JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Itamar GAL et Robert GRIZZARD

On the compositum of all degree d extensions of a number field

Tome 26, n° 3 (2014), p. 655-672.

<http://jtnb.cedram.org/item?id=JTNB_2014__26_3_655_0>

Journal de Théorie des Nombres
de Bordeaux **26** (2014), 655–672

On the compositum of all degree d extensions of a number field

par Itamar GAL et Robert GRIZZARD

Résumé. Nous étudions le compositum $k^{[d]}$ de toutes les extensions de degré d d'un corps de nombres k dans une clôture algébrique fixée. Nous démontrons que $k^{[d]}$ contient toutes les sous-extensions de degré inférieur à d si et seulement si $d \leq 4$. Nous montrons que quand $d > 2$, il n'existe pas de majorant $c = c(d)$ sur le degré des éléments nécessaires pour engendrer les sous-extensions finies de $k^{[d]}/k$. En se restreignant aux sous-extensions galoisiennes, nous montrons qu'un tel majorant n'existe pas sous certaines conditions sur les diviseurs de d, mais que l'on peut prendre $c = d$ quand d est premier. Cette question a été inspirée par les travaux de Bombieri et Zannier sur les hauteurs dans des extensions similaires, et examinés par Checcoli.

Abstract. We study the compositum $k^{[d]}$ of all degree d extensions of a number field k in a fixed algebraic closure. We show $k^{[d]}$ contains all subextensions of degree less than d if and only if $d \leq 4$. We prove that for $d > 2$ there is no bound $c = c(d)$ on the degree of elements required to generate finite subextensions of $k^{[d]}/k$. Restricting to Galois subextensions, we prove such a bound does not exist under certain conditions on divisors of d, but that one can take $c = d$ when d is prime. This question was inspired by work of Bombieri and Zannier on heights in similar extensions, and previously considered by Checcoli.

1. Introduction

Let k be a field. Throughout this paper, all extensions of k will be assumed to lie in a fixed algebraic closure $\overline{k}$. We are interested in fields obtained by adjoining to k all roots of irreducible polynomials of a given

Manuscrit reçu le 25 avril 2013, révisé le 28 octobre 2013, accepté le 19 novembre 2013.
The second author's research was partially supported by a grant from the National Security Agency, H98230-12-1-0254.
Mots clefs. Number fields, infinite algebraic extensions, Galois theory, permutation groups.
Classification math. 12F10, 11R21, 20B05.

degree d. For any positive integer d we will write

$$k^{[d]} = k(\beta \mid [k(\beta) : k] = d), \text{ and} \tag{1.1}$$

$$k^{(d)} = k(\beta \mid [k(\beta) : k] \leq d) = k^{[2]}k^{[3]}k^{[4]} \cdots k^{[d]}. \tag{1.2}$$

We have $k^{[1]} = k^{(1)} = k$, and for all d it is clear that $k^{[d]}$ and $k^{(d)}$ are normal extensions of k. We are primarily interested in the case where k is a number field, in which case these are infinite Galois extensions. When $d > 2$ it is natural to ask what polynomials of degree less than d split in $k^{[d]}$. If $c < d$ and all irreducible polynomials of degree c split in $k^{[d]}$, then $k^{[c]} \subseteq k^{[d]}$. Notice that this occurs in particular when c divides d, since every degree c extension admits a degree d/c extension. If all polynomials of degree less than d split in $k^{[d]}$, then $k^{[d]} = k^{(d)}$. We will prove the following results along these lines.

Theorem 1.1. *If k is a number field* †*, then*

(a) $k^{[2]} \subseteq k^{[d]}$ for all $d \geq 2$,

(b) $k^{[3]} \subseteq k^{[4]}$, and

(c) for each $d \geq 5$, there exists a prime $p < d$ such that $k^{[p]} \not\subseteq k^{[d]}$.

The following corollary is immediate.

Corollary 1.1. *If k is a number field, then $k^{[d]} = k^{(d)}$ if and only if $d < 5$.*

We now introduce the notion of boundedness for an extension of fields. We will use this language to state our remaining results.

Definition. We say an infinite extension M of k is *bounded over k* (or that M/k is *bounded*) if there exists a constant c such that all finite subextensions of M/k can be generated by elements of degree less than or equal to c. If there is no such c, we say that M/k is *unbounded*.

If all finite Galois subextensions of M/k can be generated by elements of degree less than or equal to c, we say M/k is *Galois bounded*; otherwise we say M/k is *Galois unbounded*.

It was first shown by Checcoli that, for a number field k, the extension $k^{(d)}/k$ is not in general Galois bounded (see [5], Theorem 2, part ii). We will address the question of how boundedness and Galois boundedness depend on d for the fields $k^{(d)}$ and $k^{[d]}$. Further restricting attention to abelian Galois extensions greatly simplifies the discussion. It is easily seen that $k_{\text{ab}}^{(d)}$ is bounded over k for all d, where the subscript denotes the maximal abelian subextension. This is contained in the proof of [7, Proposition 2.1] and can

†Many of our results contain the hypothesis that k is a number field or global function field. However, the astute reader will notice after reading the proofs that this hypothesis could be replaced with more technical restrictions on the field k – specifically, that certain embedding problems have solutions over k.

be seen in the statement of [5, Theorem 1.4]. It follows from the fact that a finite abelian group can be written as a product of cyclic groups, where the trivial subgroup is the intersection of subgroups of index not exceeding the greatest order of a cyclic factor.

In the case where k is a number field, Bombieri and Zannier ask in [3] whether, for any given constant T, only finitely many points in $k^{(d)}$ have absolute Weil height (see [2], p. 16 for a definition) at most T. Such a finiteness property is called the *Northcott property*. This problem has been further discussed in [20] and [6], but remains open. In Theorem 1 of [3] it is proved that this property is enjoyed by $k_{\mathrm{ab}}^{(d)}$, and the boundedness of $k_{\mathrm{ab}}^{(d)}/k$ plays a role in the proof. The authors of the present work are hopeful that understanding the boundedness properties in $k^{[d]}$ and $k^{(d)}$ will be useful in understanding such problems.

