THE LEAST NONSPLIT PRIME IN GALOIS EXTENSIONS OF $\mathbb{Q}$

Jeffrey D. Vaaler*
José Felipe Voloch**

1. Introduction

Let k be a Galois extension of $\mathbb{Q}$ with $[k:\mathbb{Q}] = d \geq 2$. The purpose of this paper is to give an upper bound for the least prime which does not split completely in k in terms of the degree d and the discriminant Δ_k. Our estimate improves on the bound given by Lagarias, Montgomery and Odlyzko [3]. We note, however, that with the assumption of the generalized Riemann hypothesis much stronger bounds have been obtained by Murty [7]. In fact the analytic method employed in [7] can be used to produce an unconditional bound of the same general type as ours. The case of an abelian extension was considered earlier by Bach and Sorensen [1] and Oesterlé [8].

Our method is essentially elementary. It is based on an application of the product formula to the binomial coefficient $\binom{\alpha}{N}$, where α is an irrational algebraic integer in k and $\text{Trace}_{k/\mathbb{Q}}(\alpha) = 0$. A similar idea has been used in [11] to give a lower bound on the number of primes that do split completely in k. At one point in our argument we appeal to the prime number theorem with an error term in which all constants are given explicitly. Thus for each d we obtain a bound on the least prime which does not split completely provided $|\Delta_k|$ is large compared with d. In the special case $k = \mathbb{Q}(\sqrt{p})$ a somewhat

* Research of the first author was supported in part by the National Science Foundation (DMS-9622556) and the Texas Advanced Research Project,

** Research of the second author was supported in part by the National Security Agency (MDA904-97-1-0037).

simpler argument can be used which avoids the prime number theorem and leads to a result valid for all discriminants. The simpler argument differs insignificantly from that used by Gauss in the course of his first proof of quadratic reciprocity [2, art. 129].

THEOREM 1. *If*

$$\exp(\max\{105, 25(\log d)^2\}) \leq 8|\Delta_k|^{1/2(d-1)}, \tag{1.1}$$

then there exists a prime p such that p does not split completely in k and

$$p \leq 26d^2|\Delta_k|^{1/2(d-1)}. \tag{1.2}$$

2. Nonarchimedean estimates

Throughout this section we assume that all primes $p \leq dN(d-1)^{-1}$ split in k, where $N \geq d$ is a positive integer parameter. We further assume that α is a nonzero algebraic integer in k with $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \delta$ and $\mathrm{Trace}_{k/\mathbb{Q}}(\alpha) = 0$. Then we write $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_\delta$ for the *distinct* conjugates of α in k and

$$f(x) = \prod_{i=1}^{\delta}(x - \alpha_i)$$

for the minimal polynomial of α over $\mathbb{Q}$. Obviously f is a monic, irreducible polynomial in $\mathbb{Z}[x]$ with $2 \leq \delta = \deg(f)$ and $\delta \mid d$. We also define

$$A_N(\alpha) = \mathrm{Norm}_{k/\mathbb{Q}}\Big\{\binom{\alpha}{N}\Big\} = (-1)^{dN}(N!)^{-d}\Big\{\prod_{n=0}^{N-1} f(n)\Big\}^{d/\delta}, \tag{2.1}$$

where $\binom{x}{N}$ is the binomial coefficient. Clearly $A_N(\alpha)$ is a nonzero rational number.

LEMMA 2. *For each prime p with $p \leq dN(d-1)^{-1}$, the congruence*

$$f(x) \equiv 0 \mod p$$

has at least one root in the set $\{0, 1, 2, \ldots, [(\delta - 1)p/\delta]\}$.

