ON THE VANISHING OF THE DENSITY IN ARTIN'S CONJECTURE ON PRIMITIVE ROOTS

GIACOMO CHERUBINI AND ANTONELLA PERUCCA

Abstract. Let K be a number field, and let $\alpha \in K^\times$ be not a root of unity. Consider the set consisting of the primes $\mathfrak{p}$ of K such that $(\alpha \bmod \mathfrak{p})$ is well-defined and generates the multiplicative group of the residue field at $\mathfrak{p}$. According to Artin's conjecture on primitive roots, this set admits a natural density. We investigate the reasons for which this density must be zero, making more explicit a famous result by Lenstra from 1977.

1. Introduction

This paper concerns Artin's conjecture on primitive roots, and we refer the reader to Moree's survey [8] for an introduction to this topic. Our starting point is a result by Cooke and Weinberger [4] from 1975 (that generalizes a result by Hooley [5]), which proves Artin's conjecture for all number fields conditionally under GRH.

Let K be a number field (and work within a fixed algebraic closure $\overline{K}$ of K). We let $\alpha \in K^\times$ be not a root of unity. For all results concerning Artin's conjecture mentioned in this paper, *we assume GRH* for the cyclotomic-Kummer extensions $K(\zeta_N, \sqrt[n]{\alpha})$ of K, where n, N are positive integers such that $n \mid N$. We build on the following result, where μ is the Möbius function:

Theorem 1 (Cooke and Weinberger)**.** *Assume GRH, and call S the set consisting of the primes $\mathfrak{p}$ of K such that $(\alpha \bmod \mathfrak{p})$ is well-defined and generates the multiplicative group of the residue field at $\mathfrak{p}$. The set S admits a natural density, which we call* $\mathrm{dens}(\alpha)$*, and we have*

$$\mathrm{dens}(\alpha) = \sum_{n \geqslant 1} \frac{\mu(n)}{[K(\zeta_n, \sqrt[n]{\alpha}) : K]}\,.$$

Moreover, $\mathrm{dens}(\alpha)$ *is also the natural density of the set of primes $\mathfrak{p}$ of K such that $\mathfrak{p}$ does not split completely in $K(\zeta_\ell, \sqrt[\ell]{\alpha})$ for any prime number ℓ.*

For any prime number ℓ, we call S_ℓ the set of primes $\mathfrak{p}$ such that $(\alpha \bmod \mathfrak{p})$ is well-defined and non-zero, and its index (namely, the index of $\langle(\alpha \bmod \mathfrak{p})\rangle$ in the multiplicative group at $\mathfrak{p}$) is coprime to ℓ. Remark that $S = \bigcap_\ell S_\ell$.

We call h the largest positive *squarefree* integer such that $\alpha \in K^{\times h}$. One condition that forces $\mathrm{dens}(\alpha) = 0$ is the existence of a prime number ℓ such that $K(\zeta_\ell, \sqrt[\ell]{\alpha}) = K$, namely such that $\zeta_\ell \in K$ and $\ell \mid h$. Remark that this condition even implies $\mathrm{dens}(S_\ell) = 0$. Over $K = \mathbb{Q}$, this is (conditionally under GRH) the only reason to have $\mathrm{dens}(\alpha) = 0$ because, as Hooley proved in [5], $\mathrm{dens}(\alpha)$ is non-zero for all rational numbers different from $0, \pm 1$ that are not squares.

The aim of this work is understanding the vanishing of the density in Artin's conjecture. Clearly, all works that describe the density (for example, [7]) improve, in particular, such understanding. Most notably, in [6, Theorem (4.6)] Lenstra provides a very general characterization of the vanishing of the density:

Theorem 2 (Lenstra)**.** *We have* $\mathrm{dens}(\alpha) \neq 0$ *if and only if the following holds: there is an automorphism in* $\mathrm{Gal}(K(\zeta_h)/K)$ *that (by varying ℓ among the prime numbers) is not the identity on any of the fields $K(\zeta_\ell, \sqrt[\ell]{\alpha})$ that are contained in $K(\zeta_h)$.*

We aim at making this result more explicit. The first assertion of the following result is also shown in [6, Corollary (4.8)]:

Theorem 3. *If $h = 1$, then we have* $\mathrm{dens}(\alpha) \neq 0$. *If h is a prime number, then we have* $\mathrm{dens}(\alpha) = 0$ *if and only if $\zeta_h \in K$.*

Roskam in [10, Theorem 3] made an example over a quadratic field where $\mathrm{dens}(\alpha) = 0$ and there is no prime divisor q of h such that $\zeta_q \in K$:

Example 4. *Let $K = \mathbb{Q}(\sqrt{5})$ and $\alpha = \beta^{15}$ where $\beta = (-3)(-\frac{5+\sqrt{5}}{2})$, so that $h = 15$. Then* $\mathrm{dens}(\alpha) = 0$ *because $K(\sqrt{\alpha})$, $K(\zeta_3)$, and $K(\zeta_5)$ are the three quadratic subextensions of the biquadratic extension $\mathbb{Q}(\zeta_{15})/K$. Indeed, there is no Galois automorphism of $\overline{K}/K$ that is not the identity on all the three fields $K(\sqrt{\alpha})$, $K(\zeta_3)$, and $K(\zeta_5)$ (which are the fields $K(\zeta_\ell, \sqrt[\ell]{\alpha})$ for $\ell = 2, 3, 5$).*

Since $\mathrm{dens}(\alpha) = 0$ if α is a square, we may suppose that h is odd. The following result shows that the previous example is, in a certain sense, the only possible example:

Theorem 5. *If h is the product of two odd prime numbers h_1 and h_2, then we have* $\mathrm{dens}(\alpha) = 0$ *if and only if at least one of the two following conditions holds: the field K contains ζ_{h_1} or ζ_{h_2}; the extension $K(\zeta_h)/K$ is biquadratic and its three quadratic subextensions are $K(\sqrt{\alpha})$, $K(\zeta_{h_1})$, and $K(\zeta_{h_2})$ (which are the fields $K(\zeta_\ell, \sqrt[\ell]{\alpha})$ for $\ell = 2, h_1, h_2$).*

Call C_n the cyclic group of order n, and call an abelian extension bicubic if its Galois group is isomorphic to $C_3 \times C_3$.

