UNIFORM BOUNDS FOR THE DENSITY IN ARTIN'S CONJECTURE ON PRIMITIVE ROOTS

ANTONELLA PERUCCA AND IGOR E. SHPARLINSKI

Abstract. We consider Artin's conjecture on primitive roots over a number field K, reducing an algebraic number $\alpha \in K^\times$. Under the Generalised Riemann Hypothesis, there is a density $\operatorname{dens}(\alpha)$ counting the proportion of the primes of K for which α is a primitive root. This density $\operatorname{dens}(\alpha)$ is a rational multiple of an Artin constant $A(\tau)$ that depends on the largest integer $\tau \geqslant 1$ such that $\alpha \in (K^\times)^\tau$. The aim of this paper is bounding the ratio $\operatorname{dens}(\alpha)/A(\tau)$, under the assumption that $\operatorname{dens}(\alpha) \neq 0$. Over $\mathbb{Q}$, this ratio is between 2/3 and 2, these bounds being optimal. For a general number field K we provide upper and lower bounds that only depend on K.

1. Introduction

We consider Artin's conjecture on primitive roots over number fields, pointing the reader to Moree's survey [6] for an extensive introduction to this topic. The classical conjecture concerns the field $\mathbb{Q}$ and the reductions of a rational number $\alpha \notin \{0, \pm 1\}$ which is not a square. Then, under the Generalised Riemann Hypothesis (GRH), the following set of prime numbers p has a positive Dirichlet density $\operatorname{dens}(\alpha)$: the primes p such that α is a primitive root modulo p, which means that $v_p(\alpha) = 0$ and that $(\alpha \bmod p)$ generates $(\mathbb{Z}/p\mathbb{Z})^\times$. Letting $\tau \geqslant 1$ be the largest integer such that α is a τ-th power in $\mathbb{Q}^\times$, the heuristic density is the Artin constant

$$A(\tau) := \prod_{\ell \mid \tau} \left(1 - \frac{1}{\ell - 1}\right) \prod_{\ell \nmid \tau} \left(1 - \frac{1}{\ell(\ell-1)}\right),$$

where ℓ varies over the prime numbers. It is known that $A(1) \sim 0.37$ and $A(\tau) \leqslant A(1)$ is a positive rational multiple of $A(1)$. The density $\operatorname{dens}(\alpha)$ is a positive rational multiple of $A(\tau)$, and the aim of this work is bounding the ratio $\operatorname{dens}(\alpha)/A(\tau)$.

If $\tau = 1$, then we have

$$\frac{84}{85} \leqslant \frac{\operatorname{dens}(\alpha)}{A(1)} \leqslant \frac{6}{5}$$

where the bounds are attained for $\alpha = -15$ and $\alpha = -3$, respectively. In general, we have the following bounds (attained for $\alpha = (-15)^{15}$ and $\alpha = (-3)^3$, respectively):

$$\frac{2}{3} \leqslant \frac{\operatorname{dens}(\alpha)}{A(\tau)} \leqslant 2\,.$$

2010 *Mathematics Subject Classification.* 11A07, 11M26, 11R45.

Key words and phrases. primitive root, Artin's conjecture.

We deduce that the largest Artin density over $\mathbb{Q}$ is $\mathrm{dens}(-3) = \frac{6}{5}A(1) \sim 0.45$.

We also consider this problem for a general number field K (denote by $\mathcal{O}$ the ring of integers). We again assume the GRH (more precisely, we assume the Extended Riemann Hypothesis for the zeta function of number fields). We suppose that $\alpha \in K^\times$ is not a root of unity and it is not a square in $K^\times$, and we exclude the finitely many primes $\mathfrak{p}$ of K such that $v_\mathfrak{p}(\alpha) \neq 0$, which ensures that $(\alpha \bmod \mathfrak{p})$ is well-defined and non-zero. Then $\mathrm{dens}(\alpha)$ is the density of the primes $\mathfrak{p}$ of K such that $(\alpha \bmod \mathfrak{p})$ generates the cyclic group $(\mathcal{O}/\mathfrak{p})^\times$.

For every positive integer n let $\zeta_n = \exp(2\pi i/n)$. Denote by B the square-free part of the smallest even integer $\Omega \geqslant 1$ such that the largest abelian subextension of $K/\mathbb{Q}$ is contained in the cyclotomic field $\mathbb{Q}(\zeta_\Omega)$ (in particular, B depends only on K). We restrict to the case $\mathrm{dens}(\alpha) \neq 0$ (see Lenstra's work [5] for a study of this condition) and in particular the largest integer τ such that $\alpha \in (K^\times)\,\tau$ is odd. By Theorem 5.1 we have

$$\frac{\mathrm{dens}(\alpha)}{A(\tau)} \leqslant \prod_{\ell \mid B, \ell \mid \tau} \frac{\ell - 1}{\ell - 2} \prod_{\ell \mid B, \ell \nmid \tau} \frac{\ell^2 - \ell}{\ell^2 - \ell - 1} \leqslant 2 \prod_{\ell \mid (B/2)} \frac{\ell - 1}{\ell - 2}\,.$$

So we have an upper bound that only depends on B: since $A(\tau)$ can be arbitrarily small by varying τ, our uniform bound has an advantage with respect to the trivial bound $\mathrm{dens}(\alpha) \leqslant 1$.

