

# NON-CROSSED PRODUCT BOUNDS OVER HENSELIAN FIELDS

TIMO HANKE, DANNY NEFTIN, AND JACK SONN

ABSTRACT. The existence of finite dimensional central division algebras with no maximal subfield that is Galois over the center (called noncrossed products), was for a time the biggest open problem in the theory of division algebras, before it was settled by Amitsur.

Motivated by Brussel's discovery of noncrossed products over  $\mathbb{Q}((t))$ , we describe the "location" of noncrossed products in the Brauer group of general Henselian valued fields with arbitrary value group and global residue field. We show that within the fibers defined canonically by Witt's decomposition of the Brauer group of such fields, crossed products and noncrossed products are, roughly speaking, separated by an index bound. This generalizes a result of the first and third author for rank 1 valued Henselian fields.

Furthermore, we prove that all fibers which are not covered by the rank 1 case, and where the characteristic of the residue field does not interfere, contain noncrossed products.

We show by example that, unlike in the rank 1 case, the value of the index bound does not depend on the number of roots of unity that are present. Thus, the index bounds are in general of a different nature than in the rank 1 case.

## 1. INTRODUCTION

A finite-dimensional division algebra over its center  $F$  is called a *crossed product* if it has a maximal commutative subfield which is Galois over  $F$ , otherwise a *noncrossed product*.

After Amitsur settled the fundamental long-standing problem of existence of noncrossed products in [2], they were subsequently discovered over more familiar fields. Most notably, Brussel showed in [3], [4] that noncrossed products exist over complete discrete rank 1 valued fields with a global residue field<sup>1</sup>, e.g. over  $\mathbb{Q}((x))$ . From this basic case, their existence over many other fields was derived, e.g. over all finitely generated fields that are neither finite nor global ([4]), and over all function fields of curves over complete discrete valuation rings ([5], [6]).

---

*Date:* September 1, 2012.

The authors would like to thank Eli Aljadeff for financially supporting a visit of the first author the Technion, and Julia Hartmann for a financial support of the second's author visit to RWTH Aachen.

<sup>1</sup>By a global field we mean a finite extension of  $\mathbb{Q}$  or a finite extension of  $\mathbb{F}_q(t)$  where  $\mathbb{F}_q$  is a finite field.

The basic setup used for Brussel’s discovery is Witt’s description ([15]) of the Brauer group of a complete discrete rank 1 valued field. More precisely, Witt’s theorem describes the inertially split part  $\text{SBr}(F)$  which consists of all elements of the Brauer group that are split by an unramified extension (cf. [10, §5]). Witt’s theorem applies more generally to Henselian fields  $F$  with arbitrary value group  $\Gamma$  (see [14], [11, §5], [1, Theorem 3.2]), e.g. to the field of iterated Laurent series  $\mathbb{Q}((x_1)) \cdots ((x_r))$ , and gives an isomorphism:

$$(1.1) \quad \text{SBr}(F) \cong \text{Br}(K) \oplus \text{Hom}(G_K, \Delta/\Gamma)$$

where  $K$  is the residue field and  $G_K$  is its absolute Galois group,  $\Delta$  is the divisible hull of  $\Gamma$ ,  $\Delta/\Gamma$  is equipped with the discrete topology, and  $\text{Hom}$  is the group of continuous homomorphisms.

Assume  $K$  is a global field. In [9], the first and third author took the approach of fixing an element  $\chi \in \text{Hom}(G_K, \Delta/\Gamma)$  and considering the *fiber*  $\text{Br}(K) + \chi$ . We call  $\chi$  *cyclic* if  $\text{Im}(\chi)$  is cyclic. For cyclic  $\chi$ , [9] shows that for every  $N \in \mathbb{N}$  there are only two possible cases:

- (I) all division algebras of index  $N$  in the fiber over  $\chi$  are crossed products;
- (II) the fiber over  $\chi$  contains infinitely many noncrossed products of index  $N$ .

Furthermore, and most importantly, there are bounds on the exponents in the prime decomposition of  $N$  such that case (I) occurs “below the bounds” and case (II) “above”. A precise formulation of this result is the special case of Theorem 1.1 below in which  $\chi$  is assumed to be cyclic<sup>2</sup>.

All that was known about the appearance of noncrossed products in the more complicated case of non-cyclic  $\chi$  were two examples ([8], [7]) in which noncrossed products of index 8 appear in the fiber over  $\chi$ . In both of them,  $\text{Im}(\chi)$  is the Klein 4 group.

In the present paper, we show that the phenomenon from [9] holds more generally for arbitrary  $\chi$  (Theorem 1.1), and that “away from char  $K$ ” noncrossed products appear in every noncyclic fiber (Theorem 1.2).

Note that by [11, Theorem 5.15(a)] the index of an element in the fiber over  $\chi$  is always a multiple of  $|\chi| := |\text{Im}(\chi)|$ .

**Theorem 1.1.** *There exists a collection of bounds  $b_p = b_p(\chi) \in \mathbb{N} \cup \{\infty\}$  where  $p$  runs through the rational primes, such that for every natural number  $m = \prod p^{n_p}$ :*

- (a) *if  $n_p \leq b_p(\chi)$  for all  $p$ , then all division algebras of index  $m|\chi|$  in the fiber over  $\chi$  are crossed products.*

---

<sup>2</sup>In order to see that Theorem 1.1 for cyclic  $\chi$  was proved in [9] not only for rank 1 valued fields, one should replace [9, Brussel’s Lemma, p.322] by [10, Corollary 5].

- (b) if  $n_p > b_p(\chi)$  for some  $p$ , then the fiber over  $\chi$  contains infinitely many noncrossed products of index  $m|\chi|$ .

Our proof of Theorem 1.1 includes the cyclic case and is significantly simpler than [9].

Note that  $b_p(\chi) = \infty$  is allowed and hence, as shown in [9], it may happen that for some cyclic  $\chi$  only (I) occurs. However, in striking contrast to the cyclic case, we show:

Let  $K(\chi)$  be the fixed field of the kernel of  $\chi$ .

**Theorem 1.2.** *If  $p \neq \text{char } K$  and the  $p$ -Sylow subgroup of  $\text{Im}(\chi)$  is non-cyclic then*

- (i)  $b_p(\chi) < \infty$ ,
- (ii)  $K(\chi)$  does not contain the  $p$ -th roots of unity implies  $b_p(\chi) = 0$ .

*In particular, the fiber over  $\chi$  contains noncrossed products whenever the maximal prime-to-char  $K$  subgroup of  $\text{Im}(\chi)$  is non-cyclic.*

This is in contrast to the cyclic case because, according to [9],  $b_p(\chi) = \infty$  can occur for cyclic  $\chi$  even if  $K(\chi)$  does not contain the  $p$ -th roots of unity. Thus, neither of statements (i) and (ii) of Theorem 1.2 holds for cyclic  $\chi$ .

In Section 4, we demonstrate how a description of the bounds obtained from the proof of Theorem 1.1 can be used to compute the bounds in examples and to obtain new noncrossed products of low index.

## 2. EXISTENCE OF BOUNDS

**2.1. Setup.** Let  $F$  be a Henselian valued field with value group  $\Gamma$  and residue field a global field  $K$ . Let  $\Delta$  denote the divisible hull of  $\Gamma$ . Let  $G_K$  denote the absolute Galois group of  $K$ . The group  $\text{Hom}(G_K, \Delta/\Gamma)$  is understood as the group of continuous homomorphisms,  $\Delta/\Gamma$  equipped with the discrete topology.

For any  $\chi \in \text{Hom}(G_K, \Delta/\Gamma)$ , we write  $K(\chi)$  for the fixed field of the kernel of  $\chi$ , which is a finite abelian extension of  $K$  with Galois group  $\text{Im}(\chi)$ . Throughout the paper, we consider the character  $\chi$  as fixed and set  $M := K(\chi)$ .

