

Number Theory

# Contents lists available at ScienceDirect

# C. R. Acad. Sci. Paris, Ser. I



www.sciencedirect.com

# On fields of algebraic numbers with bounded local degrees

# Corps de nombres algébriques à degrés locaux bornés

# Sara Checcoli<sup>a</sup>, Umberto Zannier<sup>b</sup>

<sup>a</sup> Dipartimento di Matematica, Largo Bruno Pontecorvo, 5, 56127 Pisa, Italy <sup>b</sup> Scuola Normale Superiore di Pisa, Piazza dei Cavalieri, 7, 56126 Pisa, Italy

### ARTICLE INFO

Article history: Received 28 July 2010 Accepted after revision 10 December 2010 Available online 22 December 2010

Presented by Christophe Soulé

### ABSTRACT

It is well known that if a field  $K \subseteq \overline{\mathbb{Q}}$  is contained in the compositum of all extensions of  $\mathbb{Q}$  of degree at most *d*, then it has uniformly bounded local degrees. One may ask whether the converse holds. The answer is easily seen to be affirmative if the extension  $K/\mathbb{Q}$  is abelian, but we provide a counterexample to the general assertion. This is built up from a certain family of *pq*-groups.

© 2010 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.

# RÉSUMÉ

Il est bien connu que si un corps  $K \subseteq \overline{\mathbb{Q}}$  est contenu dans le compositum de toutes les extensions de  $\mathbb{Q}$  de degré inférieur à d, alors il est à degrés locaux uniformément bornés. On se demande si la réciproque est vraie. On prouve facilement que c'est le cas si l'extension K est abélienne, mais cela n'est pas vrai dans le cas général, comme le montre un contre-exemple construit à partir d'une certaine famille de pq-groupes.

© 2010 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.

# 1. Introduction

In [1] Bombieri and Zannier studied the Northcott property (of the finiteness of elements of bounded absolute Weil height) for certain infinite extensions of  $\mathbb{Q}$ . The paper considered in particular the field  $\mathbb{Q}^{(d)}$ , which is the compositum in  $\overline{\mathbb{Q}}$  of all number fields of degree at most d over  $\mathbb{Q}$ . The Northcott property was proved for the compositum of all abelian extensions of  $\mathbb{Q}$  of bounded degree (while for  $\mathbb{Q}^{(d)}$  the question remains open). In this proof a crucial role was played by the uniform boundedness of local degrees of the field  $\mathbb{Q}^{(d)}$ . (By definition an algebraic extension K of  $\mathbb{Q}$  has uniformly bounded local degrees if for every prime number p and every place  $v_p$  of K which extends the p-adic one, the completion of K with respect to  $v_p$  is a finite extension of  $\mathbb{Q}_p$  of degree bounded by a constant which does not depend on p.)

This may lead to the question, not entirely free of independent interest, whether every algebraic extension K of  $\mathbb{Q}$  with uniformly bounded local degrees is contained in  $\mathbb{Q}^{(d)}$  for some positive integer d. It is easy to see that this is the case if the extension  $K/\mathbb{Q}$  is abelian, as remarked in Section 2. However in Section 3 we give a negative answer to the general question, proving the following result:

**Theorem 1.1.** There exists a family  $\{K_m\}_{m \ge 1}$  of (nonabelian) finite Galois extensions of  $\mathbb{Q}$  such that their compositum  $K = \prod_{m \ge 1} K_m$  in  $\overline{\mathbb{Q}}$  has uniformly bounded local degrees, but it is not contained in  $\mathbb{Q}^{(d)}$  for any positive integer d (so K cannot be generated by elements of bounded degree).

E-mail addresses: checcoli@mail.dm.unipi.it (S. Checcoli), u.zannier@sns.it (U. Zannier).

<sup>1631-073</sup>X/\$ – see front matter © 2010 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved. doi:10.1016/j.crma.2010.12.007

We shall give a proof of this theorem based on a group-theoretical construction (for which we thank A. Lucchini), followed by an application of Shafarevich's Theorem about realization of solvable groups as Galois groups. This strategy ensures that the constructed field has uniformly bounded local degrees at all primes except two, i.e. those which ramify wildly. A bound for the local degrees at such primes is obtained using another result of Shafarevich concerning the number of generators of *p*-extensions of *p*-adic fields.

#### 2. Some preliminary remarks

We start by recalling a well-known property of the field  $\mathbb{Q}^{(d)}$  which is among the main motivations for the question posed in 1.

