KUMMER THEORY FOR FUNCTION FIELDS

FÉLIX BARIL BOUDREAU AND ANTONELLA PERUCCA

ABSTRACT. We develop Kummer theory for algebraic function fields in finitely many transcendental variables. We consider any finitely generated Kummer extension (possibly, over a cyclotomic extension) of an algebraic function field, and describe the structure of its Galois group. Our results show in a precise sense how the questions of computing the degrees of these extensions and of computing the group structures of their Galois groups reduce to the corresponding questions for the Kummer extensions of their constant fields.

1. INTRODUCTION

Let $M \geqslant 1$ be an integer and let K be a field containing a primitive M-th root of unity. A Kummer extension of K of exponent dividing M is an Abelian field extension of K obtained by adjoining M-th roots of elements of $K^\times$, the multiplicative subgroup of K. Kummer theory says that any Abelian extension of K of exponent dividing M is of this form and, in fact, Abelian extensions of K of exponent dividing M correspond bijectively with subgroups of the quotient group $K^\times/K^{\times M}$. In this work, we develop Kummer theory for arbitrary algebraic function fields and go beyond the classical theory: Using parameters that measure the divisibility of elements up to constants, we completely solve the problem of understanding the nature of Kummer theory over algebraic function fields by showing in a precise way that this theory reduces to the Kummer theory over the corresponding constant fields.

1.1. **Overview of the main results.** We consider a function field K/k, work within a fixed algebraic closure $\overline{K}$ of K, and suppose without loss of generality that k is algebraically closed in K. For any element $\alpha \in K^\times \backslash k^\times$, and any prime number $\ell \neq \operatorname{char}(k)$, we can speak of its *$\ell$-divisibility parameter modulo constants over K*. This is the largest non-negative integer D such that $\alpha \in kK^{\times \ell^D}$.

For an integer $M \geqslant 1$ not divisible by $\operatorname{char}(k)$, and a choice ζ_M of primitive M-th root of unity in $\overline{K}$, the field $K(\zeta_M)$ is a cyclotomic extension of K. Given a finitely generated subgroup G of $K^\times$, we consider the Kummer extensions

$$K(\zeta_M, \sqrt[N]{G})/K(\zeta_M) \qquad \text{where } N \mid M \,. \tag{1}$$

In this article we show that, to compute the degree and the structure of the Galois group of the above Kummer extensions, we may reduce to computations involving only the constant field k.

By Kummer theory, we may suppose that $N = \ell^n$ for some prime number ℓ and some integer $n \geqslant 1$. We can write $G = G_0 G'$ where $G_0 := G \cap k^\times$ and where G' is a subgroup of G such that $G' \cap k^\times = \{1\}$. We denote by r the rank of G' and we suppose that r is strictly positive (for $r = 0$, see Remark 37). A careful choice of basis for G', which we call *ℓ-good basis modulo constants* (see Definition 28), allows us to conduct a finer analysis of Galois group structures of Kummer extensions. The following result, which combines Corollary 27 and Theorem 31, considers the so-called *geometric Kummer extension* $K\bar{k}(\sqrt[\ell^n]{G})/K\bar{k}$:

Theorem 1. *There is a basis $\{\alpha_1, \ldots, \alpha_r\}$ of G' such that, calling D_i the ℓ-divisibility parameter modulo constants of α_i over $K(\zeta_\ell)$, the integer $\sum_{i=1}^n D_i$ is maximal (by varying the basis of G'). The multiset of the D_i's is uniquely determined (it only depends on K/k and G), and for every $n \geqslant 1$ we have*

$$\operatorname{Gal}(K\bar{k}(\sqrt[\ell^n]{G})/K\bar{k}) \simeq \prod_{i=1}^r \mathbb{Z}/\ell^{\max(n-D_i, 0)}\mathbb{Z} \,.$$

To simplify the notation, suppose that $\zeta_M \in k$. We deduce the following result on the cardinality of the Kummer extensions (see Theorem 33):

Theorem 2. *With the above notation, let $c_i \in k^\times$ be such that α_i/c_i is in $K^{\times \ell^{D_i}}$. Then we have*

$$[K(\sqrt[\ell^n]{G}) : K] = [k, \sqrt[\ell^n]{G_0}, \sqrt[\ell^{\min(n,D_1)}]{c_1}, \ldots, \sqrt[\ell^{\min(n,D_r)}]{c_r}) : k] \cdot \prod_{i=1}^{r} \ell^{\max(n-D_i,0)}.$$

Up to relabelling, we suppose without loss of generality that $D_1 \leqslant D_2 \leqslant \cdots \leqslant D_r$. Our main result gives the precise Galois group structure of the Kummer extension $K(\sqrt[\ell^n]{G})/K$ (see Theorem 36):

Theorem 3. *With the above notation, let $d_i \in \mathbb{Z}_{\geqslant 0} \cup \{\infty\}$ be maximal such that the class of c_i is an ℓ^{d_i}-th power in $k^\times/\langle G_0, c_j : j > i\rangle$. Then there is a group isomorphism*

$$\mathrm{Gal}\left(K\left(\sqrt[\ell^n]{G}\right)/K\right) \simeq \mathrm{Gal}\left(k\left(\sqrt[\ell^n]{G_0}\right)/k\right) \times \prod_{i=1}^{r} \mathbb{Z}/\ell^{\max(n-\min(D_i,d_i),0)}\mathbb{Z}.$$

Thanks to the above results, to determine the cardinality and the structure of the Galois group of the Kummer extensions in (1), as described in the last section, it suffices to compute the parameters D_i's and the constant elements c_i's, and this then reduces to computations involving only the constant field k. Such computations can be done (in principle) for all finite fields, but there is also an explicit finite procedure to perform them for number fields and p-adic fields (see [1, 6]).

The structure of the paper is as follows: Section 2 contains background theory on algebraic function fields and a lemma about rank 1 discrete valuations and ℓ-divisibility modulo constants of elements. Sections 3 and 4 are devoted to studying extensions of function fields (with some general results that can be of independent interest). The theory of divisibility modulo constants is developed in Section 5, and our main results for Kummer theory are proven in Section 6.

The idea of using parameters to consider the divisibility of elements in a given field comes from past works of the second-named author on Kummer theory for number fields. Nevertheless, we consider a completely new setting and we provide several auxiliary results to develop Kummer theory for function fields in full generality.

1.2. **Related Literature.** Our paper addresses a natural question of Kummer theory for function fields. The closest reference we have found is a paper from 1942 in Duke Math. J. by MacLane and Schilling [4]. The authors consider algebraic function fields K/k with k algebraically closed in K and study algebraic extensions L/k_L of them, generated by radicals. A radical is an element of $\alpha \in L$ that has a positive integral power α^n in K up to an element that is algebraic over k, that is $\alpha^n\gamma \in K^\times$ for some $\gamma \in k_L^\times$. Extensions generated by radicals include, in particular, cyclotomic-Kummer extensions. The motivation of [4] came from class field theory considerations and focus on the theory of divisors and the willingness to generalize the main correspondence of Kummer theory. Their work differs from our explicit study of field extensions with divisibility parameters, and the results are very different. However, one may notice the same (natural) principle of setting constant elements aside. Indeed, they also decompose a radical extension with the intermediate extension that is the largest constant extension, which they call *coefficient extension* (see [4, §9 and §10 and in particular p.153, Corollary 1].

Although a classical subject, Kummer theory continues to be an active topic of research. On the side of algebraic function fields, most of the literature seems to concentrate on the global function fields. For example, the notion of genus field, analogous to the one for number fields, was introduced in [7] for an algebraic function field K of a rational function field $\mathbb{F}_q(t)$, in analogy with the number field side. There, the author computed the genus field for Kummer extensions of the form $K = \mathbb{F}_q(t)(\sqrt[\ell]{D})$ for a prime number ℓ different from $\mathrm{char}(\mathbb{F}_q)$ and a polynomial in $\mathbb{F}_q[t]$ that is ℓ-th power free. The results were then generalized to the compositum of linearly disjoint such extensions in [8], using Carlitz modules.

The reader should also be aware of the following work. In [5, Theorems 1 and 4], the author studies, for a given rational global function field $\mathbb{F}_q(t)$ of some characteristic $p > 0$, the "cyclotomic

extension" $\mathbb{F}_q(t)(\Lambda_P)$ of $\mathbb{F}_q(t)$ generated by the P-torsion points Λ_P, of a Drinfeld $\mathbb{F}_q[t]$-module, for any monic irreducible polynomial in $\mathbb{F}_q[t]$ of degree d_P. This is a Galois extension of groups isomorphic to $(\mathbb{F}_q[t]/\langle P \rangle)^\times$. The let h_P^+ be the class number of the subextension of $\mathbb{F}_q(t)(\Lambda_P)$ corresponding to the subgroup $\mathbb{F}_q^\times$ of $(\mathbb{F}_q[t]/\langle P \rangle)^\times$. The author shows that if p divides h_P^+, then there is an integer $0 < m < q^{d_P} - 1$, multiple of $q - 1$, such that the m-th Bernoulli-Carlitz number's minimal numerator is divisible by P. This result is analogous to a result by Kummer over $\mathbb{Q}$. Hence, despite similar names, when restricted to the "ground" algebraic function field $\mathbb{F}_q(t)$, where *loc. cit* and our manuscript have a common intersection, the questions studied in these two manuscripts are of different nature.

2. PREREQUISITES ON FUNCTION FIELDS AND NOTATION

An *algebraic function field (or function field, for short)* is a triple (K, k, n), comprised of a field K containing a field k such that K is finitely generated over k of transcendence degree $\mathrm{trdeg}(K/k)$ equal to some positive integer n. In this case, we write K/k (and can refer to it as a *function field in n variables*). Let $\{t_1, t_2, \cdots, t_n\}$ be a transcendence basis for K over k. The function field K/k is a *rational function field* if $K = k(t_1, t_2, \cdots, t_n)$ and it is a *global function field* if $n = 1$ and k is a finite field.