Theorem 6. *Suppose that h is the product of three odd prime numbers h_1, h_2, and h_3. Then we have* $\mathrm{dens}(\alpha) = 0$ *if and only if at least one of the following conditions holds:*

- *(i) the field K contains ζ_{h_i} for some $i \in \{1, 2, 3\}$; or, for two distinct $i, j \in \{1, 2, 3\}$ the extension $K(\zeta_{h_i h_j})/K$ is biquadratic and its three quadratic subfields are $K(\sqrt{\alpha})$, $K(\zeta_{h_i})$, $K(\zeta_{h_j})$ or $K(\zeta_{h_1})$, $K(\zeta_{h_2})$, $K(\zeta_{h_3})$;*
- *(ii) we have $\zeta_3 \in K$ and $K(\zeta_h)/K$ is bicubic and its four intermediate extensions are $K(\sqrt[3]{\alpha})$, $K(\zeta_{h_1})$, $K(\zeta_{h_2})$, $K(\zeta_{h_3})$;*
- *(iii) the Galois group of $K(\zeta_h)/K$ is isomorphic to $C_4 \times C_2$ such that, under this isomorphism, the field $K(\sqrt{\alpha})$ corresponds to the subgroup $\langle (1, 0) \rangle$ and the subgroups $K(\zeta_{h_1})$, $K(\zeta_{h_2})$, $K(\zeta_{h_3})$ correspond up to reordering to the subgroups $\langle (1, 1) \rangle$, $\langle (0, 1) \rangle$, $\langle (2, 1) \rangle$.*

A detailed analysis for the case where h has a small number of prime factors would be in principle possible, see Remark 13. In general, we can prove:

Theorem 7. *For every positive integer n there exists a constant $c_K(n)$ (independent from α) such that the following holds: if h is the product of prime numbers h_1 to h_n that are all greater than $c_K(n)$ and $\zeta_{h_i} \notin K$ for $i \in \{1, \dots, n\}$, then* $\mathrm{dens}(\alpha) > 0$.

For a finite abelian group $\mathcal{G}$ and for a prime number p we call *p-part* of $\mathcal{G}$ the subgroup of $\mathcal{G}$ that consists of all elements of order a power of p (this is also a quotient of $\mathcal{G}$). For brevity, we call groups $H_1, \dots, H_n$ *of vanishing type* in a group G if the following holds: $H_1, \dots, H_n$ are non-trivial proper subgroups of G; their union is G and their intersection is $\{0\}$.

Theorem 8. *Suppose that* $\mathrm{dens}(\alpha) = 0$ *and that for no prime number q we have $\zeta_q \in K$ and $q \mid h$. Then there exist a prime number p and prime numbers ℓ_i (for $i = 1, \dots, n$) such that one of the following holds:*

- *We have $\ell_i \mid h$ for every i. Calling L the compositum of the fields $K(\zeta_{\ell_i})$, the p-parts of the groups* $\mathrm{Gal}(L/K(\zeta_{\ell_i}))$ *are of vanishing type in the p-part of* $\mathrm{Gal}(L/K)$.
- *We have $\ell_1 = p$ and $\zeta_p \in K$ and $\ell_i \mid h$ for every $i > 1$. Calling L the compositum of $K(\sqrt[p]{\alpha})$ and the fields $K(\zeta_{\ell_i})$ for $i \neq 1$, the p-parts of the groups* $\mathrm{Gal}(L/K(\sqrt[p]{\alpha}))$ *and* $\mathrm{Gal}(L/K(\zeta_{\ell_i}))$ *for $i \neq 1$ are of vanishing type in the p-part of* $\mathrm{Gal}(L/K)$.

Fixing the number of prime divisors of h, the above groups of vanishing type and their union belong (up to isomorphism) to a finite list that is independent of K and α.

Some of our observations straight-forwardly extend if we replace α by a finitely generated subgroup Γ of $K^\times$: in this case the group $\mathrm{Gal}(K(\sqrt[p]{\Gamma})/K)$ may not be cyclic.

The overview of the paper is as follows: the results on Artin's conjecture are proven in Section 2; explicit examples of K and α for which $\mathrm{dens}(\alpha) = 0$ because of the different reasons considered in our results are presented in Section 3; the results about (and the explicit computations with) finite abelian groups are collected in Sections 4 and 5 and they are of independent interest.

2. The density in Artin's conjecture

We keep the notation from the introduction and write $K_\ell := K(\zeta_\ell, \sqrt[\ell]{\alpha})$. We call J_h the set consisting of the prime divisors of h and J_K the set consisting of the primes q such that $\zeta_q \in K$.

Remark 9. *We require h to be squarefree because, if H is the largest positive integer such that $\alpha \in K^{\times H}$, it's only the prime divisors of H that matter for our problem. Indeed, if $\beta \in K^\times$ is not a perfect power, then $\alpha := \beta^h$ and $\alpha := \beta^H$ give rise to the same fields K_ℓ.*

Recall that if there is a prime number q such that $\zeta_q \in K$ and $\alpha \in K^{\times q}$ (namely, $q \mid h$), then we have $\mathrm{dens}(\alpha) = 0$. If we exclude this case, then the sets J_h and J_K are disjoint.