Finally, we prove that there exists an explicit positive constant c_B that only depends on B (in particular, it only depends on K) such that

$$\frac{\mathrm{dens}(\alpha)}{A(\tau)} \geqslant c_B\,.$$

Our results for $\mathbb{Q}$ rely on the explicit formulas for $\mathrm{dens}(\alpha)$ provided by Hooley [2]. For general K, our upper bound stems from the following observation (where by 'index' we mean the index of $(\alpha \bmod \mathfrak{p})$, namely the index of the group $\langle(\alpha \bmod \mathfrak{p})\rangle$ inside $(\mathcal{O}/\mathfrak{p})^\times$): the set of primes $\mathfrak{p}$ of K such that the index is 1 is contained in the set of primes $\mathfrak{p}$ of K such that all prime divisors of the index divide B. Finally, our lower bound is based on insights on the so-called *entanglements*, namely the interdependencies among the cyclotomic-Kummer extensions $K(\zeta_\ell, \sqrt[\ell]{\alpha})/K$, where ℓ varies in the set of prime numbers.

We may replace α by a finitely generated and torsion-free subgroup G of $K^\times$ of positive rank, and then compare the Artin density $\mathrm{dens}(G)$ to a suitable Artin constant $\mathcal{A}_\mathcal{R}$ (see Definition 1). We are able to provide upper and lower bounds for $\mathrm{dens}(G)/\mathcal{A}_\mathcal{R}$ that only depend on K, see Corollary 5.3.

Finally remark that Section 4 contains Kummer theory results describing the entanglements among the field extensions $K(\zeta_\ell, \sqrt[\ell]{G})/K$, where ℓ varies in the set of prime numbers. Those results are unconditional and are of independent interest.

Acknowledgements. The first author got curious about the fact that -3 maximizes the Artin density over the rational numbers. Then discussions between the two authors in 2022 at the Max-Planck-Institut für Mathematik in Bonn and the University of Luxembourg led to the uniform bounds over $\mathbb{Q}$. The hospitality of both institutions is gratefully acknowledged. Finally, the first author generalised the bounds to number fields in 2024. We thank Hendrik Lenstra, Pieter Moree, Pietro Sgobba and Kate Stange for encouragement, and Olli Järviniemi for confirming the plausibility of our main result. Last but not least, we are grateful to Fritz Hörmann for providing the very general proof of Proposition 4.4. During the preparation of this work, I.S. was supported in part by Australian Research Council Grants DP230100530 and DP230100534.

2. The Artin density for the rational numbers

In this section we work over $\mathbb{Q}$, keeping the notation of the introduction and assuming the GRH. Remark that we use the notation ℓ to denote prime numbers, and μ is the Moebius function.

Let $\alpha \in \mathbb{Q}\backslash\{0, \pm 1\}$ be not a square in $\mathbb{Q}^\times$, and call δ the square-free integer such that α/δ is a square in $\mathbb{Q}^\times$. Denote by τ the largest integer for which $\alpha \in (\mathbb{Q}^\times)^\tau$ and remark that τ is odd. By Hooley's work [2], the Artin density can then be written as

$$\mathrm{dens}(\alpha) = A(\tau)\begin{cases} 1 & \text{if } \delta \not\equiv 1 \pmod 4, \\ 1 - \mu(|\delta|) f_\tau(\delta) & \text{otherwise}, \end{cases} \tag{2.1}$$

where

$$f_\tau(\delta) = \prod_{\ell|\delta,\ \ell|\tau} \frac{1}{\ell-2} \prod_{\ell|\delta,\ \ell\nmid\tau} \frac{1}{\ell^2-\ell-1}\,.$$

As the above quantities $\mu(|\delta|)$ and $f_\tau(\delta)$ are only needed for the case $\delta \equiv 1(\bmod 4)$ we may define δ, as done by Moree in [6], as the discriminant of $\mathbb{Q}(\sqrt{\alpha})$.

Theorem 2.1. *For $\tau = 1$, we have $\frac{\mathrm{dens}(\alpha)}{A(1)} \leqslant \frac{6}{5}$ and for arbitrary τ*

$$2 \geqslant \frac{\mathrm{dens}(\alpha)}{A(\tau)} \geqslant \begin{cases} \frac{84}{85} & \text{if } \tau = 1, \\ \frac{18}{19} & \text{if } \tau \text{ is power of } 3, \\ \frac{2}{3} & \text{if } 3 \mid \tau \text{ and } t = 5, \\ \frac{14}{15} & \text{if } 3 \nmid \tau \text{ and } t = 5, \\ 1 - \frac{1}{\min\{19, t-2\}} & \text{if } 3 \mid \tau \text{ and } t \geqslant 7, \\ 1 - \frac{1}{5\min\{19, t-2\}} & \text{if } 3 \nmid \tau \text{ and } t \geqslant 7, \end{cases}$$

where t is the smallest prime which exceeds 3 and divides τ, if it exists, and $t = 0$ otherwise, and each of the lower and upper bounds is attained.