Proof. Let p be a prime with $p \leq dN(d-1)^{-1}$. All embeddings of k in an algebraic closure $\overline{\mathbb{Q}_p}$ are contained in $\mathbb{Q}_p$. Hence all roots of f occur in $\mathbb{Z}_p$ and therefore f splits in $\mathbb{Z}/p\mathbb{Z}[x]$. Let $a_1, a_2, \ldots, a_\delta$ be elements of $\{0, 1, 2, \ldots, p-1\}$ such that

$$f(x) \equiv \prod_{i=1}^{\delta}(x - a_i) \mod p.$$

If $p \leq \delta$ then the result is trivial, so we may assume that $\delta < p$. Because $\text{Trace}_{k/\mathbb{Q}}(\alpha) = 0$ we have

$$\sum_{i=1}^{\delta} a_i \equiv 0 \mod p. \tag{2.2}$$

Now assume, contrary to the statement of the lemma, that $(\delta - 1)p/\delta < a_i \leq p - 1$ for each $i = 1, 2, \ldots, \delta$. Then we get

$$(\delta - 1)p < \sum_{i=1}^{\delta} a_i \leq \delta(p - 1),$$

which contradicts (2.2)

LEMMA 3. *The number $A_N(\alpha)$ is a nonzero integer.*

Proof. Let p be a prime with $p \leq N$. As before all roots of f occur in $\mathbb{Z}_p$. It follows that $\binom{\alpha_i}{N}$ belongs to $\mathbb{Z}_p$ for each $i = 1, 2, \ldots, \delta$. In particular the p-adic absolute value of $A_N(\alpha)$ satisfies $|A_N(\alpha)|_p \leq 1$ for each $p \leq N$, and of course for $p > N$ the bound $|A_N(\alpha)|_p \leq 1$ is trivial. Thus $A_N(\alpha)$ is a nonzero integer.

LEMMA 4. *For each prime p such that $N < p \leq dN(d-1)^{-1}$, we have*

$$\log |A_N(\alpha)|_p \leq d\delta^{-1}(-\log p). \tag{2.3}$$

Proof. As $\log |N!|_p = 0$ for $N < p$, we find that

$$\begin{aligned}
\log |A_N(\alpha)|_p &= d\delta^{-1}\Big\{\sum_{n=0}^{N-1} \log |f(n)|_p\Big\} - d\log |N!|_p \\
&= d\delta^{-1} \sum_{n=0}^{N-1} \sum_{\substack{m=1\\ p^m | f(n)}}^{\infty} (-\log p) \\
&\le d\delta^{-1}(-\log p) \sum_{\substack{n=0\\ p|f(n)}}^{N-1} 1.
\end{aligned} \tag{2.4}$$

By hypothesis we have $d \le N < p \le dN(d-1)^{-1}$, and therefore

$$[(\delta - 1)p/\delta] \le [(d-1)p/d] < (d-1)p/d \le N.$$

By Lemma 2 the sum on the right of (2.4) contains at least one nonzero term and this verifies (2.3).

THEOREM 5. *If* $\exp(\max\{105, 25(\log d)^2\}) \le N$ *then*

$$\sum_p \log |A_N(\alpha)|_p \le -N\delta^{-1}. \tag{2.5}$$

Proof. We use the explicit error term in the prime number theorem obtained by Rosser and Schoenfeld [10, Theorem 2]. An easy consequence of their result is that

$$\Big|\sum_{p\le X} \log p \; - X\Big| \le (1/2)X \exp\{-(2/5)\sqrt{\log X}\}$$

for all $X \ge \exp(105)$. It follows that

$$\Big|\sum_{p\le X} \log p \; - X\Big| \le \frac{X}{d(2d-1)} \tag{2.6}$$

whenever $\exp(\max\{105, 25(\log d)^2\}) \le X$. Now let $\exp(\max\{105, 25(\log d)^2\}) \le N$, set $X = dN(d-1)^{-1}$ and $\epsilon = (d(2d-1))^{-1}$. Then (2.3) and (2.6) imply that

$$\begin{aligned}\sum_p \log|A_N(\alpha)|_p &\le d\delta^{-1} \sum_{N<p\le X} (-\log p)\\ &= d\delta^{-1}\big\{(N-X) + (\sum_{p\le N}\log p - N) + (X - \sum_{p\le X}\log p)\big\}\\ &\le d\delta^{-1}\{N - X + \epsilon(N+X)\}\\ &= -N\delta^{-1}.\end{aligned}$$