The following theorems summarize our results on boundedness and Galois boundedness.

Theorem 1.2. *If k is a number field, then $k^{[d]}$ is bounded over k if and only if $d \leq 2$.*

Theorem 1.3. *If k is any field and p is a prime number, then $k^{[p]}$ is Galois bounded over k. More precisely, all finite Galois subextensions of $k^{[p]}/k$ can be generated by elements of degree at most p over k.*

We will also establish the following partial converse to Theorem 1.3.

Theorem 1.4. *If k is a number field or global function field and $d > 2$, then $k^{[d]}/k$ is Galois unbounded in the following cases:*

(a) d is divisible by a square;

(b) d is divisible by two primes p and q such that $q \equiv 1 \pmod{p}$.

In particular, this includes the case where d is even and greater than 2.

In terms of the fields $k^{(d)}$, Theorems 1.2, 1.3, and 1.4 immediately imply the following.

Corollary 1.2. *Let k be a number field. Then*

(a) $k^{(2)}/k$ is bounded,

(b) $k^{(3)}/k$ is Galois bounded but not bounded, and

(c) $k^{(d)}/k$ is Galois unbounded for $d \geq 4$.

This paper is organized as follows. Sections 2 and 3 are devoted to preliminaries and background material on group theory and Galois theory. In Section 4 we prove Theorem 1.1; parts (a) and (b) appeal to existing results on embedding problems, while part (c) follows by a purely group theoretic argument. We conclude Section 4 with an elementary construction which gives part (a) in the case where $k = \mathbb{Q}$. In Section 5 we prove Theorems 1.2

and 1.4 using explicit constructions. Finally, in Section 6 we prove Theorem 1.3 as an immediate corollary of a purely group theoretic statement (see Proposition 6.1).

Acknowledgments

The authors would like to thank Daniel Allcock, Sara Checcoli, Joseph Gunther, Andrea Lucchini, Jeffrey Vaaler, and anonymous referees for numerous useful communications. We would also like to express our appreciation to the `GAP` group. Although we did not use computer calculations directly for any of the results in this paper, we used the `GAP` software package extensively to improve our understanding of the group theoretic aspects of these problems.

2. Preliminaries on group theory

We recall some standard definitions. A *transitive group* of degree d will mean a finite permutation group acting faithfully and transitively on a set Ω of size d, such as the Galois group of an irreducible degree d polynomial acting on the roots. A transitive group is *primitive* if there is no nontrivial partition of Ω such that the group has an induced action on the blocks of the partition. Since all such blocks must be equal in size, any transitive group of prime degree must be primitive. For more background on transitive and primitive groups, see [8] or [21].

Let us fix some notation for finite groups. We will denote by C_d, D_d, A_d, and S_d the cyclic, dihedral, alternating, and symmetric groups of degree d, respectively. Note that D_d has order $2d$. We denote the Klein 4-group by V.

A *subdirect product* G of some collection of groups $\{G_i\}_i$ is a subgroup of the direct product $\prod_i G_i$ with the property that the projection map from G to each factor G_i is surjective. We will sometimes write $G \leq_{sd} \prod_i G_i$ to abbreviate that G is such a group.

Let H_1, H_2 and Q be groups, and let $\alpha_1 : H_1 \to Q$ and $\alpha_2 : H_2 \to Q$ be surjective group homomorphisms. The *fibered product* of H_1 with H_2 over Q (with respect to the maps α_1 and α_2) is defined to be the subgroup $H_1 \times_Q H_2$ of the direct product $H_1 \times H_2$ given by

$$H_1 \times_Q H_2 = \{(h_1, h_2) \in H_1 \times H_2 \mid \alpha_1(h_1) = \alpha_2(h_2)\}.$$

Notice that we have

$$|H_1 \times_Q H_2| = \frac{|H_1| \cdot |H_2|}{|Q|}. \tag{2.1}$$

The following lemma can be found in different forms in many texts, and is variously attributed to Goursat or Goursat and Lambek. A short proof can be found in [4], p. 864.

Lemma 2.1 (Goursat's Lemma)**.** *Let H_1 and H_2 be groups. The set of subdirect products of $H_1 \times H_2$ is equal to the set of fibered products $H_1 \times_Q H_2$. In particular, every subdirect product of $H_1 \times H_2$ is of the form $H_1 \times_Q H_2$.*

3. Galois theory and embedding problems

The following elementary proposition highlights the role of Galois theory in the proofs of our results.

Proposition 3.1. *Let k be a perfect field and let L/k be a finite Galois extension of fields. The following are equivalent:*

(a) L is generated by elements of degree d over k;
(b) in $\mathrm{Gal}(L/k)$ the trivial group is the intersection of subgroups of index d;
(c) $\mathrm{Gal}(L/k)$ is a subdirect product of transitive groups of degree d.

Proof. The equivalence (a) and (b) follows immediately from the Galois correspondence and the primitive element theorem. If (a) is satisfied, then L is a compositum of the splitting fields of some degree d polynomials. It follows from basic Galois theory that $\mathrm{Gal}(L/k)$ is a subdirect product of these Galois groups, which are transitive groups of degree d, so (c) is satisfied. Suppose (c) is satisfied, so we have $\mathrm{Gal}(L/k)$ acting on a disjoint union of sets of size d, transitively on each set. Then all point-stabilizers have index d, and the intersection of these subgroups is trivial, yielding (b). □

In order to establish Theorem 1.1, we must discuss the embedding problem in Galois theory. Let K/k be a Galois extension of fields, G a finite group, and N a normal subgroup of G with a short exact sequence

$$1 \to N \to G \xrightarrow{\phi} \mathrm{Gal}(K/k) \to 1. \tag{3.1}$$

These data give us the *embedding problem* $(K/k, G, N)$. A *solution* to the embedding problem is an extension L/k with $L \supseteq K$ such that $\mathrm{Gal}(L/k) \cong G$ and the natural map $\mathrm{Gal}(L/k) \to \mathrm{Gal}(K/k)$ agrees with ϕ. Hence, a solution to the embedding problem is described by the following commutative diagram.