Proof. We rely on the explicit formula (2.1). If $\delta \not\equiv 1(\mathrm{mod} 4)$ we have $\mathrm{dens}(\alpha)/A(\tau) = 1$, so we may restrict to the case $\delta \equiv 1(\mathrm{mod} 4)$. We need to maximize

$$f_\tau(\delta) = \prod_{\ell|\delta,\ \ell|\tau} F(\ell) \prod_{\ell|\delta,\ \ell\nmid\tau} G(\ell)\,,$$

where

$$F(\ell) := \frac{1}{\ell-2} \quad , \quad G(\ell) := \frac{1}{\ell^2-\ell-1}\,.$$

To get an upper (respectively, lower) bound we have to choose δ with negative (respectively, positive) Moebius function $\mu(|\delta|)$. We can take $|\delta|$ prime (respectively, the product of two primes) because $f_\tau(\delta)$ does not increase by adding prime factors to δ. Remark that

$$\begin{aligned} F(3) &= 1 > G(3) = 1/5 \geqslant \max\{F(\ell), G(\ell) : \ \ell \geqslant 5, \ \text{prime}\}; \\ F(5) &= 1/3 > G(5) = 1/19 \geqslant \max\{F(\ell), G(\ell) : \ \ell \geqslant 23, \ \text{prime}\}. \end{aligned} \tag{2.2}$$

We have in particular

$$f_1(\delta) = \prod_{\ell \mid \delta} G(\ell) \leqslant \min_{\ell \mid \delta} G(\ell) \leqslant G(3) = \frac{1}{5} = f_1(-3)\,.$$

So, supposing $\tau = 1$, for $\alpha = -3$ we get the largest value $\mathrm{dens}(\alpha)/A(1) = 6/5$. Now consider a general $\tau \geqslant 1$. We have

$$f_\tau(\delta) = \prod_{\ell \mid \delta,\ \ell \mid \tau} F(\ell) \prod_{\ell \mid \delta,\ \ell \nmid \tau} G(\ell) \ll \max\left\{ \max_{\ell \mid \delta,\ \ell \mid \tau} F(\ell), \max_{\ell \mid \delta,\ \ell \nmid \tau} G(\ell) \right\}.$$

Thus, considering (2.2), we get $f_\tau(\delta) \leqslant f_3(-3) = 1$. So for $\alpha = (-3)^3$ we get the largest value $\mathrm{dens}(\alpha)/A(\tau) = 2$.

To get a lower bound, we have to find the optimal choice for two distinct odd primes ℓ_1, ℓ_2 and take $\delta \in \{\pm \ell_1 \ell_2\}$, recalling that $\delta \equiv 1 \bmod 4$. By (2.2) we can take $\ell_1 = 3$. In the first four cases of the lower bound we may take $\ell_2 = 5$ and hence $\delta = -15$, so we easily conclude those cases by computing $\mathrm{dens}((-15)^\tau)/A(\tau)$.

In the penultimate case (where $5 \nmid \tau$) by (2.2) we take $\ell_2 = 5$ if $t \geqslant 23$ and $\ell_2 = t$ otherwise and obtain

$$f_\tau(\delta) = F(3) \max\{G(5), F(t)\} = \frac{1}{\min\{19, t-2\}}\,.$$

In the last case, a similar argument leads to the same choice of δ and hence

$$f_\tau(\delta) = G(3) \max\{G(5), F(t)\} = \frac{1}{5 \min\{19, t-2\}}\,,$$

which concludes the proof. □

Example 2.2. *By Hooley's formula* (2.1) *we clearly obtain the largest value for* $\mathrm{dens}(\alpha)$ *with* $\tau = 1$. *Then the largest Artin density over* $\mathbb{Q}$ *is* $\mathrm{dens}(-3) = \frac{6}{5} A(1)$. *In fact,* -3 *maximizes the Artin density because if the index of* $(-3 \bmod p)$ *is odd, then it is automatically coprime to* 3 *(indeed, we are considering primes* p *that do not split completely in* $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$*).*

3. Setup for the general case

3.1. **Notation.** *We assume the Extended Riemann Hypothesis for the zeta function of number fields.*

Let K be a number field, and work within a fixed algebraic closure of K. Write ζ_n for a primitive n-th root of unity.

Let $\alpha \in K^\times$ be not a root of unity, while G is a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. While considering the reductions of α (respectively, G) modulo primes of K we tacitly exclude the finitely many primes $\mathfrak{p}$ such that the reduction modulo $\mathfrak{p}$ is not well-defined or it is not contained in the multiplicative group of the residue field at $\mathfrak{p}$. Thanks to this restriction we have a well-defined multiplicative index of α modulo $\mathfrak{p}$ (respectively, of G modulo $\mathfrak{p}$) in the multiplicative group of the residue field at $\mathfrak{p}$.

We call $\operatorname{dens}(\alpha)$ the density of primes $\mathfrak{p}$ of K for which $\operatorname{ind}(\alpha \bmod \mathfrak{p}) = 1$. We similarly define $\operatorname{dens}(G)$ requiring $\operatorname{ind}(G \bmod \mathfrak{p}) = 1$.

3.2. **Artin constants.** By the very general framework developed by the first author with Järviniemi and Sgobba [3, 4], we know in particular that the Artin density $\operatorname{dens}(G)$ is a rational multiple of the following Artin constant (which is at least $A(1)$ and it is strictly less than 1):

$$\prod_{\ell \text{ prime}} \left(1 - \frac{1}{\ell^r(\ell-1)}\right) .$$

We now define a rational multiple of the above constant with the aim of producing an Artin constant that better fits $\operatorname{dens}(G)$:

Definition 1. *For every prime ℓ let r_ℓ be an integer in the range from 0 to r, such that $r_\ell = r$ holds for all but finitely many ℓ. Then we define the Artin constant*

$$A_{\mathcal{R}} := \prod_{\ell \textit{ prime}} \left(1 - \frac{1}{\ell^{r_\ell}(\ell-1)}\right) .$$

Given G as above, for every prime ℓ we define r_ℓ as the rank of the group $G/(G \cap K^{\times \ell})$. Then we have $A_{\mathcal{R}} > 0$ if we suppose that $r_2 > 0$ (in fact, $r_2 = 0$ implies that G consists of squares and hence $\operatorname{dens}(G) = 0$).