3. Archimedean estimates

In this section we assume that f is a polynomial in $\mathbb{R}[x]$ with $\deg(f) = M \ge 1$. Then we write $\alpha_1, \alpha_2, \dots, \alpha_L$ for the *distinct* roots of f in $\mathbb{C}$ so that

$$f(x) = c_0 \prod_{l=1}^{L} (x-\alpha_i)^{e(l)} \quad \text{with} \quad e(l) \in \{1, 2, \dots\} \quad \text{and} \quad c_0 \ne 0.$$

It follows that the Mahler measure $\mu(f)$ is given by

$$\log\mu(f) = \log|c_0| + \sum_{l=1}^{L} e(l)\log^+|\alpha_l|.$$

We also require the norm

$$\|f\|_\infty = \sup\{|f(z)| : z \in \mathbb{C},\ |z| \le 1\}.$$

And we will use two well known inequalities (see [5, equation (4)], [6], or [9, Lemma 2])

$$2^{-M}\|f\|_\infty \le \mu(f) \le \|f\|_\infty \quad \text{and} \quad \log\mu(f') \le \log M + \log\mu(f). \tag{3.1}$$

By the square free kernel of f we understand the polynomial

$$q(x) = \prod_{l=1}^{L} (x - \alpha_l).$$

LEMMA 6. *Let f be a polynomial in $\mathbb{R}[x]$, q the square free kernel of f, and*

$$B_f = \{\beta \in \mathbb{R} : f'(\beta) = 0 \text{ and } f(\beta) \neq 0\}.$$

Then we have

$$|B_f| \leq L - 1 \quad \text{and} \quad \sum_{\beta \in B_f} \log^+ |\beta| \leq \log \|q\|_\infty. \tag{3.2}$$

Proof. There exists a polynomial $p(x)$ in $\mathbb{R}[x]$ uniquely determined by the identity

$$\frac{f'(x)}{f(x)} = \sum_{l=1}^{L} \frac{e(l)}{x - \alpha_l} = \frac{p(x)}{q(x)}.$$

Clearly we have

$$B_f = \{\beta \in \mathbb{R} : p(\beta) = 0\}.$$

¿From the identity $f'(x)q(x) = f(x)p(x)$ we find that $\deg(p) = L - 1$ and the leading coefficient of p is M. Therefore $|B_f| \leq L - 1$ and

$$\log M + \sum_{\beta \in B_f} \log^+ |\beta| \leq \log \mu(p). \tag{3.3}$$

Then the basic inequalities (3.1) imply that

$$\begin{aligned} \log \mu(p) + \log \mu(f) &= \log \mu(q) + \log \mu(f') \\ &\leq \log \|q\|_\infty + \log M + \log \mu(f). \end{aligned} \tag{3.4}$$

The remaining inequality in (3.2) follows from (3.3) and (3.4).

LEMMA 7. *Let f be a polynomial in $\mathbb{R}[x]$ and q the square free kernel of f. Then we have*

$$\int_U^V \Big|\frac{d}{dx} \log^+ |f(x)|\Big| \, dx \leq M\big\{\log^+ |U| + \log^+ |V| + 2\log^+ \|q\|_\infty\big\} + 2L \log^+ \|f\|_\infty. \tag{3.5}$$

Proof. Write $B_f(U, V)$ for the set of distinct roots of f' which occur in the interval (U, V) and which are not roots of f. To begin with we will establish the inequality

$$\int_U^V \Big|\frac{d}{dx} \log^+ |f(x)|\Big| \, dx \leq \log^+ |f(U)| + \log^+ |f(V)| + 2 \sum_{\beta \in B_f(U,V)} \log^+ |f(\beta)|. \tag{3.6}$$