Let  $\mathbb{P}$  be the set of finite rational primes and for  $p \in \mathbb{P}$  denote by  $v_p(n)$  the maximal exponent  $e$  such that  $p^e | n$  for any natural number  $n$ .

**2.2. Theorem 1.1.** For  $\alpha \in \text{Br}(K)$  we denote by  $\alpha^M$  the image of  $\alpha$  in  $\text{Br}(M)$  under the restriction map. The index formula [11, Theorem. 5.15(a)] gives: <sup>3</sup>

$$\text{ind}(\alpha + \chi) = |\chi| \text{ind } \alpha^M.$$

<sup>3</sup>[11, Theorem. 5.15(a)] does not require that  $K$  is a global field.

Therefore, in order to prove Theorem 1.1, we consider the following condition on the field  $K$ .

(I <sub>$m$</sub> ) For every  $\alpha \in \text{Br}(K)$  with  $\text{ind } \alpha^M = m$ , the division algebra underlying  $\alpha + \chi$  is a crossed product.

For a global field  $K$  we shall prove the existence of bounds  $b_p(\chi)$  such that (I <sub>$m$</sub> ) holds if and only if  $v_p(m) \leq b_p(\chi)$  for all  $p \in \mathbb{P}$ . The details of our proof will reveal that if (I <sub>$m$</sub> ) does not hold then there are in fact infinitely many  $\alpha \in \text{Br}(K)$  with  $\text{ind } \alpha^M = m$  such that the division algebra underlying  $\alpha + \chi$  is a noncrossed product (Remark 2.4). Then the proof of Theorem 1.1 will be completed.

**2.3. Galois Covers.** We say that a field  $L \supseteq M$  is a *cover* of  $M/K$  if  $L/K$  is Galois. In this case, we call  $m := [L : M]$  the *degree* of the cover and speak of  $L$  as an  *$m$ -cover*.

The division algebra underlying  $\alpha + \chi$  is a crossed product if and only if the division algebra underlying  $\alpha^M$  contains a maximal subfield which is Galois over  $K$  (see [10, Corollary 5] or [3, p. 381, Corollary] for complete discrete rank-1 valued  $F$ ). Such maximal subfields are characterized as the  $m$ -covers of  $M/K$  that split  $\alpha$ , where  $m = \text{ind } \alpha^M$  (see e.g. [13, Corollary 13.3]). Condition (I <sub>$m$</sub> ) is therefore equivalent to:

(A <sub>$m$</sub> ) Every  $\alpha \in \text{Br}(K)$  with  $\text{ind } \alpha^M = m$  is split by an  $m$ -cover of  $M/K$ .

*Remark 2.1.* (i) For the equivalence of (I <sub>$m$</sub> ) and (A <sub>$m$</sub> ) it is not required that  $K$  is a global field.

(ii) Condition (A <sub>$m$</sub> ) is a condition on  $M = K(\chi)$  rather than on  $\chi$ . (A <sub>$m$</sub> ) can be considered more generally for any Galois extension  $M/K$ . In fact, the form of  $M$  turns out to be irrelevant for the remaining part of §2, i.e. from now on  $M$  may be replaced by an arbitrary finite Galois extension of the global field  $K$ .

**2.4. Covers with prescribed local degrees.** By a prime  $\mathfrak{p}$  of  $K$  we mean a finite or infinite prime, and we write  $K_{\mathfrak{p}}$  for the completion at  $\mathfrak{p}$ . Let  $L$  be a cover of  $M/K$ . We call  $[L : M]_{\mathfrak{p}} := [L_{\mathfrak{P}} : M_{\mathfrak{P} \cap M}]$  the *local degree* of  $L$  at  $\mathfrak{p}$ , where  $\mathfrak{P}$  is any prime of  $L$  dividing  $\mathfrak{p}$ . Our first goal is to translate (A <sub>$m$</sub> ) to a condition about the existence of covers of  $M/K$  with prescribed local degrees at finitely many primes of  $K$  (see Proposition 2.3 below).

Let  $\alpha \in \text{Br}(K)$ . Since  $K$  is a global field, by the theorem of Albert-Hasse-Brauer-Noether (see e.g. [13, §18.4]), the splitting fields of  $\alpha$  are characterized by their local degrees, i.e. for any Galois extension  $L/K$ :

(2.1)  $L$  splits  $\alpha$  if and only if  $\text{ind}_{\mathfrak{p}} \alpha \mid [L : K]_{\mathfrak{p}}$  for all primes  $\mathfrak{p}$  of  $K$ ,

where  $\text{ind}_{\mathfrak{p}} \alpha := \text{ind } \alpha^{K_{\mathfrak{p}}}$ . Hence, for any cover  $L$  of  $M/K$ :

(2.2)  $L$  splits  $\alpha$  if and only if  $\text{ind}_{\mathfrak{p}} \alpha^M \mid [L : M]_{\mathfrak{p}}$  for all primes  $\mathfrak{p}$  of  $K$ ,

where  $\text{ind}_{\mathfrak{p}} \alpha^M := \text{ind} \alpha^{M_{\mathfrak{p}}}$  for any prime  $\mathfrak{p}$  of  $M$  dividing  $\mathfrak{p}$ . We analyze in detail the possible local indices  $\text{ind}_{\mathfrak{p}} \alpha^M$  for all  $\alpha \in \text{Br}(K)$  with  $\text{ind} \alpha^M = m$  for a given  $m$ .

For a fixed  $p \in \mathbb{P}$ , let  $u_1, u_2, \dots$  be the family of numbers  $v_p([M : K]_{\mathfrak{p}})$  where  $\mathfrak{p}$  runs over all primes of  $K$ , ordered so that  $u_1 \geq u_2 \geq \dots$ . If  $u_1 > u_2$  then the unique prime  $\mathfrak{p}$  of  $K$  with  $v_p([M : K]_{\mathfrak{p}}) = u_1$  is called *p-isolated* in  $M/K$ . We denote by  $g_p$  the gap  $u_1 - u_2$ , so that  $g_p > 0$  if and only if there is a *p-isolated* prime. We shall call a prime  $\mathfrak{p}$  of  $K$  *isolated* if it is *p-isolated* for some  $p$ .

Note that if  $M/K$  is cyclic then, as a consequence of the Chebotarev density theorem, there are no isolated primes. Moreover, any prime that is isolated in a non-cyclic extension  $M/K$  must ramify non-trivially. Hence, only finitely many primes can be isolated in any given  $M/K$ . Infinite primes are never isolated.

**Lemma 2.2.** *Let  $\alpha \in \text{Br}(K)$ . If  $\mathfrak{p}$  is *p-isolated* in  $M/K$  then*

$$(2.3) \quad v_p(\text{ind}_{\mathfrak{p}} \alpha^M) \leq \max\{v_p(\text{ind} \alpha^M) - g_p, 0\}.$$

*Proof of Lemma 2.2.* Set  $k := v_p(\text{ind}_{\mathfrak{p}} \alpha^M)$ ,  $n := v_p(\text{ind} \alpha^M)$ , and let  $u_1, u_2$  be as above. Clearly,  $n \geq k$ . The assertion to prove is:  $k = 0$  or  $n \geq k + g_p$ . Assume  $k > 0$ . Since  $v_p([M : K]_{\mathfrak{p}}) = u_1$  and  $k > 0$  we have  $v_p(\text{ind}_{\mathfrak{p}} \alpha) = k + u_1$ . Since the sum of Hasse invariants of  $\alpha$  is 0, there exists a prime  $\mathfrak{p}_1 \neq \mathfrak{p}$  of  $K$  with  $v_p(\text{ind}_{\mathfrak{p}_1} \alpha) \geq k + u_1$ . But  $v_p([M : K]_{\mathfrak{p}_1}) \leq u_2$ , hence  $n \geq v_p(\text{ind}_{\mathfrak{p}_1} \alpha^M) \geq k + u_1 - u_2 = k + g_p$ .  $\square$

Let  $m \in \mathbb{N}$ . For a finite prime  $\mathfrak{p}$  of  $K$  define  $d_{\mathfrak{p}}(m) \in \mathbb{N}$  by requiring for every  $p \in \mathbb{P}$ ,  $v_p(d_{\mathfrak{p}}(m)) = \max\{v_p(m) - g_p, 0\}$  if  $\mathfrak{p}$  is *p-isolated*, and  $v_p(d_{\mathfrak{p}}(m)) = v_p(m)$  otherwise. For a real (resp. complex) prime  $\mathfrak{p}$  of  $M$  set  $d_{\mathfrak{p}}(m) := \gcd(m, 2)$  (resp.  $d_{\mathfrak{p}}(m) := 1$ ). Clearly,  $d_{\mathfrak{p}}(m) | m$  for any  $\mathfrak{p}$ .