Example 3.1. *For $G = \langle \alpha \rangle$ we have $r_\ell \in \{0, 1\}$. Suppose that α is not a square in $K^\times$, and call τ the largest (odd) integer such that $\alpha \in (K^\times)^\tau$. Then we have $r_\ell = 0$ if and only if $\ell \mid \tau$, which implies that $A_{\mathcal{R}} = A(\tau)$.*

4. Entanglements

The results in this section are unconditional. We denote by Q the product of the prime numbers q such that $\zeta_q \in K$. Moreover, we denote by B the square-free part of the smallest even integer $\Omega \geqslant 1$ such that the largest abelian subextension of $K/\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_\Omega)$. In particular, we have $Q \mid B$. Remark that Q and B are constants that only depend on K (more precisely, they only depend on the largest abelian subextension of $K/\mathbb{Q}$). We remark that for the results in this section it is possible to replace B by any positive multiple of it which is again square-free.

Remark 4.1. *Because of our choice of B the following holds. For all primes $\ell \nmid B$ the cyclotomic fields $K(\zeta_\ell)$ are linearly disjoint and have maximal degree $\ell - 1$ over K.*

Moreover, for any fixed prime $\ell \nmid B$, and denoting any prime by $\widetilde{\ell}$, we have

$$K(\zeta_\ell) \cap \prod_{\widetilde{\ell} \neq \ell} K(\zeta_{\widetilde{\ell}}) = K\,.$$

Consequently, we have

$$K(\zeta_B) \cap \prod_{\ell \nmid B} K(\zeta_\ell) = K\,.$$

Proposition 4.2. *For every prime $\ell \nmid B$ the degree of the cyclotomic-Kummer extension $K(\zeta_\ell, \sqrt[\ell]{G})/K$ equals $\ell^{r_\ell}(\ell-1)$. For every prime ℓ such degree divides $\ell^{r_\ell}(\ell-1)$.*

Proof. The second assertion is straight-forward by classical Kummer theory. By Remark 4.1 we are left to prove that for $\ell \nmid B$ the degree of $K(\zeta_\ell, \sqrt[\ell]{G})/K(\zeta_\ell)$ equals ℓ^{r_ℓ}. We claim that r_ℓ is the rank of $G/(G \cap K(\zeta_\ell)^{\times \ell})$, so the assertion follows from classical Kummer theory. The claim holds because $\ell \neq 2$ so with the language of [1] the parameters for ℓ-divisibility of G are the same over K and over $K(\zeta_\ell)$. □

Proposition 4.3. *For every prime $\ell \nmid B$ we have $K(\zeta_\ell, \sqrt[\ell]{G}) \cap K(\zeta_\infty) = K(\zeta_\ell)$. Moreover, (for any choice of the ℓ-th roots) we have $K(\sqrt[\ell]{G}) \cap K(\zeta_\infty) = K$. For all primes $\ell \nmid B$ the cyclotomic-Kummer extensions $K(\zeta_\ell, \sqrt[\ell]{G})/K$ are linearly disjoint over K.*

Proof. The field $K(\zeta_\ell, \sqrt[\ell]{G}) \cap K(\zeta_\infty)$ is an abelian extension of K so by Schinzel's result on abelian radical extensions [7, Theorem 2] it must be contained in $K(\zeta_\ell)$ because $\ell \nmid Q$. The second assertion follows because the extensions $K(\zeta_\ell)/K$ and $K(\sqrt[\ell]{G})/K$ have coprime degrees.

For the last assertion it suffices to observe that for every prime $\ell \nmid B$ and by varying $\widetilde{\ell}$ in the prime numbers we have

$$K(\zeta_\ell, \sqrt[\ell]{G}) \cap \prod_{\widetilde{\ell} \nmid \ell B} K(\zeta_{\widetilde{\ell}}, \sqrt[\widetilde{\ell}]{G}) \subseteq K(\zeta_\ell) \cap \prod_{\widetilde{\ell} \nmid \ell B} K(\zeta_{\widetilde{\ell}}, \sqrt[\widetilde{\ell}]{G}) = K(\zeta_\ell) \cap \prod_{\widetilde{\ell} \nmid \ell B} K(\zeta_{\widetilde{\ell}}) = K\,.$$

The inclusion is because $K(\sqrt[\ell]{G})/K$ and $K(\sqrt[\widetilde{\ell}]{G})/K$ have coprime degrees and then we may apply the first part of the statement. The former equality again follows from the first part of the statement, while the latter equality is a consequence of Remark 4.1. □

Let B_G be the squarefree integer which is the smallest positive multiple of B such that for any fixed prime $\ell \nmid B_G$ and denoting any prime by $\widetilde{\ell}$ we have

$$K(\zeta_\ell, \sqrt[\ell]{G}) \cap \prod_{\widetilde{\ell} \neq \ell} K(\zeta_{\widetilde{\ell}}, \sqrt[\widetilde{\ell}]{G})) = K$$

(the existence of B_G follows from Kummer theory, see [3, Section 3] by the first author and Järviniemi). We remark that in the following results we could replace B_G by a positive multiple of it which is again square-free.