In this manuscript, a *valuation on K/k* is a surjective map v from K to $\mathbb{Z} \cup \{\infty\}$, with $\mathbb{Z}$ the additive group of integers and ∞ a symbol subject to the rules $n + \infty = \infty + n = \infty + \infty = \infty$ for all $n \in \mathbb{Z}$. The map v is satisfying for all $f_1, f_2 \in K^\times$ the properties $v(f_1 f_2) = v(f_1) + v(f_2)$ and $v(f_1 + f_2) \geq \min\{v(f_1), v(f_2)\}$, is such that if $f \in k^\times$, then $v(f) = 0$ and $v(0) = \infty$. In particular, our valuations are *discrete* in the usual terminology.

The ring $\mathcal{O}_v$ of all $f \in K^\times$ satisfying $v(f) \geq 0$, is called the *valuation ring* of v. It is a local ring whose maximal ideal $\mathfrak{m}_v$ is the set of $f \in \mathcal{O}_v$ satisfying $v(f) > 0$. The field $k_v := \mathcal{O}_v/\mathfrak{m}_v$ is called the *residue field* of v. It can be seen as a field extension of k and the transcendence degree $\mathrm{trdeg}(k_v/k)$ of k_v over k will be the *dimension of v over k*. A *prime divisor* of K/k is a valuation of K/k of dimension $n-1$ over k. Each prime divisor is a discrete valuation of *rank* 1 (that is, $\mathcal{O}_v$ has Krull dimension 1) and k_v is a function field of transcendence degree $n-1$ over k. We denote by $\mathrm{Prime}(K/k)$ the set of prime divisors of K/k.

The *constant field* of K/k is the algebraic closure $\widetilde{k}$ of k inside K. The extension $\widetilde{k}/k$ is finite as
$$[\widetilde{k} : k] = [\widetilde{k}(t_1, \cdots, t_n) : k(t_1, \cdots, t_n)] \leq [K : k(t_1, \cdots, t_n)]$$
is finite. Therefore, $K/\widetilde{k}$ is an algebraic function field of n variables over $\widetilde{k}$.

Fixing an algebraic closure $\overline{K}$ of K, if M is a positive integer not divisible by $\mathrm{char}(k)$, we denote by ζ_M a primitive root of unity in $\overline{K}$ (or inside the algebraic closure $\overline{k}$ of k in $\overline{K}$) of order M and we obtain a cyclotomic extension $k(\zeta_M)/k$.

Throughout the text, ℓ is a prime number different from $\mathrm{char}(k)$. We define $k(\zeta_{\ell^\infty})/k$ inside $\overline{K}$ as the union, over the integers $n \geq 1$, of the cyclotomic extensions $k(\zeta_{\ell^n})/k$. We also write v_ℓ for the ℓ-adic valuation on $\mathbb{Q}^\times$. Also, if G is a group, then $G = \langle \alpha_1, \cdots, \alpha_r \rangle$ means that G is generated by a finite set of elements $\{\alpha_1, \cdots, \alpha_r\}$.

Lemma 4. *Let $f \in K^\times \backslash \widetilde{k}$ and $c \in \widetilde{k}^\times$.*

   (i) *For all $v \in \mathrm{Prime}(K/k)$ we have $v(c) = 0$ and $v(cf) = v(f)$.*
   (ii) *There is a finite non-empty set S of $\mathrm{Prime}(K/k)$ such that $v(f) \neq 0$ for all $v \in S$ and $v(f) = 0$ for all $v \notin S$. More precisely, S has at least two elements, v_1, v_2 respectively satisfying $\mathrm{ord}_{v_1}(f) > 0$ and $\mathrm{ord}_{v_2}(f) < 0$.*
   (iii) *There are only finitely many positive integers n such that $f \in \widetilde{k}K^{\times n}$. In particular, there is no prime number ℓ such that f is infinitely ℓ-divisible (not even up to constant elements).*

Proof.   (i) This follows immediately from the fact that v is also a valuation on $K/\widetilde{k}$.
   (ii) The finiteness of S is classical divisor theory and the rest is proven in [10, p.99, Ch VI, §14 and p.175, Ch VII, §4 bis].

(iii) This follows from (i) and (ii) since if $cf \in \widetilde{k}K^{\times n}$, then n divides $v(cf) = v(f)$ for all $v \in \mathrm{Prime}(K/k)$.

$\square$

3. Extensions of function fields

3.1. **General results.** The following results hold for fields that are not necessarily function fields.

Definition 5. Let K and L be two extensions of a field k that are contained in some algebraically closed field. The field K is said to be *linearly disjoint from L over k* if every finite set of elements of K that is linearly independent over k is linearly independent over L.

Remark that if K and L are linearly disjoint over k, then K and L' are linearly disjoint over k for any intermediate extension $k \subseteq L' \subseteq L$.

Lemma 6. *Let k be a field that is algebraically closed in some field K. Let α be an element of a fixed algebraic closure $\overline{k}$ over k. Then $k(\alpha)$ and K are linearly disjoint over k, or equivalently, $k(\alpha) \otimes_k K$ is a field, and we have $[k(\alpha) : k] = [K(\alpha) : K]$. In particular, the minimal polynomial of α over K and over k are the same.*

Proof. Let $m(x)$ be the minimal polynomial of α over k. Any constant factor of $m(x)$ over K has its coefficients algebraic over k, hence in k. Therefore, $m(x)$ is irreducible over K and the statement follows. $\square$

Lemma 7 ([9, p.253, Proposition 8.4.1])**.** *If a field k is algebraically closed in K and $\{T_i\}_{i \in I}$ is an algebraically independent set over K, then $k(\{T_i\}_{i \in I})$ is algebraically closed in $K(\{T_i\}_{i \in I})$.*

Lemma 8. *Let K/k be a field extension such that k is algebraically closed in K. Fix some algebraic closure $\overline{K}$ of K and fix an algebraic closure $\overline{k}$ of k contained in $\overline{K}$. Let F/K be a finite extension such that $F \subseteq KL$ for some field $L \subseteq \overline{k}$ that is separable over k. Then $(F \cap \overline{k})/k$ is finite and we have $F = K(F \cap \overline{k})$.*

Proof. Notice that, as F/K is finite we may suppose, up to replacing L by a subfield, that L/k is finite. Thus, L/k is primitive. Since we have $K \cap L = k$, then $K \otimes_k L$ is a field by Lemma 6.

We now prove the statement by induction on the degree of F/K. If $[F : K] = 1$, the statement is trivial because $F \cap \overline{k} = k$. Now suppose that $[F : K] > 1$ and that the statement holds for all field extensions of lesser degree.

Suppose that $F \otimes_k L$ is a field. Then the inclusion $K \to F$ yields an injective ring morphism $\phi_1 : K \otimes_k L \to F \otimes_k L$. We also have injective ring morphisms $\phi_2 : F \otimes_k L \to \overline{K}$ and $\phi : K \otimes_k L \to \overline{K}$, that are given on elementary tensors by $x \otimes y \mapsto xy$. One sees the three morphisms satisfy the compatibility $\phi = \phi_2 \circ \phi_1$. Since $F \subseteq KL$, then $\mathrm{im}(\phi) = KL = \mathrm{im}(\phi_2)$ and hence ϕ_1 is an isomorphism. Since L is a k-module, the functor $\bullet \otimes_k L$ is faithfully flat hence $F = K$, contradicting that $[F : K] > 1$.

If $F \otimes_k L$ is not a field, then, by Lemma 6 the field k is not algebraically closed in F and so there is a non-trivial extension $k_1 := F \cap \overline{k}$ of k. So we have $[F : Kk_1] < [F : K]$ and $F \subseteq (Kk_1)(Lk_1)$ and Lk_1/k_1 is separable. By induction hypothesis the field extension $(F \cap \overline{k})/k_1$ is finite and we have $F = (Kk_1)(F \cap \overline{k}) = K(F \cap \overline{k})$. $\square$

3.2. **Algebraic extensions of function fields.** Given two algebraic function fields L/k_L and K/k, we say that the former is an *extension* of the latter if L/K and k_L/k are extensions of fields. Moreover, if both L/K and k_L/k are algebraic, we say the extension of function fields is *algebraic*. From now on, an *extension of function fields* will mean an algebraic extension of algebraic function fields. With the above notation we say that $L'/k_{L'}$ is a *subextension* of L/k_L if $L'/k_{L'}$ is an extension of K/k and L/k_L is an extension of $L'/k_{L'}$. Suppose that L/k_L is an extension of K/k. Then the transcendence degree of L over k_L equals the one of K over k. The constant field of L is $\widetilde{k}_L = \overline{k} \cap L$ and it is algebraic over k (for convenience, the field k_L will not be specified if it equals k). In particular, $K \cap \widetilde{k}_L = \widetilde{k}$. We call the extension of function fields *finite* in case L/K and k_L/k are finite. We call the extension of function fields *Galois* if L/K is

Galois. In this case, $\widetilde{k}_L/\widetilde{k}$ is Galois (see Lemma 10) however k_L/k is not necessarily Galois. We call the extension of function fields *Abelian* (respectively, *of exponent N*) if it is Galois and the Galois group of L/K is Abelian (respectively, of exponent N). Note that for an Abelian extension we have that $\widetilde{k}_L/k$ is also Abelian while for an Abelian extension of exponent N, we have that $\widetilde{k}_L/k$ is Abelian with exponent dividing N.

