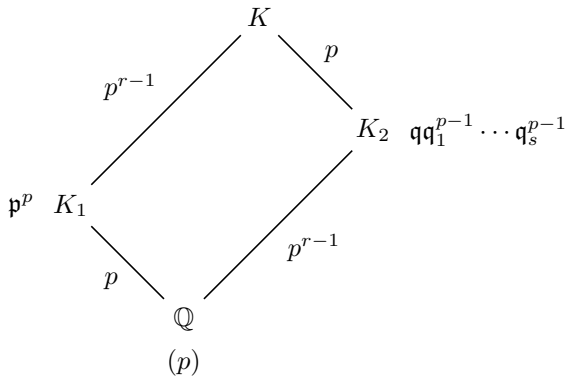
$$\prod_{i=1}^{s} \mathfrak{P}_i^{p-2}$$

where $s = \frac{p^r-1}{p-1}$. Since the inertial degree $f(\mathfrak{P}_i \mid p) = 1$, we have $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{P}_i) = p$ for all $i \in [\![1, s]\!]$. Thus we obtain

$$v_p(D_K) = v_p\left(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{D}(K/\mathbb{Q}))\right) = v_p\left(\prod_{i=1}^{s} \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{P}_i)^{p-2}\right) = (p-2)s,$$

which is the required value.

Fields of the second type: Let us now consider a field $K = \mathbb{Q}(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_r})$ such that $p \notin \mathcal{P}(m)$, $m_1^{p-1} \not\equiv 1 \bmod p^2$ and $\forall i \in [\![2, r]\!], m_i^{p-1} \equiv 1 \bmod p^2$. The proof is simpler in this case. Fix $K_1 = \mathbb{Q}(\sqrt[p]{m_1})$ and $K_2 = \mathbb{Q}(\sqrt[p]{m_2}, \ldots, \sqrt[p]{m_r})$. Remark that K_2 is a real Kummer field of the first type. Therefore, following Westlund [10] and the previous result, for $s = \frac{p^{r-1}-1}{p-1}$ we obtain the following situation.



By multiplicativity of the ramification index, for any $\mathfrak{P}$ above p in K, one has $p \mid e(\mathfrak{P} \mid p)$. Thus the splitting of p in K is as follows:

$$(p) = \mathfrak{P}^p(\mathfrak{P}_1 \ldots \mathfrak{P}_s)^{p(p-1)}.$$

Now let us find $v_p(D_K)$. We have

$$D_K = D_{K_1}^{[K:K_1]} \mathrm{N}_{K_1/\mathbb{Q}}(\mathfrak{d}(K/K_1)) = D_{K_1}^{[K:K_1]} \mathrm{N}_{K_1/\mathbb{Q}}(\mathrm{N}_{K/K_1}(\mathfrak{D}(K/K_1)))$$

and the part of $\mathfrak{D}(K/K_1)$ over $\mathfrak{p}$ is $(\mathfrak{P}_1 \cdots \mathfrak{P}_s)^{p-2}$. Indeed p is coprime to 1 and $p-1$. We know by [10] that $v_p(D_{K_1}) = p$ so

$$v_p(D_K) = [K : K_1]p + v_p\left(\mathrm{N}_{K/\mathbb{Q}}((\mathfrak{P}_1 \cdots \mathfrak{P}_s))^{p-2}\right).$$

Since the inertial degree is trivial everywhere, $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{P}_i) = p$ for all $i \in [\![1, s]\!]$. Finally we obtain

$$v_p(D_K) = p^r + v_p(p^{s(p-2)}) = p^r + s(p-2).$$

Fields of the third type: Let us now consider a field $K = \mathbb{Q}(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_r})$ such that $p \in \mathcal{P}$, and $\forall i \in [\![2, r]\!], m_i^{p-1} \equiv 1 \bmod p^2$. Again fix $K_1 = \mathbb{Q}(\sqrt[p]{m_1})$ and $K_2 = \mathbb{Q}(\sqrt[p]{m_2}, \ldots, \sqrt[p]{m_r})$. Remark that K_2 is a real Kummer field of the first type. Therefore, following Westlund [10] and the previous result, for $s = \frac{p^{r-1}-1}{p-1}$ we obtain the decomposition as the previous case. Therefore the proof is identical. The only thing which changes is $v_p(D_{K_1})$. It is equal to $2p-1$ in this case [10]. □

4. Extensions with two exponents

We were not able to prove similar results for general Kummer extensions with two exponents, but only on a restricted family of them.