A proof of our next result has been communicated by Fritz Hörmann.

Proposition 4.4. *Let K be a field, let L_1, L_2, M be finite abelian extensions of K and consider the field $E := ML_1 \cap L_2$. Assuming that $L_1 \cap L_2 = K$, the Galois group* $\mathrm{Gal}(E/K)$ *of E/K is a quotient of a subgroup of the Galois group* $\mathrm{Gal}(M/K)$ *of M/K.*

Proof. The compositum $F := L_1L_2M$ is again a finite abelian extension of K. We write $G := \mathrm{Gal}(F/K)$ and for $X \in \{L_1, L_2, M\}$ we write $G_X := \mathrm{Gal}(F/X)$. By our assumption, we have $G = G_{L_1}G_{L_2}$. First observe that we have

$$\mathrm{Gal}(E/K) \cong \frac{G_{L_1}G_{L_2}}{G_{L_2}(G_{L_1} \cap G_M)} \cong \frac{G_{L_1}}{(G_{L_1} \cap G_M)(G_{L_1} \cap G_{L_2})}\,, \tag{4.1}$$

where the second isomorphism is obtained by observing that $G_{L_2} \cap (G_L \cap G_M) = 1$ (by the definition of F) and hence

$$\frac{G_{L_1}G_{L_2}}{G_{L_2}(G_{L_1} \cap G_M)} \cong \frac{\frac{G_{L_1}G_{L_2}}{G_{L_2}}}{G_{L_1} \cap G_M} \cong \frac{\frac{G_{L_1}}{G_{L_1} \cap G_{L_2}}}{G_{L_1} \cap G_M} \cong \frac{G_{L_1}}{(G_{L_1} \cap G_M)(G_{L_1} \cap G_{L_2})}\,.$$

The last group in (4.1) is a quotient of

$$\frac{G_{L_1}}{G_{L_1} \cap G_M} \cong \frac{G_{L_1}G_M}{G_M}\,.$$

Finally, this last group is a subgroup of

$$\frac{G_{L_1}G_{L_2}}{G_M} \cong \mathrm{Gal}(M/K)\,.$$

□

We recall that the exponent of an abelian extension is defined as the exponent of its Galois group.

We instantly derive from Proposition 4.4 one of our main tools.

Corollary 4.5. *Let L_1, L_2 and M be finite abelian extensions of K such that $L_1 \cap L_2 = K$. Then the field $ML_1 \cap L_2 \subseteq L_2$ is an abelian extension of K of degree dividing $[M : K]$ and of exponent dividing the exponent of M/K.*

We also need the following result.

Proposition 4.6. *For every prime ℓ let G_ℓ be a subgroup of G. Consider the field*

$$F := \prod_{\ell \mid B} K(\zeta_\ell, \sqrt[\ell]{G_\ell}) \cap \prod_{\ell \nmid B} K(\zeta_\ell, \sqrt[\ell]{G_\ell})\,.$$

Then we have

$$F \subseteq \Big(K(\zeta_B) \prod_{q \mid Q} K(\sqrt[q]{G_q})\Big) \cap K(\zeta_{B_G/B})$$

and F/K is a Kummer extension of exponent dividing Q and degree dividing Q^{r_Q}, where $r_Q := \max_{q \mid Q} \operatorname{rank} G_q$.

Proof. The second assertion follows from the first as a consequence of Corollary 4.5 (setting $M = \prod_{q|Q} K(\sqrt[q]{G_q})$, $L_1 = K(\zeta_B)$ and $L_2 = K(\zeta_{B_G/B})$) because M/K is a Kummer extension of exponent dividing Q and degree dividing Q^{r_Q}. Also remark that by the definition of B_G we have

$$F = \prod_{\ell|B} K(\zeta_\ell, \sqrt[\ell]{G_\ell}) \cap \prod_{\ell|(B_G/B)} K(\zeta_\ell, \sqrt[\ell]{G_\ell})\,.$$

For any prime $\widetilde{\ell}$, we consider the $\widetilde{\ell}$-part $F_{\widetilde{\ell}}$ of F, namely the largest subextension of F whose degree is a power of $\widetilde{\ell}$. For a prime $q \mid Q$ we clearly have

$$F_q \subseteq \Big(K(\sqrt[q]{G_q}) \prod_{\ell|(B/q)} K(\zeta_\ell) \Big) \cap \prod_{\ell|(B_G/B)} K(\zeta_\ell)\,.$$

So we conclude by proving that for $\widetilde{\ell} \nmid Q$ we have $F_{\widetilde{\ell}} = K$.

For $\widetilde{\ell} \nmid B$ we have

$$F_{\widetilde{\ell}} \subseteq \prod_{\ell|B} K(\zeta_\ell) \cap \Big(K(\zeta_{\widetilde{\ell}}, \sqrt[\tilde{\ell}]{G_{\widetilde{\ell}}}) \prod_{\ell|(B_G/B),\, \ell\neq\widetilde{\ell}} K(\zeta_\ell) \Big)\,.$$

Considering the former field on the right-hand-side, $F_{\widetilde{\ell}}/K$ is abelian. So we may replace the latter field by its largest abelian subextension. Since $\zeta_{\widetilde{\ell}} \notin K$, by Schinzel's Theorem on abelian radical extensions [7, Theorem 2] we then have

$$F_{\widetilde{\ell}} \subseteq \prod_{\ell|B} K(\zeta_\ell) \cap \prod_{\ell|(\widetilde{\ell}B_G/B)} K(\zeta_\ell) = K\,,$$

where the equality holds by Remark 4.1.