**Proposition 2.3.** *Condition  $(A_m)$  is equivalent to:*

$$(B_m) \quad \text{For every finite set } S \text{ of primes of } K, M/K \text{ has an } m\text{-cover } L \text{ such that } d_{\mathfrak{p}}(m) | [L : M]_{\mathfrak{p}} \text{ for any } \mathfrak{p} \in S.$$

*Proof of Proposition 2.3.*  $(B_m) \Rightarrow (A_m)$ : Let  $\alpha \in \text{Br}(K)$  with  $\text{ind} \alpha^M = m$ . We construct an  $m$ -cover  $L$  of  $M/K$  that splits  $\alpha$ . Let  $S$  be the set of primes  $\mathfrak{p}$  of  $K$  such that  $\text{ind}_{\mathfrak{p}} \alpha \neq 1$ . By assumption, there is an  $m$ -cover  $L$  of  $M/K$  such that  $d(m)_{\mathfrak{p}} | [L : M]_{\mathfrak{p}}$  for each  $\mathfrak{p} \in S$ . Let  $\mathfrak{p} \in S$  and  $p \in \mathbb{P}$ . If  $\mathfrak{p}$  is not *p-isolated* then

$$v_p(\text{ind}_{\mathfrak{p}} \alpha^M) \leq v_p(m) = v_p(d_{\mathfrak{p}}(m)) \leq v_p([L : M]_{\mathfrak{p}}).$$

If  $\mathfrak{p}$  is *p-isolated* then Lemma 2.2 implies

$$v_p(\text{ind}_{\mathfrak{p}} \alpha^M) \leq \max\{v_p(m) - g_p, 0\} = v_p(d_{\mathfrak{p}}(m)) \leq v_p([L : M]_{\mathfrak{p}}).$$

Thus,  $\text{ind}_{\mathfrak{p}} \alpha^M | [L : M]_{\mathfrak{p}}$  for any  $\mathfrak{p}$ , i.e.  $L$  splits  $\alpha$  by (2.2).

$(A_m) \Rightarrow (B_m)$ : Let  $S$  be any finite set of primes of  $K$ . We construct the element  $\alpha \in \text{Br}(K)$ , to which we apply  $(A_m)$ , by its primary decomposition  $\alpha = \prod_{p|m} \alpha_p$ . To this end, fix a  $p \in \mathbb{P}$  with  $p|m$  and let

$n := v_p(m)$ . We explain below how to choose the Hasse invariants of  $\alpha_p \in \text{Br}(K)$  such that  $\text{ind}_{\mathfrak{p}} \alpha_p^M = p^n$  for any non- $p$ -isolated  $\mathfrak{p} \in S$  and such that  $\text{ind}_{\mathfrak{p}}(\alpha_p^M) = p^{\max\{n-g_p, 0\}}$  for any  $p$ -isolated  $\mathfrak{p} \in S$ . Then  $\alpha := \prod_{p|m} \alpha_p$  clearly satisfies  $d_{\mathfrak{p}}(m) | \text{ind}_{\mathfrak{p}} \alpha^M$  for any  $\mathfrak{p} \in S$ . Since by enlarging  $S$  we can assume wlog. that  $S$  contains non- $p$ -isolated primes for each  $p|m$ , this implies  $\text{ind} \alpha^M = m$ . Applying  $(A_m)$  to  $\alpha$ , there is an  $m$ -cover  $L$  of  $M/K$  which splits  $\alpha^M$ . By (2.2), such an  $L$  satisfies  $d(m)_p | [L : M]_{\mathfrak{p}}$  for any  $\mathfrak{p} \in S$ .

We now define  $\alpha_p$  as above by its Hasse invariants, denoted  $\text{inv}_{\mathfrak{p}} \alpha_p$ . Let  $u_1, u_2$  be as above. By enlarging  $S$ , assume wlog. that  $S$  contains two primes  $\mathfrak{p}_1, \mathfrak{p}_2$  with  $v_p([M : K]_{\mathfrak{p}_i}) = u_i$ . (Either  $\mathfrak{p}_1$  is  $p$ -isolated or  $M/K$  has no  $p$ -isolated primes.) Set  $\text{inv}_{\mathfrak{p}} \alpha_p := 0$  for any  $\mathfrak{p} \notin S$ . At every  $\mathfrak{p} \in S \setminus \{\mathfrak{p}_1, \mathfrak{p}_2\}$  choose  $\text{inv}_{\mathfrak{p}} \alpha_p$  to be of order  $p^r$  where  $r = n + v_p([M : K]_{\mathfrak{p}})$ . The order of all invariants we have set so far is at most  $p^{n+u_2}$ . We can thus choose  $\text{inv}_{\mathfrak{p}_2} \alpha_p$  of order  $p^{n+u_2}$  such that  $x := \sum_{\mathfrak{p} \neq \mathfrak{p}_1} \text{inv}_{\mathfrak{p}} \alpha_p$  has order equal to  $p^{n+u_2}$ . (In the case  $p^{n+u_2} = 2$  we further assume wlog. that  $|S|$  is even.) Setting  $\text{inv}_{\mathfrak{p}_1} \alpha_p := -x$  defines an  $\alpha_p \in \text{Br}(K)$  with  $\text{ind}_{\mathfrak{p}}(\alpha_p^M) = p^n$  for every  $\mathfrak{p} \in S \setminus \{\mathfrak{p}_1\}$  and with  $\text{ind}_{\mathfrak{p}_1} \alpha_p^M = p^{n+u_2-u_1} = p^{n-g_p}$  if  $n \geq g_p$  and 1 otherwise, as desired.  $\square$

*Remark 2.4.* The proof of Proposition 2.3 shows that if there are noncrossed products  $\alpha + \chi$  with  $\text{ind}(\alpha^M) = m$  then there are infinitely many such noncrossed products. Indeed, if  $(B_m)$  fails for a set  $S_0$ , it fails for every set  $S$  containing  $S_0$ . The proof reveals that for every such set  $S$ , there is an  $\alpha$  whose Hasse invariants are non-zero at primes of  $S$  and  $\alpha + \chi$  is a noncrossed product. In particular, there are infinitely many such classes  $\alpha$ .

For a prime  $\mathfrak{p}$  of  $K$  we say the cover  $L$  has *full local degree* at  $\mathfrak{p}$  if  $[L : M]_{\mathfrak{p}} = [L : M]$  for finite  $\mathfrak{p}$ , or  $[L : M]_{\mathfrak{p}} = \gcd(2, [L : M])$  for real  $\mathfrak{p}$ , or if  $\mathfrak{p}$  is complex. For a set  $S$  of primes of  $K$  we say  $L$  has *full local degree in  $S$*  if  $L$  has full local degree at each  $\mathfrak{p} \in S$ . If  $\mathfrak{p}$  is not isolated then the condition  $d_{\mathfrak{p}}(m) | [L : M]_{\mathfrak{p}}$  is equivalent to saying that  $L$  has full local degree at  $\mathfrak{p}$ .