Definition 14. Let L/K be a real Kummer extension with two exponents p, q. We will call a *power-free basis of* L/K and denote by $\mathfrak{IB}(L/K)$ the basis $\mathfrak{IB}(M) \otimes \mathfrak{IB}(K)$.

Proposition 18. *Let $L = K(\sqrt[p]{m_1}, \dots, \sqrt[p]{m_r})$ with $K = \mathbb{Q}(\sqrt[q]{n_1}, \dots, \sqrt[q]{n_s})$ be a real Kummer extension with two exponents. Let $a \in \mathcal{P}(m) \cup \mathcal{P}(n)$. Write $\delta_m = \delta_{(a \in \mathcal{P}(m))}$ and $\delta_n = \delta_{(a \in \mathcal{P}(n))}$. If $a \notin \{p, q\}$, then one has*

$$v_a(D_L(\mathfrak{IB}(L/K))) = [L : \mathbb{Q}] \left(\frac{p-1}{p} \delta_m + \frac{q-1}{q} \delta_n \right).$$

If $a \in \{p, q\}$ then one has

$$v_a(D_L(\mathfrak{IB}(L/K))) = \begin{cases} [L : \mathbb{Q}] \left(r + \dfrac{p-1}{p} \delta_m + \dfrac{q-1}{q} \delta_n \right) & \text{if } a = p, \\ [L : \mathbb{Q}] \left(s + \dfrac{p-1}{p} \delta_m + \dfrac{q-1}{q} \delta_n \right) & \text{if } a = q. \end{cases}$$

Proof. With the notations used during the proof of Theorem 3, remark that $M_{\mathfrak{IB}(L/K)} = M_{\mathfrak{IB}(L')} \otimes M_{\mathfrak{IB}(K)}$ where $L' = \mathbb{Q}(\sqrt[p]{m_1}, \dots, \sqrt[p]{m_r})$. Then apply v_a to $\det M^2_{\mathfrak{IB}(L/K)}$ in the different cases. □

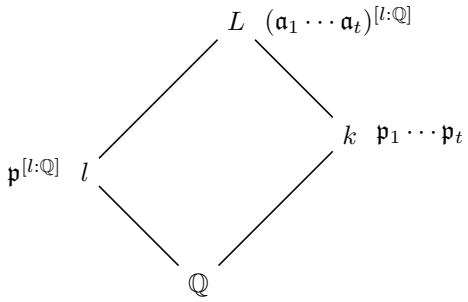
Remember that to prove Theorem 4, one only has to study the splitting of primes different from the exponent p, as the p-valuation of the discriminant of the order generated by $\mathfrak{IB}(K)$ is automatically smaller than the one of the discriminant of $[K : \mathbb{Q}]\mathcal{O}_K$. We will see that it is not as simple over extensions with two exponents.

Proposition 19. *Let $L = K(\sqrt[p]{m_1}, \dots, \sqrt[p]{m_r})$ with $K = \mathbb{Q}(\sqrt[q]{n_1}, \dots, \sqrt[q]{n_s})$ be a real Kummer extension with two exponents. Let $a \in \mathcal{P}(m) \cup \mathcal{P}(n) \setminus \{p, q\}$. Then the splitting of a in $L/\mathbb{Q}$ and $v_a(D_L)$ satisfy the following:*

(1) $a \in \mathcal{P}(m) \setminus \mathcal{P}(n) \implies \exists t \geqslant 1, (a) = (\mathfrak{a}_1 \dots \mathfrak{a}_t)^p$ *and* $v_a(D_L) = [L : \mathbb{Q}]\frac{p-1}{p}$;
(2) $a \in \mathcal{P}(n) \setminus \mathcal{P}(m) \implies \exists t \geqslant 1, (a) = (\mathfrak{a}_1 \dots \mathfrak{a}_t)^p$ *and* $v_a(D_L) = [L : \mathbb{Q}]\frac{q-1}{q}$;
(3) $a \in \mathcal{P}(m) \cap \mathcal{P}(n) \implies \exists t \geqslant 1, (a) = (\mathfrak{a}_1 \dots \mathfrak{a}_t)^{pq}$ *and* $v_a(D_L) = [L : \mathbb{Q}]\frac{pq-1}{pq}$.

