Towards a Schinzel–Wójcik theorem for number fields

Paul Pollack

University of Georgia
Department of Mathematics
Athens, Georgia 30601, USA
pollack@uga.edu

Abstract

Schinzel and Wójcik have shown that for every $\alpha, \beta \in \mathbb{Q}^\times \setminus \{\pm 1\}$, there are infinitely many primes p where $v_p(\alpha) = v_p(\beta) = 0$ and where α and β generate the same multiplicative group mod p. We prove a weaker result in the same direction for algebraic numbers α, β. Let $\alpha, \beta \in \bar{\mathbb{Q}}^\times$, and suppose $|N_{\mathbb{Q}(\alpha,\beta)/\mathbb{Q}}(\alpha)| \neq 1$ and $|N_{\mathbb{Q}(\alpha,\beta)/\mathbb{Q}}(\beta)| \neq 1$. Then for some positive integer $C = C(\alpha, \beta)$, there are infinitely many prime ideals P of $\mathcal{O}_{\mathbb{Q}(\alpha,\beta)}$ where $v_P(\alpha) = v_P(\beta) = 0$ and where the group $\langle \beta \bmod P \rangle$ is a subgroup of $\langle \alpha \bmod P \rangle$ with $[\langle \alpha \bmod P \rangle : \langle \beta \bmod P \rangle]$ dividing C. A key component of the proof is a theorem of Corvaja and Zannier bounding the greatest common divisor of shifted S-units.

Keywords: Schinzel–Wójcik problem, multiplicative order, Artin's primitive root conjecture, subspace theorem

MSC classification (2020): Primary 11R44; Secondary 11A07, 11R04, 11J25

1 Introduction

In 1992, Schinzel and Wójcik proved the following elegant result: For every $\alpha, \beta \in \mathbb{Q}^\times \setminus \{\pm 1\}$, there are infinitely many primes p (not dividing the numerator or denominator of α, β) for which the mod p reductions of α and β generate the same subgroup of $\mathbb{F}_p^\times$ [SW92]. Their arguments, which amplify those found in unpublished work of J. S. Wilson, J. W. S. Cassels, and J. G. Thompson, are ingenious but elementary. Our interest here is in extensions of their result to algebraic number fields.

Suppose α and β are nonzero elements of a number field K. We let

$$\mathcal{P}_K(\alpha, \beta) = \{P \in \mathrm{MaxSpec}(\mathcal{O}_K) : v_P(\alpha) = v_P(\beta) = 0, \langle \alpha \bmod P \rangle = \langle \beta \bmod P \rangle\}.$$

(Since α, β are not assumed algebraic integers, the mod P reductions refer to the images in $\mathcal{O}_P/P\mathcal{O}_P$, where $\mathcal{O}_P$ is the localization of $\mathcal{O}_K$ at P.) The number field Schinzel–Wójcik problem is to prove the infinitude of $\mathcal{P}_K(\alpha, \beta)$ for as many choices of α, β, K as possible.[1]

[1] As will emerge shortly, $\mathcal{P}_K(\alpha, \beta)$ is infinite for some K containing α, β if and only if it is infinite for $K = \mathbb{Q}(\alpha, \beta)$. So K could be omitted from the statement of the problem.

Quite a lot can be said if one is willing to assume plausible but unproved hypotheses. For instance, working under the assumption of the Generalized Riemann Hypothesis, Järviniemi and Perucca have advanced a "Master Theorem" for problems connected with Artin's primitive root conjecture [JP23]. That theorem implies that (under GRH) $\mathcal{P}_K(\alpha, \beta)$ is infinite whenever α, β are multiplicatively independent. In fact, one has the analogous conclusion with α, β replaced by any finite list of multiplicatively independent elements. This last conclusion is also contained in work of Wójcik [Wój96], conditional not on GRH but on Schinzel's Hypothesis H [SS58] concerning simultaneous prime values of integer polynomials [Wój96].

If we insist on unconditional results, our knowledge is much more modest. In [JP21], Just and the author showed that $\mathcal{P}_K(\alpha, \beta)$ is infinite when K is imaginary quadratic and α, β are nonzero integers of K, not roots of unity. In [Pol], a sufficient condition is presented for $\mathcal{P}_K(\alpha, \beta)$ to be infinite. Here K can be any number field and α, β any nonzero elements of K, but verifying the condition requires finding a suitable "auxiliary prime ideal" in the Galois closure of K. While such a prime appears easy to compute in practice (for any choice of α, β, K where one expects $\mathcal{P}_K(\alpha, \beta)$ to be infinite), we do not know a priori that this prime always exists.

In this paper we prove an unconditional theorem not requiring a search for auxiliary primes. The catch is that we do not obtain equality of the groups generated by α and β but only a bounded index statement.

Theorem 1. *Let $\alpha, \beta \in \bar{\mathbb{Q}}^\times$, both contained in the number field K, and neither a root of unity. Assume either that α, β are multiplicatively dependent or that $|N_{K/\mathbb{Q}}(\alpha)| \neq 1$ and $|N_{K/\mathbb{Q}}(\beta)| \neq 1$. For some constant C (that may depend on α, β), there are infinitely many prime ideals P of $\mathcal{O}_K$ where $v_P(\alpha) = v_P(\beta) = 0$ and where the group $\langle \beta \bmod P \rangle$ is a subgroup of $\langle \alpha \bmod P \rangle$ having index dividing C.*

It would be desirable to weaken the hypotheses on α, β. Unfortunately this would seem to require a new idea, as explained in the concluding remarks.

Let us sketch our proof of Theorem 1. Suppose K and K' are number fields containing α and β with $K \subseteq K'$. Suppose also that P' is a nonzero prime ideal of $\mathcal{O}_{K'}$ lying above the nonzero prime ideal P of $\mathcal{O}_K$. Then $v_P(\alpha) = v_P(\beta) = 0$ if and only if $v_{P'}(\alpha) = v_{P'}(\beta) = 0$. The embedding $\mathcal{O}_P/P\mathcal{O}_P \hookrightarrow \mathcal{O}_{P'}/P'\mathcal{O}_{P'}$ shows that the subgroups generated by $\alpha \bmod P$ and $\beta \bmod P$ can be identified with those generated by $\alpha \bmod P'$ and $\beta \bmod P'$. So the conclusion of Theorem 1 holds for K if and only if it holds for K'. In particular, by passing to the Galois closure, we can (and will) assume that K is Galois over $\mathbb{Q}$.