For $\widetilde{\ell} \mid B$ with $\widetilde{\ell} \nmid Q$ we may reason analogously because we have

$$F_{\widetilde{\ell}} \subseteq \Big(K(\zeta_{\widetilde{\ell}}, \sqrt[\tilde{\ell}]{G_{\widetilde{\ell}}}) \prod_{\ell|(B/\widetilde{\ell})} K(\zeta_\ell) \Big) \cap \prod_{\ell|(B_G/B)} K(\zeta_\ell)\,,$$

which concludes the proof. □

As remarked above, B and B_G in Proposition 4.6 can be replaced by positive square-free multiples that still satisfy $B \mid B_G$.

Remark 4.7. *As a special case of Proposition 4.6 we have*

$$\prod_{\ell|B} K(\zeta_\ell, \sqrt[\ell]{G}) \cap \prod_{\ell\nmid B} K(\zeta_\ell, \sqrt[\ell]{G}) \subseteq K(\zeta_B, \sqrt[Q]{G}) \cap K(\zeta_{B_G/B}).$$

5. General bounds for the Artin density

All densities mentioned in this section exist thanks to the results in [3] by the first author and Järviniemi (which are conditional under the Extended Riemann Hypothesis). Let B be as in Section 4. We denote by $\mathrm{dens}_B(G)$ the density of the primes $\mathfrak{p}$ of K such that for every prime divisor $\ell \mid B$ we have $\ell \nmid \mathrm{ind}(G \bmod \mathfrak{p})$. For any prime ℓ, we write $\mathrm{dens}_\ell(G)$ for the density of the primes $\mathfrak{p}$ of K such that $\ell \nmid \mathrm{ind}(G \bmod \mathfrak{p})$. Finally, we denote by $\widetilde{\operatorname{dens}}_B(G)$ the density of the primes $\mathfrak{p}$ of K such that for every $\ell \nmid B$ we have $\ell \nmid \operatorname{ind}(G \bmod \mathfrak{p})$.

Theorem 5.1. *Suppose that* $\operatorname{dens}(G) \neq 0$ *(in particular,* $r_2 > 0$*). Then we have*

$$\frac{\operatorname{dens}(G)}{A_{\mathcal{R}}} \leqslant \prod_{\ell \mid B} \left(1 - \frac{1}{\ell^{r_\ell}(\ell-1)}\right)^{-1} \leqslant 2 \prod_{\ell \mid (B/2)} \frac{\ell-1}{\ell-2}\,.$$

Proof. The second inequality is clear because we can estimate the factor $\ell = 2$ using $r_2 = 1$ and each factor $\ell \neq 2$ using $r_\ell = 0$.

For every prime $\ell \nmid B$ the degree of $K(\zeta_\ell, \sqrt[\ell]{G})/K$ equals $\ell^{r_\ell}(\ell-1)$ by Proposition 4.2. Moreover, such fields are linearly disjoint by Proposition 4.3. Remark that by Hooley's method (see Moree's survey [6]) the condition $\ell \nmid \operatorname{ind}(G \bmod \mathfrak{p})$ can be replaced by $\mathfrak{p}$ not splitting completely in $K(\zeta_\ell, \sqrt[\ell]{G})$. We deduce that

$$\widetilde{\operatorname{dens}}_B(G) = \prod_{\ell \nmid B} \operatorname{dens}_\ell(G) = \prod_{\ell \nmid B} \left(1 - \frac{1}{\ell^{r_\ell}(\ell-1)}\right)\,. \tag{5.1}$$

Since

$$\frac{\operatorname{dens}(G)}{A_{\mathcal{R}}} \leqslant \frac{\widetilde{\operatorname{dens}}_B(G)}{A_{\mathcal{R}}} = \prod_{\ell \mid B} \left(1 - \frac{1}{\ell^{r_\ell}(\ell-1)}\right)^{-1}\,,$$

we conclude the proof. □

We recall the definition of B_G from Section 4.

Theorem 5.2. *There exists a positive constant* c_B *that depends only on* B *such that if* $\operatorname{dens}(G) \neq 0$ *then we have*

$$\frac{\operatorname{dens}(G)}{A_{\mathcal{R}}} \geqslant c_B\,.$$

Proof. We replace B by the smallest square-free positive multiple $\mathscr{B}$ so that for every prime $\ell \nmid B$ the integer $\ell - 1$ is at least $2Q$, where, as before, Q denotes the product of the prime numbers q such that $\zeta_q \in K$. Observing that $Q \leqslant B$ we see that $\mathscr{B}$ only depends on the original value for B. We call $\mathscr{B}_G$ the least common multiple between $\mathscr{B}$ and B_G and remark that $\mathscr{B}_G$ is squarefree. We point out that our proof strategy involves concentrating on the prime divisors of $\mathscr{B}_G$, distinguishing the primes that divide $\mathscr{B}$ by those who don't.