Theorem 10. *Suppose that for every prime q such that $\zeta_q \in K$ we have $q \nmid h$. There exists a finite abelian extension L/K and finitely many subextensions L_i/K such that we have $\mathrm{dens}(\alpha) \neq 0$ if and only if there is an automorphism in $\mathrm{Gal}(L/K)$ that is not the identity on any of the L_i's. We may take as L_i's the fields K_ℓ for $\ell \in J_h \cup J_K$ and let L be their compositum.*

Proof. By Theorem 1, $\mathrm{dens}(\alpha)$ is the density of the primes $\mathfrak{p}$ that do not split completely in any of the fields K_ℓ, where ℓ is a prime number. To study the vanishing of the density we only need to study a finite set of prime numbers. Indeed, we can define the complement as the set of all primes ℓ such that K_ℓ is not contained in the compositum of the fields $K_{\ell'}$ for all $\ell \neq \ell'$ (by [9, Proposition 4.3] the constructed set is finite).

By our assumption on α, for every prime ℓ the extension K_ℓ/K is non-trivial (namely, there is no prime ℓ such that $\zeta_\ell \in K$ and $\ell \mid h$). The primes ℓ such that $\zeta_\ell \notin K$ and $\ell \nmid h$ are in the complement of the set that we constructed. Indeed, equivalently K_ℓ is not contained in the compositum of the fields $K(\zeta_{\ell'})$ for all $\ell \neq \ell'$ (and this holds because the extension K_ℓ/K is not abelian by Schinzel's theorem [11, Theorem 2]). For $\ell \in J_h \cup J_K$, the extension K_ℓ/K is abelian: we may take for L their compositum and conclude. □

Thus we have the following criterion:

Remark 11. *Suppose that for all primes q such that $\zeta_q \in K$ we have $q \nmid h$. Let M be a positive squarefree integer such that, with the notation of Theorem 10, we have $L = K(\zeta_M, \sqrt[M]{\alpha})/K$. Then we have $\mathrm{dens}(\alpha) = 0$ if and only if $\mathrm{Gal}(K(\zeta_M, \sqrt[M]{\alpha})/K)$ is the union of its subgroups $\mathrm{Gal}(K(\zeta_M, \sqrt[M]{\alpha})/K(\zeta_\ell, \sqrt[\ell]{\alpha}))$, where ℓ varies over the prime divisors of M.*

Proof of Theorem 3. Suppose that $h = 1$. By Theorem 10, the field L is the compositum of the fields $K_\ell = K(\sqrt[\ell]{\alpha})$ for $\ell \in J_K$. These fields are non-trivial and have pairwise coprime degrees over K, so the automorphism as in Theorem 10 can be found, implying that $\mathrm{dens}(\alpha) \neq 0$.

Now suppose that h is prime. Clearly, if $\zeta_h \in K$ we have $\mathrm{dens}(\alpha) = 0$ so suppose that K_h is non-trivial. With respect to the previous case, we have the additional field $K_h = K(\zeta_h)$. We may replace K_h by a subextension that has degree ℓ_h where ℓ_h is prime. We have field extensions with pairwise disjoint degrees, possibly with the exceptions of two fields of degree ℓ_h. These two fields are either equal or linearly disjoint over K, and in both cases we can find an automorphism that is not the identity on neither of the fields and we may easily conclude. □

Remark 12. *If L is a finite non-trivial Galois extension of K, then there exists an automorphism of $\overline{K}/K$ that is not the identity over L. If L_1 and L_2 are two finite non-trivial Galois extensions of K, then there exists an automorphism of $\overline{K}/K$ that is neither the identity on L_1 nor on L_2. Indeed, this is clear if the two fields are linearly disjoint over K, else it suffices to extend an automorphism that is not the identity on the non-trivial extension $L_1 \cap L_2$. Alternatively, see Remark 20 applied to the Galois group of L_1L_2/K with the subgroups $\mathrm{Gal}(L_1L_2/L_i)$ for $i = 1, 2$).*

Proof of Theorem 5. Suppose that ζ_{h_1} and ζ_{h_2} are both not contained in K. With the notation of Theorem 10 we have to consider some non-trivial extensions of K, namely $L_1 := K(\zeta_{h_1})$, $L_2 := K(\zeta_{h_2})$ and the fields $K_\ell = K(\sqrt[\ell]{\alpha})$ for ℓ such that $\zeta_\ell \in K$. Since the fields K_ℓ have pairwise coprime degrees, by decomposing the problem w.r.t. the prime parts of the corresponding Galois groups we reduce to the situation where we have L_1, L_2, and where L_3 is one of the fields K_ℓ's. Call $L = L_1L_2L_3$ and define $G := \mathrm{Gal}(L/K)$ and $H_i := \mathrm{Gal}(L/L_i)$.

We may assume that none of the fields L_1, L_2, and L_3 is contained in another one, else we may reduce to handling at most two extensions (see Remark 12). Thus the subgroups H_i's are non-trivial and proper, and G is not cyclic. We may then conclude by Theorem 21, in particular we must have $L_3 = K(\sqrt{\alpha})$. □

Proof of Theorem 6. We imitate the proof of Theorem 5. Consider the fields $L_i := K(\zeta_{h_i})$ for $i = 1, 2, 3$. Suppose that, for some $q \in J_K$, the field $L_4 := K(\sqrt[q]{\alpha})$ is such that $\mathrm{Gal}(L/K)$ is the union of its subgroups $\mathrm{Gal}(L/L_i)$ for $i = 1, 2, 3, 4$, where $L = L_1L_2L_3L_4$. If $\mathrm{Gal}(L/K)$ is the union of three of these subgroups, we are reduced to the situation of Theorem 5. Else, we may apply Theorem 25 to conclude. □

Notice that in Theorem 6 we don't make apparent use of the case in Theorem 25 where the group is isomorphic to $C_2 \times C_2 \times C_2$: this is because we need all subgroups to have order 4 (as the corresponding subextensions need to be cyclic for our application) and then we are left with just one case where three of the corresponding subextensions are the three quadratic subextensions of a biquadratic extension.