We will prove that $\mathcal{P}_K(\alpha^n, \beta)$ is infinite for some $n \in \mathbb{Z}^{>0}$. This implies Theorem 1 with $C = n$. Let us suppose for now that α and β are multiplicatively independent; the contrary case will prove easy to dispense with. In §2, we show that when $\#\mathcal{P}_K(\alpha, \beta) < \infty$, a certain fundamental identity holds between the conjugates of α and β. (This piece of the argument is inspired by earlier work in [SW92, JP21, Pol].) Hence, if $\#\mathcal{P}_K(\alpha^n, \beta) < \infty$ for every n, then an entire sequence of identities follows. Sections 3 and 4 collect results needed to analyze this family of relations; one particularly important ingredient is a theorem of Corvaja and Zannier [CZ05] from Diophantine analysis. In §5 we put all the pieces together, arguing that at least one identity in our sequence must fail.

2 The fundamental identity

Proposition 2. *Let K be a Galois number field. Suppose that $\alpha, \beta \in K^\times$ are multiplicatively independent (so that in particular, neither is a root of unity). If $\#\mathcal{P}_K(\alpha, \beta) < \infty$, then there is a $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ for which*

$$\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} ((\tau \circ \sigma)(\alpha) - \sigma(\beta)) = \pm F(\alpha, \beta) \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} (1 - \sigma(\alpha\beta)), \tag{1}$$

where

$$F(\alpha,\beta) = \left(\prod_{v_P(\alpha)>0} N(P)^{v_P(\beta)} \prod_{v_P(\alpha)<0} N(P)^{v_P(\alpha)} \prod_{\substack{v_P(\alpha)=0\\ v_P(\beta)<0}} N(P)^{v_P(\beta)}\right)\left(\prod_{P:\ \substack{v_P(\alpha)\neq 0 \text{ or}\\ v_P(\beta)\neq 0}} N(P)^{v_P(1-\alpha\beta)}\right)^{-1}. \quad (2)$$

We preface the proof of Proposition 2 by introducing some relevant notation and terminology. We fix a strictly increasing sequence of primes q for which

(i) $\alpha^q \neq \beta$,

(ii) $q\mathcal{O}_K$ is comaximal with both $\alpha\mathcal{O}_K$ and $\beta\mathcal{O}_K$,

(iii) as $q \to \infty$ through our sequence, $q \to -1$ in $\hat{\mathbb{Z}}$ (the profinite completion of $\mathbb{Z}$).

To see that such a sequence exists, note that condition (i) is violated for at most one prime q (as α is not a root of unity), while (ii) is satisfied for all but finitely many primes q. Invoking Dirichlet's theorem on primes in progressions, we can construct an infinite, strictly increasing sequence of primes whose nth term is congruent to -1 modulo $n!$. Throwing away the finitely many terms for which (i) and (ii) fail, we obtain a sequence satisfying all of (i)–(iii). We refer to this fixed sequence of primes as our filter sequence. For brevity, we signal limiting behavior as $q \to \infty$ through the filter sequence by the phrase

$$\text{“as } q \xrightarrow{\hat{\mathbb{Z}}} -1\text{”}.$$

We say a claim holds “eventually” if it holds for all q sufficiently far out in the filter sequence.

Proof of Proposition 2. For each q in the filter sequence, we write

$$(\alpha^q - \beta)\mathcal{O}_K = \prod_P P^{e_{P,q}}, \quad \text{where each} \quad e_{P,q} = v_P(\alpha^q - \beta), \quad (3)$$

the product extending over all nonzero prime ideals of $\mathcal{O}_K$.

We consider first the contribution to the right-hand side of (3) from (the finitely many) primes P belonging to the support of $\alpha\mathcal{O}_K$ or $\beta\mathcal{O}_K$. Fix such a P. If $v_P(\alpha) > 0$, then $e_{P,q} = v_P(\alpha^q - \beta) = v_P(\beta)$ eventually, by the strong triangle inequality. Similarly, if $v_P(\alpha) < 0$, then $e_{P,q} = v_P(\alpha^q - \beta) = v_P(\alpha^q) = qv_P(\alpha)$ eventually. Suppose now that $v_P(\alpha) = 0$. If $v_P(\beta) < 0$ then $e_{P,q} = v_P(\beta)$, while if $v_P(\beta) > 0$ we have $e_{P,q} = 0$. Since only finitely many primes belong to the support of $\alpha\mathcal{O}_K$ or $\beta\mathcal{O}_K$, we may — eventually — split the right-hand side of (3) into the five products

$$\prod_{P\in\mathcal{P}_K(\alpha,\beta)} P^{e_{P,q}} \prod_{\substack{v_P(\alpha)=v_P(\beta)=0\\ P\notin\mathcal{P}_K(\alpha,\beta)}} P^{e_{P,q}} \prod_{v_P(\alpha)>0} P^{v_P(\beta)} \prod_{v_P(\alpha)<0} P^{qv_P(\alpha)} \prod_{\substack{v_P(\alpha)=0\\ v_P(\beta)<0}} P^{v_P(\beta)}. \quad (4)$$

Here is the key observation (already present in [SW92]): If $v_P(\alpha) = v_P(\beta) = 0$, and $e_{P,q} > 0$, then $\alpha^q = \beta$ in $\mathcal{O}_P/P\mathcal{O}_P$. Hence either $\langle \alpha \bmod P\rangle = \langle \beta \bmod P\rangle$, so that $P \in \mathcal{P}_K(\alpha,\beta)$, or q divides $\#(\mathcal{O}_P/P\mathcal{O}_P)^\times = NP - 1$. So if we take norms in (4) and reduce modulo q, the second product will make a trivial contribution.

It will be convenient to work not modulo q but modulo a prime ideal of $\mathcal{O}_K$ above q. For each q in our filter sequence, we fix once and for all a prime ideal Q of $\mathcal{O}_K$ lying above q. Our work so far shows that, eventually, we have the mod Q congruence

$$N\Big(\prod_P P^{e_{P,q}}\Big) \equiv \prod_{P \in \mathcal{P}_K(\alpha,\beta)} N(P)^{e_{P,q}} \prod_{v_P(\alpha)>0} N(P)^{v_P(\beta)} \prod_{v_P(\alpha)<0} N(P)^{v_P(\alpha)} \prod_{\substack{v_P(\alpha)=0 \\ v_P(\beta)<0}} N(P)^{v_P(\beta)}.$$

(Here we applied Fermat's little theorem to replace $N(P)^{qv_P(\alpha)}$ with $N(P)^{v_P(\alpha)}$. To know that the right-hand side is Q-adically integral, so that it makes sense to reduce mod Q, we use our assumption that $q\mathcal{O}_K$ is comaximal with $\alpha\mathcal{O}_K$ and $\beta\mathcal{O}_K$.)