Remark 9. If L/k_L is an extension of K/k, then L/K is finite if and only if $\widetilde{k}_L/\widetilde{k}$ is finite if and only if k_L/k is finite. The second implication holds because the extensions $\widetilde{k}_L/k_L$ and $\widetilde{k}/k$ are both finite. For the first implication choose transcendence variables $x_1, \ldots, x_n$ for K/k, recall that the two extensions $K/\widetilde{k}(x_1, \ldots, x_n)$ and $L/\widetilde{k}_L(x_1, \ldots, x_n)$ are finite and write

$$[L:K][K:\widetilde{k}(x_1,\ldots,x_n)] = [L:\widetilde{k}(x_1,\ldots,x_n)] = [L:\widetilde{k}_L(x_1,\ldots,x_n)][\widetilde{k}_L:\widetilde{k}].$$

Lemma 10. *Let L/k_L be an extension of K/k. If L/K is separable, then $\widetilde{k}_L/\widetilde{k}$ is separable. If L/K is normal, then $\widetilde{k}_L/k$ and $\widetilde{k}_L/\widetilde{k}$ are normal. Consequently,*

  (i) *if L/K is Galois, then $\widetilde{k}_L/\widetilde{k}$ is Galois;*
  (ii) *if L/K is Galois and $\widetilde{k}_L/k$ is separable, then $\widetilde{k}_L/k$ is Galois;*
  (iii) *if L/K is separable, then $\widetilde{k}_L^N/k$ is Galois, where $\widetilde{k}_L^N$ is the normal closure of $\widetilde{k}_L$ in $\overline{k}$.*

Proof. We first prove that $\widetilde{k}_L/\widetilde{k}$ is separable, assuming that L/K is separable. We may suppose that $\widetilde{k}_L/\widetilde{k}$ is finite because if this extension is not separable, then there is some element $\alpha \in \widetilde{k}_L$ such that $\widetilde{k}(\alpha)/\widetilde{k}$ is finite and not separable. We may also suppose that $\widetilde{k}_L/\widetilde{k}$ is normal, up to replacing $\widetilde{k}_L$ by its normal closure in $\overline{k}$. Now assume that $\widetilde{k}_L/\widetilde{k}$ is not separable. Up to replacing $\widetilde{k}$ by a separable extension, we may suppose that $\widetilde{k}_L/\widetilde{k}$ is purely inseparable. So let p be the finite characteristic of $\widetilde{k}$ and let $\alpha \in \widetilde{k}_L \setminus \widetilde{k}$ be such that $\alpha^{p^m} \in \widetilde{k}$ holds for some positive integer m. As $K \cap \widetilde{k}_L = \widetilde{k}$, we have $\alpha \in L \setminus K$ such that $\alpha^{p^m} \in K$, contradicting the separability of L/K.

We now assume that L/K is normal and prove that $\widetilde{k}_L/k$ is normal, which immediately implies that $\widetilde{k}_L/\widetilde{k}$ is normal. Consider an element of $\widetilde{k}_L$, namely some $\alpha \in L$ that is algebraic over k. The conjugates of α are in L because L/K is normal and they are all algebraic over k, so they are in $\widetilde{k}_L$. The last assertion is immediate. $\qquad\square$

3.3. **Constant and geometric extensions.** We say that an algebraic extension L/k_L of K/k is *constant* if $L = Kk'$ for some algebraic extension k' of k. Note that we may replace k' by $k'\widetilde{k}$ because $L = K(k'\widetilde{k})$ and $k'\widetilde{k}/k$ is algebraic. Hence, we may suppose without loss of generality that $\widetilde{k} \subseteq k'$.

Theorem 11. *Let K/k be a function field, and let k' be an algebraic extension of $\widetilde{k}$. If K or k' is separable over $\widetilde{k}$ (in particular, if $\widetilde{k}$ is perfect), then the constant field of Kk' is k'.*

Proof. Set $L := Kk'$ and denote by $\widetilde{k}_L$ its constant field. By Theorem 19 the extension $\widetilde{k}_L/k'$ is finite and purely inseparable. So it suffices to prove that $\widetilde{k}_L/k'$ is separable.

Suppose that $k'/\widetilde{k}$ is separable and fix $\alpha \in k'$ such that $k' = \widetilde{k}(\alpha)$. Since the minimal polynomial of α over K divides the one over $\widetilde{k}$, we deduce that $L = K(\alpha)$ is separable over K. To conclude remark that, for an element of $\widetilde{k}_L$, the minimal polynomial over $\widetilde{k}$ is the same as the one over K by Lemma 6.

Now suppose that $K/\widetilde{k}$ is separable and let $x_1, \cdots, x_n \in K$ be a transcendental basis over $\widetilde{k}$. Notice that $K/\widetilde{k}(x_1, \cdots, x_n)$ is a finite separable extension and hence L is a finite separable extension of $k'(x_1, \cdots, x_n)$. We deduce that $\widetilde{k}_L(x_1, \cdots, x_n)/k'(x_1, \cdots, x_n)$ is a finite separable extension. So $\widetilde{k}_L/\widetilde{k}$ and hence $\widetilde{k}_L/k'$ is separable by Lemma 10. $\qquad\square$

Lemma 12. *If C/K is a finite constant Galois extension and K'/K is a finite Galois extension whose maximal constant subextension is L/K, then CL/K is the maximal constant subextension of CK'/K.*

Proof. Write $C = k_C K$ and $L = k_L K$ for some fields k_C, k_L containing $\widetilde{k}$ and contained in $\overline{k}$. The extension CL/K is constant because we have $CL = k_C k_L K$. If it is not maximal, let M/K be the maximal constant subextension of CK'/K. By Galois theory, we have $M = CL'$ for some subextension L'/K of K'/K. Now, L' strictly contains L, and L'/K must be constant by Lemma 8, contradicting the maximality of L. □

If L/k_L is an extension of K/K, then $\widetilde{k} \subseteq L \cap \overline{k}$. This extension is said to be *geometric* if the converse inclusion holds. We call an extension *geometric* if $L \cap \overline{k} = \widetilde{k}$ (remark that the inclusion $\supseteq$ always holds). Notice that an algebraic extension is geometric if and only if $\widetilde{k}_L = \widetilde{k}$.

Remark 13. An algebraic extension $L/\widetilde{k}_L$ of $K/\widetilde{k}$ that is constant and geometric must be trivial. For a constant extension we have $L = Kk'$ for some $\widetilde{k} \subseteq k' \subseteq \overline{k}$ and $k' \subseteq (L \cap \overline{k}) \subseteq \widetilde{k}_L$ so, assuming $\widetilde{k}_L = \widetilde{k}$, we get $k' = \widetilde{k}$ and hence $L = K$.

Remark 14. An algebraic separable extension of function fields of prime degree is constant if and only if it is not geometric. The "only if" direction is a consequence of Remark 13. Conversely, suppose that the extension is not geometric. So there exists some $\gamma \in \widetilde{k}_L \backslash \widetilde{k}$. Since $\widetilde{k}_L \subseteq \overline{k}$ we deduce that $\gamma \notin K$ hence it is a primitive element for L/K, showing that $L = K\widetilde{k}(\gamma)$ is constant.

Recall that any group whose order is the power of a prime ℓ has a normal subgroup of index ℓ.

Lemma 15. *Let ℓ be a prime number different from* $\mathrm{char}(k)$. *Let L/k_L be a finite Galois extension of K/k such that the degree of L/K is a power of ℓ. In particular, there exists a Galois subextension of L/K of degree ℓ. Write L'/K for the largest subextension of exponent ℓ (namely, the compositum of all such extensions). Then L/k_L is geometric if and only if $L'/k_{L'}$ is geometric.*

Proof. If $\widetilde{k}_L = \widetilde{k}$, then $\widetilde{k}_{L'} = \widetilde{k}$. Conversely, suppose that $\widetilde{k}_L/\widetilde{k}$ is not trivial. This extension is finite (because L/K is finite) and Galois (by Lemma 10) and its degree is a power of ℓ (by Lemma 6). Then it has a Galois subextension of degree ℓ. This extension is of the form $\widetilde{k}(\alpha)/\widetilde{k}$ where $\alpha \in \overline{k}\backslash\widetilde{k}$. Since $\alpha \in L'$ we deduce that $\widetilde{k}_{L'} \neq \widetilde{k}$. □

3.4. **Cyclotomic extensions.** An extension L/k_L of K/k is called *cyclotomic* if $L \subseteq K(\zeta_m)$ holds for some integer $m \geqslant 1$. Since $K(\zeta_m)/K$ is finite and Abelian, a cyclotomic extension of function fields is finite and Abelian.

In the following results, ℓ is a prime number different from $\mathrm{char}(k)$ and $k(\zeta_{\ell^\infty}) = \cup_{n \geqslant 1} k(\zeta_{\ell^n})$.

Proposition 16. *Let K/k be a function field. For every $M \geqslant 1$ that is not divisible by* $\mathrm{char}(k)$, *the constant field of $K(\zeta_M)/k$ is $\widetilde{k}(\zeta_M)$. Moreover, the constant field of $K(\zeta_{\ell^\infty})/k$ is $\widetilde{k}(\zeta_{\ell^\infty})$.*

Proof. By the assumption on M, the field extension $\widetilde{k}(\zeta_M)/\widetilde{k}$ is separable. Hence, by Theorem 11 the constant field of $K(\zeta_M)$ is $\widetilde{k}(\zeta_M)$. The field $\widetilde{k}(\zeta_{\ell^\infty})$ is contained in the constant field of $K(\zeta_{\ell^\infty})$ because its elements are algebraic over k. The converse implication holds because an element of $K(\zeta_{\ell^\infty})$ that is algebraic over k is an element of $K(\zeta_{\ell^m})$ for some integer $m \geqslant 1$ and hence is contained in the constant field of $K(\zeta_{\ell^m})$, which we have shown to be $\widetilde{k}(\zeta_{\ell^m})$. □

Remark 17. Let K/k be a field extension such that k is algebraically closed in K. Fix some algebraic closure $\overline{K}$ of K and choose an algebraic closure $\overline{k}$ of k contained in $\overline{K}$. Let F/K be a finite extension of degree coprime to $\mathrm{char}(k)$ that is contained in $K\overline{k}$. Then Lemma 8 applies. Indeed, it is clear that $F \subset KL'$ for some finite and normal extension L' of k. Let L/k be the maximal separable subextension of L'/k hence L'/L is purely inseparable. So KL'/KL has degree a power of $\mathrm{char}(k)$ and it has FL/KL as a subextension. This is only possible if $FL = KL$, giving $F \subseteq KL$.