**Lemma 2.5.** *Let  $m' | m$ . Suppose there is a finite set  $S_0$  of non-isolated primes of  $K$  such that any  $m$ -cover of  $M/K$  with full local degree in  $S_0$  contains an  $m'$ -cover. Then  $(B_m)$  implies  $(B_{m'})$ .*

*Proof.* For a given finite set  $S$  let  $L$  be an  $m$ -cover as predicted by  $(B_m)$  for  $S \cup S_0$ . Since the primes in  $S_0$  are non-isolated,  $L$  has full local degree in  $S_0$ . By assumption,  $L$  contains an  $m'$ -cover  $L'$  of  $M/K$ . For all primes  $\mathfrak{p}$  of  $K$ ,  $d_{\mathfrak{p}}(m) | [L : M]_{\mathfrak{p}}$  implies  $d_{\mathfrak{p}}(m') | [L' : M]_{\mathfrak{p}}$ . Hence,  $L'$  satisfies the conditions required by  $(B_{m'})$ .  $\square$

**2.5. Reduction to prime powers.** Our next step is to reduce  $(B_m)$  from arbitrary  $m \in \mathbb{N}$  to prime-powers. Except for the part concerning

the characteristic of  $K$  (Lemma 2.7 below), this reduction is identical to the corresponding one in [9].

Let  $m = \prod p^{n_p}$  be the prime factorization. By taking field composita of covers, if  $(B_{p^{n_p}})$  holds for all  $p|m$  then  $(B_m)$  holds. We show

**Proposition 2.6.**  $(B_m)$  holds if and only if  $(B_{p^{n_p}})$  holds for all  $p|m$ .

We first treat the wild case separately:

**Lemma 2.7.** If  $p = \text{char } K$  then  $(B_{p^n})$  holds for all  $n \in \mathbb{N}$ .

*Proof.* Let  $n \in \mathbb{N}$  and  $S$  a finite set of primes of  $K$ . For every  $\mathfrak{p} \in S$  there is a cyclic  $p^n$ -extension  $L'(\mathfrak{p})/K_{\mathfrak{p}}$  which is disjoint from  $M_{\mathfrak{p}}$  (see [12, Satz 10.4]<sup>4</sup>). By the Grunwald-Wang theorem, there is a cyclic  $p^n$ -extension  $L'/K$  whose completion at  $\mathfrak{p}$  is  $L'_{\mathfrak{p}} = L'(\mathfrak{p})$  for all  $\mathfrak{p} \in S$ . Let  $L := L'M$ . Since  $L'_{\mathfrak{p}} \cap M_{\mathfrak{p}} = K_{\mathfrak{p}}$ , one has  $[L : M]_{\mathfrak{p}} = p^n$  for all  $\mathfrak{p} \in S$ . Thus,  $L$  is a  $p^n$ -cover of  $M/K$  with full local degree in  $S$ .  $\square$

It remains to show that  $(B_m)$  implies  $(B_{p^{n_p}})$  for all  $p|m$  with  $p \neq \text{char } K$ .

*Proof of Prop. 2.6.* Let  $p|m$  with  $p \neq \text{char } K$ . By [9, §7, p. 325, Corollary], there are infinitely many primes  $\mathfrak{p}$  of  $K$  such that any  $m$ -cover of  $M/K$  with full local degree at  $\mathfrak{p}$  contains a  $p^n$ -cover of  $M/K$ . (Note that the assumption  $M/K$  cyclic is never used in the proof of [9, §7, p. 325, Corollary].) Since there are only finitely many isolated primes, we can choose such a  $\mathfrak{p}$  that is non-isolated. The proof is completed by setting  $S_0 := \{\mathfrak{p}\}$  in Lemma 2.5.  $\square$

**2.6. An invariant subgroup.** We are now in the position to complete the proof of Theorem 1.1. As outlined in §2.2, and using Propositions 2.3 and 2.6, it remains to prove Proposition 2.8 below. Let  $p \in \mathbb{P}$  be fixed.

**Proposition 2.8.** For any  $n \in \mathbb{N}$ ,  $(B_{p^n})$  implies  $(B_{p^{n-1}})$ .

Indeed, the bound  $b_p(\chi)$  of Theorem 1.1 is the maximal  $n$  for which  $(B_{p^n})$  holds for  $M = K(\chi)$  if such a maximum exists, and  $b_p(\chi) = \infty$  otherwise. For more details on the description of  $b_p(\chi)$  see Corollary 2.11 below.

For any cover  $L$  of  $M/K$  we consider the group extension

$$(2.4) \quad 1 \rightarrow \text{Gal}(L/M) \rightarrow \text{Gal}(L/K) \rightarrow \text{Gal}(M/K) \rightarrow 1.$$

We will analyze several kinds of constraints that are imposed on (2.4) by the condition that  $L$  has full local degree in  $S_0$ , for certain chosen sets  $S_0$ . More precisely, after showing that the kernel  $A := \text{Gal}(L/M)$  can be assumed to be abelian, we focus on constraints regarding the

---

<sup>4</sup>Koch's book was translated to English. However, Theorem 10.4 in the English version contains a typo: "finitely generated" should be replaced by "on countably many generators".

conjugation action of  $B := \text{Gal}(M/K)$  on  $A$ . The analysis of this action is the main ingredient in the proofs of both Proposition 2.8 and Theorem 1.2 below.

In view of Lemma 2.7 we assume from now on that  $p \neq \text{char } K$ . Fix  $p^n$  and set  $T := M \cap K(\mu_{p^\infty})$ . For the proof of Proposition 2.8, it will suffice to analyze the action of  $\text{Gal}(M/T)$  on  $A$ .

**Lemma 2.9.** *There exists a finite set  $S_0$  of non-isolated primes of  $K$  such that for any  $p^n$ -cover  $L$  of  $M/K$  with full local degree in  $S_0$ : the kernel  $A$  is abelian, the group  $\text{Gal}(M/T)$  acts trivially on  $A$ , and  $A$  has rank at most 2.*

*Proof.* At first fix a  $\sigma \in \text{Gal}(M/T)$ . By the Chebotarev density theorem, the Galois extension  $M(\mu_{p^n})/K$  has infinitely many unramified finite primes  $\mathfrak{P}$  of  $M(\mu_{p^n})$  whose Frobenius element restricts to the identity on  $K(\mu_{p^n})$  and to  $\sigma$  on  $M$ . Of those infinitely many  $\mathfrak{P}$  choose one such that  $\mathfrak{p} := \mathfrak{P} \cap K$  is non- $p$ -isolated in  $M/K$  and  $p$  does not divide the norm  $N(\mathfrak{p})$ . (There are only finitely many  $\mathfrak{P}$  that do not satisfy this, since  $p \neq \text{char } K$ .) Since  $p \nmid N(\mathfrak{p})$  and  $\mu_{p^n} \subset K_{\mathfrak{p}}$ , we have  $N(\mathfrak{p}) \equiv 1 \pmod{p^n}$ .

Assume a  $p^n$ -cover  $L$  of  $M/K$  has full local degree at the chosen  $\mathfrak{p}$ . Let  $\mathfrak{P}$  be a prime of  $L$  dividing  $\mathfrak{p}$ . The decomposition group  $\text{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$  then equals  $\text{Gal}(L/M^\sigma)$  where  $M^\sigma$  is the fixed field of  $\sigma$ . We will show that  $\text{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$  is abelian, thus  $\sigma$  acts trivially on  $\text{Gal}(L/K)$ : Since  $\text{char } K \nmid N(\mathfrak{p})$ ,  $L_{\mathfrak{P}}/K_{\mathfrak{p}}$  is tame. Therefore,  $\text{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$  is a metacyclic group, generated by the inertia group  $I_{\mathfrak{P}}$  and the Frobenius element, and the Frobenius acts on  $I_{\mathfrak{P}}$  by raising each element to the power  $N(\mathfrak{p})$ . Since  $\mathfrak{p}$  is unramified in  $M$ ,  $|I_{\mathfrak{P}}|$  divides  $p^n$ . Hence  $\text{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$  is abelian, because  $N(\mathfrak{p}) \equiv 1 \pmod{p^n}$ .