Continuing, suppose P is a fixed prime not belonging to the support of α or β. Then

$$e_{P,q} = v_P(\alpha^{q+1} - \alpha\beta) = v_P((\alpha^{q+1} - 1) + (1 - \alpha\beta)). \tag{5}$$

The valuation $v_P(\alpha^{q+1} - 1) \to \infty$ as $q \xrightarrow{\hat{\mathbb{Z}}} -1$; indeed, for every positive integer m, $\#(\mathcal{O}_P/P^m\mathcal{O}_P)^\times = \#(\mathcal{O}_K/P^m)^\times$ eventually divides $q+1$, yielding $v_P(\alpha^{q+1} - 1) \geq m$. Since $1 - \alpha\beta \neq 0$ (as α, β are multiplicatively independent), eventually $v_P(\alpha^{q+1} - 1) > v_P(1 - \alpha\beta)$, so that from (5),

$$e_{P,q} = v_P(1 - \alpha\beta) \quad \text{eventually.} \tag{6}$$

So under our assumption that $\#\mathcal{P}_K(\alpha,\beta) < \infty$, we have eventually

$$\prod_{P \in \mathcal{P}_K(\alpha,\beta)} N(P)^{e_{P,q}} = \prod_{P \in \mathcal{P}_K(\alpha,\beta)} N(P)^{v_P(1-\alpha\beta)}. \tag{7}$$

We claim that, eventually, the right-hand side is congruent modulo Q to

$$\prod_{P:\ v_P(\alpha)=v_P(\beta)=0} N(P)^{v_P(1-\alpha\beta)}. \tag{8}$$

Indeed, there are only finitely many prime ideals P for which $v_P(\alpha) = v_P(\beta) = 0$ and $v_P(1 - \alpha\beta) > 0$. For each of these, (6) shows that eventually

$$v_P(\alpha^q - \beta) = e_{P,q} = v_P(1 - \alpha\beta) > 0.$$

Hence, either $P \in \mathcal{P}_K(\alpha,\beta)$ or $N(P) \equiv 1 \pmod{Q}$. So any (nontrivial) factor in (8) not already part of the right-hand product in (7) is 1 modulo Q.

Thus, if we set

$$F_0(\alpha,\beta) = \prod_{v_P(\alpha)>0} N(P)^{v_P(\beta)} \prod_{v_P(\alpha)<0} N(P)^{v_P(\alpha)} \prod_{\substack{v_P(\alpha)=0 \\ v_P(\beta)<0}} N(P)^{v_P(\beta)},$$

then

$$N\Big(\prod_P P^{e_{P,q}}\Big) \equiv F_0(\alpha,\beta) \prod_{P:\ v_P(\alpha)=v_P(\beta)=0} N(P)^{v_P(1-\alpha\beta)} \pmod{Q}.$$

Since

$$N((1-\alpha\beta)\mathcal{O}_K) = F_1(\alpha,\beta) \prod_{P:\ v_P(\alpha)=v_P(\beta)=0} N(P)^{v_P(1-\alpha\beta)}$$

for

$$F_1(\alpha,\beta) = \prod_{\substack{P:\ v_P(\alpha)\neq 0 \text{ or} \\ v_P(\beta)\neq 0}} N(P)^{v_P(1-\alpha\beta)},$$

we conclude that

$$N\Big(\prod_P P^{e_{P,q}}\Big) \equiv F(\alpha,\beta)\cdot N((1-\alpha\beta)\mathcal{O}_K) \pmod{Q} \tag{9}$$

with

$$F(\alpha,\beta) := F_0(\alpha,\beta)/F_1(\alpha,\beta).$$

We are now ready to prove our fundamental identity (1). Notice that

$$N((1-\alpha\beta)\mathcal{O}_K) = \pm N_{K/\mathbb{Q}}(1-\alpha\beta) = \pm \prod_{\sigma\in \mathrm{Gal}(K/\mathbb{Q})} (1-\sigma(\alpha\beta)). \tag{10}$$

On the other hand,

$$N\Big(\prod_P P^{e_{P,q}}\Big) = N((\alpha^q-\beta)\mathcal{O}_K) = \pm N_{K/\mathbb{Q}}(\alpha^q-\beta). \tag{11}$$

If q is unramified in K, which certainly holds eventually, then modulo Q,

$$\begin{aligned} N_{K/\mathbb{Q}}(\alpha^q-\beta) &\equiv \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} (\sigma(\alpha)^q - \sigma(\beta)) \\ &\equiv \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} ((\mathrm{Frob}_{Q/q}\circ\sigma)(\alpha) - \sigma(\beta)). \end{aligned} \tag{12}$$

Assembling (9)–(12), we see that eventually

$$\prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} ((\mathrm{Frob}_{Q/q}\circ\sigma)(\alpha) - \sigma(\beta)) \equiv \pm F(\alpha,\beta) \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} (1-\sigma(\alpha\beta)) \pmod{Q}.$$

By passing to a subsequence of q, we can assume that the element $\mathrm{Frob}_{Q/q} \in \mathrm{Gal}(K/\mathbb{Q})$ is independent of q, and the same for the choice of $\pm$ sign. This last congruence holding for infinitely many q implies the congruence must be an equality, establishing the fundamental identity (1) with $\tau = \mathrm{Frob}_{Q/q}$. □

Remark. Our proof shows that the element τ in the statement of Proposition 2 can be taken to have the form $\mathrm{Frob}_{Q/q}$ for an infinite subsequence of q belonging to our original filter sequence (where each Q is a prime ideal of $\mathcal{O}_K$ lying above the corresponding rational prime q). While not needed for the proof of Theorem 1, this observation will be useful in our concluding remarks.

3 Preparation from Diophantine analysis

In this section we collect several results from Diophantine analysis needed for the proof of Theorem 1. These statements require some setup; see Chapters 1 and 2 of Corvaja and Zannier's tract [CZ18] for further discussion. If L is a number field, we let M_L^∞ and M_L^0 denote the collection of infinite (Archimedean) and finite (non-Archimedean) places of L, respectively, and we set $M_L = M_L^\infty \cup M_L^0$. If $\nu \in M_L^\infty$ corresponds to the real embedding σ, we normalize $|\cdot|_\nu$ so that $|x|_\nu = |\sigma(x)|_{\mathbb{R}}^{1/[L:\mathbb{Q}]}$. If ν corresponds to the pair of

complex nonreal embeddings $\{\sigma, \bar{\sigma}\}$, we let $|x|_\nu = |\sigma(x)|_{\mathbb{C}}^{2/[L:\mathbb{Q}]}$. Finally, if $\nu \in M_L^0$ corresponds to the nonzero prime ideal P of $\mathcal{O}_L$, we let $|x|_\nu = N(P)^{-v_P(x)/[L:\mathbb{Q}]}$.

The absolute height (henceforth, simply height) of $x \in \bar{\mathbb{Q}}$ is defined as $H(x) := \prod_{\nu \in M_L} \max\{1, |x|_\nu\}$, where L is any number field containing x. Its logarithmic height is $h(x) := \log H(x)$; equivalently, $h(x) = \sum_{\nu \in M_L} \log^+ |x|_\nu$, where $\log^+ t = \max\{0, \log t\}$. The word "absolute" is justified by our normalizations of the $|\cdot|_\nu$, which ensure that $H(x)$ and $h(x)$ are independent of the ambient field L.