Remark 13. *In the same spirit of Theorem 6, it would be possible to analyze the vanishing of the density in case h has a small number of prime factors. The group-theoretical reason is that we can rely on Remark 24.*

Proof of Theorem 7. Suppose that for all $h_i \in J_h$ we have $\zeta_{h_i} \notin K$. By Theorem 10 and by reducing to p-groups (considering the p-parts of the given groups) we have to consider the Galois group of $K(\sqrt[p]{\alpha})/K$ in case $\zeta_p \in K$ (thus, $p \nmid h$) and at most n p-groups that are the p-part of the Galois group of $K(\zeta_\ell)/K$ for $\ell \in J_h$ (we only need to consider those groups that are non-trivial). So we have at most $n+1$ fields to consider, requiring that there is an automorphism of their compositum that is not the identity on any of them. Considering the corresponding group-theoretical problem, we have a p-group that should not be the union of at most $n+1$ proper subgroups. There are only finitely many primes ℓ, depending only on K, □

We call $\mathcal{P}$ the set of the prime numbers. We define the p-part of a finite abelian extension of K as its subextension whose Galois group is the p-part of the original Galois group.

Lemma 14. *Suppose that for every prime divisor q of h we have $\zeta_q \notin K$. Let*

$$F : J_h \cup J_K \to \mathcal{P}$$

be a function satisfying the following: for $q \in J_K$, we have $F(q) = q$; for $\ell \in J_h$ the prime $F(\ell)$ divides $[K(\zeta_\ell) : K]$. We have $\mathrm{dens}(\alpha) \neq 0$ if and only if we can find a function F as above, such that for all p in the image of F the set of preimages $F^{-1}(p)$ has the following property: there is an automorphism of $\overline{K}/K$ that, for all $\ell \in F^{-1}(p)$, is not the identity on the p-part of $K(\zeta_\ell, \sqrt[\ell]{\alpha})$.

Proof. The statement is the formal way of expressing a very natural idea. If we have a finite abelian extension L/K the following holds: a Galois automorphism is not the identity on L if and only if there exists a prime number p that divides $[L : K]$ such that said automorphism is not the identity on the p-part of L/K. □

Remark 15. *Thanks to Lemma 14, we are reduced to analyze for finitely many prime numbers p a family of finite and non-trivial abelian extensions whose Galois group is a p-group. The requested automorphism always exists if the cardinality of $F^{-1}(p)$ does not exceed p, see Remark 23.*

Proof of Theorem 8. The last assertion is because the number of groups of vanishing type is at most the number of prime divisors of h plus 1, so we may invoke Remark 23.

With the notation of Lemma 14, fix a function F and some prime p such that the property in Lemma 14 does not hold for $F^{-1}(p)$. (Aside: We may choose for practicality F and p such that $n := \#F^{-1}(p)$ is as small as possible, or p is as small as possible.) Let $\ell_1, \dots, \ell_n$ be the elements of $F^{-1}(p)$, setting $\ell_1 = p$ if $p \in F^{-1}(p)$. Write $K_{\ell_i} := K(\zeta_{\ell_i}, \sqrt[\ell_i]{\alpha})$ and L for their compositum. It follows from the definition of F that the p-parts of the extensions $\mathrm{Gal}(K_{\ell_i}/K)$ are non-trivial. Thus $\mathrm{Gal}(L/K_{\ell_i})$ is a proper subgroup of $\mathrm{Gal}(L/K)$ for every i. By the definition of L the intersection of the groups $\mathrm{Gal}(L/K_{\ell_i})$ is the identity. Moreover, the missing property for $F^{-1}(p)$ implies that the union of $\mathrm{Gal}(L/K_{\ell_i})$ is $\mathrm{Gal}(L/K)$. Finally, the missing property for $F^{-1}(p)$ implies that $\mathrm{Gal}(L/K)$ is not cyclic. Considering that $\mathrm{Gal}(K_{\ell_i}/K)$ is cyclic, the group $\mathrm{Gal}(L/K_{\ell_i})$ cannot be $\{0\}$. □

3. Examples

We present some examples to illustrate the cases in Theorem 6 that stem from Theorem 25.

Example 16. *Suppose that $K(\zeta_{7\cdot 13})$ is a bicubic extension whose four intermediate subextensions of degree 3 are $K(\zeta_7)$, $K(\zeta_{13})$, $K(\zeta_{19})$, and $K(\zeta_{31})$. Then $\mathrm{dens}(\alpha) = 0$ if $h = 7 \cdot 13 \cdot 19 \cdot 31$. Moreover, in case $\zeta_3 \in K$, we have $\mathrm{dens}(\alpha) = 0$ if $h = pqr$ and $K(\sqrt[3]{\alpha}) = K(\zeta_s)$, where $\{p, q, r, s\} = \{7, 13, 19, 31\}$. We may take as K the number field generated by the following elements:*

$$\sqrt{-7};\ \sqrt{-2(13+3\sqrt{13})};\ \zeta_5, \sqrt{-31}, \theta_{31};\ \zeta_9, \sqrt{-19}, \eta_{19}^3;\ \eta_7\eta_{13}\eta_{19},\ \eta_7^2\eta_{13}\eta_{31}$$

where we consider Gauss sums with the following powers:

$$\theta_{31}^5 := 3286\zeta_5 + 2046\zeta_5^2 + 6231\zeta_5^3 + 1116\zeta_5^4 \in \mathbb{Q}(\zeta_5)$$
$$\eta_7^3 := -14\zeta_3 + 7\zeta_3^2 \in \mathbb{Q}(\zeta_3)$$
$$\eta_{13}^3 := 13\zeta_3 + 52\zeta_3^2 \in \mathbb{Q}(\zeta_3)$$
$$\eta_{31}^3 := 31\zeta_3 - 155\zeta_3^2 \in \mathbb{Q}(\zeta_3)$$
$$\eta_{19}^9 := -156978\zeta_9^2 + 7087\zeta_9^3 - 178866\zeta_9^4 - 99180\zeta_9^5 - 137522\zeta_9^6 - 599184\zeta_9^7 \in \mathbb{Q}(\zeta_9)\,.$$