Now let  $\Sigma$  be a set of generators of  $\text{Gal}(M/T)$ , or  $\Sigma = \{1\}$  if  $M = T$ . For each  $\sigma \in \Sigma$  choose a prime  $\mathfrak{p}_\sigma$  as described in the first paragraph of the proof. Then  $S_0 := \{\mathfrak{p}_\sigma \mid \mathfrak{p} \in \Sigma\}$  has the desired property.  $\square$

By Lemma 2.5, Proposition 2.8 is completed once we show

**Proposition 2.10.** *Let  $S_0$  be as in Lemma 2.9. Any  $p^n$ -cover of  $M/K$  with full local degree in  $S_0$  contains a  $p^{n-1}$ -cover of  $M/K$ .*

*Proof.* We have assumed  $p \neq \text{char } K$ . Let  $B = \text{Gal}(M/K)$ . Let  $L$  be a  $p^n$ -cover of  $M/K$  with full local degree in  $S_0$ . By Lemma 2.9, the kernel  $A$  is abelian. The subgroup  $A[p]$  of  $p$ -torsion elements is a characteristic subgroup and hence invariant under the action of  $B$  (we say  $B$ -invariant). It suffices to find a  $B$ -invariant subgroup  $A_0 \leq A[p]$  of order  $p$ ; then the fixed field  $L^{A_0}$  is the desired  $p^{n-1}$ -cover. If  $A$  is cyclic then  $A[p]$  itself is such a subgroup, hence assume  $A$  non-cyclic for the rest of the proof.

Recall that  $A[p]$  is an  $\mathbb{F}_p$ -vector space and that any action of some group  $H$  on  $A[p]$  is a representation of  $H$  over  $\mathbb{F}_p$ . In this sense, the



$H$ -invariant subgroups of order  $p$  are the  $H$ -invariant subspaces of dimension 1.

By Lemma 2.9,  $B$  acts on  $A$  through  $\text{Gal}(T/K)$ . Let  $\text{Gal}(T/K) = P \oplus C$  with  $P$  the  $p$ -part and  $|C|$  prime-to- $p$ . Then  $|C|$  divides  $p - 1$ . Since  $|C|$  is prime to  $p$ , any representation of  $C$  over  $\mathbb{F}_p$  is semisimple and hence decomposes into a product of irreducible representations. Since  $\mathbb{F}_p$  contains the  $|C|$ -th roots of unity, the irreducible representations of  $C$  are of dimension 1. Thus, there is a  $C$ -invariant subgroup  $A_0 \leq A[p]$  of order  $p$ .

By Lemma 2.9,  $A$  has rank 2, i.e.  $A[p] \cong C_p \times C_p$ . This group has exactly  $p + 1$  order  $p$  subgroups, say  $A_0, \dots, A_p$ , which are permuted by the action of  $B$ . Thus, we have an induced action of  $B$  on the set of indices  $\{0, \dots, p\}$ .

We know  $A_0$  is  $C$ -invariant. If  $A_0$  is  $P$ -invariant then  $A_0$  is  $B$ -invariant and we are done. Assume  $A_0$  is not  $P$ -invariant. Since  $P$  is a  $p$ -group there are two  $P$ -orbits on  $\{0, \dots, p\}$ , say  $\{0, \dots, p - 1\}$  and  $\{p\}$ . Since  $P$  and  $C$  commute and  $A_0$  is  $C$ -invariant, each of  $A_0, \dots, A_{p-1}$  is also  $C$ -invariant. Hence the remaining subgroup  $A_p$  is  $C$ -invariant and  $P$ -invariant and we are done.  $\square$

**2.7. Summary.** Let  $\chi \in \text{Hom}(G_K, \Delta/\Gamma)$  and  $M = K(\chi)$ .

**Corollary 2.11.** *The bound  $b_p(\chi)$  is the maximal  $n$  such that for every finite set  $S$  of primes of  $K$  there is a  $p^n$ -cover  $L$  of  $M/K$  with the following properties:*

- (i)  $d_{\mathfrak{p}}(p^n) \mid [L : M]_{\mathfrak{p}}$  for any  $\mathfrak{p} \in S$ ,
- (ii)  $A = \text{Gal}(L/M)$  is abelian of rank at most 2,
- (iii)  $\text{Gal}(M/T)$  acts trivially on  $A$ .

If no maximal  $n$  exists then  $b_p(\chi) = \infty$ .

*Proof.* Let  $S_0$  be a finite set of primes of  $K$  that are non-isolated in  $M/K$ . Suppose that any  $p^n$ -cover of  $L$  with full local degree in  $S_0$  has a certain property. Then this property can be added to the condition  $(B_{p^n})$  without changing the truth value of  $(B_{p^n})$ , because the set  $S$  in  $(B_{p^n})$  can be enlarged by  $S_0$ . By Lemma 2.9, this argument applies to the properties (ii) and (iii). Hence, the Corollary is a consequence of Proposition 2.8.  $\square$

*Remark 2.12.* Regarding condition (i) in Corollary 2.11, if  $\mathfrak{p}$  is not isolated then  $d_{\mathfrak{p}}(p^n) \mid [L : M]_{\mathfrak{p}}$  is equivalent to saying that  $L$  has full local degree at  $\mathfrak{p}$ .

Regarding condition (iii) in Corollary 2.11, if  $M$  and  $K(\mu_{p^\infty})$  are disjoint over  $K$  then (iii) is equivalent to saying that the group extension (2.4) is central.

## 3. FINITENESS OF BOUNDS

**3.1. The exponents of kernels.** Suppose we are in the setup described in §2.1. Let  $p \in \mathbb{P}$  be fixed and different from  $\text{char } K$ . Denote by  $p^s$  the number of  $p$ -power roots of unity in  $M$  and by  $r$  the maximal number for which  $\mu_{2^r} \subseteq M(\sqrt{-1})$ . As before set  $T := K(\mu_{p^\infty}) \cap M$ .

In §2 we showed that if a cover  $L$  of  $M/K$  has full local degree in  $S_0$  then the choice of  $S_0$  can put constraints on the action of  $\text{Gal}(M/T)$  on  $A = \text{Gal}(L/M)$  to the extent that this action is even trivial. This was sufficient to prove the existence of the bounds. Now, in order to prove the finiteness of the bounds, we analyze constraints on the action of the entire group  $B = \text{Gal}(M/K)$  on  $A$ . The set  $S_0$  for this purpose will be constructed from the families  $Q_\sigma$  that we define next for each  $\sigma \in B$ .

Fix an element  $\sigma \in B$  and let  $f_\sigma$  be the order of the restriction  $\sigma|_T$  of  $\sigma$  to  $T$ . We define  $Q_\sigma$  to be the set of all primes  $\mathfrak{p}$  of  $K$ , unramified in  $M$ , whose Frobenius automorphism in  $M/K$  is  $\sigma$ , and such that the norm  $N(\mathfrak{p})$  is prime to  $p$  and is of order strictly greater than  $f_\sigma$  as an element of  $(\mathbb{Z}/p^{s+1}\mathbb{Z})^*$  (resp. mod  $(\mathbb{Z}/2^{r+2}\mathbb{Z})^*$  if  $p = 2$ ).

**Lemma 3.1.** *For every  $\sigma \in B$ , the set  $Q_\sigma$  is infinite.*

*Proof.* Assume without loss of generality that  $\sqrt{-1} \in M$ . Otherwise, repeat the proof for a lift  $\tau \in \text{Gal}(M(\sqrt{-1})/K)$  of  $\sigma$  to deduce that  $Q_\tau$  is infinite. Since  $Q_\tau \subseteq Q_\sigma$  and  $f_\tau \geq f_\sigma$  the assertion for  $\sigma$  follows. Note that under this assumption we have  $r = s$ , so we will use only  $s$  in the rest of the proof. Set  $T' := K(\mu_{p^{s+1}})$  (resp.  $T' := K(\mu_{2^{s+2}})$  if  $p = 2$ ) and note that  $T' \cap M = T$ .