Everything we need is a consequence of the following deep theorem of Schlickewei, which improved on earlier work of Schmidt. For a proof, see e.g. Chapter 7 of Bombieri and Gubler's monograph [BG06]. Several further applications are detailed in [CZ18].

If S is a set of places of L containing all the infinite places, $\mathcal{O}_{L,S}$ denotes the collection of S-integers of L, meaning the set of $x \in L$ with $|x|_\nu \le 1$ for all $\nu \notin S$.

Schmidt–Schlickewei Subspace Theorem. *Let L be a number field and let S be a finite set of places of L containing all the infinite places. For each $\nu \in S$, let $\ell_{i,\nu}$, $i = 1, 2, \dots, n$, be linearly independent linear forms in n variables with coefficients from L. Let $\varepsilon > 0$. Then the solutions $\mathbf{x} = [x_1, \dots, x_n] \in (\mathcal{O}_{L,S})^n$ to the inequality*

$$\prod_{\nu \in S} \prod_{i=1}^{n} |\ell_{i,\nu}(\mathbf{x})|_\nu \le \left(\prod_{\nu \in M_L} \max\{|x_1|_\nu, \dots, |x_n|_\nu\} \right)^{-\varepsilon}$$

all lie in a certain finite union of proper L-vector subspaces of L^n.

The following consequence of the subspace theorem seems to be well-known but we include a proof for completeness. By an S-unit, we mean a unit in the ring $\mathcal{O}_{L,S}$. That is, $x \in L$ is an S-unit if $|x|_\nu = 1$ for all $\nu \notin S$.

Proposition 3. *Let L be a number field and let S be a finite set of places of L containing all the infinite places. Let $\nu_0 \in S$. Only finitely many S-units u satisfy*

$$\log |1 - u|_{\nu_0} \le -\varepsilon \cdot h(u). \tag{13}$$

Proof. We apply the subspace theorem with $n = 2$ and $\mathbf{x} = [1, u]$, noting that a proper L-subspace of L^2 will contain $[1, u]$ for at most a single value of u. For $\nu \ne \nu_0$, let

$$\ell_{1,\nu}(x_1, x_2) = x_2 \quad \text{and} \quad \ell_{2,\nu}(x_1, x_2) = x_1,$$

and take

$$\ell_{1,\nu_0}(x_1, x_2) = x_1, \qquad \ell_{2,\nu_0}(x_1, x_2) = x_1 - x_2.$$

By the subspace theorem, all but finitely many $u \in \mathcal{O}_{L,S}$ satisfy

$$\left(\prod_{\substack{\nu \in S \\ \nu \ne \nu_0}} |u|_\nu \right) |1 - u|_{\nu_0} > \left(\prod_{\nu \in M_L} \max\{1, |u|_\nu\} \right)^{-\varepsilon/2} = H(u)^{-\varepsilon/2}.$$

In the statement of Proposition 3, u is not only an element of $\mathcal{O}_{K,S}$ but an S-unit. So by the product formula, $\prod_{\nu \in S} |u|_\nu = 1$, and $\prod_{\nu \in S, \nu \ne \nu_0} |u|_\nu = |u|_{\nu_0}^{-1}$. We conclude that all but finitely many S-units u satisfy $|1 - u|_{\nu_0} > |u|_{\nu_0} \cdot H(u)^{-\varepsilon/2}$. This implies immediately that (13) has finitely many solutions

among S-units u with $|u|_{\nu_0} > H(u)^{-\varepsilon/2}$. Suppose u is a solution to (13) where $|u|_{\nu_0} \le H(u)^{-\varepsilon/2}$. Since $|1-u|_{\nu_0} \le H(u)^{-\varepsilon}$, we have $|u|_{\nu_0} \ge 1 - H(u)^{-\varepsilon}$. Hence,

$$H(u)^{-\varepsilon/2} \ge |u|_{\nu_0} \ge 1 - H(u)^{-\varepsilon} \ge 1 - H(u)^{-\varepsilon/2},$$

implying $H(u) \le 2^{2/\varepsilon}$. Since u has bounded height and bounded degree (being an element of L), the number of such u is finite by a theorem of Northcott (see [BG06, Theorem 1.6.8, p. 25]). □

The following corollary of Proposition 3 will be used to prove Theorem 1 for multiplicatively dependent α, β.

Corollary 4. *Let L be a number field. Let S be a finite set of places of L containing all the infinite places. Let $\gamma \in L^\times$, not a root of unity. There are only finitely many $n \in \mathbb{Z}^{>0}$ for which $1-\gamma^n$ is an S-unit.*

Proof. Enlarging S if necessary, we can assume that γ is an S-unit. Since γ is not a root of unity, $H(\gamma) > 1$, and there is some $\nu_0 \in S$ with $|\gamma|_{\nu_0} > 1$. Then for large n, we have $|1-\gamma^n|_{\nu_0} \ge \frac{1}{2}|\gamma|_{\nu_0}^n \ge \exp(cn)$, for a constant $c > 0$. Let $\varepsilon = \frac{c}{h(\gamma)\cdot \#S}$. It follows from Proposition 3 that if n is sufficiently large,

$$|1-\gamma^n|_\nu > H(\gamma^n)^{-\varepsilon} = \exp(-cn/\#S) \qquad \text{for all } \nu \in S.$$

Hence, $\prod_{\nu\in S}|1-\gamma^n|_\nu \ge \exp(cn)\prod_{\nu\in S,\,\nu\ne\nu_0}\exp(-cn/\#S) > 1$ for large n, implying (by the product formula) that $1-\gamma^n$ is not an S-unit. □

The next result is due to Corvaja and Zannier [CZ05, see (13) and Proposition 2]; it builds on earlier joint work with Bugeaud [BCZ03]. Here $\log^- t = \min\{0, \log t\}$.

Proposition 5. *Let L be a number field and let S be a finite set of places of L containing all the infinite places. Let $\varepsilon > 0$. There are only finitely many multiplicatively independent pairs of S-units u, v satisfying*

$$\sum_{\nu\in M_K} \log^- \max\{|1-u|_\nu, |1-v|_\nu\} \le -\varepsilon \max\{h(u), h(v)\}.$$

4 A lemma concerning multiplicative independence

We require one final preliminary result before proceeding to the proof of Theorem 1.

Lemma 6. *Let $K/\mathbb{Q}$ be a Galois number field. Assume α, β are multiplicatively independent elements of $K^\times$ with $|N_{K/\mathbb{Q}}(\alpha)| \ne 1$ and $|N_{K/\mathbb{Q}}(\beta)| \ne 1$. There is a positive integer N_0 such that the following holds: If n is a positive integer exceeding N_0, then for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$,*

$$\tau(\alpha)^{-n}\beta,\ \sigma(\alpha)^n\sigma(\beta) \quad \textit{are multiplicatively independent.}$$

Proof. We fix $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and argue that

$$\tau(\alpha)^{-n}\beta,\ \sigma(\alpha)^n\sigma(\beta) \quad \text{are multiplicatively independent for all sufficiently large } n. \tag{14}$$

Since there are finitely many possibilities for σ, Lemma 6 follows.