(3.2)
$$\begin{array}{ccccccccc} & & & & \mathrm{Gal}(L/k) & & & & \\ & & & & \downarrow \wr & \searrow & & & \\ 1 & \longrightarrow & N & \longrightarrow & G & \xrightarrow{\phi} & \mathrm{Gal}(K/k) & \longrightarrow & 1. \end{array}$$

For our purposes, all that is important is finding an extension L/k such that $L \supseteq K$ and $\mathrm{Gal}(L/k) \cong G$, and therefore we will not mention the map ϕ in what follows.

A celebrated result in this context is a theorem of Shafarevich, which states that if k any number field or global function field, any solvable group can be realized as the Galois group of some extension of k. Since products of solvable groups are solvable, this allows us to realize a solvable group as the Galois group of infinitely many extensions, whose pairwise intersections are k. A full proof of Shafarevich's Theorem, along with more background on embedding theory, can be found in [15].

The following proposition is a simple yet important observation which is used implicitly throughout the proof of Theorem 1.1.

Proposition 3.2. *Let k be a field and let K/k be a finite extension. Then $K \subseteq k^{[d]}$ if and only if the following two conditions are met.*

(i) We can find a group H which is a subdirect product of transitive groups of degree d with some normal subgroup N such that there is a short exact sequence

$$1 \to N \to H \to \mathrm{Gal}(K/k) \to 1. \tag{3.3}$$

(ii) We can solve the corresponding embedding problem, i.e. find $L \supseteq K$ such that $\mathrm{Gal}(L/k) \cong H$.

Proof. If $K \subseteq k^{[d]}$, then K is contained in some finite Galois extension L/k generated by elements of degree d. By Proposition 3.1, we have that $\mathrm{Gal}(L/k)$ is a subdirect product of transitive groups of degree d, and (i) and (ii) are clearly satisfied via the short exact sequence

$$1 \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L/k) \to \mathrm{Gal}(K/k) \to 1. \tag{3.4}$$

Conversely, if (i) and (ii) are satisfied, then we have $K \subseteq L$ as in (ii), and $L \subseteq k^{[d]}$ by (i) and Proposition 3.1. □

4. Proof of Theorem 1.1

We implicitly apply Proposition 3.2 throughout. For integers $m < d$, we are interested in whether or not $k^{[m]} \subseteq k^{[d]}$. Let K be the splitting field of an irreducible polynomial of degree m in $k[x]$. In the case $m = 2$, we must have that $\mathrm{Gal}(K/k) \cong C_2$, and we use the following result due to O. Neumann (cf. [16], Theorem 2) in order to conclude that $K \subseteq k^{[d]}$.

Proposition 4.1. *Let K/k be a quadratic extension of number fields and let $d \geq 3$. Then there is a solution to the embedding problem $(K/k, S_d, A_d)$ arising from*

$$1 \to A_d \to S_d \to \mathrm{Gal}(K/k) \to 1. \tag{4.1}$$

In other words, every irreducible quadratic splits in the splitting field of some degree d polynomial (with symmetric Galois group).

This establishes part (a) of Theorem 1.1, that $k^{[2]} \subseteq k^{[d]}$ for all $d \geq 2$, and in particular it tells us that $k^{[3]} = k^{(3)}$. At the end of this section we give a short, elementary proof of part (a) of Theorem 1 in the case where $k = \mathbb{Q}$.

For part (b) of Theorem 1 it now suffices to consider the case $m = 3, d = 4$. We must have $\mathrm{Gal}(K/k) \cong S_3$ or C_3. The following is a special case of a classical result of Shafarevich that gives the solution to all embedding problems with nilpotent kernel (see [18], Claim 2.2.5).

Proposition 4.2. *Let k be a number field and let $f(x) \in k[x]$ be an irreducible cubic with splitting field K. Let V denote the Klein 4-group.*

(a) If $\mathrm{Gal}(K/k) \cong S_3$, then there is a solution to the embedding problem $(K/k, S_4, V)$ arising from

$$1 \to V \to S_4 \to \mathrm{Gal}(K/k) \to 1.$$

(b) If $\mathrm{Gal}(K/k) \cong C_3$, then there is a solution to the embedding problem $(K/k, A_4, V)$ arising from

$$1 \to V \to A_4 \to \mathrm{Gal}(K/k) \to 1.$$

In other words, every irreducible cubic splits in the splitting field of some quartic.

This proves that $k^{[3]} \subseteq k^{[4]}$, and combining with part (a) of Theorem 1 we now have that $k^{[4]} = k^{(4)}$.

To prove part (c) of Theorem 1.1 we consider the case $d \geq 5$. We will show that, for certain primes $p < d$, if $\mathrm{Gal}(K/k) \cong C_p$, then there is no possible subdirect product of transitive groups of degree d having $\mathrm{Gal}(K/k)$ as a quotient. That is, we cannot even find groups H and N satisfying a short exact sequence as in (3.3) above. We begin with a lemma.

Lemma 4.1. *For any integer $d \geq 5$ there exists a prime number $p \in (\frac{d}{2}, d)$ such that, if G is a transitive subgroup of S_d containing a p-cycle, then either $G = S_d$ or $G = A_d$.*

Proof. The transitive groups of degree d are well-known for small d – see for example [4] for the groups up to degree 11; GAP (see [13], [19]) has a library of all of them for $d \leq 30$. It can be checked easily that we can use $p = 3$ when $d = 5$, and we can use $p = 5$ when $d = 6, 7$; in each of these cases, S_d and A_d are the only transitive subgroups with order divisible by p. Therefore all that remains is to prove our lemma in the case $d \geq 8$.

There exists at least one prime $p \in (\frac{d}{2}, d-2)$. This follows from Bertrand's Postulate, first proved by Chebyshev, which states that for $m > 3$ there exists a prime in the interval $(m, 2m-2)$ – see [12], p. 343, Theorem 418; cf. p. 373. Let p be such a prime, and suppose G is a transitive subgroup of S_d containing some p-cycle g. Without loss of generality, $g = (1\ 2\ 3\ \cdots\ p)$.