We first claim that  $\text{Gal}(T'/K)$  contains an element  $\sigma'$  of order greater than  $f_\sigma$  whose restriction to  $T$  is  $\sigma|_T$ . The group  $\text{Gal}(T/T^\sigma)$  is naturally identified with a subgroup  $U$  of  $(\mathbb{Z}/p^s\mathbb{Z})^*$ , and  $\text{Gal}(T'/T^\sigma)$  is identified with the full preimage of  $U$  under the natural projection  $\pi : (\mathbb{Z}/p^{s+1}\mathbb{Z})^* \rightarrow (\mathbb{Z}/p^s\mathbb{Z})^*$  (resp.  $\pi : (\mathbb{Z}/2^{s+2}\mathbb{Z})^* \rightarrow (\mathbb{Z}/2^s\mathbb{Z})^*$  if  $p = 2$ ). The claim follows since each element of  $(\mathbb{Z}/p^s\mathbb{Z})^*$  has a preimage under  $\pi$  of a greater order.

Since  $\sigma$  and  $\sigma'$  agree on  $T$ , Chebotarev's density theorem implies that there are infinitely many primes  $\mathfrak{p}$  of  $K$ , with  $p \nmid N(\mathfrak{p})$ , whose Frobenius automorphism is  $\sigma'$  in  $T'/K$  and is  $\sigma$  in  $M/K$ . Such primes are in  $Q_\sigma$  since the order of the norm of  $\mathfrak{p}$  as an element in  $(\mathbb{Z}/p^{s+1}\mathbb{Z})^*$  (resp. in  $(\mathbb{Z}/2^{s+2}\mathbb{Z})^*$ ) is the same as the order of their Frobenius automorphism in  $K(\mu_{p^{s+1}})/K$  (resp. in  $K(\mu_{2^{s+2}})/K$ ).  $\square$

For a prime  $\mathfrak{p}$  of  $K$  denote by  $e_{\mathfrak{p}}(L/K)$  the ramification index of  $\mathfrak{p}$  in a Galois extension  $L/K$ .

**Lemma 3.2.** *Let  $S_0$  be as in Lemma 2.9 and let  $\sigma \in B$ . Suppose that a  $p^n$ -cover  $L$  of  $M/K$  has full local degree in  $S_0$  and at  $\mathfrak{p} \in Q_\sigma$ . Then  $e_{\mathfrak{p}}(L/K) \mid p^s$  if  $p$  is odd and  $e_{\mathfrak{p}}(L/K) \mid 2^{r+1}$  if  $p = 2$ .*

*Proof.* By Lemma 2.9, the kernel  $A$  is abelian and the action of  $B$  on  $A$  factors through the action of  $\text{Gal}(M/T)$ . Thus,  $\sigma$  acts on the inertia group  $I \subseteq A$  of  $\mathfrak{p}$  in  $L/K$  as an automorphism of order at most  $f_\sigma$ .

Assume on the contrary there is an element  $a \in I$  of order  $p^{s+1}$  (resp.  $2^{r+2}$  if  $p = 2$ ). Since  $\mathfrak{p}$  is tamely ramified in  $L$ ,  $\sigma$  acts on  $I$  by raising each element to the power  $N(\mathfrak{p})$  and hence defines an automorphism of order greater than  $f_\sigma$  on  $\langle a \rangle$ , contradiction.  $\square$

**Proposition 3.3.** *Assume the  $p$ -Sylow subgroup of  $B$  is non-cyclic. There exists a finite set  $S_0$  of non-isolated primes of  $K$  such that for any  $p^n$ -cover  $L$  of  $M/K$  with full local degree in  $S_0$ :  $\text{Gal}(L/M)$  is abelian of rank at most 2 and exponent at most  $p^s$  (resp.  $2^{r+2}$  if  $p = 2$ ).*

If the  $p$ -Sylow subgroup of  $B$  is non-cyclic then Proposition 3.3 allows us to improve on Corollary 2.11 by adding the following property to the list:

(iv)  $\exp A|p^s$  if  $p$  is odd and  $\exp A|2^{r+2}$  if  $p = 2$ .

In particular, since  $A$  has rank at most 2,  $b_p(\chi) \leq 2s$  if  $p$  is odd and  $b_p(\chi) \leq 2(r+2)$  if  $p = 2$ . This proves Theorem 1.2.

Proposition 3.3 relies on the following group theoretical proposition, whose proof is the subject of subsection §3.2 below.

**Proposition 3.4.** *Let*

$$(3.1) \quad 1 \rightarrow A \rightarrow G \xrightarrow{\pi} B \rightarrow 1$$

*be an extension of non-trivial abelian  $p$ -groups  $A, B$ . If  $B$  is non-cyclic and  $\pi^{-1}\langle x \rangle$  is cyclic for all  $x \in B$  then  $|A| = 2$ .*

*Proof of Proposition 3.3.* Replacing  $K$  with the fixed field of the  $p$ -Sylow subgroup of  $B$  we can assume wlog. that  $B$  is a  $p$ -group. By assumption  $B$  is non-cyclic (abelian).

Choose  $S_0$  to be the set from Lemma 2.9 joined with one non-isolated prime  $\mathfrak{p}_\sigma \in Q_\sigma$  for each  $\sigma \in B$ . Suppose  $L$  is a  $p^n$ -cover of  $M/K$  with full local degree in  $S_0$ .

By Lemma 2.9,  $A$  is abelian of rank at most 2. Since the  $p^s$ -torsion subgroup  $A[p^s]$  is a characteristic subgroup of  $A$ , it is a normal subgroup of  $\text{Gal}(L/K)$  and hence the fixed field  $L_0 := L^{A[p^s]}$  is Galois over  $K$ . If  $p = 2$  then we consider  $L_0 := L^{A[2^{r+1}]}$  instead, which is also Galois over  $K$ . To prove our claim it suffices to show that  $L_0 = M$  (resp.  $[L_0 : M] \leq 2$  if  $p = 2$ ).

Fix an element  $\sigma \in B$  and let  $\mathfrak{P}_\sigma$  be a prime of  $L$  which divides  $\mathfrak{p}_\sigma$ . Let  $I_\sigma \subseteq A$  be the inertia group of  $\mathfrak{P}_\sigma$  in  $L/K$ . By Lemma 3.2,  $|I_\sigma| \leq p^s$  (resp.  $|I_\sigma| \leq 2^{r+1}$ ) and hence  $I_\sigma \subseteq A[p^s]$  (resp.  $I_\sigma \subseteq A[2^{r+1}]$ ). Thus,  $L_0/K$  is unramified at  $\mathfrak{p}_\sigma$  and hence  $\mathfrak{P}_\sigma \cap L_0$  has a cyclic decomposition group in  $L_0/K$ . Since  $L_0$  has full local degree at  $\mathfrak{p}$ , the decomposition group of  $\mathfrak{P}_\sigma \cap L_0$  in  $L_0/K$  is  $\text{Gal}(L_0/M^\sigma)$  and hence  $L_0/M^\sigma$  is a cyclic extension.

Since  $L_0/M^\sigma$  is cyclic for all  $\sigma \in B$  and since  $B$  is non-cyclic, Proposition 3.4 applied to the group extension

$$1 \rightarrow \text{Gal}(L_0/M) \rightarrow \text{Gal}(L_0/K) \rightarrow \text{Gal}(M/K) \rightarrow 1$$

shows  $L_0 = M$  (resp.  $[L_0 : M] \leq 2$  if  $p = 2$ ), proving the claim.  $\square$

**3.2. Central group extensions.** The remaining ingredient is a proof of Proposition 3.4. We begin with elementary properties of commutators in a central group extension

$$(3.2) \quad 1 \rightarrow A \rightarrow G \rightarrow B \rightarrow 1$$

of abelian groups  $A, B$ . Let  $s : B \rightarrow G$  be a section of  $G \rightarrow B$  (not necessarily a homomorphism).