Let μ_K denote the (finite) group of roots of unity contained in K. As shown by Skolem [Sko47] (see also [Iwa53, Lemma 3]), the group $K^\times/\mu_K$ is free abelian. Let $\pi_1, \pi_2, \pi_3, \dots$ be a sequence of elements of $K^\times$ whose images in $K^\times/\mu_K$ form a basis. If $\delta \in K^\times$ and $\delta = \zeta\pi_1^{e_1}\pi_2^{e_2}\pi_3^{e_3}\cdots$ for some $\zeta \in \mu_K$, we associate

to δ the infinite dimensional vector $\mathbf{V}(\delta) := [e_1, e_2, e_3, \dots] \in \oplus_{i=1}^{\infty}\mathbb{Z}$. Observe that elements $\delta, \gamma \in K^\times$ are multiplicatively dependent if and only if $\mathbf{V}(\delta)$ and $\mathbf{V}(\gamma)$ are linearly dependent over $\mathbb{Z}$, or equivalently over $\mathbb{Q}$.

Put

$$\mathbf{a} = \mathbf{V}(\tau(\alpha)), \quad \mathbf{b} = \mathbf{V}(\beta), \quad \mathbf{a}' = \mathbf{V}(\sigma(\alpha)), \quad \mathbf{b}' = \mathbf{V}(\sigma(\beta)).$$

Let $\mathcal{N}$ denote the set of positive integers n for which $-n\mathbf{a} + \mathbf{b}$ and $n\mathbf{a}' + \mathbf{b}'$ are $\mathbb{Q}$-linearly dependent. Since $-n\mathbf{a} + \mathbf{b} = \mathbf{V}(\tau(\alpha)^{-n}\beta)$ and $n\mathbf{a}' + \mathbf{b}' = \mathbf{V}(\sigma(\alpha)^n\sigma(\beta))$, the observation recorded at the end of the last paragraph reduces to the proof of (14) to the claim that $\#\mathcal{N} < \infty$. We proceed by contradiction, assuming $\mathcal{N}$ is an infinite set.

We first establish that $\mathbf{a}$ and $\mathbf{a}'$ are $\mathbb{Q}$-linearly dependent. Indeed, if this fails, then some 2×2 submatrix of the $2 \times \infty$ matrix $\begin{bmatrix}\mathbf{a}\\ \mathbf{a}'\end{bmatrix}$ is nonsingular, say $\begin{bmatrix}a_j & a_k\\ a'_j & a'_k\end{bmatrix}$. The corresponding submatrix of $\begin{bmatrix}-n\mathbf{a}+\mathbf{b}\\ n\mathbf{a}'+\mathbf{b}'\end{bmatrix}$ has determinant

$$\begin{vmatrix}-na_j + b_j & -na_k + b_k\\ na'_j + b'_j & na'_k + b'_k\end{vmatrix} = -n^2(a_ja'_k - a_ka'_j) + (\text{linear polynomial in } n),$$

which is nonzero for large n. Then $-n\mathbf{a} + \mathbf{b}$ and $n\mathbf{a}' + \mathbf{b}'$ are $\mathbb{Q}$-linearly independent for all sufficiently large n, contradicting that $\mathcal{N}$ is infinite.

It follows that $\tau(\alpha)$ and $\sigma(\alpha)$ are multiplicatively dependent. Write $\tau(\alpha)^A = \sigma(\alpha)^B$, where A and B are integers, not both zero. Since $|N_{K/\mathbb{Q}}(\tau(\alpha))| = |N_{K/\mathbb{Q}}(\sigma(\alpha))| = |N_{K/\mathbb{Q}}(\alpha)| \neq 1$, we conclude that $A = B$. Hence, $\tau(\alpha)$, $\sigma(\alpha)$ differ (multiplicatively) by a root of unity in K, giving

$$\mathbf{a} = \mathbf{a}'.$$

This last equality implies that for every $n \in \mathcal{N}$, the vectors $-n\mathbf{a}+\mathbf{b}$ and $(n\mathbf{a}'+\mathbf{b}')+(-n\mathbf{a}+\mathbf{b}) = \mathbf{b}+\mathbf{b}'$ are linearly dependent over $\mathbb{Q}$. If $\mathbf{b}+\mathbf{b}' = \mathbf{0}$, then $\beta\sigma(\beta)$ is a root of unity, contradicting that $|N_{K/\mathbb{Q}}(\beta)| \neq 1$. So $\mathbf{b}+\mathbf{b}'$ is nonzero. It follows that for each $n \in \mathcal{N}$,

$$-n\mathbf{a} + \mathbf{b} \in \mathbb{Q} \cdot (\mathbf{b} + \mathbf{b}').$$

Applying this for two different $n \in \mathcal{N}$ and subtracting, we get that $\mathbf{a} \in \mathbb{Q} \cdot (\mathbf{b} + \mathbf{b}')$ and then that $\mathbf{b} \in \mathbb{Q} \cdot (\mathbf{b}+\mathbf{b}')$. The latter forces $\mathbf{b}$ and $\mathbf{b}'$ to be dependent over $\mathbb{Q}$. Thus, β and $\sigma(\beta)$ are multiplicatively dependent. Writing $\beta^{A'} = \sigma(\beta)^{B'}$ with integers A', B', we see upon taking norms that $A' = B'$. (We use here that $|N_{K/\mathbb{Q}}(\beta)| = |N_{K/\mathbb{Q}}(\sigma(\beta))| \neq 1$.) Thus, β and $\sigma(\beta)$ differ by a root of unity, and $\mathbf{b} = \mathbf{b}'$. Hence, $\mathbf{a} \in \mathbb{Q}\cdot(\mathbf{b}+\mathbf{b}') = \mathbb{Q}\cdot\mathbf{b}'$, and so $\mathbf{a}' = \mathbf{a}$ and $\mathbf{b}'$ are $\mathbb{Q}$-dependent. Therefore $\sigma(\alpha)$ and $\sigma(\beta)$ are multiplicatively dependent. This contradicts our assumption that α, β are multiplicatively independent. □

5 Proof of Theorem 1, modulo multiplicative independence

We now put the pieces together to prove Theorem 1.

Proof of Theorem 1. As discussed in the introduction, we may assume that K is Galois over $\mathbb{Q}$.