Since G is transitive, for each $i \in \{p+1, \ldots, d\}$ there is some element $\sigma_i \in G$ such that $\sigma_i(1) = i$. If we let $g_i = \sigma_i g \sigma_i^{-1}$, then g_i will be a p-cycle in G whose support contains i. Since p is prime, each $\langle g_i \rangle$ acts primitively on its support, which is a set of size p. Since $p > \frac{d}{2}$, the pairwise intersections of the supports of the groups $\langle g_i \rangle$ are nontrivial. Therefore we can apply Proposition 8.5 from [21] inductively to see that the subgroup $H = \langle g, g_{p+1}, g_{p+2}, \ldots, g_d \rangle$ is a primitive subgroup of S_d. Since H contains a p-cycle and $p < d-2$, Theorem 13.9 from [21] tells us that either $H = S_d$ or $H = A_d$, and since $H \leq G$, our proof is complete. □

Part (c) will be an immediate corollary of the following proposition.

Proposition 4.3. *For any integer $d \geq 5$ there exists some prime $p < d$ such that, if $G \leq_{sd} G_1 \times \cdots \times G_n$ is a subdirect product of transitive groups of degree d, then G has no quotient that is cyclic of order p.*

Proof. Fix $d \geq 5$. By Lemma 4.1, there is a prime $p \in (\frac{d}{2}, d)$ such that the only transitive subgroups of S_d containing a p-cycle are S_d and A_d. We proceed by induction on n, noting that the case $n = 1$ follows immediately by our choice of p. In general, we will have that $G \leq_{sd} G_0 \times G_n$, where G_n is a transitive group of degree d and G_0 is a subdirect product of $n-1$ such groups. If N is any normal subgroup of G, we have that $N \leq_{sd} N_0 \times N_n$ for some normal subgroups $N_0 \trianglelefteq G_0$ and $N_n \trianglelefteq G_n$. By Goursat's Lemma, we may write G as a fibered product $G = G_0 \times_Q G_n$ for some group Q which is a quotient of both G_0 and G_n. Similarly, we have $N = N_0 \times_R N_n$ for some group R which is a quotient of both N_0 and N_n.

By the inductive hypothesis, neither G_0/N_0 nor G_n/N_n has order p. Suppose that $G/N \cong C_p$. Since G/N surjects onto both G_0/N_0 and G_n/N_n, the latter two groups must be trivial. Therefore, using (2.1), we have

$$p = \frac{|G|}{|N|} = \frac{|G_0| \cdot |G_n|/|Q|}{|N_0| \cdot |N_n|/|R|} = |G_0/N_0| \cdot |G_n/N_n| \cdot \frac{|R|}{|Q|} = \frac{|R|}{|Q|}. \tag{4.2}$$

This means that $|R|$ is divisible by p, and therefore $|G_n|$ and $|N_n|$ are both divisible by p as well. This means G_n must be isomorphic to either S_d or A_d. Hence the only possibilities for Q are S_d, A_d, C_2, or 1, and the only possibilities for R are S_d or A_d. None of these possibilities allows for the equality in (4.2). □

This establishes part (c) of Theorem 1.1. Indeed, it shows that $k^{[p]} \subsetneq k^{[d]}$, for p and d as above, whenever k is any field that admits a degree cyclic Galois extension of degree p.

In summary, if $d \leq 4$, an irreducible polynomial in $k[x]$ of degree less than d splits in the splitting field of a *single irreducible polynomial* of degree d. When $d > 4$, however, some irreducible polynomials of degree less than d do not split *in any compositum of such splitting fields*. We conclude this

section by demonstrating that part (a) of Theorem 1.1 can be proved by a very elementary construction when $k = \mathbb{Q}$.

Elementary proof that $\mathbb{Q}^{[2]} \subseteq \mathbb{Q}^{[d]}$ *for all* $d \geq 2$. In general, $k^{[\ell]} \subseteq k^{[d]}$ if $\ell | d$. Hence it will suffice to show that $\sqrt{p} \in \mathbb{Q}^{[\ell]}$ for any prime $\ell \geq 3$, whenever p is a rational prime or $p = -1$. If p is any rational prime or equal to ± 1, define

$$f_p(x) = x^\ell - \ell(\ell p + 1)x + (\ell - 1)(\ell p + 1) \tag{4.3}$$

The discriminant Δ_p of this polynomial is given by the following (see for example [14]):

$$(-1)^{(\ell-1)(\ell-2)/2}\Delta_p = -(\ell - 1)^{\ell-1}\ell^{\ell+1}(\ell p + 1)^{\ell-1} \cdot p. \tag{4.4}$$

In particular, it follows that $\sqrt{p}$ will be in the splitting field of either $f_p(x)$ or $f_{-p}(x)$. We now show that $f_p(x)$ is irreducible. First notice that if $\ell \neq p$ then $f_p(x + 1)$ is Eisenstein at ℓ. Next we consider the case where $\ell = p$. To handle this case we use the following version of Dumas's Irreducibility Criterion. A proof can be found in [17, Section 2.2.1], where the langauge of Newton diagrams is used.

Proposition 4.4 (Dumas's Irreducibility Criterion)**.** *Let* $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$. *Suppose there exists a prime* q *such that* $v_q(a_0) = 0$, $v_q(a_i)/i > v_q(a_n)/n$ *for* $i \in \{1, \ldots, n\}$ *and* $\gcd(v_q(a_n), n) = 1$. *Here* $v_q(\cdot)$ *denotes the greatest power of* q *dividing the argument. Then* $f(x)$ *is irreducible.*

Applying Dumas's criterion in the case $l = p$, we find that a sufficient condition for the irreducibility of f_p is the existence of a prime q and an integer m such that q^m exactly divides $p^2 + 1$, such that q is coprime to $p - 1$, and and such that m is coprime to p. Notice that

$$(p^2 + 1) - (p + 1)(p - 1) = 2. \tag{4.5}$$

Since 2 is an integer combination of p^2+1 and $p-1$, it follows that $\gcd(p^2 + 1, p - 1)$ divides 2. Also notice that

$$p^2 + 1 = (p - 1)^2 + 2(p - 1) + 2 \equiv 2 \pmod 4. \tag{4.6}$$

Thus $p^2 + 1$ is not a power of 2, and we can take q to be any one of its odd prime factors. Now choose m such that q^m exactly divides $p^2 + 1$. Since $p^2 + 1 < q^p$ for $p, q \geq 3$, it follows that $1 < m < p$. Thus m is coprime to p, which completes the proof. □

5. Unboundedness: proofs of Theorems 1.2 and 1.4

In the spirit of Proposition 3.1, let G be a finite group and d a positive integer. Suppose that H is a subgroup of G that cannot be written as an intersection of subgroups of index less than or equal to d in G. If G is the Galois group of a field extension L/k, this implies that the fixed field K of H is not generated over k by elements of degree less than or equal to d. In order to prove unboundedness results, we must exhibit groups with these properties which can be realized as Galois groups of subextensions of $k^{[d]}$. The example in the next lemma will be applied toward establishing Theorem 1.2.