Lemma 18. *Let $f \in K^\times$. The following statements are equivalent:*
   (i) *There exists $g \in K\overline{k}$ such that $f = g^\ell$.*
   (ii) *For some choice of ℓ-th root $\sqrt[\ell]{f}$ of f, the extension $K(\sqrt[\ell]{f})/K$ is constant.*
   (iii) *For every ℓ-th root $\sqrt[\ell]{f}$ of f, the extension $K(\sqrt[\ell]{f})/K$ is constant.*

Moreover, these statements are implied by

    (iv) There exist $c \in \widetilde{k}$ and $b \in K$ such that $f = cb^\ell$.
and, if $\zeta_\ell \in K$ (or if $f \in K^{\times \ell}$), they are equivalent to it.

Proof. First notice that if $f \in K^{\times \ell}$ then all conditions (i) to (iv) hold (remark that $K(\zeta_\ell)/K$ is constant). So now we may suppose that $f \notin K^{\times \ell}$ hence the polynomial $x^\ell - f$ is irreducible in $K[x]$ by [3, Theorem 9.1 of Chapter VI]. In particular, the extension $K(\sqrt[\ell]{f})/K$ has degree ℓ for any choice of the ℓ-th root of f.

To complete the proof of the last assertion we show that (iii) implies that there is some $c \in \widetilde{k}(\zeta_\ell)$ and $b \in K(\zeta_\ell)$ such that $f = cb^\ell$. We may clearly reduce to the case $f \notin K(\zeta_\ell)^{\times \ell}$. Recall from Proposition 16 that the constant field of $K(\zeta_\ell)$ is $\widetilde{k}(\zeta_\ell)$. By assumption the extension $K(\zeta_\ell, \sqrt[\ell]{f})/K(\zeta_\ell)$ is constant, so there is an extension $k'/\widetilde{k}(\zeta_\ell)$ that has degree ℓ (by Lemma 6) such that $K(\zeta_\ell, \sqrt[\ell]{f}) = K(\zeta_\ell)k'$. By Kummer theory over $\widetilde{k}(\zeta_\ell)$ and over $K(\zeta_\ell)$ there is $c \in \widetilde{k}(\zeta_\ell)^\times$ such that $k'(\zeta_\ell) = \widetilde{k}(\zeta_\ell, \sqrt[\ell]{c})$ and we have $fc^{-1} \in K(\zeta_\ell)^{\times \ell}$. Thus we have $f = cb^\ell$ where b is an ℓ-th root of fc^{-1} in $K(\zeta_\ell)$.

We are left to prove the equivalence of $(i),(ii)$, and (iii) in the case where $f \notin K^{\times \ell}$, noticing that $(iii) \Rightarrow (ii)$ is obvious.

$(i) \Rightarrow (ii)$: By Lemma 8 (that can be applied thanks to Remark 17) we deduce that $K(g)/K$ is constant, so we conclude by choosing $\sqrt[\ell]{f} = g$.

$(ii) \Rightarrow (i)$: By assumption, $K(\sqrt[\ell]{f}) = Kk'$ with k' a subfield of $\overline{k}$ and we may take $g = \sqrt[\ell]{f}$.

$(ii) \Rightarrow (iii)$: Let $\alpha, \beta \in \overline{K} \backslash K$ be such that $\alpha^\ell = \beta^\ell = f$. Suppose that $K(\alpha)/K$ is constant hence $K(\beta)/K$ is contained in the constant extension $K(\alpha, \zeta_\ell)/K$. By Lemma 8 (that can be applied thanks to Remark 17) we deduce that $K(\beta)/K$ is constant. $\qquad\square$

4. An auxiliary result on function fields extensions

The following result generalizes [9, p.254, Theorem 8.4.2] from transcendence degree 1 to any finite transcendence degree. We let K/k be a function field, and we suppose that k is algebraically closed in K.

Theorem 19. *If k' is an extension of k, then there exists a function field L/k_L that is an extension of K/k such that $L = k_L K$ and there is a $\widetilde{k}$-isomorphism $\lambda : k_L \to k'$. The above properties imply that $\widetilde{k}_L$ is a purely inseparable finite extension of k_L. Finally, if $\hat{L}$, $k_{\hat{L}}$, $\hat{\lambda}$ are also as above, there exists a K-isomorphism $\hat{L} \to L$ extending $\lambda^{-1} \circ \hat{\lambda}$.*

Proof. Let $n = \operatorname{trdeg}(K/k)$ and fix a transcendence basis $x_1, \cdots, x_n$ of K over k.

Let $\{t_i\}_{i \in I}$ be a transcendence basis of k' over k and choose elements $\{T_i\}_{i \in I}$ that are algebraically independent over K. Mapping $t_i \mapsto T_i$ gives a k-morphism from k' to some algebraic closure of $K(\{T_i\}_{i \in I})$. We denote its image by k_L and we define $L := k_L K$.

Let $t \in K \backslash k$ be transcendental over k, and suppose that it is algebraic over k_L. Then it is algebraic also over $k(\{T_i\}_{i \in I})$ because the extension $k_L/k(\{T_i\}_{i \in I})$ is algebraic. Therefore, we have without loss of generality. (and up to clearing the denominators) a relation of the form

$$f_r t^r + \cdots + f_0 = 0$$

with $f_i \in k[T_1, \cdots, T_m]$, not all zero. Some of the f_i must be nonconstant, else t would be algebraic over k. Hence, we have a non-trivial algebraic relation over K of the elements $T_1, \cdots, T_m$, contradicting the algebraic independence of the T_i's. Therefore, we have $k_L \cap K = k$ and $x_1, \ldots, x_n$ are algebraically independent over k_L. Now, k_L contains k and we have

$$[L : k_L(x_1, \ldots, x_n)] \leqslant [K : k(x_1, \cdots, x_n)] < \infty.$$

Hence, L/k_L is a function field.

We now prove the last assertion. Setting $\theta := \lambda^{-1} \circ \hat{\lambda}$, we prove that we obtain a K-isomorphism $\rho : \hat{L} \to L$ by defining

$$\rho\left(\frac{\sum_{i=1}^n \alpha_i \beta_i}{\sum_{j=1}^m \gamma_j \delta_j}\right) = \frac{\sum_{i=1}^n \alpha_i \theta(\beta_i)}{\sum_{j=1}^m \gamma_j \theta(\delta_j)} \qquad \text{where } \alpha_i, \gamma_j \in K \text{ and } \beta_i, \delta_j \in k_{\hat{L}} \text{ and } \sum_{j=1}^m \gamma_j \delta_j \neq 0.$$

We claim that for elements $A_i \in K$ and $B_i \in k_{\hat{L}}$ we have

$$(2) \qquad \sum_{i=1}^{n} A_i B_i = 0 \text{ if and only if } \sum_{i=1}^{n} A_i \theta(B_i) = 0 \,.$$

Then the formula for ρ produces an element in L and different expressions for an element of $\hat{L}$ lead to the same image and the map ρ is injective. We immediately see that ρ is a K-morphism, and it is surjective because θ is invertible.

Notice that (2) only involves a finite number of elements and so we may assume that $k_{\hat{L}}$ and k_L are finitely generated over k.

Let k'/k have transcendence basis $t_1, \cdots, t_m$ and that is generated over $k(t_1, \cdots, t_m)$ by some elements α_i. Then by construction the elements $T_i = \lambda^{-1}(t_i)$ are a transcendence basis of k_L (and they are algebraically independent over K) which generate k_L together with the elements $\lambda^{-1}(\alpha_i)$. The correspondence $t_i \mapsto T_i$ maps the minimal polynomial of α to the one of $\lambda^{-1}(\alpha_i)$. The analogous statement holds for $k_{\hat{L}}$, and we deduce that (2) holds.

If k_L/k is purely transcendental with transcendental basis $\{T_i\}_{i \in I}$, by Lemma 7 the field $k_L = k(T_i)_{i \in I}$ is algebraically closed in $L = K(T_i)_{i \in I}$. So the constant field of L is k_L. In general, k_L/k will have an intermediate extension k'_L/k that is purely transcendental. By applying what is above, we may replace K/k by $k'_L K/k'_L$ and are left to deal with the case where k_L/k is algebraic. Since $k_L K/k_L$ is a function field, the extension $\widetilde{k}_L/k_L$ is finite. We are left to prove that $\widetilde{k}_L/k_L$ is purely inseparable.

So write $\widetilde{k}_L = k(\gamma_1, \cdots, \gamma_r)$ for some $\gamma_1, \cdots, \gamma_r$ algebraic over k. We prove the result by induction on r. The result holds trivially for $r = 0$. Now, suppose the result holds for some $r - 1 \geqslant 0$ and let $k_1 = k(\gamma_1, \cdots, \gamma_{r-1})$ and $L_1 := Kk_1 = K(\gamma_1, \cdots, \gamma_{r-1})$. Let k_2 be the algebraic closure of k_1 in L_1. To conclude, it suffices to prove that $\widetilde{k}_L$ is purely inseparable over k_2. Since γ_r is algebraic over k, the same is true for the coefficients of the minimal polynomial $\min(\gamma_r, L_1)$ of γ_r over L_1. So $\min(\gamma_r, L_1) \in k_2[X]$ and hence $\min(\gamma_r, L_1) = \min(\gamma_r, k_2)$, so we have

$$[L_1(\gamma_r) : k_2] = [L_1(\gamma_r) : L_1][L_1 : k_2] = [k_2(\gamma_r) : k_2][L_1 : k_2]$$

and we deduce $[L_1 : k_2] = [L_1(\gamma_r) : k_2(\gamma_r)]$.