Proof. The proof is quite similar to the one of Proposition 17. Using Lemma 3, one can assume that there is at most one $i_0 \in [\![1, r]\!]$ such that $a \mid m_{i_0}$ and at most one $j_0 \in [\![1, s]\!]$ such that $a \mid n_{j_0}$. Assume also that i_0 and j_0 are equal to 1 when they exist. Fix l the field equal to the compositum of the simple subfields of L' and K generated by m_{i_0} and n_{i_0}. Depending on the cases, l is equal to $\mathbb{Q}(\sqrt[p]{m_1})$, $\mathbb{Q}(\sqrt[q]{n_1})$ or $\mathbb{Q}(\sqrt[p]{m_1})\mathbb{Q}(\sqrt[q]{n_1})$. Now let k be the field such that $lk = L$. Now it is easy

to see that a completely ramifies in l and does not ramify in k. Thus there is $t \geqslant 1$ such that the splitting of a is as follows.



(a)

Since $a \notin \{p, q\}$, $\gcd(a, [l : \mathbb{Q}]) = 1$, therefore the part of the different $\mathfrak{D}(L/\mathbb{Q})$ above a is equal to

$$\prod_{i=1}^{t} \mathfrak{a}^{[l:\mathbb{Q}]-1}.$$

One can conclude by using the same arguments than in the proof of Proposition 17. □

Remark 4. One can remark from Proposition 18 and Proposition 19 that if $a \in \mathcal{P}(m) \cap \mathcal{P}(n) \setminus \{p, q\}$ then $v_a(D_K) \geqslant v_a(\mathbb{Z}[\mathfrak{IB}(L)])$. Therefore if $\mathcal{P}(m) \cap \mathcal{P}(n) \setminus \{p, q\} \neq \emptyset$ then the counterpart of Theorem 4 for Kummer extension with two exponents does not hold.

Theorem 6. *Let $L = K(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_r})$ with $K = \mathbb{Q}(\sqrt[q]{n_1}, \ldots, \sqrt[q]{n_s})$ be a real Kummer extension with two exponents. Denote by $\mathcal{O}$ the order $\mathbb{Z}[\mathfrak{IB}(L)]$, and $A = (\mathcal{P}(m) \cap \mathcal{P}(n)) \setminus \{p, q\}$ and $P_A = \prod_{a \in A} a$. Then the following properties are true.*

- $\forall a \in \mathcal{P}(m) \cup \mathcal{P}(n) \setminus (A \cup \{p, q\})$, $\mathcal{O}$ *is $a-$maximal.*
- $P_A[L : \mathbb{Q}]\mathcal{O}_L < \mathcal{O}$.

Proof. Let $a \in \mathcal{P}(m) \cup \mathcal{P}(n) \setminus (A \cup \{p, q\})$. From Proposition 18 and Proposition 19, $v_a(D_L(\mathcal{O})) = v_a(D_L(\mathcal{O}_L))$ so $\mathcal{O}$ is indeed $a-$maximal. Consider $a \in A$. Then we have $v_a(D_L(\mathcal{O})) = [L : \mathbb{Q}] \left(\frac{p-1}{p} + \frac{q-1}{q}\right)$, and

$$v_a\left(D_L(P_A[L : \mathbb{Q}]\mathcal{O}_L)\right) = v_a(P_A^{2[L:\mathbb{Q}]} D_L) = 2[L : \mathbb{Q}] + v_a(D_L).$$

Since $v_a(D_L) = [L : \mathbb{Q}]\frac{pq-1}{pq}$, we obtain

$$v_a\left(D_L(P_A[L : \mathbb{Q}]\mathcal{O}_L)\right) = [L : \mathbb{Q}](\frac{2pq + pq - 1}{pq}) \geqslant v_a(D_L(\mathcal{O})).$$