**Remark 1.** It is well known that, for any prime number p, there are only finitely many extensions of  $\mathbb{Q}_p$  of degree at most d. Moreover, a bound for their number exists depending only on d (a formula for this number is given in [5]). Therefore, the compositum of all these extensions has a degree over  $\mathbb{Q}_p$  which is finite and depends only on d. In particular, this compositum contains the completion of  $\mathbb{Q}^{(d)}$  with respect to any valuation  $v_p$  extending the p-adic one. And so the field  $\mathbb{Q}^{(d)}$  has uniformly bounded local degrees.

The next remark is about the exponent of the Galois group of an extension with uniformly bounded local degrees.

**Remark 2.** If *L* is a number field and K/L is a Galois extension with uniformly bounded local degrees, then Gal(K/L) has finite exponent.

**Proof.** We let *B* be a bound for the local degrees of *K*/*L*. We fix a finite Galois extension *E* of *L* contained in *K* and we take  $\sigma \in \text{Gal}(E/L)$ . By Chebotarev's Density Theorem (see [3], Th. 7.11) there exist a prime  $\wp$  of *L*, a prime b of *E* unramified above  $\wp$  and a conjugate  $\tau$  of  $\sigma$  that generates the decomposition group  $D(\mathfrak{b}|\wp)$  which is cyclic and equal to  $\text{Gal}(E_{\mathfrak{b}}/L_{\wp})$ , where  $E_{\mathfrak{b}}$  and  $L_{\wp}$  denote the completions of *E* and *L* with respect to b and  $\wp$  respectively. By assumption,  $|\text{Gal}(E_{\mathfrak{b}}/L_{\wp})| \leq B$ , thus  $\sigma^{B!} = \tau^{B!} = id$  and  $\exp(\text{Gal}(E/L)) \leq B!$ . Since Gal(K/L) is the inverse limit of the family  $\{\text{Gal}(E/L)\}_E$ , where *E* varies among the finite Galois extension of *L* contained in *K*, we have  $\exp(G) \leq B!$ .

Remark 2, beyond its general usefulness, also easily clarifies the abelian case. In fact we have:

**Proposition 2.1.** Let  $K/\mathbb{Q}$  be an abelian extension with uniformly bounded local degrees. Then there exists a positive integer d such that K is contained in  $\mathbb{Q}^{(d)}$ .

**Proof.** If  $G = \text{Gal}(K/\mathbb{Q})$  then, from Remark 2,  $\exp(G) \leq B$  for some positive integer B and  $G = \varprojlim G_m$  where  $G_m = \text{Gal}(K_m/\mathbb{Q})$  and  $K_m$  is any finite abelian extensions of  $\mathbb{Q}$  contained in K. For every m,  $G_m$  is a finite abelian group and we can write it as a product of finite cyclic groups  $G_m = \prod_{i=1}^n U_i$ . We let  $H_i$  be the subgroup of  $G_m$  defined as  $H_i := \prod_{j \neq i} U_j$ . We have  $[G_m : H_i] = |U_i| = \exp(U_i) \leq B$  for all *i*'s and  $\bigcap_{i=1}^n H_i = id$ . Therefore  $K_m$  is the compositum of the fields  $\{K_m^{H_i}\}_i$  and  $[K_m^{H_i} : \mathbb{Q}] = [G_m : H_i] \leq B$ . Hence  $K_m \subseteq \mathbb{Q}^{(B)}$  for every  $m \geq 1$  which implies  $K \subseteq \mathbb{Q}^{(B)}$ .

# 3. Proof of Theorem 1.1

We now want to prove that there exists an extension  $K/\mathbb{Q}$  with uniformly bounded local degrees such that K is not contained in  $\mathbb{Q}^{(d)}$  for any integer d. This will follow on constructing the field K as the compositum of a family of finite Galois extensions  $\{K_m\}_m$  such that, setting  $G_m := \text{Gal}(K_m/\mathbb{Q})$ , the family of groups  $\{G_m\}_m$  satisfies the following conditions:

- (i) the exponent of  $G_m$  is bounded by a constant which does not depend on m;
- (ii) there exists a strictly increasing sequence of positive integers  $\{c_m\}_m$  such that whenever  $G_m$  is isomorphic to a quotient H/N and H is a subgroup of a direct product  $H_1 \times \cdots \times H_s$ , then  $|H_i| \ge c_m$  for at least one index *i*.

We shall later produce these groups and the field *K* and prove that they satisfy the above conditions. We notice at once that conditions (i) and (ii) are not artificial: the first is motivated by Remark 2 above; as to the second, we now show that it ensures that the field *K* is not contained in  $\mathbb{Q}^{(d)}$ :

**Proposition 3.1.** Let  $\{K_m\}_m$  be a family of Galois extensions of  $\mathbb{Q}$  such that the family of groups  $\{G_m = \text{Gal}(K_m/\mathbb{Q})\}_m$  satisfies condition (ii), and denote by K the compositum of all the  $K_m$ 's. Then K is not contained in  $\mathbb{Q}^{(d)}$  for any positive integer d.