If $c \in \widetilde{k}_L$ and $p := \mathrm{char}(k)$, there is an integer $u \geqslant 0$ (taking $p^u = 1$ if $p = 0$) for which the element c^{p^u} is separable over $k_2(\gamma_r)$. By separability, we have $k_2(\gamma_r, c^{p^u}) = k_2(\delta)$ for some primitive element δ. We can write

$$[L_1(\gamma_r) : k_2(\gamma_r, c^{p^u})] = [L_1(\delta) : k_2(\delta)] = [L_1 : k_2] = [L_1(\gamma_r) : k_2(\gamma_r)],$$

where the second inequality is because a separable extension is linearly disjoint from an inseparable extension. Hence, $c^{p^u} \in k_2(\gamma_r)$, so c is purely inseparable over $k_L = k_2(\gamma_r)$. $\qquad\square$

5. Divisibility modulo constants

5.1. **Divisibility parameter modulo constants.** Let K/k be a function field and let ℓ be a prime number different from $\mathrm{char}(k)$. We will see in Lemma 20 that for any $\alpha \in K^\times \backslash \widetilde{k}^\times$ there exists a maximal integer $D \geqslant 0$ such that $\alpha \in \widetilde{k}^\times K^{\times \ell^D}$, which we call ℓ-*divisibility parameter modulo constants over* K. We say that $\alpha \in K^\times$ is ℓ-*indivisible modulo constants* if $D = 0$, which means $\alpha \notin \widetilde{k}^\times K^{\times \ell}$.

Lemma 20. *Let* $\alpha \in K^\times \backslash \widetilde{k}^\times$. *There is an integer* $D \geqslant 0$ *which is the largest integer* n *for which* $\alpha \in \widetilde{k}^\times K^{\times \ell^n}$. *Moreover, if* $\alpha = c\beta^{\ell^n}$ *for some* $c \in \widetilde{k}^\times$, *for some* $\beta \in K^\times$, *and for some integer* $n \geqslant 0$, *we have* $D = n$ *if and only if* β *is* ℓ-*indivisible modulo constants. Consequently, for all but finitely many primes* ℓ, α *is* ℓ-*indivisible modulo constants.*

Proof. There is $v \in \mathrm{Prime}(K/k)$ such that $v(\alpha) \neq 0$ (see Lemma 4 (ii)). This shows that D is well-defined and it also proves the last assertion. If β is not ℓ-indivisible modulo constants, we can write $\beta = c_1 \beta_1^\ell$ for some $c_1 \in \widetilde{k}^\times$ and for some $\beta_1 \in K^\times$. Then $\alpha = (cc_1)\beta_1^{\ell^{n+1}} \in \widetilde{k}^\times K^{\times \ell^{n+1}}$, implying that $n < D$. Conversely, suppose that $n < D$ and write $\alpha = c_2 \beta_2^{\ell^D}$ for some $c_2 \in \widetilde{k}^\times$ and

for some $\beta_2 \in K^\times$. We can write $\beta^{\ell^n} = (c_2 c_1^{-1})\beta_2^{\ell^D}$ hence there is $\gamma \in \overline{k}$ such that $\beta = \gamma \beta_2^{\ell^{D-n}}$. Since $\gamma \in K \cap \overline{k} = \widetilde{k}$ we deduce that β is not ℓ-indivisible modulo constants. $\qquad\square$

Lemma 21. *Let $\alpha \in K^\times$, and suppose that $\zeta_\ell \in K$. For any $M \geqslant 1$ not divisible by $\mathrm{char}(k)$ the ℓ-divisibility parameter D of α over $K/\widetilde{k}$ is the same over $K(\zeta_M)/k(\zeta_M)$. If L/k_L is a finite constant extension of K, then the ℓ-divisibility parameter D of α over K is the same over L.*

Proof. Write $\alpha = c\beta^{\ell^D}$ with $c \in \widetilde{k}^\times$, $\beta \in K^\times$. Since β is ℓ-indivisible modulo constants (and a constant extension of prime degree is geometric), the extension $K(\sqrt[\ell]{\beta})$ is not contained in $K\overline{k}$. We deduce that the extension $L(\zeta_{\ell^{D+1}}, \sqrt[\ell^{D+1}]{\alpha})/K$ is not contained in $K\overline{k}$, which makes it impossible to have $\alpha = c_L g^{\ell^{D+1}}$ with $c_L \in \widetilde{k}_L^\times$, $g \in L^\times$. $\qquad\square$

Example 22. Let $K = k(t)$, let s be a positive integer and let $\alpha = c\prod_{i=1}^s P_i^{n_i}$ where $c \in k^\times$, P_i are distinct monic irreducible polynomials in $k[t]$, and $n_i \in \mathbb{Z}\setminus\{0\}$. Then the divisibility parameter of α over K is $D_K = \min\{v_\ell(n_i), 1 \leqslant i \leqslant s\}$ because $k[t]$ is a unique factorization domain.

Suppose that $c = 1$ and let n be a non-zero integer pairwise coprime with each n_i. Consider the function field L/k such that $L = K(y)$ for some choice of y in an algebraic closure $\overline{K}$ of K such that $y^n = \alpha$ (the function field L/k is called *superelliptic* if n and all n_i are positive).

If ℓ divides n, then the ℓ-divisibility parameters of α over L is $\mathrm{ord}_\ell(n)$. If ℓ divides the greatest common divisor of the n_i's, then the ℓ-divisibility parameter of α over L (equivalently, over K) is $\min\{v_\ell(n_i), 1 \leqslant i \leqslant s\}$.

Remark 23. Suppose that $\alpha \in K^\times \setminus \widetilde{k}$, and let $n \geqslant 1$. If L/K is a constant extension containing ζ_{ℓ^n}, then we have
$$[L(\sqrt[\ell^n]{\alpha}) : L] = [L(\sqrt[\ell^D]{\alpha}) : L] \cdot \ell^{n-D} \qquad \text{for } n > D.$$
Indeed, by Lemma 21 the ℓ-divisibility parameter D over L is the same as over K and hence $\alpha \notin L^{\times \ell^{D+1}}$. We conclude by Kummer theory.

5.2. **Independence modulo constants.** Let K/k be a function field and let $n \geqslant 1$ be an integer coprime with $\mathrm{char}(K)$. If G is a subgroup of $K^\times$, then we write $K(\sqrt[n]{G})$ for the extension of K generated by all the $\sqrt[n]{\alpha}$, with $\alpha \in G$. This extension is uniquely determined by G, as a subfield of a fixed algebraic closure $\overline{K}$. In particular, if $\{\alpha_1, \cdots, \alpha_r\}$ is a minimal subset of $K^\times$ of generators for G, then by [3, Corollary 6.1.16] we have
$$K(\sqrt[n]{G}) = K(\sqrt[n]{\alpha_1}, \cdots, \sqrt[n]{\alpha_r}) = K(\sqrt[n]{\alpha_1}) \cdot \ldots \cdot K(\sqrt[n]{\alpha_r})$$
and we have a canonical group isomorphism
$$\mathrm{Gal}(K(\sqrt[n]{G})/K) \xrightarrow{\simeq} \mathrm{Gal}(K(\sqrt[n]{\alpha_1})/K) \times \cdots \times \mathrm{Gal}(K\sqrt[n]{\alpha_r})/K).$$
We now suppose that n is the power of some prime number ℓ and hence we will suppose that $\zeta_\ell \in K$ (as we are interested in the Kummer extensions, we may replace K by $K(\zeta_\ell)$).

Definition 24. We say elements $\alpha_1, \ldots, \alpha_r \in K^\times$ are ℓ-*independent modulo constants* if for each vector $(x_1, \cdots, x_r) \in \mathbb{Z}^r$ not in $(\ell\mathbb{Z})^r$, the element $\prod_{i=1}^r \alpha_i^{x_i}$ is ℓ-indivisible modulo constants.

Lemma 25. *Let $\alpha_1, \cdots, \alpha_r \in K^\times$ be ℓ-independent modulo constants. The group generated by the images of $\alpha_1, \cdots, \alpha_r$ in the quotient group $\frac{K^\times}{\overline{k}^\times}$ has rank r. In particular, the α_i's generate a subgroup G of $K^\times$ that is torsion-free and of rank r.*

Proof. The latter assertion is readily seen to be a consequence of the former. Suppose that $\eta := \prod_{i=1}^r \alpha_i^{x_i}$ for some non-zero vector $(x_1, \cdots, x_r) \in \mathbb{Z}^r$. Up to replacing η, we may suppose without loss of generality that not all x_i are divisible by ℓ. Since η is not ℓ-indivisible modulo constants, this contradicts the assumption of ℓ-independence modulo constants. $\qquad\square$

The function fields appearing in the next theorem are implicitly considered as function fields over the same field k.

Theorem 26. *Let G be a torsion-free subgroup of $K^\times$ of rank $r > 0$, and write $G = \langle \alpha_1, \ldots, \alpha_r \rangle$ with $\alpha_i \in K^\times$. The following are equivalent:*

(i) The elements $\alpha_1, \ldots, \alpha_r$ are ℓ-independent modulo constants.

(ii) The Kummer extension $K(\sqrt[\ell]{G})/K$ has degree ℓ^r and it is geometric.

(iii) For every $m \geqslant n \geqslant 1$ the Kummer extension $K(\zeta_{\ell^m}, \sqrt[\ell^n]{G})/K(\zeta_{\ell^m})$ has degree ℓ^{rn} and it is geometric.

(iv) For every $n \geqslant 1$ the Kummer extension $K(\zeta_{\ell^\infty}, \sqrt[\ell^n]{G})/K(\zeta_{\ell^\infty})$ has degree ℓ^{rn} and it is geometric.

(v) For every $n \geqslant 1$ the Kummer extension $\overline{k}K(\sqrt[\ell^n]{G})/\overline{k}K$ has degree ℓ^{rn} and it is geometric.

(As the given Kummer extensions have exponent dividing ℓ^n and rank at most r, their degree being ℓ^{rn} implies that their Galois group is $(\mathbb{Z}/\ell^n\mathbb{Z})^r$.)