Now consider $a \in \{p, q\}$. Since the situation is the same for p or q, we can choose $a = p$ for example. First assume that $p \notin \mathcal{P}(m) \cup \mathcal{P}(n)$. Then again from Proposition 18 we have $v_p(D_L(\mathcal{O})) \leqslant r[L : \mathbb{Q}]$. Moreover since $v_p([L : \mathbb{Q}]) = r$ we get

$$v_p\left(D_L(P_A[L : \mathbb{Q}]\mathcal{O}_L)\right) \geqslant 2r[L : Q] \geqslant r[L : \mathbb{Q}].$$

Now let us assume that $p \in \mathcal{P}(m) \cup \mathcal{P}(n)$. Then we have

$$v_p(D_L(\mathcal{O})) = [L : \mathbb{Q}] \left(r + \frac{p-1}{p} + \frac{q-1}{q} \right) \leqslant [L : \mathbb{Q}](r + 2).$$

Since $p \in \mathcal{P}(m) \cup \mathcal{P}(n)$, there is a subfield l of L of the form $\mathbb{Q}(\sqrt[p]{\prod_i m_i})$ (resp. $\mathbb{Q}(\sqrt[q]{\prod_i n_i})$), such that $p \mid m$ (resp. $p \mid n$). Consequently, p ramifies completely in l and we know that $v_p(D_l) = 2p - 1$ (resp. $v_p(D_l) = p$). Recall that $D_L = D_l^{[L:l]} \mathrm{N}_{l/\mathbb{Q}}(\mathfrak{d}(L/l)) \geqslant D_l^{[L:l]}$. Thus we obtain

$$v_p\left(D_L(P_A[L : \mathbb{Q}]\mathcal{O}_L)\right) \geqslant 2r[L : Q] + [L : \mathbb{Q}] \geqslant [L : \mathbb{Q}](r + 2).$$

□

Acknowledgments. Andrea Lesavourey is funded by the Direction Générale de l'Armement (Pôle de Recherche CYBER), with the support of Région Bretagne.

References

[1] Jean-François Biasse and Christine Vredendaal. Fast multiquadratic s-unit computation and application to the calculation of class groups. *The Open Book Series*, 2:103–118, 01 2019.

[2] A. P. Chalmeta. *On the Units and the Structure of the 3-Sylow Subgroups of the Ideal Class Groups of Pure Bicubic Fields and their Normal Closures*. PhD thesis, 2006.

[3] H. Cohen. *Advanced Topics in Computational Number Theory*. Graduate Texts in Mathematics. Springer New York, 2012.

[4] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, Berlin, Heidelberg, 1993.

[5] Andrea Lesavourey, Thomas Plantard, and Willy Susilo. Short principal ideal problem in multicubic fields. *Journal of Mathematical Cryptology*, 14(1):359 – 392, 01 Jan. 2020.

[6] J. Neukirch. Algebraic number theory. 1999.

[7] Paulo Ribenboim. *Classical theory of algebraic numbers*. Springer Science & Business Media, 2013.

[8] P. Samuel. *Algebraic theory of numbers*. Hermann, 1970.

[9] Bernhard Schmal. Diskriminanten,$\mathbb{Z}$-ganzheitsbasen und relative ganzheitsbasen bei multiquadratischen zahlkörpern. *Archiv der Mathematik*, 52:245–257, 1989.

[10] Jacob Westlund. On the fundamental number of the algebraic number-field $k(\sqrt[p]{m})$. *Transactions of the American Mathematical Society*, 11(4):388–392, 1910.

Appendix A: Proofs of some result on dihedral groups

Here we consider a prime p, t a generator of the multiplicative group $\mathbb{F}_p^*$ and the semi-direct product $G \cong \langle \tau, \sigma \mid \tau^{p-1} = \sigma^p = 1, \tau\sigma\tau^{-1} = \sigma^t \rangle$. Recall that for any $u \in \langle \sigma \rangle$ and any $a \in [\![0, p-1]\!]$ one has $\tau^a u \tau^{-a} = u^{t^a}$ so any element of G can be written in the form $\tau^a\sigma^b$ or $\sigma^c\tau^d$ for some a, b, c, d. Remark further that if $g = \prod_i \tau^{a_i}\sigma^{b_i} \in G$ then the corresponding a and d are equal to $\sum_i a_i$.