Indeed, the first eight generators (which generate a subfield K') belong to the linearly disjoint extensions $\mathbb{Q}(\zeta_7)$, $\mathbb{Q}(\zeta_{13})$, $\mathbb{Q}(\zeta_{5\cdot 31})$, $\mathbb{Q}(\zeta_{9\cdot 19})$ and they ensure that the extensions $K(\zeta_m)/K$ with $m = 7, 13, 19, 31$ are cubic. Notice that $\sqrt{-2(13+3\sqrt{13})}$ generates the quartic cyclic subextension of $\mathbb{Q}(\zeta_{13})/\mathbb{Q}$ because $-2(13+3\sqrt{13})$ is the square of the trace from $\mathbb{Q}(\zeta_{4\cdot 13})$ to $\mathbb{Q}(\zeta_{13})$ of the quartic Gauss sum.

The Galois group of $K'(\zeta_{7\cdot 13\cdot 19\cdot 31})/K'$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^4$. Since $\zeta_3 \in K'$, by Kummer theory the corresponding group of radicals is generated by $\eta_7, \eta_{13}, \eta_{19}, \eta_{31}$. The last generators in the list then ensure that the Galois group of $K(\zeta_{7\cdot 13\cdot 19\cdot 31})/K$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$ and that the extensions $K(\zeta_m)/K$ with $m = 7, 13, 19, 31$ are distinct but contained in $K(\zeta_{7\cdot 13})$. In the latter example, we may take $\alpha = (\eta_s^3)^{pqr}$.

Example 17. *Let F be the compositum of $\mathbb{Q}(i)$ and the cubic subextension of $\mathbb{Q}(\zeta_{13})/\mathbb{Q}$. Let $\eta_5^4 = -15 + 20\zeta_4$ and $\eta_{13}^4 = 65 - 156\zeta_4$ in $\mathbb{Q}(i)$ be the fourth powers of the quartic Gauss sums corresponding to the fields $\mathbb{Q}(\zeta_{20})$ and $\mathbb{Q}(\zeta_{52})$ respectively.*

The Galois group of $F(\zeta_{15})/F$ is isomorphic to $C_4 \times C_2$. The subgroup corresponding to $F(\zeta_3)$ is $\langle(1,0)\rangle$, and the one corresponding to $F(\zeta_5)$ is $\langle(0,1)\rangle$. The subfield corresponding to $\langle(1,1)\rangle$ is the quadratic extension $F(\sqrt{-15})$. Finally, the subfield corresponding to $\langle(2,1)\rangle$ is the quartic cyclic field generated by $\eta_5\sqrt{-3}$. Extending the field F by $\eta_{13}\eta_5\sqrt{-3}$ has the effect that the subfield corresponding to the last subgroup is $F(\zeta_{13})$ thus, if $K = F$ and $\alpha = (-15)^{3\cdot 5\cdot 13}$ (so that $h = 3\cdot 5\cdot 13$), we have $\mathrm{dens}(\alpha) = 0$. We can vary this example by enlarging F with the cubic subextension of $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ and by $\sqrt{(-7)(-15)}$, so that $F(\sqrt{-15}) = F(\zeta_7)$. Then $h = 3 \cdot 5 \cdot 7 \cdot 13$ implies $\mathrm{dens}(\alpha) = 0$.

Example 18. *We may generalize Example 16 to any odd prime number p. Namely, there exists a number field K and prime numbers $q_1, \dots, q_{p+1}$ such that $\mathrm{Gal}(K(\zeta_{q_1q_2})/K)$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$ and the subextensions of $K(\zeta_{q_1q_2})/K$ of degree p are the fields $K(\zeta_{q_i})$ with $i = 1, \dots, p+1$.*

In this case, the following holds: if $h = q_1 \cdots q_{p+1}$, *then* $\mathrm{dens}(\alpha) = 0$. *Moreover, supposing that* $\zeta_p \in K$, *we also have* $\mathrm{dens}(\alpha) = 0$ *if* $K(\sqrt[p]{\alpha}) = K(\zeta_{q_j})$ *for some* $j \in \{1, \dots, p+1\}$ *and* $h = \prod_{i \neq j} q_i$.

To prove the existence of $K, q_1, \dots, q_{p+1}$, *as done in Example 16, we may first construct a number field* K' *containing* ζ_p *such that the extensions* $K'(\zeta_{q_i})/K'$ *are linearly independent and of degree* p *and then apply Kummer theory to enlarge* K' *and conclude. For the former step we may use appropriate Gauss sums as generators, assuming that suitable roots of unity are contained in the field* K'. *For the latter step, calling* γ_i *the radical such that* $\gamma_i^p \in K'$ *and* $K'(\gamma_i) = K'(\zeta_{q_i})$, *we may add the generators* $\gamma_1^j \gamma_2 \gamma_{j+2}$ *for every* $j = 1, \dots, p-1$.