We first dispense with the case where α, β are multiplicatively dependent. Write $\alpha^A = \beta^B$, where A and B are integers, not both 0. Since α, β are not roots of unity, in fact A, B are both nonzero. Let $\mathcal{Q}$ be the set of maximal ideals of $\mathcal{O}_K$ that appear in the support of $(\beta^q - 1)\mathcal{O}_K$ for a prime q not dividing B. Let

S be the set of finite places of K corresponding to the prime ideals in $\mathcal{Q}$ together with all of the infinite places of K. Then $1-\beta^q$ is an S-unit for all primes q not dividing B. As there are infinitely many such q, Corollary 4 (with $L=K$ and $\gamma=\beta$) shows that $\mathcal{Q}$ must be infinite.

Let Q be any element of $\mathcal{Q}$ with $v_Q(\alpha)=v_Q(\beta)=0$. We can find a prime q not dividing B for which Q belongs to the support of β^q-1. Then the order of β mod Q divides q. Since q is coprime to B, it follows that β and $\beta^B=\alpha^A$ generate the same multiplicative subgroup mod Q, so that $Q\in\mathcal{P}_K(\alpha^{|A|},\beta)$. As there are infinitely many choices for Q, the set $\mathcal{P}_K(\alpha^{|A|},\beta)$ is infinite. This yields Theorem 1 with $C=|A|$.

Henceforth we assume α,β are multiplicatively independent with $|N_{K/\mathbb{Q}}(\alpha)|\neq 1$ and $|N_{K/\mathbb{Q}}(\beta)|\neq 1$. We show there is some $n\in\mathbb{Z}^{>0}$ for which $\mathcal{P}_K(\alpha^n,\beta)$ is infinite; this gives Theorem 1 with $C=n$.

Suppose for a contradiction that $\#\mathcal{P}_K(\alpha^n,\beta)<\infty$ for all $n\in\mathbb{Z}^{>0}$. By Proposition 2, for every $n\in\mathbb{Z}^{>0}$ there is a $\tau\in\mathrm{Gal}(K/\mathbb{Q})$ and a choice of $\pm$-sign such that

$$\prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})}((\tau\circ\sigma)(\alpha)^n-\sigma(\beta))=\pm F(\alpha^n,\beta)\prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})}(1-\sigma(\alpha^n)\sigma(\beta))\,. \tag{15}$$

For later use we note from (2) that that $F(\alpha^n,\beta)\mathcal{O}_K$ is supported only on prime ideals belonging to the support of some conjugate of α or β. In (15), both τ and the choice of sign may depend on n. However, by replacing $\mathcal{N}$ with an infinite subset, we may (and will) assume τ and the sign are constant.

Let S_0 denote the set of prime ideals belonging to the support of any conjugate of α or β. For each $n\in\mathcal{N}$, we consider the equation of fractional ideals induced by (15), removing the contribution from S_0. (All the factors in (15) generate nonzero fractional ideals of K: The right-hand side is nonzero, by the assumed multiplicative independence of α,β, so each factor on the left is nonzero too.) Let

$$I_\sigma=\prod_{P\notin S_0}P^{v_P((\tau\circ\sigma)(\alpha)^n-\sigma(\beta))},\quad J_\sigma=\prod_{P\notin S_0}P^{v_P(1-\sigma(\alpha)^n\sigma(\beta))}.$$

(Here the notation suppresses the dependence on $n\in\mathcal{N}$.) Then I_σ and J_σ are integral ideals. Furthermore, since $F(\alpha,\beta)$ is supported entirely on S_0, we deduce from (15) that

$$\prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})}I_\sigma=\prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})}J_\sigma,$$

an equation involving only integral ideals of $\mathcal{O}_K$. It follows that

$$I_{\mathrm{id}}=\prod_{P\notin S_0}P^{v_P(\tau(\alpha)^n-\beta)}$$

divides $\prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})}J_\sigma$ (as integral ideals), and so

$$I_{\mathrm{id}}\quad\text{divides}\prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})}\gcd(I_{\mathrm{id}},J_\sigma).$$

(Here the gcd of two ideals is the smallest ideal containing both.) Hence, there is a $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$ with

$$N(\gcd(I_{\mathrm{id}},J_\sigma))\geq N(I_{\mathrm{id}})^{1/[K:\mathbb{Q}]}. \tag{16}$$

It will be convenient if σ is the same for all $n\in\mathcal{N}$; we ensure this by passing to a smaller infinite subset of $\mathcal{N}$.

Observe that

$$\log N(I_{\mathrm{id}}) = \sum_{P \notin S_0} v_P(\tau(\alpha)^n - \beta) \log N(P). \tag{17}$$

Identifying S_0 with the corresponding subset of M_K^0,

$$\begin{aligned}\sum_{P \notin S_0} v_P(\tau(\alpha)^n - \beta) \log N(P) &= -[K:\mathbb{Q}] \sum_{\nu \in M_K^0 \setminus S_0} \log |\tau(\alpha)^n - \beta|_\nu \\ &= -[K:\mathbb{Q}] \sum_{\nu \in M_K^0 \setminus S_0} \log |1 - \tau(\alpha)^{-n}\beta|_\nu \\ &= [K:\mathbb{Q}] \sum_{\nu \in M_K^\infty \cup S_0} \log |1 - \tau(\alpha)^{-n}\beta|_\nu. \end{aligned} \tag{18}$$

(To go from the second line to the third, we applied the product formula in additive form, according to which $\sum_{\nu \in M_K} \log |1 - \tau(\alpha)^{-n}\beta|_\nu = 0$.) Let $S = M_K^\infty \cup S_0$. Then every conjugate of α and β is an S-unit. Since $\tau(\alpha)$ is not a root of unity, there is some $\nu_0 \in S$ with $|\tau(\alpha)|_{\nu_0} < 1$. Then for a certain constant $c_1 > 0$, we will have

$$\log |1 - \tau(\alpha)^{-n}\beta|_{\nu_0} > c_1 n \quad \text{for all large } n \in \mathcal{N}.$$

Now fixing an $\varepsilon > 0$, Proposition 3 implies that for all large $n \in \mathcal{N}$,

$$\sum_{\nu \in S,\, \nu \neq \nu_0} \log |1 - \tau(\alpha)^{-n}\beta|_\nu \geq -\varepsilon((\#S) - 1) \cdot h(\tau(\alpha)^{-n}\beta) \geq -\varepsilon((\#S) - 1))(n \cdot h(\alpha) + h(\beta)).$$