Lemma 7. *The subgroups of G are of the form $\langle \tau^a, \sigma \rangle$ with $a \in [\![0, p-2]\!]$ or of the form $\langle \tau^a\sigma^b \rangle$ with $a \in [\![1, p-2]\!]$ and $b \in [\![0, p-1]\!]$*

Proof. Consider a subgroup $H = \langle g_1, \dots, g_r \rangle = \langle \tau^{a_1}\sigma^{b_1}, \dots, \tau^{a_r}\sigma^{b_r} \rangle$ with $(a_i, b_i) \in [\![0, p-2]\!] \times [\![0, p-1]\!]$. First assume $\tau \in H$. Then one can write $H = \langle \tau, \sigma^{b_1}, \dots, \sigma^{b_r} \rangle$ i.e. H is either $\langle \tau \rangle$ or $\langle \tau, \sigma \rangle$. Now assume $\sigma \in H$ instead. Then $H = \langle \sigma, \tau^{a_1}, \dots, \sigma^{a_r} \rangle$ and there is $d \in [\![0, p-2]\!]$ such that H is $\langle \tau^d, \sigma \rangle$. Finally assume that neither τ nor σ belongs to H. One can see that for $i \neq j$ two integers in $[\![1, r]\!]$

$$(a_i = a_j) \wedge (b_i \neq b_j) \implies \exists b \neq 0 \mid \sigma^b \in H \implies \sigma \in H$$

from which we deduce

$$\forall (i, j) \in [\![1, r]\!], i \neq j \implies a_i \neq a_j.$$

Let $d = \gcd(a_1, \dots, a_r)$. Using Bézout's identity one can see that there is $b \in [\![0, p-1]\!]$ such that $\tau^d\sigma^b$ is an element of H. Let us show that H is in fact equal to $\langle \tau^d\sigma^b \rangle$. Consider $i \in [\![1, r]\!]$ and write $h_i = (\tau^d\sigma^b)^{\frac{a_i}{d}}$. There is $c_i \in [\![0, p-1]\!]$ such that $h_i = \tau^{a_i}\sigma^{c_i}$. Following a previous reasoning we conclude that $h_i = g_i$. This is true for all $i \in [\![1, r]\!]$ so $H = \langle \tau^d\sigma^b \rangle$. □

Lemma 8. *The subgroups of G of the form $\langle \tau^a\sigma^b \rangle$ with $(a, b) \in [\![1, p-2]\!] \times \{0, 1\}$ have order $o(\tau^a) = o(t^a)$.*

Proof. Given an integer k one has $(\tau^a\sigma^b)^k = \sigma^e\tau^{ak}$ with

$$e = bt^a + bt^{2a} + \cdots + bt^{ka} = bt^a \frac{1 - t^{ka}}{1 - t^a}.$$

thus

$$\sigma^e\tau^a = 1 \iff (ak \equiv 0 \bmod (p-1)) \wedge (e = bt^a \frac{1 - t^{ka}}{1 - t^a} \equiv 0 \bmod p).$$

Then remark that one has also

$$ak \equiv 0 \bmod (p-1) \implies t^{ak} = 1 \bmod p \implies e \equiv 0 \bmod p.$$

□

Lemma 9. *The subgroups of G with order $p-1$ are the p groups of the form $\langle \tau\sigma^b \rangle$ with $b \in [\![0, p-1]\!]$.*

Proof. A subgroup of G of order $p-1$ does not contain σ so it is necessarily of the form $\langle \tau^a \sigma^b \rangle$. Since $o(\tau^a \sigma^b) = o(\tau^a)$ one has

$$o(\tau^a \sigma^b) = p-1 \implies \langle \tau^a \rangle = \langle \tau \rangle$$

therefore there is $c \in [\![0, p-1]\!]$ such that $\tau\sigma^c \in \langle \tau^a \sigma^b \rangle$. □

*Univ Rennes, CNRS, IRISA

Email address: andrea.lesavourey@irisa.fr