Proof. $(iii) \Leftrightarrow (iv)$ Fix $n \geqslant 1$. By Kummer theory, the degrees of the given extensions do not exceed ℓ^{rn}. The degree of $K(\zeta_{\ell^\infty}, \sqrt[\ell^n]{G})/K(\zeta_{\ell^\infty})$ divides the one of $K(\zeta_{\ell^m}, \sqrt[\ell^n]{G})/K(\zeta_{\ell^m})$. Conversely, since the degree in (iii) is constant in m, the two extensions $K(\zeta_{\ell^\infty})$ and $K(\zeta_{\ell^n}, \sqrt[\ell^n]{G})$ are linearly disjoint over $K(\zeta_{\ell^n})$ and hence the degree of the Kummer extension equals ℓ^{rn} also over $K(\zeta_{\ell^\infty})$. Now we may suppose that the given extensions have degree ℓ^{nr} and we only need to show that if one of them is geometric, the other is also geometric. By Proposition 16, the constant field of $K(\zeta_{\ell^m})/k$ is $\widetilde{k}(\zeta_{\ell^m})$ while the one of $K(\zeta_{\ell^\infty})/k$ is $\widetilde{k}(\zeta_{\ell^\infty})$ by Proposition 16. Moreover, we can write $K(\zeta_{\ell^\infty}, \sqrt[\ell^n]{G}) = \bigcup_{m=1}^{\infty} K(\zeta_{\ell^m}, \sqrt[\ell^n]{G})$.

Suppose that all extensions $K(\zeta_{\ell^m}, \sqrt[\ell^n]{G})/K(\zeta_{\ell^m})$ are geometric. An element $\gamma \in K(\zeta_{\ell^\infty}, \sqrt[n]{G})$ that is algebraic over k belongs to some field $K(\zeta_{\ell^m}, \sqrt[\ell^n]{G})$. Our assumption on this field then implies $\gamma \in \widetilde{k}(\zeta_{\ell^m})$. This shows that $K(\zeta_{\ell^\infty}, \sqrt[n]{G}) \cap \overline{k} = \widetilde{k}(\zeta_{\ell^\infty})$.

Now suppose that $K(\zeta_{\ell^\infty}, \sqrt[n]{G})/K(\zeta_{\ell^\infty})$ is geometric. An element of $K(\zeta_{\ell^m}, \sqrt[n]{G})$ that is algebraic over k belongs to $\widetilde{k}(\zeta_{\ell^\infty})$ and hence to $\widetilde{k}(\zeta_{\ell^u})$ for some $u \geqslant m$. We conclude by proving that $K(\zeta_{\ell^m}, \sqrt[n]{G}) \cap \widetilde{k}(\zeta_{\ell^u}) = \widetilde{k}(\zeta_{\ell^m})$. If we had $\zeta_{\ell^{m+1}}$ in $K(\zeta_{\ell^m}, \sqrt[n]{G}) \backslash K(\zeta_{\ell^m})$, then the degree of $K(\zeta_{\ell^m}, \sqrt[n]{G})/K(\zeta_{\ell^m})$ would not be the same as the one of $K(\zeta_{\ell^\infty}, \sqrt[n]{G})/K(\zeta_{\ell^\infty})$, contradiction.

$(iii) \Rightarrow (ii)$ This is immediate by taking $m = n = 1$.

$(ii) \Rightarrow (iii)$ Since $K(\sqrt[\ell]{G})/K$ is geometric, we deduce that $K(\zeta_{\ell^m}, \sqrt[\ell]{G})/K(\zeta_{\ell^m})$ has also degree ℓ^r. By Kummer theory, we deduce that $K(\zeta_{\ell^m}, \sqrt[\ell^n]{G})/K(\zeta_{\ell^m})$ has degree ℓ^{rn}. By Lemma 15 it suffices to prove that $K(\zeta_{\ell^m}, \sqrt[\ell]{G})/K(\zeta_{\ell^m})$ is geometric. This extension is a tower of extensions of degree ℓ that are nonconstant and hence geometric by Remark 14, so we may conclude.

$(i) \Leftrightarrow (ii)$ Property (ii) is equivalent to the fact that for every $\alpha \in G$ that is not an ℓ-th power in G the extension $K(\sqrt[\ell]{\alpha})/K$ is geometric of degree ℓ (because the Galois group of $K(\sqrt[\ell]{G})/K$ has exponent dividing ℓ, and an extension of degree ℓ is geometric if and only if it is not constant). Recalling that $\zeta_\ell \in K$, by Lemma 18 the above property precisely means that every element $\alpha := \prod_{i=1}^r \alpha_i^{x_i}$ is ℓ-indivisible up to constants whenever the integers x_i's are not all divisible by ℓ.

$(i) \Leftrightarrow (v)$. The extension $\overline{k}K(\sqrt[\ell^n]{G})/\overline{k}K$ is always geometric. Indeed, the constant field of $\overline{k}K(\sqrt[\ell^n]{G})$ is a finite extension of the constant field of $\overline{k}K$ hence it is $\overline{k}$. Property (i) means that any element $\alpha := \prod_{i=1}^r \alpha_i^{x_i}$ (where the integers x_i's are not all divisible by ℓ) is ℓ-indivisible modulo constants. Property (v) (the assertion on the degree) means, by Kummer theory, that any such element is not an ℓ-th power in $\overline{k}K$. We may conclude by Lemma 18 $(i) \Leftrightarrow (iv)$. $\qquad\square$

Corollary 27. *Suppose that $\alpha_1, \ldots, \alpha_r \in K^\times$ can be expressed as $\alpha_i = c_i \beta_i^{\ell^{D_i}}$, where $c_i \in \widetilde{k}$ and where the elements $\beta_1, \ldots, \beta_r$ are ℓ-independent modulo constants over K. For every $n \geqslant 1$ and for every M such that $\ell^n \mid M$, the maximal constant subextension of $K(\zeta_M, \sqrt[\ell^n]{G})/K$ is*

$$L_{M,n} := K(\zeta_M, \sqrt[\ell^{\min(D_1,n)}]{\alpha_1}, \ldots, \sqrt[\ell^{\min(D_r,n)}]{\alpha_r}).$$

Moreover, we have

$$\mathrm{Gal}(K(\zeta_M, \sqrt[\ell^n]{G})/L_{M,n}) \simeq \mathrm{Gal}(\overline{k}K(\sqrt[\ell^n]{G})/\overline{k}K) \simeq \prod_{i=1}^r \mathbb{Z}/\ell^{\max(n-D_i,0)}\mathbb{Z}.$$

Proof. By definition of the ℓ-divisibility parameters, $L_{M,n}$ is a constant extension of K contained in $K(\zeta_M, \sqrt[\ell^n]{G})$. Remark that we have

$$\overline{k}K(\sqrt[\ell^n]{G}) = \overline{k}K(\sqrt[\ell^{\max(n-D_1,0)}]{\beta_1}, \ldots, \sqrt[\ell^{\max(n-D_r,0)}]{\beta_r}).$$

Theorem 26 ensures that the latter field is a geometric extension of $\bar{k}K$ whose Galois group is isomorphic to $\prod_{i=1}^{r} \mathbb{Z}/\ell^{\max(n-D_i,0)}\mathbb{Z}$. To conclude, it suffices to show that $K(\zeta_M, \sqrt[\ell^n]{G}) \cap \bar{k}K = L_{M,n}$. This is the case because the degree of $K(\zeta_M, \sqrt[\ell^n]{G})/L_{M,n}$ is a multiple of $\bar{k}K(\sqrt[\ell^n]{G})/\bar{k}K$ hence it equals $\sum_{i=1}^{r} \max(n-D_i, 0)$ (it is at most this number by Kummer theory as $\sqrt[\ell^n]{\alpha_i}$ is an $\ell^{\max(n-D_i,0)}$-th root of $\sqrt[\ell^{\min(D_i,n)}]{\alpha_i}$). $\qquad\square$

5.3. **Good basis modulo constants.** In the following definition, we let D_i be the ℓ-divisibility parameters of α_i over K.

Definition 28. Consider a finitely generated subgroup G of $K^{\times}$ that intersects $\tilde{k}$ only trivially and that has positive rank r. Let $\{\alpha_1, \ldots, \alpha_r\}$ be a basis of G. This basis is said to be an ℓ-*good basis modulo constants* if, equivalently:

(i) the quantity $\sum_{i=1}^{r} D_i$ is maximal among the bases of G;
(ii) we can write $\alpha_i = c_i \beta_i^{\ell^{D_i}}$ where $c_i \in \tilde{k}$ and $\beta_i \in K$ and $\beta_1, \ldots, \beta_r$ are ℓ-independent modulo constants.

The multiset of $D_1, \cdots, D_r$ is uniquely determined by K and G (see Remark 32). We call it the ℓ-*divisibility parameters modulo constants of G over K.*

Proposition 29. *Definition 28 is well-posed, namely the equivalence holds true.*

Proof. (i)$\Rightarrow$(ii) By the definition of the ℓ-divisibility parameters we can write $\alpha_i = c_i \beta_i^{\ell^{D_i}}$ where $c_i \in \tilde{k}$ and $\beta_i \in K$. Suppose that the β_i's are not ℓ-independent modulo constants. So there are a non-empty subset $J \subseteq \{1, \ldots, r\}$ and integers x_j coprime to ℓ such that $\beta := \prod_{j \in J} \beta_j^{x_j}$ is not ℓ-indivisible modulo constants. We may suppose without loss of generality that $1 \in J$ and $D_1 = \max\{D_j : j \in J\}$. We may additionally suppose that $x_1 = 1$ (by raising β to some power y_1 such that $x_1 y_1 \equiv 1 \bmod \ell$ and then discarding an ℓ-th power). Define

$$\alpha := \prod_{j \in J} \alpha_j^{x_j \ell^{D_1 - D_j}} .$$

By inspecting the factor $j = 1$, we may replace α_1 by α and still get a basis of G. Moreover, by construction

$$\alpha \beta^{-\ell^{D_1}} = \prod_{j \in J} \alpha_j^{x_j \ell^{D_1 - D_j}} \left(\prod_{j \in J} \beta_j^{x_j \ell^{D_1}} \right)^{-1} = \prod_{j \in J} c_j^{x_j \ell^{D_1 - D_j}}$$

is a constant hence (since β is not ℓ-indivisible modulo constants) the first divisibility parameter of α is strictly larger than D_1, contradicting the maximality of $\sum_{i=1}^{r} D_i$.