Lemma 5.1. *Let p be an odd prime number, and let*

$$G = D_p^{n-1} \times C_p = \langle r_1, s_1, \ldots, r_{n-1}, s_{n-1}, r_n \rangle \tag{5.1}$$

be the direct product of $n-1$ copies of the dihedral group D_p and a cyclic group of order p, where for $i \in \{1, \ldots, n-1\}$ the i^{th} $D_p = \langle r_i, s_i \rangle$ is generated by the p-cycle r_i and the 2-cycle s_i, and $C_p = \langle r_n \rangle$. Let

$$H = \langle r_1 r_n, r_2 r_n, \ldots, r_{n-1} r_n \rangle \leq G. \tag{5.2}$$

If B is a subgroup of G with $H \lneq B \leq G$, then $r_n \in B$. In particular, the intersection of all such subgroups B strictly contains H.

Proof. Let $G_p = \langle r_1, \ldots, r_n \rangle$ be the unique Sylow p-subgroup of G, considered as an n-dimensional $\mathbb{F}_p$-vector space. Any Sylow 2-subgroup G_2 of G will be an $(n-1)$-dimensional $\mathbb{F}_2$-vector space which acts by conjugation on G_p, so that $G = G_p \rtimes G_2$.

Let $H \lneq B \leq G$. Note that H is a codimension 1 subspace of G_p, so if B contains any element of order p not in H, then B contains all of G_p. If B contains any involution $\tau \in G$, notice that there will be some i such that τ acts non-trivially on the i^{th} copy of D_p, so that $\langle r_i r_n, \tau \rangle$ will contain r_n. Since every nontrivial element of G is either of order p, an involution, or of order $2p$ (a power of which is an involution), this completes our proof. □

Corollary 5.1. *Let k be a number field or a global function field, and let p be an odd prime number. Then $k^{[p]}/k$ is unbounded.*

Proof. Let G and H be as in Lemma 5.1. Since G is solvable we have an extension L/k with $\mathrm{Gal}(L/k) \cong G$. Let L^H be the fixed field in L of H, and notice that $L^H \subseteq k^{[p]}$. It is clear from our construction that $[L^H : k] = p \cdot 2^{n-1}$. The Galois correspondence tells us that every proper subextension of L^H/k corresponds to a subgroup B of G with $H \lneq B \leq G$. Furthermore, since the intersection of all such groups strictly contains H, the compositum of all proper subextensions of L^H/k is strictly a subfield of L^H. This shows that L^H is not generated by elements of degree less than $p \cdot 2^{n-1}$. □

Notice that the field extension L^H/k in the proof above is *not* Galois (H is not normal in G). As we will prove in the next section, this was necessarily so.

In order to prove our Galois unboundedness results, we must now introduce extraspecial p-groups. We write H_p for the finite Heisenberg group of order p^3, when p is a prime. This group is defined as the multiplicative group of upper triangular matrices of the form

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix},$$

with a, b, and c belonging to the finite field $\mathbb{F}_p$.

The group H_p plays an important role in our Galois unboundedness results. We review some of its properties. First, H_p has a natural action on the three-dimensional vector space $\mathbb{F}_p^3$. Analyzing this action, it is easy to see that when an element of H_p acts on a vector, the third coordinate is fixed, and H_p acts faithfully and transitively on a 2-dimensional affine subspace (the subspace with third coordinate equal to 1, say), which has p^2 elements. Thus we see that H_p is isomorphic to a transitive group of degree p^2.

The group H_p is an *extraspecial p-group*, meaning its center, commutator, and Frattini subgroups coincide and have order p. We can construct larger extraspecial p-groups as follows. Let n be a positive integer, and consider the normal subgroup $N_{p,n}$ of the direct product H_p^n given by

$$N_{p,n} = \{(z_1^{a_1}, \ldots, z_n^{a_n}) \mid \Sigma_{i=1}^n a_i \equiv 0 \pmod{p}\}, \tag{5.3}$$

where z_i generates the center of the i^{th} copy of H_p. The quotient $H_p^n/N_{p,n}$ is an extraspecial p-group of order p^{2n+1} and exponent p (except when $p = 2$, when the exponent is 4), which we will denote by $E_{p,n}$. The basic properties of these groups are discussed in [9, Section A.20].

The following lemma can be found in [5] (cf. Proposition 2.4), where it is stated only for p odd. We briefly recall the proof below.

Lemma 5.2. *Let p be a prime number. The intersection of all subgroups of index less than p^n in $E_{p,n}$ contains the commutator subgroup. In particular, this intersection is nontrivial.*

Proof. Any subgroup H of $E_{p,n}$ of index less than p^n has order greater than p^{n+1} and is therefore non-abelian by [1, Theorem 4.7 (d)]. Since H contains a pair of non-commuting elements and the commutator subgroup $[E_{p,n}, E_{p,n}]$ is cyclic of order p, we have that H contains the commutator subgroup. □

Checcoli used this fact in [5] to show that, for a number field k, the extension $k^{(d)}/k$ is not in general Galois bounded. The idea of using extraspecial

groups for this purpose is attributed to A. Lucchini. However, the author was not concerned with the question of which values of d suffered from this pathology, nor with the more general question of the boundedness of $k^{[d]}/k$. The use of extraspecial p-groups (which are certainly not the only groups with properties like the conclusion of Lemma 5.2, but are natural and easy to work with) remains our primary tool for proving that extensions are Galois unbounded. The following lemma simplifies our application of this principle.