**Proof.** We suppose that  $K \subseteq \mathbb{Q}^{(d)}$  for some positive integer d and we fix an integer m such that  $d! < c_m$ . Then  $K_m$  is contained in a compositum  $L = L_1 \dots L_s$  of Galois extensions  $L_i$ 's with  $[L_i : \mathbb{Q}] \leq d! < c_m$ . Setting  $H_i = \text{Gal}(L_i/\mathbb{Q})$  and  $H = C_m \cap L_i$ .

 $Gal(L/\mathbb{Q})$ , we notice that  $G_m = H/N$  for some normal subgroup N of H and that H is a subgroup of  $H_1 \times \cdots \times H_s$ . Since  $|H_i| < c_m$  for every *i*, this contradicts condition (ii).

The next step is to construct a family of groups satisfying conditions (i) and (ii). We anticipate the following proposition, which gives a simple sufficient condition for a group to satisfy (ii):

**Proposition 3.2.** Let *G* be a finite group with a minimal normal subgroup *W* such that |W| = m. Suppose that *G* is a quotient of a group *H* where *H* is a subgroup of a direct product  $H_1 \times \cdots \times H_s$ . Then  $|H_i| \ge m$  for some index  $i \in \{1, \ldots, s\}$ .

**Proof.** Let us write G = H/N with  $H \leq H_1 \times \cdots \times H_s$ , where  $|H_i| < m$  for every *i*. Let us denote by  $\pi : H \to H/N$  the projection map. We set  $\overline{H}_i := H \cap 1 \times \cdots \times 1 \times H_i \times \cdots \times H_r$  and we denote by  $G_i = \phi(\overline{H}_i)$  the image of  $\overline{H}_i$  in *G*. We notice that the  $G_i$ 's are all normal subgroups of *G*. We want to show by induction that  $W \subseteq G_i$  for every *i*. For i = 1 this holds by assumption. Suppose it is true for  $G_{i-1}$ . Now  $W \subseteq G_{i-1}$  and  $[G_{i-1} : G_i] < m$ , thus  $U := G_i \cap W$  is normal and nontrivial and so it contains *W*. Therefore  $W \subseteq G_i$ , completing the induction. In particular  $W \subseteq G_s$ , which is a contradiction, since  $|G_s| \leq |H_s| < m$ .

In view of this proposition, to fulfill conditions (i) and (ii) it will suffice that the groups  $G_m$ 's in the family have bounded exponents and that for every m,  $G_m$  has a minimal normal subgroup  $W_m$  such that  $|W_{m+1}| > |W_m|$ . A family of groups with these properties was produced by Andrea Lucchini; we follow his construction.

We recall that, if p is a prime, a p-group G is called *extraspecial* if its center Z(G) and its commutator subgroup [G, G] coincide and are cyclic of order p. We list in the following Lemma some properties of these groups which are of interest for our purposes.

**Lemma 1.** If *G* be an extraspecial *p*-group, then  $|G| = p^{2t+1}$ , for some integer *t* and  $\exp(G) \in \{p, p^2\}$ . If *p* is odd, an extraspecial *p*-group is uniquely determined, up to isomorphisms, by the order and the exponent. Moreover if *p* is odd and *F* is a field containing a primitive *p*-th root of unity, an extraspecial group of order  $p^{2t+1}$  has p - 1 faithful and completely irreducible modules over *F* of dimension  $p^t$  as vector spaces over *F*.

**Proof.** A detailed description of extraspecial groups together with a proof of these results can be found in [2], Ch.A, §20 and Ch.B, §9, Prop. 9.16.

The construction of the family  $\{G_m\}_m$  can now be made as follows. We fix two odd primes p and q, with p dividing q-1 (so the field  $\mathbb{F}_q$  contains a primitive p-th root of unity). For every positive integer m we denote by  $E_m$  the extraspecial group of order  $p^{2m+1}$  and exponent p and by  $W_m$  a faithful and absolutely irreducible  $E_m$ -module of dimension  $p^m$  over  $\mathbb{F}_q$ . We set  $G_m := W_m \rtimes E_m$  (the semidirect product being taken via the natural action of  $E_m$  on its module  $W_m$ ).

**Proposition 3.3.** The family  $\{G_m\}_m$  satisfies conditions (i) and (ii) with  $c_m = q^{p^m}$ .

**Proof.** For every *m*, we have  $\exp(G_m) = pq$ . Moreover  $W_m$  is normal in  $G_m$  and minimal, since as a module it is irreducible. The result now follows from Proposition 3.2.