By the independence and maximality of the cyclotomic-Kummer extensions at primes not dividing $\mathscr{B}_G$ (as described in Section 4) we have

$$\operatorname{dens}(G) = \operatorname{dens}_{\mathscr{B}_G}(G) \prod_{\ell \nmid \mathscr{B}_G} \operatorname{dens}_\ell(G) = \operatorname{dens}_{\mathscr{B}_G}(G) \prod_{\ell \nmid \mathscr{B}_G} \left(1 - \frac{1}{\ell^{r_\ell}(\ell-1)}\right)\,.$$

Thus we have

$$\frac{\operatorname{dens}(G)}{A_{\mathcal{R}}} = \frac{\operatorname{dens}_{\mathscr{B}_G}(G)}{\prod_{\ell \mid \mathscr{B}_G} \left(1 - \frac{1}{\ell^{r_\ell}(\ell-1)}\right)} \geqslant \frac{\operatorname{dens}_{\mathscr{B}_G}(G)}{\prod_{\ell \mid (\mathscr{B}_G/\mathscr{B})} \left(1 - \frac{1}{\ell^{r_\ell}(\ell-1)}\right)}\,.$$

Since $\mathrm{dens}(G) \neq 0$ we must have $\mathrm{dens}_{\mathscr{B}}(G) \neq 0$ so there exists a Galois automorphism τ on

$$\prod_{\ell | \mathscr{B}} K(\zeta_\ell, \sqrt[\ell]{G}),$$

which is not the identity on any of the fields $K(\zeta_\ell, \sqrt[\ell]{G})$. We can fix a set of generators of G and for any $\ell \mid \mathscr{B}$ we choose one of those generators, call it α_ℓ, which is not fixed by τ, setting $\alpha_\ell = 1$ if no such generator exists. We then call $\tau\mid_L$ the restriction of τ to the field

$$L := \prod_{\ell | \mathscr{B}} K(\zeta_\ell, \sqrt[\ell]{\alpha_\ell})\,.$$

For every positive integer N we write $K_N := \prod_{\ell | N} K(\zeta_\ell, \sqrt[\ell]{G})$. We then define $f_{\mathscr{B}_G,\tau}(G)$ as the number of automorphisms in $\mathrm{Gal}(K_{\mathscr{B}_G}/K)$ whose restriction to L is $\tau\mid_L$, and such that for every $\ell \mid (\mathscr{B}_G/\mathscr{B})$ the restriction to $K(\zeta_\ell, \sqrt[\ell]{G})$ is not the identity. By our choice of τ we clearly have

$$\frac{f_{\mathscr{B}_G,\tau}(G)}{[K_{\mathscr{B}_G} : K]} \leqslant \mathrm{dens}_{\mathscr{B}_G}(G)$$

so we are left to prove that there is a constant $c^\star_B$ (that depends only on B) such that

$$\frac{f_{\mathscr{B}_G,\tau}(G)}{[K_{\mathscr{B}_G} : K]} \geqslant c^\star_B \prod_{\ell | (\mathscr{B}_G/\mathscr{B})} \left(1 - \frac{1}{\ell^{r_\ell}(\ell-1)}\right)\,. \tag{5.2}$$

We consider the field

$$E := L \cap K_{\mathscr{B}_G/\mathscr{B}}\,.$$

We can write

$$\frac{f_{\mathscr{B}_G,\tau}(G)}{[K_{\mathscr{B}_G} : K]} = \frac{1}{[L:E]} \cdot \frac{f_{\mathscr{B}_G,\tau|E}(G)}{[K_{\mathscr{B}_G/\mathscr{B}} : K]}, \tag{5.3}$$

where $f_{\mathscr{B}_G,\tau|E}(G)$ counts the automorphisms in $\mathrm{Gal}(K_{\mathscr{B}_G/\mathscr{B}}/K)$ whose restriction to E equals $\tau\mid_E$ and such that for every $\ell \mid (\mathscr{B}_G/\mathscr{B})$ the restriction to $K(\zeta_\ell, \sqrt[\ell]{G})$ is not the identity. Indeed, once we have fixed a suitable automorphism in $\mathrm{Gal}(K_{\mathscr{B}_G/\mathscr{B}}/K)$, then we only need to extend it in a prescribed way to $LK_{\mathscr{B}_G/\mathscr{B}}$, and we have $[LK_{\mathscr{B}_G/\mathscr{B}} : K_{\mathscr{B}_G/\mathscr{B}}] = [L:E]$. Since $[L:E] \leqslant [L:K] \leqslant \prod_{\ell|\mathscr{B}} \ell(\ell-1)$, the inverse of $[L:E]$ can be bounded from below only in terms of B.

If $\mathscr{B}_G = \mathscr{B}$, then the last ratio in (5.3) is 1 and we may conclude, so in what follows we will suppose that $\mathscr{B}_G$ has more prime divisors with respect to $\mathscr{B}$.

Recall that by our choice of $\mathscr{B}$ we have

$$[K_{\mathscr{B}_G/\mathscr{B}} : K] = \prod_{\ell | (\mathscr{B}_G/\mathscr{B})} \frac{1}{\ell^{r_\ell}(\ell-1)}$$

so, by (5.2), we are left to prove that there exists a constant $c_B^\sharp$ depending only on B such that

$$f_{\mathscr{B}_G,\tau|E}(G) \geqslant c_B^\sharp \prod_{\ell|(\mathscr{B}_G/\mathscr{B})} \left(\ell^{r_\ell}(\ell-1)-1\right)\,. \tag{5.4}$$

By Proposition 4.6 (setting $G_\ell = \langle \alpha_\ell \rangle$ for $\ell \mid \mathscr{B}$ and $G_\ell = G$ otherwise, so in particular $r_Q = 1$) we deduce that E/K is a Kummer extension of degree dividing Q contained in $K(\zeta_{\mathscr{B}_G/\mathscr{B}})$.