Lemma 5.3. *Let d be a positive integer. Suppose there is a prime number p such that there is a solvable group G which is a subdirect product of transitive groups of degree d, and a quotient of G is isomorphic to H_p. Then $k^{[d]}/k$ is Galois unbounded for any number field or global function field k.*

Proof. By Shafarevich's Theorem, for any positive integer n we can realize G^n as the Galois group of some extension L/k, and we will have $L \subseteq k^{[d]}$. There will be a Galois subextension K/k with Galois group H_p^n, and the subfield of K corresponding to the normal subgroup defined in (5.3) will have Galois group $E_{p,n}$, and will therefore not be generated by elements of degree less than p^n. □

The following lemma gives a construction of a permutation group that will allow us to apply Lemma 5.3 in our proof of part (b) of Theorem 1.4.

Lemma 5.4. *Let $d = pq$, where p and q are primes with $q \equiv 1 \pmod{p}$. Then there exists a transitive group of degree d which is isomorphic to $C_q^p \rtimes H_p$.*

Proof. Write $q = mp + 1$. Consider p sets Ω_i of size q, written $\Omega_i = \{1_i, 2_i, \ldots, q_i\}$ for $i \in \mathbb{F}_p$. We write Ω for the disjoint union of the sets Ω_i. We will construct a group G of permutations of Ω, which acts imprimitively with respect to the partition into the sets Ω_i. Let σ be the permutation $(1\ 2\ \cdots\ q)$. The q-cycle σ is normalized by some $(q-1)$-cycle η in the symmetric group S_q and, since $q \equiv 1 \pmod{p}$, we have that η^m is a product of m disjoint p-cycles; we set $\tau = \eta^m$. The permutations σ and τ induce permutations on each set Ω_i, which we denote by σ_i and τ_i.

We define $\alpha = \tau_0\tau_1\cdots\tau_{p-1}$, $\beta = \tau_0^0\tau_1^1\cdots\tau_{p-1}^{p-1}$, and define γ to be the permutation on Ω sending j_i to j_{i+1}. Let $A = \langle\sigma_0, \sigma_1, \cdots, \sigma_{p-1}\rangle \cong C_q^p$, and $B = \langle\alpha, \beta, \gamma\rangle$. Notice that our construction ensures that A is normalized by B. The interested reader will verify that $B \cong H_p$ via

$$(5.4) \qquad \alpha \mapsto \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \beta \mapsto \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \gamma \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

The example below with $p = 3$, $q = 7$ makes the isomorphism more clear. The Heisenberg group B acts simultaneously on m "planes" of p^2 points, each plane consisting of points j_i with $i \in \mathbb{F}_p$ and j running over the indices in one of the disjoint p-cycles that make up τ.

We let

$$G = A \rtimes B \tag{5.5}$$

and notice that G acts transitively on Ω (indeed, $\langle \sigma_0, \gamma \rangle$ is already transitive on Ω). □

It would be quite tedious to write explicitly the generators of the group constructed in the proof of Lemma 5.4 for general p and q, but we will make this construction more clear by giving an example with $d = 21 = 3 \cdot 7$.

Example. We assume the notation of the preceding proof. The 7-cycle $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7)$ is normalized by the 6-cycle $\eta = (2\ 6\ 5\ 7\ 3\ 4)$. Squaring this permutation yields a product of 3-cycles $\tau = (2\ 5\ 3)(6\ 7\ 4)$, which normalizes σ. As described above, we have

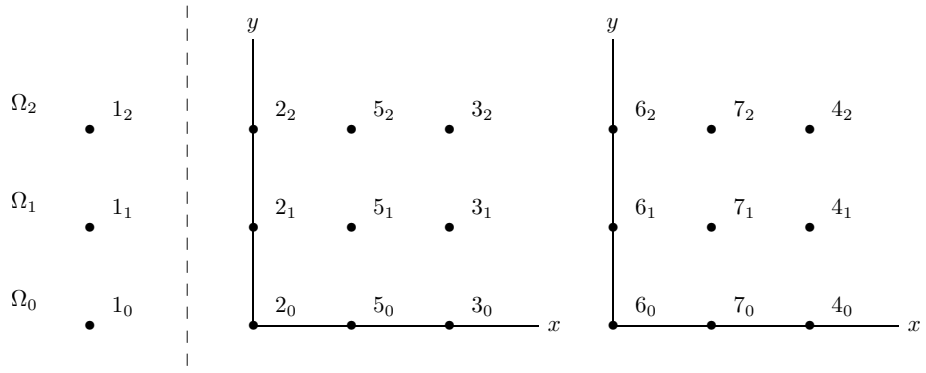
$$\Omega = \{ j_i \mid i \in \mathbb{F}_p, j \in \{1, \dots, 7\} \}.$$

The permutations defined in the proof are given as follows:

$$\begin{aligned}
\sigma_0 &= (1_0\ 2_0\ 3_0\ 4_0\ 5_0\ 6_0\ 7_0), \\
\sigma_1 &= (1_1\ 2_1\ 3_1\ 4_1\ 5_1\ 6_1\ 7_1), \\
\sigma_2 &= (1_2\ 2_2\ 3_2\ 4_2\ 5_2\ 6_2\ 7_2), \\
\tau_0 &= (2_0\ 5_0\ 3_0) \cdot (6_0\ 7_0\ 4_0), \\
\tau_1 &= (2_1\ 5_1\ 3_1) \cdot (6_1\ 7_1\ 4_1), \\
\tau_2 &= (2_2\ 5_2\ 3_2) \cdot (6_2\ 7_2\ 4_2), \\
\alpha &= \tau_0 \tau_1 \tau_2, \\
\beta &= \tau_1 \tau_2^2, \\
\gamma &= (1_0\ 1_1\ 1_2) \cdot (2_0\ 2_1\ 2_2) \cdots (7_0\ 7_1\ 7_2), \quad \text{and} \\
G &= \langle \sigma_0, \sigma_1, \sigma_2 \rangle \rtimes \langle \alpha, \beta, \gamma \rangle.
\end{aligned}$$

To verify that $\langle \alpha, \beta, \gamma \rangle \cong H_3$ as given by (5.4), we consider the following way of visualizing Ω.