**Lemma 3.5.** *Commutators in  $G$  are bimultiplicative. The map*

$$\beta : B \times B \rightarrow A, (x, y) \mapsto [s(x), s(y)]$$

*does not depend on the choice of  $s$  and is bimultiplicative.*

*Proof.* Since  $[G, G] \subseteq A \subseteq Z(G)$  we have

$$[ab, x] = abxb^{-1}a^{-1}x^{-1} = a(bxb^{-1}x^{-1})xa^{-1}x^{-1} = [a, x][b, x].$$

Similarly one checks  $[x, ab] = [x, a][x, b]$ , i.e. commutators are bimultiplicative. The statement about  $\beta$  follows from this.  $\square$

We next look at the meaning of the condition that  $\pi^{-1}\langle x \rangle$  is cyclic for  $x \in B$ . For  $x = 1$  it means  $A$  is cyclic, and for  $x \neq 1$  one has:

**Lemma 3.6.** *Assume  $A$  is cyclic. For  $x \in B, x \neq 1$ ,  $\pi^{-1}\langle x \rangle$  is cyclic if and only if  $A$  is trivial or generated by  $s(x)^{\text{ord } x}$ .*

In order to prove Proposition 3.4 we now assume  $A, B$  are non-trivial  $p$ -groups and  $A$  is cyclic. The map

$$\gamma : B[p] \rightarrow A/A^p, x \mapsto s(x)^p$$

is obviously independent of the choice of  $s$ .

**Lemma 3.7.** *Assume  $A, B$  are non-trivial  $p$ -groups and  $A$  is cyclic.*

- (i) *For  $x \in B[p], x \neq 1$ ,  $\pi^{-1}\langle x \rangle$  is cyclic if and only if  $\gamma(x) \neq 1$ .*
- (ii) *If  $p$  is odd then  $\gamma$  is a homomorphism.*
- (iii) *If  $p = 2$  then  $\gamma$  is a homomorphism if and only if  $\beta(x, y) \in A^2$  for all  $x, y \in B[2]$ .*

*Proof.* (i) is Lemma 3.6. Since  $[G, G] \subseteq A \subseteq Z(G)$ , we have  $(s(x)s(y))^p = s(x)^p s(y)^p \beta(x, y)^{\frac{p(p-1)}{2}}$  for all  $x, y \in B$ . In particular, for all  $x, y \in B[p]$ :

$$\gamma(xy) = s(xy)^p A^p = (s(x)s(y))^p A^p = \gamma(x)\gamma(y)\beta(x, y)^{\frac{p(p-1)}{2}}.$$

Thus  $\gamma$  is a homomorphism if and only if  $\beta(x, y)^{\frac{p(p-1)}{2}} \in A^p$ . If  $p = 2$  then  $\frac{p(p-1)}{2} = 1$ , proving (iii). For  $p$  odd we use Lemma 3.5 to see that  $\beta(x, y) \in A[p]$  for all  $x, y \in B[p]$ , so the term  $\beta(x, y)^{\frac{p(p-1)}{2}}$  vanishes.  $\square$

*Proof of Proposition 3.4.* Let  $A, B$  be non-trivial abelian  $p$ -groups,  $A$  cyclic and  $B$  non-cyclic. By hypothesis and (i) of Lemma 3.7,  $\gamma(x) \neq 1$  for all  $x \in B[p], x \neq 1$ . Therefore, if  $\gamma$  is a homomorphism then it is injective, in contradiction to  $A$  being cyclic and  $B$  non-cyclic. Hence,  $\gamma$  is not a homomorphism. By Lemma (ii) and (iii) of 3.7, we have  $p = 2$  and an element in  $A[2] \setminus A^2$ . This implies  $|A| = 2$ .  $\square$

#### 4. EXAMPLES

Suppose we are in the setup described in §2.1. For  $p \in \mathbb{P}$ , let  $p^{s_p(M)}$  denote the number of  $p$ -power roots of unity in  $M$ .

If  $\alpha + \chi$  has index equal to  $|\chi|$  then the division algebra contained in  $\alpha + \chi$  is a crossed product, because  $\alpha$  is split by  $K(\chi)$ . Therefore, non-crossed products of index  $p^2$  are possible only if  $|\chi| = p$ , in particular only if  $\chi$  is cyclic.

Suppose  $\chi$  is non-cyclic with  $|\chi| = p^2$ . If  $b_p(\chi) = 0$  then the fiber over  $\chi$  contains infinitely many noncrossed products of index  $p|\chi|$ . By Theorem 1.2, this happens, e.g., whenever  $s_p(M) = 0$ . The present section gives examples of bicyclic  $\chi$  with  $|\chi| = p^2$  and  $b_p(\chi) = 0$  but  $s_p(M) \geq 1$ . We point out that such a phenomenon is in contrast to the case of cyclic  $\chi$  for which one always has  $b_p(\chi) \geq s_p(M)$  (see [9]).

For  $p = 2$  an example as described above was given over  $K = \mathbb{Q}$  in [8] and over  $K = \mathbb{F}_q(t)$  for all  $q \equiv 3 \pmod{8}$  in [7, Example 2.8]. These turn out to be special cases of our Examples 4.1 and 4.3 below.

We start with  $K = \mathbb{Q}$  and  $p = 2$ :

*Example 4.1.* Let  $q, l$  be odd primes such that  $q \equiv 3 \pmod{4}, q \not\equiv -l \pmod{8}$  and  $q$  a non-square modulo  $l$ . Note that for any odd prime  $l$  a suitable  $q$  can be chosen using Dirichlet's theorem.<sup>5</sup> Let  $\mathbb{Q}(\chi) = \mathbb{Q}(\sqrt{q}, \sqrt{-l})$  Corollary 2.11 and the following claim show  $b_p(\chi) = 0$ .

*Claim.* The extension  $M/\mathbb{Q}$  has no isolated primes and there is no 2-cover  $L$  of  $M/K$  with local degree  $[L : M]_l = 2$ .

*Proof.* Set  $K_1 := \mathbb{Q}(\sqrt{q}), K_2 := \mathbb{Q}(\sqrt{-l})$  and  $M := K(\chi)$ .

We first check that  $M/\mathbb{Q}$  has no isolated primes. The prime  $l$  ramifies in  $K_2$  and is inert in  $K_1$ , so  $[M : \mathbb{Q}]_l = 4$ . *Case  $l \equiv 3 \pmod{4}$ :* By reciprocity,  $l$  is a square modulo  $q$ , hence  $-l$  is a non-square modulo  $l$ . The prime  $q$  thus ramifies in  $K_q$  and is inert in  $K_2$ , so  $[M : \mathbb{Q}]_q = 4$ . *Case  $l \equiv 1 \pmod{4}$ :* Since  $q \not\equiv -l \pmod{8}$ , we have  $\mathbb{Q}_2(\sqrt{q}) \neq \mathbb{Q}_2(\sqrt{-l})$ , so  $[M : \mathbb{Q}]_2 = 4$ . In any case,  $M/\mathbb{Q}$  has no isolated prime.

Now assume  $L$  is a 2-cover of  $M/\mathbb{Q}$  with full local degree at  $l$ . Since  $K_1$  is real and  $M$  is not,  $M/K_1$  does not have a cyclic 2-cover. Since  $q \equiv 3 \pmod{4}$ ,  $-1$  is not a square in  $\mathbb{Q}_q$ . This implies that  $\mathbb{Q}_q$  does not have any totally ramified degree 4 extension, so that any ramified quadratic

<sup>5</sup>Using the reciprocity law, it is also possible to choose a suitable  $l$  for any prime  $q \equiv 3 \pmod{4}$ .

extension of  $\mathbb{Q}_q$  cannot have a cyclic 2-cover. Thus, globally,  $K_1/\mathbb{Q}$  does not have a cyclic 2-cover. The inertia field of  $l$  in  $L/\mathbb{Q}$  contains  $K_1$  and is cyclic over  $\mathbb{Q}$ , thus is equal to  $K_1$ . This is a contradiction because  $L$  is then a cyclic 2-cover of  $M/K_1$ .  $\square$

*Remark.* (i) Suppose  $\mathbb{Q}(\chi)/\mathbb{Q}$  is as in Example 4.1. Consider  $\alpha \in \text{Br}(\mathbb{Q})$  such that  $\text{ind } \alpha = 8$  and  $\text{ind } \alpha^{\mathbb{Q}(\chi)} = 2$ . Since  $l$  is not 2-isolated in  $\mathbb{Q}(\chi)$ , we can find such an  $\alpha$  with  $\text{ind}_l \alpha = 8$ . Since  $\mathbb{Q}(\chi)/\mathbb{Q}$  does not have a 2-cover  $L$  with  $[L : \mathbb{Q}(\chi)]_l = 2$ , no 2-cover of  $M/K$  splits  $\alpha$ . Hence, the underlying division algebra of  $\alpha + \chi$  is a noncrossed product of index 8.