Having found the sought family of groups, our next target is to realize them as Galois groups of extensions of  $\mathbb{Q}$ . We notice that the groups  $G_m$ 's are solvable (they are pq-groups of odd order) and thus, by Shafarevich's Theorem, realizable (for a complete proof of Shafarevich's result see [4], Chap. IX, §5). This yields a family of finite Galois extensions  $\{K_m\}_{m \ge 1}$  of  $\mathbb{Q}$  such that, for every m,  $\text{Gal}(K_m/\mathbb{Q}) \simeq G_m$ . We denote by  $K := \prod_{m \ge 1} K_m$  the compositum of this family inside  $\overline{\mathbb{Q}}$ .

We notice that, by Proposition 3.1, the field *K* is not contained in  $\mathbb{Q}^{(d)}$  for any positive integer *d*. We claim that *K* has moreover uniformly bounded local degrees, which will complete the proof of Theorem 1.1.

**Proposition 3.4.** The field K has uniformly bounded local degrees over  $\mathbb{Q}$ .

**Proof.** We fix  $\ell$  be a prime in  $\mathbb{Z}$  and  $\nu$  a place of K extending the  $\ell$ -adic one and we denote by  $K_{m,\nu}$  the completion of  $K_m$  at  $\nu$ . We distinguish three cases.

If  $\ell$  does not ramify in  $K_m$ , the extension  $K_{m,\nu}/\mathbb{Q}_\ell$  is cyclic of degree bounded by  $\exp(G_m) = pq$ .

If  $\ell$  ramifies tamely in  $K_m$ , we denote by L the maximal unramified subextension of  $K_{m,\nu}/\mathbb{Q}_\ell$ . Then the extensions  $L/\mathbb{Q}_\ell$ and  $K_{m,\nu}/L$  are both cyclic (the second being tamely and totally ramified). Thus the group  $Gal(K_{m,\nu}/\mathbb{Q}_\ell)$  has order bounded by  $(pq)^2$ .

If  $\ell$  ramifies wildly in  $K_m$ ,  $\ell$  must be equal either to p or q and we separate the discussion in two parts:

- if  $\ell = q$ , the tamely ramified part of the local extension has degree bounded by  $p^2q$ . The first ramification group is a subgroup of  $W_m$  and, by a theorem of Shafarevich (see [6], Th.1), it has thus at most  $p^2q + 1$  generators, by the previous arguments. So the local degree is bounded by  $p^2q^{(p^2q+2)}$ ;
- if  $\ell = p$  the tamely ramified part of the local extension has degree at most  $q^2p$ . The first ramification group is a subgroup of  $E_m$  and, again by Shafarevich, it has at most  $q^2p + 1$  generators. It is easy to show that if an extraspecial p-group G has a subgroup H with at most n generators, then  $|H| \leq p^{n+1}$  (this easily follows from the fact that G/Z(G) is elementary p-abelian). Then the local degree is bounded even at  $\ell = p$  by  $p^{(pq^2+3)}q^2$ .

Summing up all these results, every  $K_m$  has local degree over  $\ell$  bounded by

$$\max\left\{p^2q^{(p^2q+2)}, p^{(pq^2+3)}q^2, p^2q^2, pq\right\} < q^{(q^3+5)}.$$

Therefore, by Remark 1, we have a finite number t, independent of  $\ell$ , of completions of the  $K_m$ 's at primes above  $\ell$  and their compositum contains  $K_v$ , which is the completion of K at the place v. Thus  $[K_v : \mathbb{Q}_\ell] \leq q^{t(q^3+5)}$  is bounded by a constant which does not depend on  $\ell$ .

#### Acknowledgements

We wish to thank Andrea Lucchini for his kind interest and for providing the construction of the sought family of groups. We also thank Roberto Dvornicich and Marta Morigi for useful remarks.

# References

- [1] E. Bombieri, U. Zannier, A note on heights in certain infinite extensions of  $\mathbb{Q}$ , Rend. Mat. Acc. Linc. 12 (2001) 5–14.
- [2] K. Doerk, T. Hawkes, Finite Solvable Groups, De Gruyter, Berlin/New York, 1992.
- [3] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Springer-Verlag, Berlin, 1990.
- [4] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Grundl. Math. Wiss., vol. 323, Springer, 1999.
- [5] J.-P. Serre, Une «formule de masse» pour les extensions totalement ramifiées de degré donné d'un corps local, C. R. Acad. Sci. Paris 286 (1978) 1031– 1036.
- [6] I.R. Shafarevich, On p-extensions, AMS. Transl., Ser. 2 4 (1956) 59-72.