(ii)$\Rightarrow$(i) We cannot have a different basis $\{\alpha_1', \cdots, \alpha_r'\}$ of G such that $\sum_{i=1}^{r} D_i' > \sum_{i=1}^{r} D_i$. This is because, if n is sufficiently large, by Corollary 27 the degree of $\bar{k}K(\sqrt[\ell^n]{G})/\bar{k}K$ has ℓ-adic valuation $nr - \sum_{i=1}^{r} D_i$ while

$$[\bar{k}K(\sqrt[\ell^n]{G}) : \bar{k}K] = [\bar{k}K(\sqrt[\ell^{\max(n-D_1',0)}]{\alpha_1'}, \ldots, \sqrt[\ell^{\max(n-D_r',0)}]{\alpha_r'}) : \bar{k}K] \leqslant nr - \sum_{i=1}^{r} D_i' .$$

$\qquad\square$

Theorem 30. *Consider a finitely generated subgroup G of $K^{\times}$ of rank $r > 0$ that intersects $\tilde{k}$ only trivially. Then the following statements hold.*

(i) *The group G has an ℓ-good basis modulo constants.*
(ii) *For all sufficiently large n we have*

(3) $$[\bar{k}K(\sqrt[\ell^{n+1}]{G}) : \bar{k}K(\sqrt[\ell^n]{G})] = \ell^r .$$

(iii) *There exists an integer $\varepsilon \geqslant 0$ such that for all $n > \varepsilon$ we have*
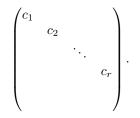
$$G \cap \tilde{k}^{\times} K^{\times \ell^n} \subseteq G^{\ell^{n-\epsilon}} .$$

Proof. Observing that $(\bar{k}K)^{\times \ell^n} = \bar{k}^{\times}(K^{\times \ell^n})$, we have $G \cap (\bar{k}K)^{\times \ell^n} = G \cap \widetilde{k}^{\times} K^{\times \ell^n}$ hence (iii) is equivalent to (ii) by Kummer theory over $\bar{k}K$. If G has an ℓ-good basis modulo constants, then (ii) is proven in Corollary 27. The converse implication is because, if there is a basis such that $\sum_i D_i > (n+1)r$, then (3) does not hold.

We conclude by proving (iii). By applying Lemma 4 to a set of generators of G, there is a finite non-empty subset S of $\mathrm{Prime}(K/k)$ of cardinality $\#S$ consisting of the divisors v such that there is some $g \in G$ such that $v(g) \neq 0$. Consider the group morphism

$$\Phi : G \to \mathbb{Z}^{\#S} \qquad g \mapsto (v(g))_{v \in S}\,.$$

The kernel of Φ is trivial because by Lemma 4 it consists of constants, thus $\Phi(G)$ is a subgroup of $\mathbb{Z}^{\#S}$ of rank r. By choosing an appropriate basis of G, the basis of $\Phi(G)$ consists of the column vectors of the following matrix, where the integers $c_1, \dots, c_r$ are the non-zero entries:

$$\begin{pmatrix} c_1 & & & & \\ & c_2 & & & \\ & & \ddots & & \\ & & & c_r & \\ & & & & \\ & & & & \end{pmatrix}.$$

Let ε be the maximum of the ℓ-adic valuation of the integers c_i's and fix $n > \varepsilon$. If $g \in G$ is such that $\ell^n \mid v(g)$ for every $v \in S$, then all the coordinates of $\Phi(g)$ with respect to the above basis are divisible by $\ell^{n-\varepsilon}$, so we deduce that $g \in G^{\ell^{n-\epsilon}}$. $\qquad \square$

Theorem 31. *Let K/k be a function field and let G be a finitely generated subgroup of $K^{\times}$. An ℓ-good basis modulo constants exists for G if and only if the rank of G is the same as the rank of G modulo constants.*

Proof. The sufficiency has been shown in Theorem 30 and the necessity follows from Corollary 27 by working over $\bar{k}K$. $\qquad \square$

Remark 32. The multiset of parameters D_i for an ℓ-good basis modulo constants is uniquely determined by K and G. This is clear from the Galois group structure in Corollary 27 by taking $n > \max\{D_i : 1 \leqslant i \leqslant r\}$. Provided that G admits an ℓ-good basis modulo constants, there is an easy algorithm to construct one from any given basis of G, which is based on the following observation: if the elements of a given basis of G are not ℓ-independent modulo constants, then there is a way to modify one element of the basis and increase $\sum_i D_i$ (following the strategy in the proof of [2, Theorem 14], which also resembles the proof of Proposition 29 $(i) \Rightarrow (ii)$).

6. Reducing to cyclotomic-Kummer extensions of the constant field

Consider a function field K/k and a Kummer extension of the form

$$K(\zeta_M, \sqrt[N]{G})/K(\zeta_M)\,,$$

where G is a finitely generated subgroup of $K^{\times}$ and M and N are positive integers such that M is divisible by N but not by $\mathrm{char}(K)$. In this section, we precisely show how the questions of computing the degree of this extension and of computing the group structure of its Galois group reduce to the corresponding questions for the Kummer extension of the constant fields.

Considering the prime factorization $N = \prod_{\ell \mid N} \ell^{v_\ell(N)}$, by Kummer theory (notice the pairwise coprime exponents of the Kummer extensions in the product group) we have a group isomorphism

$$\mathrm{Gal}(K(\zeta_M, \sqrt[N]{G})/K(\zeta_M)) \simeq \prod_{\ell \mid N} \mathrm{Gal}(K(\zeta_M, \sqrt[\ell^{v_\ell(N)}]{G})/K(\zeta_M))\,.$$

We will therefore restrict to the case where $N = \ell^n$ for some fixed prime number ℓ different from $\mathrm{char}(k)$ and for some integer $n \geqslant 1$. We may then without loss of generality replace K by $K(\zeta_\ell)$. We may also suppose that G is not a subgroup of $\widetilde{k}^{\times}$. Hence, from now on $G_0 := G \cap \widetilde{k}$ is a proper subgroup of G and we can write the set decomposition $G = G_0 G'$, where G' is a subgroup

of G isomorphic to G/G_0. Let $r > 0$ be the rank of G' and let $D_1, \ldots, D_r$ be the ℓ-divisibility parameters modulo constants of G' over K. Up to relabelling, we suppose without loss of generality that $D_1 \leqslant D_2 \leqslant \cdots \leqslant D_r$. Let $\alpha_i = c_i \beta_i^{\ell^{D_i}}$ be the elements of an ℓ-good basis modulo constants of G' over K, with $c_i \in \widetilde{k}$ and $\beta_i \in K$.

The following result reduces the problem of determining the degree of the Kummer extension $K(\zeta_M, \sqrt[\ell^n]{G})/K(\zeta_M)$ to determine the degree of a Kummer extension that only depends on $\widetilde{k}(\zeta_M)$, ℓ^n, G_0, the c_i's and the D_i's:

Theorem 33. *Define H as the subgroup of $K^\times$ generated by G_0 and by the elements $c_i^{\ell^{\max(n-D_i,0)}}$. Then we have*

$$[K(\zeta_M, \sqrt[\ell^n]{G}) : K(\zeta_M)] = [\widetilde{k}(\zeta_M, \sqrt[\ell^n]{H}) : \widetilde{k}(\zeta_M)] \cdot \prod_{i=1}^{r} \ell^{\max(n-D_i,0)}.$$

Proof. Remark that, by Lemma 6 applied to the monogenic extension $\widetilde{k}(\zeta_M, \sqrt[\ell^n]{H})/\widetilde{k}(\zeta_M)$ we have

$$[\widetilde{k}(\zeta_M, \sqrt[\ell^n]{H}) : \widetilde{k}(\zeta_M)] = [K(\zeta_M, \sqrt[\ell^n]{H}) : K(\zeta_M)].$$

We may conclude by Corollary 27 (applied to G') because the largest constant subextension of $K(\zeta_M, \sqrt[\ell^n]{G})/K(\zeta_M)$ is generated by the ℓ^n-th roots of H, in view of Lemma 12 (where C is the Kummer extension generated by G_0 and K' is the Kummer extension generated by G'). □

Definition 34. We define elements $d_1, \ldots, d_r$ in $\mathbb{Z}_{\geqslant 0} \cup \{+\infty\}$ as follows: d_i is maximal such that the image of c_i in the quotient group $\widetilde{k}(\zeta_M)^\times / \langle G_0, c_j : j > i \rangle$ is an ℓ^{d_i}-th power.

Remark 35. According to the use that we make of $d_1, \cdots, d_r$, we do not need their precise value if we know that $d_i \geqslant D_i$ for all i. However, we could compute d_i by multiplying c_i by an element of $\langle G_0, c_j : j > i \rangle$ (and using powers of the generators with exponents from 0 to $\ell^{D_i} - 1$). Notice that, if G_0, the D_i's and the c_i's are known in advance, then calculating the parameters d_i only involves computations over $\widetilde{k}(\zeta_M)$.