Remark 19. *We outline a general procedure to exhibit new and substantially different examples of* K, α *such that* $\mathrm{dens}(\alpha) = 0$. *Fix a prime number* p *and abelian* p*-groups* $H_1, \dots, H_n$ *that are of vanishing type in an abelian* p*-group* G: *for small values of* p *and* n, *such groups — if they exist — may be found with a computer search testing various possibilities for* G *(whose size divides* $n!$ *by Remark 24). We have to restrict to the case where* G/H_i *is cyclic for every* i *by Theorem 8 because* $K(\sqrt[p]{\alpha})/K$ *and the cyclotomic extensions* $K(\zeta_{\ell_i})/K$ *are cyclic. Let* E *be the exponent of* G *and work over the number field* $K = \mathbb{Q}(\zeta_{p^E})$. *Up to extending this field, we may choose primes* $\ell_1, \dots, \ell_n$ *such that the extensions* $K(\zeta_{\ell_i})/K$ *are cyclic of degree* $\#H_i$ *and they are linearly independent over* K. *In case that w.l.o.g. the group* H_1 *has size* p, *we may replace* $K(\zeta_{\ell_1})$ *by* $K(\sqrt[p]{\alpha})$ *for some* $\alpha \in K^\times$ *such that* h *is odd,* $\ell_i \mid h$ *for all* $i \neq 1$ *and such that* $K(\sqrt[p]{\alpha}) \cap K(\zeta_{\ell_2}, \dots, \zeta_{\ell_n}) = K$. *By Lemma 26, up to extending* K, *the considered cyclotomic extensions (possibly, replacing the first by the Kummer extension* $K(\sqrt[p]{\alpha})/K$*) are as in Theorem 8, the groups of vanishing type being isomorphic to the groups* H_1 *to* H_n, *and their union being isomorphic to* G.

4. Finite non-cyclic abelian groups as union of proper subgroups

Let G be a non-cyclic group: the cyclic subgroups generated by the elements of G that are different from the identity are non-trivial and proper and their set-theoretical union is G. On the other hand, it is impossible to cover a cyclic group with proper subgroups.

Remark 20. *No group* G *is the union of two proper subgroups* H_1 *and* H_2. *This is well-known, and a cardinality argument suffices (because the index of a proper subgroup is at least* 2 *and subgroups are not disjoint sets):*

$$\#(H_1 \cup H_2) = \#H_1 + \#H_2 - \#(H_1 \cap H_2) \leqslant \frac{1}{2}\#G + \frac{1}{2}\#G - 1 < \#G\,.$$

Recall our notation: we call groups $H_1, \dots, H_n$ *of vanishing type* in a group G if the following holds: $H_1, \dots, H_n$ are non-trivial subgroups of G; their union is G and their intersection is $\{0\}$. Moreover, we call them *irredundant* if there is no index $i = 1, \dots, n$ such that, removing H_i, the union of the subgroups is still G.

Theorem 21 (G. Scorza)**.** *Let* H_1, H_2, H_3 *be finite abelian groups that are of vanishing type in an abelian group* G. *Then* G *is isomorphic to* $C_2 \times C_2$ *and* H_1, H_2, *and* H_3 *are the three subgroups of* G *of order* 2.

Proof. This is a special case of [1, Theorem 2], noticing that in the proof $G/(H_1 \cap H_2 \cap H_3)$ is isomorphic to $C_2 \times C_2$ and hence the same holds for G. □

Example 22. *Let* p *be a prime number, and suppose that the group* $C_p \times C_p$ *is the union of non-trivial subgroups. Then one must take all* $p+1$ *subgroups of order* p. *Indeed, beyond the identity, each subgroup contributes with* $p-1$ *elements, and we have* $p^2 = 1 + (p+1)(p-1)$.

Remark 23. *(This remark relates to [12, Theorem 3.6] and [2, Theorem 4].) Let* G *be a finite abelian group, and let* p_0 *be the smallest prime divisor of the order of* G. *Then, if* G *is the union of* n *proper subgroups, we must have* $n \geqslant p_0 + 1$. *This is clear by cardinality reasons because each proper subgroup has index at least* p_0, *and the subgroups are not disjoint.*

Notice that, if G *has two cyclic components that have order a power of one same prime number* p, *then it is possible to cover* G *with* $p+1$ *groups (we may take the preimages of the proper non-trivial subgroups of* $C_p \times C_p$ *under a surjective group homomorphism).*

Remark 24. *Suppose that a finite abelian group G is the union of n proper subgroups whose intersection is the identity. Then, up to isomorphism, there are only finitely many possibilities for G and hence also for the subgroups. This is a consequence of [1, Theorem 6] (see also [13]). Indeed, the order of G cannot exceed $n!$.*

4.1. **The union of four subgroups intersecting at the identity.**

Theorem 25. *Let $H_1, \dots, H_4$ be groups of vanishing type in a finite abelian group G that are irredundant. Then one of the following holds:*

(i) G is isomorphic to $C_3 \times C_3$ and H_1 to H_4 are the four subgroups of G of order 3;
(ii) G is isomorphic to $C_2 \times C_2 \times C_2$ and, up to isomorphism, two subgroups are $\{0\} \times C_2 \times C_2$, and $C_2 \times \{0\} \times C_2$ and the remaining two subgroups are either $\langle (1,1,1)\rangle$ and $\langle (1,1,0)\rangle$ or $C_2 \times C_2 \times \{0\}$ and $\langle (1,1,1)\rangle$;
(iii) G is isomorphic to $C_4 \times C_2$ and the four subgroups are $\langle (1,0)\rangle$, $\langle (1,1)\rangle$, $\langle (0,1)\rangle$, and $\langle (2,1)\rangle$.

Proof. As G is the union of proper subgroups, it is not cyclic. Since G is not the union of three of these subgroups, the four subgroups are irredundant in the sense of [1] (namely, no group is contained in the union of the others). By Remark 24 the order of G does not exceed 24. Since G is non-cyclic we must have at least two cyclic components whose order is a power of one same prime number. Thus G has as quotient $C_2 \times C_2$ or $C_3 \times C_3$.