Fix a prime q dividing $[E:K]$, so in particular we have $q \mid Q$. The q-part of the extension E/K is a cyclic extension C_q/K of degree q contained in $\prod_{\ell\in\mathcal{S}_q} K(\zeta_\ell)$, where $\mathcal{S}_q$ is a subset of primes dividing $\mathscr{B}_G$, not dividing $\mathscr{B}$, and such that $q \mid [K(\zeta_\ell):K]$. We may assume that $\mathcal{S}_q$ is minimal.

Then (on the q-part of the considered Galois groups) the condition of extending the automorphism $\tau\mid_{C_q}$ is a compatibility of q-characters related to the subextensions of degree q of $K(\zeta_\ell)$ for $\ell\in\mathcal{S}_q$. And this condition is satisfied if we fix $\ell_q\in\mathcal{S}_q$ and select an appropriate automorphism on the degree q subextension of $K(\zeta_{\ell_q})/K$, such choice depending on the free choices that we can make for $K(\zeta_\ell)/K$ by varying $\ell\in\mathcal{S}_q$ with $\ell\neq\ell_q$.

For every $\ell \mid (\mathscr{B}_G/\mathscr{B})$ call Q_ℓ the product of the primes q as above such that $\ell=\ell_q$ (setting $Q_\ell=1$ for an empty product). So, up to considering fewer automorphisms, we are able to separate the conditions at the different primes, namely

$$f_{\mathscr{B}_G,\tau|E}(G) \geqslant \prod_{\ell|(\mathscr{B}_G/\mathscr{B})} g_{r_\ell,Q_\ell}, \tag{5.5}$$

where g_{r_ℓ,Q_ℓ} is the amount of automorphisms in $K(\zeta_\ell,\sqrt[\ell]{G})$ that are not the identity and that are the fewest by varying a prescribed restriction to the cyclic subextension of degree Q_ℓ of $K(\zeta_\ell)$. We have (recalling that $\ell-1\geqslant 2Q\geqslant 2Q_\ell$)

$$g_{r_\ell,Q_\ell} \geqslant \frac{[K(\zeta_\ell,\sqrt[\ell]{G}):K]}{Q_\ell}-1 = \frac{\ell^{r_\ell}(\ell-1)}{Q_\ell}-1 \geqslant \frac{1}{\min\{2,Q_\ell\}Q_\ell}\left(\ell^{r_\ell}(\ell-1)-1\right). \tag{5.6}$$

Remark that

$$\prod_{\ell|(\mathscr{B}_G/\mathscr{B})} Q_\ell \mid Q$$

and that the number of primes $\ell \mid (\mathscr{B}_G/\mathscr{B})$ such that $Q_\ell\neq 1$ is bounded by the number of prime divisors of Q, which is some constant C_K that only depends on the field K. Substituting (5.6) in (5.5) we then obtain

$$f_{\mathscr{B}_G,\tau|E}(G) \geqslant \frac{1}{2^{C_K}Q} \prod_{\ell|(\mathscr{B}_G/\mathscr{B})} \ell^{r_\ell}(\ell-1)-1,$$

which implies (5.4) and concludes the proof. □

Finally, since B depends only on K, we observe that Theorems 5.1 and 5.2 imply that $\mathrm{dens}(G)/A_{\mathcal{R}}$ can be bounded only in terms of K, which is in fact our main result.

Corollary 5.3. *There exist two positive constants $c_0(K)$ and $C_0(K)$ that depend only on K such that if $\mathrm{dens}(G) \neq 0$ then we have*

$$c_0(K) \leqslant \frac{\mathrm{dens}(G)}{A_{\mathcal{R}}} \leqslant C_0(K)\,.$$

References

[1] C. Debry and A. Perucca, *Reductions of algebraic integers*, J. Number Theory **167** (2016), 259–283. 6

[2] C. Hooley, *Artin's conjecture for primitive roots*, J. Reine Angew. Math. **225** (1967), 209–220. 2, 3

[3] O. Järviniemi and A. Perucca, *Unified treatment of Artin-type problems*, Res. Number Theory **9** (2023), Art. 10. 5, 6, 8

[4] O. Järviniemi, A. Perucca and P. Sgobba, *Unified treatment of Artin-type problems II*, submitted for publication (status: minor revisions), arXiv:2211.15614. 5

[5] H. W. Jr. Lenstra, *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. **42** (1977), 201–224. 2

[6] P. Moree, *Artin's primitive root conjecture – a survey*, Integers **12** (2012), 1305–1416. 1, 3, 9

[7] A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arithm. **32** (1977), 245–274. 6, 8

A.P.: Department of Mathematics, University of Luxembourg, Esch-sur-Alzette, L-4364, Luxembourg

Email address: `antonella.perucca@uni.lu`

I.S.: School of Mathematics and Statistics, University of New South Wales. Sydney, NSW 2052, Australia

Email address: `igor.shparlinski@unsw.edu.au`