Shown are two copies of the affine plane $z = 1$ inside of $\mathbb{F}_3^3 = \{(x, y, z) \mid x, y, z \in \mathbb{F}_3\}$. These eighteen points, together with the three points on the left, correspond to elements of Ω by the labelings. For example, the point $(2, 0, 1)$ in the plane on the left corresponds to $3_0 \in \Omega_0$. The blocks Ω_i are represented as the three horizontal rows in the diagram. The columns have been partitioned according to the cycle decomposition of permutations τ_i,



so that α, β, and γ act via the matrices given in (5.4), simultaneously on each plane of nine points.

Proof of Theorem 1.4. Recall that if c divides d, then $k^{[c]} \subseteq k^{[d]}$. Since H_p is solvable and transitive of degree p^2, if follows immediately from Lemma 5.3 that $k^{[p^2]}$ is Galois unbounded over k for any prime p, yielding part (a). Checcoli showed how to realize these groups explicitly in [5]. Since the group constructed in Lemma 5.4 is solvable, we again apply Lemma 5.3 to see that $k^{[pq]}$ is Galois unbounded over k whenever p and q are primes with $q \equiv 1 \pmod{p}$. This gives part (b).

□

Proof of Theorem 1.2. We know that $k^{[2]} = k_{\mathrm{ab}}^{(2)}$, so $k^{[2]}/k$ is bounded. If $d > 2$, then d is divisible by c, where c is either 4 or an odd prime. We have $k^{[c]} \subseteq k^{[d]}$, and by Corollary 5.1 and part (a) of Theorem 1.4, $k^{[c]}$ is unbounded over k. □

We remark that our proofs actually demonstrate that $k^{[d]}/k$ is also unbounded in the case where k is a global function field and $d \geq 3$.

6. Galois boundedness in prime degree

In this section we prove Theorem 1.3. Clearly the general technique for showing boundedness is to find subgroups of small index inside of a Galois group G, whose intersection is a given subgroup H. If we want to show Galois boundedness, we take H to be normal. We will show that we can accomplish this task when G is a subdirect product of transitive groups of prime degree.

The following lemma characterizes the transitive groups of degree p.

Lemma 6.1. *If p is a prime number and G is a transitive group of degree p, then we have $G = T \rtimes B$, where T is simple and transitive, and B is a subgroup of C_{p-1}.*

This lemma can be proved by elementary means. It can also be seen quickly using the classification of finite simple groups: a theorem of Burnside (see [21], Theorem 11.7; cf. [8], Theorem 4.1B) implies that G is either a subgroup of $C_p \times C_{p-1}$ containing C_p, or an almost simple group, meaning that there is a simple group T such that $T \leq G \leq \mathrm{Aut}(T)$; in this case we also have that G is doubly transitive, meaning that G can send any two points to any other two points. That T is itself transitive of degree p follows from [21], Proposition 7.1, which states that every normal subgroup of a primitive permutation group is transitive. The Classification Theorem for Finite Simple Groups implies that there is a very small list of possibilities for T (see [11], Corollary 4.2), and the lemma can be easily checked in these cases.

We are now ready to establish a group theoretic result, of which Theorem 1.3 will be an immediate corollary.

Proposition 6.1. *Let p be a prime number and let G be a finite subdirect product of transitive groups of degree p. If N is a normal subgroup of G, then N is an intersection of subgroups of index at most p in G.*

Proof. Let $G \leq_{sd} G_1 \times \cdots \times G_n$, where G_i is a transitive group of degree p for $i \in \{1, \ldots, n\}$. If we consider each group G_i acting transitively on a set Ω_i of size p, we have G acting faithfully on the disjoint union of these sets, which we denote by Ω. Let π_i denote the projection onto G_i, and let T_i denote the (unique) minimal normal subgroup of G_i. As mentioned following Lemma 6.1, we know that each T_i is either isomorphic to C_p or to a simple non-abelian group. We write $K_i = G \cap G_i$, which is a normal subgroup of both G and G_i. We proceed by induction on n. The case $n = 1$ follows easily from Lemma 6.1, since if N is nontrivial we must have G/N abelian of order dividing $p - 1$; if N is trivial, observe that the point-stabilizers in G have index p and trivial intersection.

For each i we have that G/K_i is a subdirect product of the groups $\{G_j\}_{j \neq i}$. Notice that we may apply the inductive hypothesis to write NK_i/K_i as an intersection of some subgroups $\{H_l/K_i\}_l$ of index at most p in G/K_i. Now the subgroups $\{H_l\}_l$ are of index at most p in G, and $NK_i = \cap_l H_l$. If K_i is trivial, then our proof is complete. Alternatively, if N acts trivially on Ω_i, notice that

$$N = \big(\cap_{x \in \Omega_i} \mathrm{Stab}_G(x)\big) \cap NK_i = \big(\cap_{x \in \Omega_i} \mathrm{Stab}_G(x)\big) \cap \big(\cap_l H_l\big). \tag{6.1}$$

Since the stabilizers $\mathrm{Stab}_G(x)$ have index p in G, we have written N as an intersection of subgroups of index at most p in G. Thus we may assume that, for each i, the subgroup K_i is nontrivial, and N acts nontrivially on Ω_i. Moreover, since K_i is nontrivial and normalized by G_i, it follows that K_i contains the unique minimal normal subgroup T_i of G_i. In particular

this means that $T_i \leq G$, and writing $T = \prod_i T_i$ we have that $T \leq G$. Furthermore, G/T is abelian of exponent dividing $p-1$.