In the latter case G is isomorphic to either $C_3 \times C_3$ or $C_3 \times C_3 \times C_2$. If G is isomorphic to $C_3 \times C_3$, we easily conclude. If G is isomorphic to $C_3 \times C_3 \times C_2$: The 8 elements of order 6 only belong to proper subgroups that have index 3; to take all of them we need to take the four subgroups of index 3 that, however, all contain $(0,0,1)$ hence this case cannot occur.

Now consider the former case. We cannot have $C_2 \times C_2$ as this group has no four irredundant subgroups. The order of G (which is a multiple of 4) then belongs to the following list: $8, 12, 16, 20, 24$.

• If G is $H \times C_p$ with $p = 3, 5$ and where H has order a power of 2: If a subgroup contains an element of order multiple of p, then it contains also the element $(0,1)$. Since the four subgroups have trivial intersection, the elements of order multiple of p are contained in three of the subgroups. The three subgroups are then such that their projections on H cover this quotient and we deduce that the three subgroups already cover the group, so this case cannot occur.

• If G is $C_8 \times C_2$: To take the elements of order 8 we need to take the two cyclic subgroups of index 2, namely $\langle (1,0)\rangle$ and $\langle (1,1)\rangle$. The remaining four elements cannot belong to one same subgroup, because three subgroups cannot cover the group. So w.l.o.g. the third group contains $(2,1)$ and its multiples $(4,0)$ and $(6,1)$ but neither $(0,1)$ nor $(4,1)$, which must then belong to the fourth subgroup. However, the four subgroups all contain $(4,0)$ and hence this case cannot occur.

• If G is $C_2 \times C_2 \times C_2 \times C_2$: This case does not occur because no four proper subgroups cover the group. Indeed, take four distinct subgroups of index 2 that, up to isomorphism, consist of the elements whose i-th projection is zero. Then $(1,1,1,1)$ is not contained in any of the groups.

• If G is $C_2 \times C_2 \times C_2$: having at most one subgroup of order 4 does not allow to cover the group, so up to isomorphism, two subgroups are $H_1 = \{0\} \times C_2 \times C_2$ and $H_2 = C_2 \times \{0\} \times C_2$. If one third subgroup has order 4, up to isomorphism it is $C_2 \times C_2 \times \{0\}$: the only element left, to be contained in the last subgroup, is then $(1,1,1)$ (and the last subgroup must have order 2 as we want irredundant groups). Else, the last two subgroups have order 2 and they must be generated respectively by the missing element $(1,1,1)$ and $(1,1,0)$.

• If G is $C_4 \times C_2$: to take the four elements of order 4 we need the two subgroups $\langle (1,0)\rangle$ and $\langle (1,1)\rangle$. Since the subgroups must be irredundant, the two remaining elements $(0,1)$ and $(2,1)$ must be contained in the two remaining subgroups (and not both in the same group). The last two groups must have exponent 2 and to avoid that they coincide they must have order 2.

• If G is $C_4 \times C_4$: To take the 12 elements of order 4, we can either take the three distinct subgroups of order 8 or we take two subgroups of order 8 and two groups of order and exponent 4 (in such a way that the elements of order 4 in the subgroups are all distinct). In the former case, the three subgroups already cover the group, so we must be in the latter case. The two subgroups

of order 4 are, up to isomorphism, $\langle(1,0)\rangle$ and $\langle(0,1)\rangle$. The remaining elements of order 4 are, up to multiples, $(1,1)$, $(1,2)$, $(1,3)$, and $(2,1)$. One of the two subgroups of order 8 should contain $(2,1)$ and one of the other three elements: this is impossible because $(2,1)$ and any of the other three elements generates the group. So this case cannot occur.

• If G is $C_4 \times C_2 \times C_2$: We concluded with a computer check (with [3]) that this case cannot occur. □

4.2. **The union of five subgroups intersecting at the identity.** Let G be a finite abelian group and suppose that $H_1, \dots, H_5$ are of vanishing type in G. By Remark 24, the order of G cannot exceed 120. Moreover, G cannot be cyclic so there is a prime p such that $C_p \times C_p$ is a quotient of G (clearly, $p < 11$). For our applications, we may suppose that G is an abelian p-group.

A computer search confirmed that there are abelian p-groups G with $\#G \leqslant 120$ and subgroups $H_1, \dots, H_5$ of vanishing type in G and irredundant. For instance, we have the following examples (for which it is immediate to verify the requested properties):

- Let $G = C_8 \times C_2$ and consider the subgroups
$$H_1 = \langle(4,1)\rangle, \quad H_2 = \langle(0,1)\rangle, \quad H_3 = \langle(2,1)\rangle,$$
$$H_4 = \langle(1,1)\rangle, \quad H_5 = \langle(1,0)\rangle.$$
The groups $H_1, \dots, H_5$ are of vanishing type in G and they are irredundant. Additionally, G/H_i is cyclic for each $i = 1, \dots, 5$. This is the only choice of subgroups $H_1, \dots, H_5$ that are of vanishing type in $C_8 \times C_2$.
- Let $G = C_4 \times C_4$ and take
$$H_1 = \langle(1,1)\rangle, \quad H_2 = \langle(1,2)\rangle, \quad H_3 = \langle(1,3)\rangle,$$
$$H_4 = \langle(1,0)\rangle, \quad H_5 = \langle(0,1),(2,0)\rangle.$$
The groups $H_1, \dots, H_5$ are of vanishing type in G and they are irredundant. Additionally, G/H_i is cyclic for each $i = 1, \dots, 5$.

We remark that we must have $p = 2, 3$. Indeed, for $p \geqslant 5$ the only non-cyclic p-group G of order at most 120 is $C_5 \times C_5$ and we cannot have five subgroups of vanishing type in it by Remark 23.