Theorem 36. *With the above notation, we have a group isomorphism*

$$\operatorname{Gal}\left(K(\zeta_M, \sqrt[\ell^n]{G})/K(\zeta_M)\right) \simeq \operatorname{Gal}\left(\widetilde{k}(\zeta_M, \sqrt[\ell^n]{G_0})/\widetilde{k}(\zeta_M)\right) \times \prod_{i=1}^{r} \mathbb{Z}/\ell^{\max(n-\min(D_i,d_i),0)}\mathbb{Z}.$$

Proof. By Lemma 6 applied to the monogenic Kummer extension $\widetilde{k}(\zeta_M, \sqrt[\ell^n]{G_0})/\widetilde{k}(\zeta_M)$ we have

$$\operatorname{Gal}(\widetilde{k}(\zeta_M, \sqrt[\ell^n]{G_0})/\widetilde{k}(\zeta_M)) \simeq \operatorname{Gal}(K(\zeta_M, \sqrt[\ell^n]{G_0})/K(\zeta_M)).$$

By Lemma 21 the ℓ-divisibility parameters of G_0 over K are the same over $K(\zeta_M)$ and by Proposition 16 the constant field of $K(\zeta_M)/\widetilde{k}$ is $\widetilde{k}(\zeta_M)$. We then work over $K(\zeta_M)/\widetilde{k}(\zeta_M)$.

Notice that multiplying α_i by an element of G_0 does not change the ℓ-divisibility parameter. Also, since the β_i's are ℓ-independent modulo constants and since we assume $D_i \leqslant D_j$ for $i < j$, then we can replace α_i by $\alpha_i \alpha_j^e$ for any $e \in \mathbb{Z}$ without altering the i-th ℓ-divisibility parameter. We perform such multiplications, modifying the elements $\alpha_r, \alpha_{r-1}, \ldots, \alpha_1$ in this order. In this way, we can achieve that c_i is an ℓ^{D_i}-th power in $\widetilde{k}(\zeta_M)^\times$ or that the largest integer d_i such that c_i is an ℓ^{d_i}-th power in $\widetilde{k}(\zeta_M)^\times$ is strictly less than D_i and is as in Definition 34. Consider the tower of Kummer extensions

$$L(\sqrt[\ell^n]{G_0}) \subseteq L(\sqrt[\ell^n]{G_0}, \sqrt[\ell^n]{\alpha_r}) \subseteq L(\sqrt[\ell^n]{G_0}, \sqrt[\ell^n]{\alpha_r}, \sqrt[\ell^n]{\alpha_{r-1}}) \subseteq \cdots \subseteq L(\sqrt[\ell^n]{G}).$$

By definition of d_i (and by Kummer theory over L, recalling that $\sqrt[\ell]{\beta_i} \notin L$) the Galois group of $L(\sqrt[\ell^n]{\alpha_i})/L$ is isomorphic to $\mathbb{Z}/\ell^{\max(n-\min(D_i,d_i),0)}\mathbb{Z}$. To conclude, we only need to prove that this extension has the same degree as

$$L(\sqrt[\ell^n]{\alpha_i}, \sqrt[\ell^n]{G_0}, \sqrt[\ell^n]{\alpha_j} : j > i)/L(\sqrt[\ell^n]{G_0}, \sqrt[\ell^n]{\alpha_j} : j > i).$$

By the radical correspondence of Kummer theory, this is equivalent to saying that there are no integers x satisfying both

$$\alpha_i^x \mod L^{\times \ell^n} \in \langle G_0, \alpha_j : j > i \rangle \mod L^{\times \ell^n} \quad \text{and} \quad \alpha_i^x \notin L^{\times \ell^n}.$$

If $d_i \geqslant D_i$ we conclude because, by Theorem 26 (applied to the β_i's), no integer z satisfies both

$$(4) \qquad \beta_i^z \bmod L^{\times \ell^n} \in \langle \widetilde{k}^{\times}, \beta_j : j \neq i \rangle \bmod L^{\times \ell^n} \quad \text{and} \quad \beta_i^z \notin L^{\times \ell^n} .$$

Now suppose that $d_i < D_i$. We have $\alpha_i^x = c_i^{\ell^y} \beta_i^{\ell^{D_i + y}}$ and without loss of generality, that $x = \ell^y$ for some integer $y \geqslant 1$. If $D_i + y < n$ we conclude because there is no integer z as in (4). Now suppose that $D_i + y \geqslant n$ and hence $\alpha_i^x \equiv c_i^x \bmod L^{\times \ell^n}$. We are left to prove that we cannot have

$$c_i^x \bmod L^{\times \ell^n} \in \langle G_0, \alpha_j : j > i \rangle \bmod L^{\times \ell^n} \quad \text{and} \quad c_i^x \notin L^{\times \ell^n} .$$

Notice that, since $\widetilde{k}(\zeta_M)$ is the constant field of L, for any $\gamma \in \widetilde{k}(\zeta_M)^{\times}$, we have $\gamma \in L^{\times \ell^n}$ if and only if $\gamma \in \widetilde{k}(\zeta_M)^{\times \ell^n}$. We claim that if $c_i^x \bmod L^{\times \ell^n}$ is in $\langle G_0, \alpha_j : j > i \rangle \bmod L^{\times \ell^n}$, then it is in $\langle G_0, c_j : j > i \rangle \bmod L^{\times \ell^n}$. This will conclude because no integer x can satisfy both

$$c_i^x \bmod \widetilde{k}(\zeta_M)^{\times \ell^n} \in \langle G_0, c_j : j > i \rangle \bmod \widetilde{k}(\zeta_M)^{\times \ell^n} \quad \text{and} \quad c_i^x \notin \widetilde{k}(\zeta_M)^{\times \ell^n}.$$

Indeed, by construction, the divisibility of c_i is the same in $\widetilde{k}(\zeta_M)^{\times}$ as the one of its image in the quotient group $\widetilde{k}(\zeta_M)^{\times}/\langle G_0, c_j : j > i \rangle$. The claim holds because Theorem 26 (applied to the β_i's) gives that an integer z such that $\alpha_j^z \bmod L^{\times \ell^n}$ is in $\langle \widetilde{k}, \alpha_h : h \neq j \rangle \bmod L^{\times \ell^n}$ must satisfy $v_\ell(z) + D_i \geqslant n$, and hence $\alpha_j^z \equiv c_j^z \bmod L^{\times \ell^n}$. $\qquad \square$

Remark 37. The extension $\widetilde{k}(\zeta_M, \sqrt[\ell^n]{G_0})/\widetilde{k}(\zeta_M)$ is finite and separable, hence, monogenic. Therefore, by Lemma 6 we have

$$[K(\zeta_M, \sqrt[\ell^n]{G_0}) : K(\zeta_M)] = [\widetilde{k}(\zeta_M, \sqrt[\ell^n]{G_0}) : \widetilde{k}(\zeta_M)].$$

Example 38. We can apply the above results multiple times if $\widetilde{k}$ is a function field. For example, let $K = \widetilde{k}(S)$ where $\widetilde{k} = \mathbb{Q}(T)$. Then by Theorem 33 we may first reduce to $\mathbb{Q}(T)$ and then to $\mathbb{Q}$. Alternatively, we can see K as a function field over $\mathbb{Q}$ and apply Theorem 33 to reduce directly from K to $\mathbb{Q}$. This is possible because the Kummer extensions $K(\zeta_M, \sqrt[N]{G})/K(\zeta_M)$ do not depend on the choice of the constant field.

Example 39. We use the notation of Example 22. Fix two distinct monic irreducible polynomials P_1 and P_2 and let $c_1, c_2 \in k^{\times}$. We consider the group

$$G = \langle c_1 P_1, c_2 P_1 P_2^2 \rangle .$$

Both generators are 2-indivisible modulo constants. We also have $G = \langle \alpha_1, \alpha_2 \rangle$, where

$$\alpha_1 := (c_1 c_2)(P_1 P_2)^2 \qquad \text{and} \qquad \alpha_2 := c_2 P_1 P_2^2 .$$

The latter is a 2-good basis because $P_1 P_2$ and $P_1 P_2^2$ are 2-independent modulo constants as they generate the same group as P_1, P_2. The 2-divisibility parameters modulo constants are $D(\alpha_1) = 1$ and $D(\alpha_2) = 0$. We have $K(\sqrt{G}) = K(\sqrt{c_1 c_2}, \sqrt{c_2 P_1})$. Thus, for any $n \geqslant 1$, we have

$$\mathrm{Gal}(K(\zeta_{2^n}, \sqrt[2^n]{G})/K(\zeta_{2^n})) \simeq \begin{cases} \mathbb{Z}/2^{n-1}\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z} & \text{if } c_1 c_2 \in \widetilde{k}^{\times 2}, \\ \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z} & \text{if } c_1 c_2 \notin \widetilde{k}^{\times 2}. \end{cases}$$

ACKNOWLEDGMENT

References

[1] B. Advocaat, C.W. Chan, A. Pajaziti, F. Perissinotto and A. Perucca: *Galois groups of Kummer extensions of number fields*, to appear in the Publ. Math. Besançon. 2

[2] C. Debry and A. Perucca, *Reductions of algebraic integers*, J. Number Theory **167** (2016), 259–283. 12

[3] S. Lang, *Algebra*, Revised third edition, Grad. Texts in Math., 211, Springer-Verlag, New York, 2002. xvi+914 pp. ISBN: 0-387-95385-X. 7, 9

[4] S. MacLane and O.F.G. Schilling, *A general Kummer theory for function fields*, Duke Math. J. 9, 125–167 (1942). 2

[5] S. Okada, *Kummer's theory for function fields*, J. Number Theory, 38, 1991, 2, 212–215. 2

[6] F. Perissinotto and A. Perucca, *Kummer theory for p-adic fields*, preprint. 2

[7] G. Peng, *The genus fields of Kummer function fields*, J. Number Theory 98, No. 2, 221-227 (2003). 2

[8] M. Rzedowski-Calderón and G.D. Villa-Salvador, *Genus fields of Kummer extensions of rational function fields*, Finite Fields Appl., 77, 2022, Paper No. 101943, 19, 2

[9] G.D. Villa Salvador, *Topics in the Theory of Algebraic Function Fields*, Math. Theory Appl. Birkhäuser Boston, Inc., Boston, MA, 2006, xviii+652 pp. 4, 7

[10] O. Zariski and P. Samuel, *Commutative algebra. Vol. II*, The University Series in Higher Mathematics, D. Van Nostrand Co., Inc., Princeton, N.J.-Toronto-London-New York, 1960, x+414 pp., MR(120249). 3