Since N acts nontrivially on each Ω_i, we know that $T_i \leq \pi_i(N)$. For each i such that T_i is non-abelian (recall that T_i is simple), we will have $T_i = [T_i, N] \leq N$. Write T_{ab} for the product of the T_i which are abelian (these are all isomorphic to C_p), and write T_{n} for the product of those which are non-abelian. We have $T_{\mathrm{n}} \leq N$, so

$$\frac{TN}{N} = \frac{T_{\mathrm{ab}}T_{\mathrm{n}}N}{N} = \frac{T_{\mathrm{ab}}N}{N} \cong \frac{T_{\mathrm{ab}}}{T_{\mathrm{ab}} \cap N}. \tag{6.2}$$

Therefore TN/N is an elementary abelian p-group. We also know that G/TN is abelian of exponent dividing $p-1$, so the short exact sequence

$$1 \to TN/N \to G/N \to G/TN \to 1 \tag{6.3}$$

splits by the Schur-Zassenhaus Theorem (Theorem 39 from Chapter 17 of [10]). Let $V = TN/N$ and $B = G/TN$, so (6.3) gives us

$$G/N = V \rtimes B. \tag{6.4}$$

We want to show that there is a collection of subgroups of index at most p in G/N whose intersection is trivial. It is clear that we can find such subgroups whose intersection is V, since B is abelian of exponent dividing $p-1$. Therefore it suffices to find subgroups of G/N of index at most p whose intersection meets V trivially.

Considering the $\mathbb{F}_p$-vector space V as a B-module, Maschke's Theorem (Theorem 1 from Chapter 18 of [10]) tells us that V decomposes as a direct sum of irreducible B-modules. Since $x^{p-1}-1$ splits over $\mathbb{F}_p$, it follows that these irreducible submodules are one dimensional. Now we have submodules V_i of index p (codimension-one submodules), which yield subgroups $V_i \rtimes B$ of index p in G/N, and the intersection of all of these meets V trivially. □

Proof of Theorem 1.3. Let k be any field, and let K/k be a finite Galois subextension of $k^{[p]}/k$, where p is prime. This implies that K is contained in a compositum L of the splitting fields of finitely many irreducible, separable polynomials of degree p over k. Let $G = \mathrm{Gal}(L/k)$ and $N = \mathrm{Gal}(L/K)$. Then G isomorphic to a subdirect product of transitive groups of degree p, and N is normal in G. Proposition 6.1 implies that N is an intersection of subgroups of index at most p in G. By the Galois correspondence, this means that K is the compositum of finitely many extensions of k of degree at most p. Therefore, K/k is generated by elements of degree at most p. (In fact, it must be generated by elements whose degrees are either equal to p or divide $p-1$.) □

References

[1] Y. Berkovich, *Groups of prime power order, Vol. 1*, Gruyter Expositions in Mathematics, **46**, Walter de Gruyter GmbH & Co. KG, Berlin, (2008), with a foreword by Zvonimir Janko.

[2] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, **4** Cambridge University Press, Cambridge, (2006).

[3] E. Bombieri and U. Zannier, *A note on heights in certain infinite extensions of* $\mathbb{Q}$, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei, Mat. Appl., **9**, 12, (2001), 5–14.

[4] G. Butler and J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra, **11**, 8, (1983), 863–911.

[5] S. Checcoli *Fields of algebraic numbers with bounded local degrees and their properties*, Trans. Amer. Math. Soc., **365**, 4, (2013), 2223–2240.

[6] S. Checcoli and M. Widmer, *On the Northcott property and other properties related to polynomial mappings*, Math. Proc. Cambridge Philos. Soc., **155**, 1, (2013), 1–12.

[7] S. Checcoli and U. Zannier, *On fields of algebraic numbers with bounded local degrees*, C. R. Math. Acad. Sci. Paris, **349**, 1-2, (2011), 11–14.

[8] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, **163**, Springer-Verlag, New York, (1996).

[9] K. Doerk and T. Hawkes, *Finite soluble groups*, volume 4 of de Gruyter Expositions in Mathematics, Walter de Gruyter & Co., Berlin, (1992).

[10] D. S. Dummit and R. M. Foote, *Abstract algebra*, John Wiley & Sons Inc., Hoboken, NJ, third edition, (2004).

[11] W. Feit, *Some consequences of the classification of finite simple groups*, in The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979), Proc. Sympos. Pure Math., **37**, (1980), Amer. Math. Soc., Providence, R.I., 175–181.

[12] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, The Clarendon Press Oxford University Press, New York, fifth edition, (1979).

[13] A. Hulpke, *Transitive permutation groups - A GAP data library* www.gap-system.org/Datalib/trans.html.

[14] D. W. Masser, *The discriminants of special equations*, Math. Gaz., **50**, **372**, (1966), 158–160.

[15] J. Neukirch, A. Schmidt, and K. Wingberg, Cohomology of number fields, volume 323 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin, second edition, (2008).

[16] O. Neumann, *On the imbedding of quadratic extensions into Galois extensions with symmetric group*, in Proceedings of the conference on algebraic geometry (Berlin, 1985), Teubner-Texte Math., **92**, (1986), Leipzig, Teubner, 285–295.

[17] V. V. Prasolov, *Polynomials*, volume 11 of Algorithms and Computation in Mathematics, Springer-Verlag, Berlin, (2004), translated from the 2001 Russian second edition by Dimitry Leites.

[18] J.-P. Serre, *Topics in Galois theory*, volume 1 of Research Notes in Mathematics, Jones and Bartlett Publishers, Boston, MA, (1992). Lecture notes prepared by Henri Damon [Henri Darmon], With a foreword by Darmon and the author.

[19] The `GAP` Group. `GAP` – Groups, Algorithms, and Programming, Version 4.5.4, (2012).

[20] M. Widmer, *On certain infinite extensions of the rationals with Northcott property*, Monatsh. Math., **162**, 3, (2011), 341–353.

[21] H. Wielandt, *Finite permutation groups*, translated from the German by R. Bercov. Academic Press, New York, (1964).

Itamar Gal
Department of Mathematics,
University of Texas at Austin
2515 Speedway, Stop C1200
Austin, TX 78712, U.S.A.
E-mail: igal@math.utexas.edu
URL: http://www.ma.utexas.edu/users/igal

Robert Grizzard
Department of Mathematics
University of Texas at Austin
2515 Speedway, Stop C1200
Austin, TX 78712, U.S.A.
E-mail: rgrizzard@math.utexas.edu
URL: http://www.ma.utexas.edu/users/rgrizzard