5. One technical result on abelian p-groups

We are going to prove, for the convenience of the reader, a general result on abelian p-groups. Notice that, in the following statement, the assumption $\sum_i H_i = G$ holds if we have $\bigcup_i H_i = G$. Moreover, if the X_j's are groups (where $j = 1, \dots, r$), then we write $\prod_{j \neq i} X_j$ to mean the following subgroup of $\prod_j X_j$:

$$\Big(\prod_{j<i} X_j \times \{0\} \times \prod_{j>i} X_j\Big).$$

Lemma 26. *Let p be a prime number, let G be a finite abelian p-group, and let H_i (where $i = 1, \dots, r$) be non-trivial subgroups of G such that*

$$\bigcap_i H_i = \{0\} \qquad \sum_i H_i = G \qquad \text{and} \qquad G/H_i \text{ is cyclic for all } i\,.$$

There exist positive integers n_j (where $j = 1, \dots, r$) and an injection $G \hookrightarrow \prod_j \mathbb{Z}/p^{n_j}\mathbb{Z}$ such that for every i we have

$$H_i = G \cap \prod_{j \neq i} \mathbb{Z}/p^{n_j}\mathbb{Z}\,.$$

For every j the number p^{n_j} divides the exponent of G.

Proof. Let $\widehat{G}$ be the Pontryagin dual of G and let $H_i^\perp \cong \widehat{G/H_i}$ be the kernel of the projection $\widehat{G} \twoheadrightarrow \widehat{H}_i$. We then have

$$\sum_i H_i^\perp = \widehat{G} \qquad \bigcap_i H_i^\perp = 0 \qquad \text{and} \qquad H_i^\perp \text{ is cyclic for all } i.$$

Fix isomorphisms $H_i^\perp \cong \mathbb{Z}/p^{n_i}\mathbb{Z}$ for appropriate positive integers n_i (the last assertion is then evident). Then the embeddings $H_i^\perp \hookrightarrow \hat{G}$ lead to an obvious homomorphism

$$f : \prod_j \mathbb{Z}/p^{n_j}\mathbb{Z} \twoheadrightarrow \widehat{G}$$

such that $H_i^\perp = f(\mathbb{Z}/p^{n_i}\mathbb{Z})$ holds for all i and which is surjective because $\sum_i H_i^\perp = \widehat{G}$. This yields a diagram with exact columns:

$$\begin{array}{ccc} H_i^\perp & \xleftarrow{\sim} & \mathbb{Z}/p^{n_i}\mathbb{Z} \\ \downarrow & & \downarrow \\ \widehat{G} & \xleftarrow{f} & \prod_j \mathbb{Z}/p^{n_j}\mathbb{Z} \\ \downarrow & & \downarrow \\ \widehat{G}/H_i^\perp & \xleftarrow{} & \prod_{j\neq i} \mathbb{Z}/p^{n_j}\mathbb{Z} \end{array}$$

Its dual is the diagram (choosing implicitly some isomorphism $\widehat{\mathbb{Z}/p^{n_j}\mathbb{Z}} \cong \mathbb{Z}/p^{n_j}\mathbb{Z}$):

$$\begin{array}{ccc} G/H_i & \xrightarrow{\sim} & \mathbb{Z}/p^{n_i}\mathbb{Z} \\ \uparrow & & \uparrow \\ G & \xrightarrow{\hat{f}} & \prod_j \mathbb{Z}/p^{n_j}\mathbb{Z} \\ \uparrow & & \uparrow \\ H_i & \hookrightarrow & \prod_{j\neq i} \mathbb{Z}/p^{n_j}\mathbb{Z} \end{array}$$

and we may conclude because the lower diagram is a pull-back (because the top horizontal map is an isomorphism). □

Acknowledgments. We thank Fritz Hörmann for Lemma 26 and Pietro Sgobba for useful comments. Antonella Perucca is the main author of this paper, which originated from a discussion of the two authors at the INdAM Institute in Rome. Giacomo Cherubini is a member of the INdAM group GNSAGA.

References

[1] Bhargava, M. *Groups as unions of proper subgroups.* Am. Math. Mon. 116, No. 5, 413-422 (2009). 6, 7
[2] Bhargava, M. *When is a group the union of proper normal subgroups?* Am. Math. Mon. 109, No. 5, 471-473 (2002). 6
[3] Cherubini, G., PARI/GP code for finding groups of vanishing type, https://sites.google.com/site/ggcherubini/publications. 8
[4] Cooke, G.; Weinberger, P. J. *On the construction of division chains in algebraic number rings, with applications to SL_2.* Commun. Algebra 3, 481-524 (1975). 1
[5] Hooley, C. *On Artin's conjecture.* J. Reine Angew. Math. 225, 209-220 (1967). 1
[6] Lenstra, H. W. jun. *On Artin's conjecture and Euclid's algorithm in global fields.* Invent. Math. 42, 201-224 (1977). 1
[7] Lenstra, H. W. jun.; Moree, P.; Stevenhagen, P. *Character sums for primitive root densities.* Math. Proc. Camb. Philos. Soc. 157, No. 3, 489-511 (2014). 1
[8] Moree, P. *Artin's primitive root conjecture – a survey.* Integers 12, No. 6, 1305-1416, A13 (2012). 1
[9] Perucca, A.; Shparlinski, I. E. *Uniform bounds for the density in Artin's conjecture on primitive roots.* Bull. Lond. Math. Soc. 57, No. 3, 978-991 (2025). 3
[10] Roskam, H. *Artin's primitive root conjecture for quadratic fields.* J. Théor. Nombres Bordx. 14, No. 1, 287-324 (2002). 2
[11] Schinzel, A. *Abelian binomials, power residues and exponential congruences.* Acta Arith. 32, 245-274 (1977). 3
[12] Tomkinson, M. J. *Groups as the union of proper subgroups.* Math. Scand. 81, No. 2, 191-198 (1997). 6
[13] Tomkinson, M. J. *Groups covered by finitely many cosets or subgroups.* Commun. Algebra 15, 845-859 (1987). 7