(ii) In Example 4.1 we can choose  $(l, q) = (3, 11), (5, 7), (7, 3)$ , etc. The example in [8] is the case  $l = 7$  and  $q = 3$ .

We now turn to arbitrary global fields  $K$  and a prime  $p \neq \text{char } K$ . Example 4.1 does not generalize immediately because its proof uses a real prime. The following argument uses a third finite prime instead of a real prime:

**Proposition 4.2.** *Let  $K$  be a global field and let  $p \in \mathbb{P}$  with  $p \neq \text{char } K$ . Assume  $s := s_p(K) > 0$ . Let  $\mathfrak{p}$  be any prime of  $K$  with  $p \nmid N(\mathfrak{p})$ . There exists a bicyclic extension  $M/K$  with group  $C_{p^s} \times C_{p^s}$  and without isolated primes such that no  $p$ -cover  $L$  of  $M/K$  has  $[L : M]_{\mathfrak{p}} = p$ .*

*Proof.* By Chebotarev's density theorem, there are primes  $\mathfrak{q}_1, \mathfrak{q}_2$  of  $K$  with  $N(\mathfrak{q}_i) \equiv 1 \pmod{p^s}$  but  $N(\mathfrak{q}_i) \not\equiv 1 \pmod{p^{s+1}}$ . By the Grunwald-Wang theorem there are cyclic extensions  $K_i/K$  of degree  $[K_i : K] = p^s$ , such that in  $K_1$ :  $\mathfrak{p}$  is inert,  $\mathfrak{q}_1$  is totally ramified,  $\mathfrak{q}_2$  splits completely, and in  $K_2$ :  $\mathfrak{q}_1$  is inert and  $\mathfrak{p}, \mathfrak{q}_2$  are totally ramified. Since  $\mathfrak{p}$  and  $\mathfrak{q}_1$  both have full local degree in  $M$ ,  $M/K$  has no isolated primes.

Since  $N(\mathfrak{q}_1) \not\equiv 1 \pmod{p^{s+1}}$  and  $\mathfrak{q}_1$  is totally ramified in  $K_1/K$ ,  $K_1/K$  does not have a cyclic  $p$ -cover. Similarly, considering  $\mathfrak{q}_2$ ,  $M/K_1$  does not have a cyclic  $p$ -cover.

Assume on the contrary there is a  $p$ -cover  $L$  of  $M/K$  with  $[L : M]_{\mathfrak{p}} = p$ . Since the inertia field of  $\mathfrak{p}$  contains  $K_1$  and is cyclic over  $K$ , it equals  $K_1$ . This shows that  $L$  is a cyclic  $p$ -cover of  $M/K_1$ , contradiction.  $\square$

*Example 4.3.* Let  $p \in \mathbb{P}$  and  $K = \mathbb{F}_q(t)$  for  $q \equiv 1 \pmod{p}$ , so that  $s := s_p(K) > 0$ . Assume  $a \notin (K^\times)^p$ . Let  $K(\chi) = K(\sqrt[p^s]{t}, \sqrt[p^s]{(t-1)(t-a)})$ . By the following claim, the proof of Proposition 4.2 applies to  $M = K(\chi)$  and the primes  $\mathfrak{p} = (t-a), \mathfrak{q}_1 = (t), \mathfrak{q}_2 = (t-1)$ . Therefore,  $b_p(\chi) = 0$ .

For  $q \equiv 3 \pmod{4}$  and  $p = 2$ , Example 4.3 is identical with [7, Example 2.8].

*Claim.* Let  $K_1 = K(\sqrt[p^s]{t})$ ,  $K_2 = K(\sqrt[p^s]{(t-1)(t-a)})$ . Then  $(t-a)$  is inert in  $K_1$  and totally ramified in  $K_2$ ,  $(t)$  is totally ramified in  $K_1$  and inert in  $K_2$ , and  $(t-1)$  splits completely in  $K_1$  and is totally ramified in  $K_2$ .

*Proof.* In  $K_1$  we have:  $t \equiv a \pmod{t-a}$  is not a  $p$ -th power and  $t \equiv 1 \pmod{t-1}$  is a  $p^s$ -th power, hence  $(t-a)$  is inert,  $(t-1)$  splits completely, and  $(t)$  is totally ramified.

In  $K_2$  we have:  $(t-1)(t-a) \equiv a \pmod{t}$  is not a  $p$ -th power, hence  $(t)$  is inert and  $(t-1), (t-a)$  are totally ramified.  $\square$

## REFERENCES

- [1] E. Aljadeff, J. Sonn, and R. Wadsworth. Projective schur groups of henselian fields. *J. Pure Appl. Algebra*, 208:833851, 2007.
- [2] S. Amitsur. On central division algebras. *Israel J. Math.*, 12:408–420, 1972.
- [3] E. Brussel. Noncrossed products and nonabelian crossed products over  $\mathbb{Q}(t)$  and  $\mathbb{Q}((t))$ . *Amer. J. Math.*, 117:377–393, 1995.
- [4] E. Brussel. Non-crossed products over function fields. *Manuscripta Math.*, 107(3):343–353, 2002.
- [5] Eric S. Brussel. Noncrossed products over  $k_p(t)$ . *Trans. Amer. Math. Soc.*, 353(5):2115–2129 (electronic), 2001.
- [6] Feng Chen. Indecomposable and noncrossed product division algebras over curves over complete discrete valuation rings. <http://arxiv.org/pdf/1004.3935v1>, April 2010.
- [7] Cécile Coyette. Mal'cev-neumann rings and noncrossed product division algebras. <http://arxiv.org/pdf/1103.0470v1>, March 2011.
- [8] T. Hanke. An explicit example of a noncrossed product division algebra. *Math. Nachr.*, 271:51–68, 2004.
- [9] T. Hanke and J. Sonn. The location of noncrossed products in the Brauer group of Laurent series fields over global fields. *Math. Ann.*, 2010. to appear.
- [10] Timo Hanke. Galois subfields of inertially split division algebras. *J. Algebra*, 2011.
- [11] B. Jacob and A. Wadsworth. Division algebras over Henselian fields. *J. Algebra*, 128:126–179, 1990.
- [12] H. Koch. *Galoissche Theorie der  $p$ -Erweiterungen.*, 1970.
- [13] R. Pierce. *Associative Algebras.* Springer-Verlag, New York, 1982.
- [14] W. Scharlau. Über die Brauer-Gruppe eines Hensel-Körpers. *Abh. Math. Sem. Univ. Hamburg*, 33:243–249, 1969.
- [15] E. Witt. Schiefkörper über diskret bewerteten Körpern. *J. Reine Angew. Math.*, 176:153–156, 1936.

LEHRSTUHL D FÜR MATHEMATIK, RWTH AACHEN, TEMPLERGRABEN 64,  
D-52062 AACHEN, GERMANY

*E-mail address:* hanke@math.rwth-aachen.de

UNIVERSITY OF MICHIGAN, 530 CHURCH ST., ANN ARBOR, MI 48109-1043  
USA

*E-mail address:* neftin@umich.edu

DEPARTMENT OF MATHEMATICS, TECHNION — ISRAEL INSTITUTE OF TECHNOLOGY, HAIFA 32000, ISRAEL

*E-mail address:* sonn@math.technion.ac.il