Taking ε small enough (for example, $\varepsilon < \frac{1}{2} c_1 h(\alpha)^{-1} (\#S)^{-1}$ suffices), we conclude that

$$\begin{aligned}\sum_{\nu \in S} \log |1 - \tau(\alpha)^{-n}\beta|_\nu &= \log |1 - \tau(\alpha)^{-n}\beta|_{\nu_0} + \sum_{\nu \in S,\, \nu \neq \nu_0} \log |1 - \tau(\alpha)^{-n}\beta| \\ &> c_1 n - \varepsilon((\#S) - 1))(n \cdot h(\alpha) + h(\beta)) \\ &> \frac{1}{2} c_1 n \end{aligned}$$

for all large enough $n \in \mathcal{N}$. Thus, referring back to (17) and (18), we have that

$$N(I_{\mathrm{id}}) \geq \exp(\frac{1}{2}[K:\mathbb{Q}] c_1 n).$$

On the other hand,

$$\log N(\gcd(I_{\mathrm{id}}, J_\sigma)) = \sum_{P \notin S_0} \min\{v_P(\tau(\alpha)^n - \beta), v_P(1 - \sigma(\alpha)^n \sigma(\beta))\} \log N(P), \tag{19}$$

which we can rewrite as

$$-[K:\mathbb{Q}] \sum_{\nu \in M_K^0 \setminus S_0} \log \max\{|1 - \tau(\alpha)^{-n}\beta|_\nu, |1 - \sigma(\alpha)^n \sigma(\beta)|_\nu\}. \tag{20}$$

By our choice of S_0, the maximum appearing here is at most 1, and so log could be replaced with $\log^-$ without changing the value of the expression. By Lemma 6, $\tau(\alpha)^{-n}\beta$ and $\sigma(\alpha)^n \sigma(\beta)$ are multiplicatively

independent for all sufficiently large values of n. Hence, by Proposition 5, for any $\varepsilon > 0$ and all sufficiently large $n \in \mathcal{N}$,

$$\begin{aligned}\sum_{\nu \in M_K^0 \setminus S_0} \log \max\{|1-\tau(\alpha)^{-n}\beta|_\nu, |1-\sigma(\alpha)^n\sigma(\beta)|_\nu\} &\geq \sum_{\nu \in M_K} \log^- \max\{|1-\tau(\alpha)^{-n}\beta|_\nu, |1-\sigma(\alpha)^n\sigma(\beta)|_\nu\} \\ &\geq -\varepsilon \max\{h(\tau(\alpha)^{-n}\beta), h(\sigma(\alpha)^n\sigma(\beta))\} \\ &\geq -\varepsilon(nh(\alpha)+h(\beta)),\end{aligned}$$

so that from (19) and (20),

$$\log N(\gcd(I_{\mathrm{id}}, J_\sigma)) \leq \varepsilon[K:\mathbb{Q}](nh(\alpha)+h(\beta)).$$

Fixing $\varepsilon < \frac{1}{2}c_1[K:\mathbb{Q}]^{-1}h(\alpha)^{-1}$, we find that for all large enough $n \in \mathcal{N}$,

$$N(\gcd(I_{\mathrm{id}}, J_\sigma)) < \exp\left(\frac{1}{2}c_1 n\right) \leq N(I_{\mathrm{id}})^{1/[K:\mathbb{Q}]},$$

contradicting (16). □

Concluding remarks

Suppose K is imaginary quadratic and that $\alpha, \beta \in K^\times$ are multiplicatively independent. Working through the arguments of §2 in this case, we find that if $\#\mathcal{P}_K(\alpha^n, \beta) < \infty$, then the identity (15) holds with τ the nontrivial automorphism of $K/\mathbb{Q}$. (Here we use the Remark following the proof of Proposition 2 alongside the fact that for an imaginary quadratic field K, the Frobenius at q is nontrivial in $\mathrm{Gal}(K/\mathbb{Q})$ when $q \equiv -1 \pmod{|\mathrm{Disc}_K|}$.) If we suppose further that $\alpha\mathcal{O}_K$ and $\beta\mathcal{O}_K$ have disjoint supports, careful inspection of (2) reveals that $F(\alpha^n, \beta) = 1$. So (15) yields

$$N_{K/\mathbb{Q}}(\bar{\alpha}^n - \beta) = N_{K/\mathbb{Q}}(1-\alpha^n\beta), \tag{21}$$

where the bar indicates the nontrivial automorphism of K. (Here we are allowed to omit the $\pm$ sign from (15), since norms from an imaginary quadratic field are nonnegative.) Now

$$N_{K/\mathbb{Q}}(1-\alpha^n\beta) - N_{K/\mathbb{Q}}(\bar{\alpha}^n - \beta) = (N_{K/\mathbb{Q}}(\alpha)^n - 1)(N_{K/\mathbb{Q}}(\beta) - 1).$$

Thus, if $N_{K/\mathbb{Q}}(\alpha) = 1$ or $N_{K/\mathbb{Q}}(\beta) = 1$, then (21) is a genuine identity for every $n \in \mathbb{Z}^{>0}$. So for α, β satisfying our assumptions (e.g., for $\alpha = \frac{2+i}{2-i}$ and $\beta = \frac{4+i}{4-i}$), we cannot hope to derive a contradiction from our sequence of identities. It follows that the norm restrictions in Theorem 1 cannot be dispensed with without a new idea.

We came to Theorem 1 by investigating what the fundamental identity (1) implies with α replaced by α^n, for $n = 1, 2, 3, \ldots$. It seems worth pointing out that (1) by itself is already enough to show $\mathcal{P}_K(\alpha, \beta)$ is infinite for "100 percent" of α, β in a Galois number field K. For simplicity in setting up the counting problem, we restrict ourselves to a formulation involving integers of K.

Let K be a degree d Galois number field, which we view as sitting inside $\mathbb{C}$, and let $\sigma_1, \ldots, \sigma_d$ be an ordering of the elements of $\mathrm{Gal}(K/\mathbb{Q})$. Put $\|\gamma\|_\infty = \max_{1 \leq i \leq d} |\sigma_i(\gamma)|_{\mathbb{C}}$ and define, for each $X > 0$,

$$\mathscr{B}(X) = \{\gamma \in \mathcal{O}_K : \|\gamma\|_\infty < X\}.$$

Then $\#\mathscr{B}(X) \sim \kappa X^d$, as $X \to \infty$, where $\kappa > 0$ is a constant depending on K (this follows from [Rie61, Hilfssatz 9]).[2] Hence, the number of ordered pairs of nonzero $\alpha, \beta \in \mathscr{B}(X)$ is asymptotic to $\kappa^2 X^{2d}$.

Proposition 7. *For each $\varepsilon > 0$ and each $X \geq 1$, the number of ordered pairs of nonzero $\alpha, \beta \in \mathscr{B}(X)$ where (1) holds, for some τ and choice of sign, is $O(X^{2d-\frac{1}{2}+\varepsilon})$. Here the constant may depend on K, ε.*

Proof. Fix an integral basis $\omega_1, \dots, \omega_d$, and write each $\gamma \in \mathcal{O}_K$ in the form $\sum_{i=1}^d h_i \omega_i$ (all $h_i \in \mathbb{Z}$). Then the vector $\mathbf{g} := [\sigma_1(\gamma), \dots, \sigma_d(\gamma)]^T$ of conjugates of γ satisfies $\mathbf{g} = M\mathbf{h}$, where $M = [\sigma_i(\omega_j)]_{1 \leq i,j \leq d}$ and $\mathbf{h} = [h_1, \dots, h_d]^T$. Hence, $\|\gamma\|_\infty = \|\mathbf{g}\|_\infty \ll \|\mathbf{h}\|_\infty$. (We allow implied constants to depend on the choice of integral basis.) Since M is invertible, we also have $\mathbf{h} = M^{-1}\mathbf{g}$, which allows us to deduce that $\|\mathbf{h}\|_\infty \ll \|g\|_\infty = \|\gamma\|_\infty$. In particular, the condition $\gamma \in \mathscr{B}(X)$ implies that each $|h_i| \leq CX$ for some constant C depending only on K.

Referring back to (2), it is straightforward to check that for nonzero $\alpha, \beta \in \mathcal{O}_K$,

$$F(\alpha, \beta) = N(I_{\alpha,\beta}), \quad \text{where} \quad I_{\alpha,\beta} := \prod_{v_P(\alpha) > 0} P^{v_P(\beta)}.$$

We consider first those cases where $F = F(\alpha, \beta)$ satisfies $F \leq X^{1/2}$. Here we count solutions to (1) corresponding to a fixed choice of τ and choice of sign, and a fixed positive integer F. If we write $\alpha = \sum_{i=1}^d h_i \omega_i$ and $\beta = \sum_{i=1}^d h_i' \omega_i$, enforcing (1) then amounts to requiring

$$\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \left(\sum_{i=1}^d (\tau \circ \sigma)(\omega_i) h_i - \sum_{i=1}^d \sigma(\omega_i) h_i' \right) \mp F \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \left(1 - \left(\sum_{i=1}^d \sigma(\omega_i) h_i \right) \left(\sum_{i=1}^d \sigma(\omega_i) h_i' \right) \right) = 0.$$

The left-hand side is a polynomial in the $2d$ variables $h_1, \dots, h_d, h_1', \dots, h_d'$ of total degree at most $2d$, and it is not the zero polynomial (e.g., since it does not vanish when all $h_i = h_i' = 0$). If $\alpha, \beta \in \mathscr{B}(X)$, then each $|h_i|, |h_i'| \leq CX$. By the Schwartz–Zippel Lemma [vzGG13, Lemma 6.44, p. 176], the number of possibilities for the integers $h_i, h_i' \in [-CX, CX]$ — and hence, the number of choices of α, β — is at most $2d(1 + 2CX)^{2d-1} = O(X^{2d-1})$. Varying τ, the choice of sign, and F, yields $O(X^{2d-\frac{1}{2}})$ solutions.

If α, β satisfy (1) with $F(\alpha, \beta) > X^{1/2}$, then there is an ideal $I = I_{\alpha,\beta}$ with norm exceeding $X^{1/2}$ for which $\beta \in I$ and $\alpha \in \mathrm{rad}(I)$. Here $\mathrm{rad}(I)$ denotes the product of the distinct prime ideals dividing I. For each nonzero ideal I, the number of nonzero $\beta \in \mathscr{B}(X) \cap I$ is $O(X^d/N(I))$, and similarly the number of nonzero $\alpha \in \mathscr{B}(X) \cap \mathrm{rad}(I)$ is $O(X^d/N(\mathrm{rad}(I)))$. (This follows from the more refined estimates of Rieger in [Rie61, Hilfssatz 9] along with the observation that there are no such β, resp. α, when $N(I) > X^d$, resp. $N(\mathrm{rad}(I)) > X^d$.) Finally (assuming as we may that $\varepsilon < \frac{1}{2}$),

$$\begin{aligned} \sum_{I:\ N(I) > X^{1/2}} \frac{X^d}{N(I)} \cdot \frac{X^d}{N(\mathrm{rad}(I))} &\leq X^{2d} \sum_I \left(\frac{N(I)}{X^{1/2}} \right)^{1-2\varepsilon} \frac{1}{N(I) N(\mathrm{rad}(I))} \\ &= X^{2d-\frac{1}{2}+\varepsilon} \prod_P \left(1 + \frac{1}{N(P)^{1+2\varepsilon}} + \frac{1}{N(P)^{1+4\varepsilon}} + \dots \right) \ll X^{2d-\frac{1}{2}+\varepsilon}, \end{aligned}$$

using in the final step that the product on P converges. □

[2] Actually $\kappa = 2^{r_1}(2\pi)^{r_2}/\sqrt{|\mathrm{Disc}_K|}$ where r_1 is the number of real embeddings of K and r_2 the number of pairs of complex nonreal embeddings.

Acknowledgements

The author is supported by the National Science Foundation (USA) under Award DMS-2001581. He thanks the referee for numerous helpful suggestions that improved the exposition.

References

[BCZ03] Y. Bugeaud, P. Corvaja, and U. Zannier, *An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$*, Math. Z. **243** (2003), 79–84.

[BG06] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.

[CZ05] P. Corvaja and U. Zannier, *A lower bound for the height of a rational function at S-unit points*, Monatsh. Math. **144** (2005), 203–224.

[CZ18] ———, *Applications of Diophantine approximation to integral points and transcendence*, Cambridge Tracts in Mathematics, vol. 212, Cambridge University Press, Cambridge, 2018.

[Iwa53] K. Iwasawa, *A note on Kummer extensions*, J. Math. Soc. Japan **5** (1953), 253–262.

[JP21] M. Just and P. Pollack, *Comparing multiplicative orders mod p, as p varies*, New York J. Math. **27** (2021), 600–614.

[JP23] O. Järviniemi and A. Perucca, *Unified treatment of Artin-type problems*, Res. Number Theory **9** (2023), no. 1, Paper No. 10, 20 pages.

[Pol] P. Pollack, *Two variants of a theorem of Schinzel and Wójcik on multiplicative orders*, Acta Arith., to appear.

[Rie61] G. J. Rieger, *Verallgemeinerung der Siebmethode von A. Selberg auf Algebraische Zahlkörper. III*, J. Reine Angew. Math. **208** (1961), 79–90.

[Sko47] Th. Skolem, *On the existence of a multiplicative basis for an arbitrary algebraic field*, Norske Vid. Selsk. Forh., Trondhjem **20** (1947), no. 2, 4–7.

[SS58] A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185–208; erratum in **5** (1958), 259.

[SW92] A. Schinzel and J. Wójcik, *On a problem in elementary number theory*, Math. Proc. Cambridge Philos. Soc. **112** (1992), 225–232.

[vzGG13] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, third ed., Cambridge University Press, Cambridge, 2013.

[Wój96] J. Wójcik, *On a problem in algebraic number theory*, Math. Proc. Cambridge Philos. Soc. **119** (1996), 191–200.