Suppose that $(u, v) \subseteq \mathbb{R}$ is a bounded open interval such that

$$1 < f(x) \quad \text{whenever} \quad u < x < v. \tag{3.7}$$

Then let

$$B_f(u, v) = \{\beta_1, \beta_2, \dots \beta_J\},$$

and write

$$u = \beta_0 < \beta_1 < \beta_2 < \cdots < \beta_J < \beta_{J+1} = v.$$

Obviously $J = 0$ in case $B_f(u, v)$ is empty. In view of (3.7) we have

$$\begin{aligned}
\int_u^v \Bigl|\frac{d}{dx} \log^+ |f(x)|\Bigr| \, dx &= \sum_{j=0}^{J} \int_{\beta_j}^{\beta_{j+1}} \Bigl|\frac{f'(x)}{f(x)}\Bigr| \, dx \\
&= \sum_{j=0}^{J} \Bigl| \int_{\beta_j}^{\beta_{j+1}} \frac{f'(x)}{f(x)} \, dx \Bigr| \\
&= \sum_{j=0}^{J} \bigl| \log f(\beta_{j+1}) - \log f(\beta_j) \bigr| \\
&\le \sum_{j=0}^{J} \max\bigl(\log^+ |f(\beta_{j+1})|, \ \log^+ |f(\beta_j)|\bigr) \\
&\le \log^+ |f(u)| + \log^+ |f(v)| + 2 \sum_{\beta \in B_f(u,v)} \log^+ |f(\beta)|.
\end{aligned} \tag{3.8}$$

It is clear that (3.8) continues to hold if

$$f(x) < -1 \quad \text{whenever} \quad u < x < v. \tag{3.9}$$

Next we write

$$\{x \in \mathbb{R} : U < x < V, \ 1 < |f(x)|\} = \bigcup_{k=1}^{K} (u_k, v_k),$$

where $\{(u_k, v_k) : k = 1, 2, \dots K\}$ is a finite, disjoint collection of open intervals. Then we have

$$\int_U^V \Bigl|\frac{d}{dx} \log^+ |f(x)|\Bigr| \, dx = \sum_{k=1}^{K} \int_{u_k}^{v_k} \Bigl|\frac{d}{dx} \log^+ |f(x)|\Bigr| \, dx \tag{3.10}$$

and so we can apply the estimate in (3.8) to each term in the sum on the right of (3.10). In doing so we note that if $U < u_k < V$ then, since $x \to \log^+|f(x)|$ is continuous, we have $\log^+|f(u_k)| = 0$, and similarly if $U < v_k < V$. It follows then that

$$\begin{aligned}\int_U^V \Big|\frac{d}{dx}\log^+|f(x)|\Big|\,dx &= \sum_{k=1}^K \int_{u_k}^{v_k}\Big|\frac{d}{dx}\log^+|f(x)|\Big|\,dx\\ &\le \log^+|f(U)| + \log^+|f(V)| + 2\sum_{k=1}^K \sum_{\beta\in B(u_k,v_k)} \log^+|f(\beta)|\\ &= \log^+|f(U)| + \log^+|f(V)| + 2\sum_{\beta\in B_f(U,V)} \log^+|f(\beta)|,\end{aligned}$$

and this verifies the inequality (3.6).

In order to further estimate the terms on the right of (3.6) we employ the inequality

$$|f(z)| \le \|f\|_\infty \max(1,|z|)^M,$$

which follows easily from the maximum modulus theorem (see [9, Lemma 4]). Also, we have

$$\log^+|w_1w_2| \le \log^+|w_1| + \log^+|w_2|$$

for all pairs of complex numbers w_1 and w_2. Combining these observations we find that

$$\log^+|f(z)| \le \log^+\|f\|_\infty + M\log^+|z|. \tag{3.11}$$

Now we can combine (3.2), (3.6), (3.11) and so establish the bound:

$$\begin{aligned}&\int_U^V \Big|\frac{d}{dx}\log^+|f(x)|\Big|\,dx\\ &\quad\le M\log^+|U| + M\log^+|V| + (2|B_f|+2)\log^+\|f\|_\infty + 2M\sum_{\beta\in B_f}\log^+|\beta|. \qquad (3.12)\\ &\quad\le M\log^+|U| + M\log^+|V| + 2L\log^+\|f\|_\infty + 2M\log^+\|q\|_\infty\end{aligned}$$

This proves the lemma.

LEMMA 8. *Let f be a polynomial in $\mathbb{Z}[x]$, q the square free kernel of f, $\deg(f) = M$ and $\deg(q) = L$. Let N be a positive integer and assume that f has no roots in the set $\{0, 1, 2, \dots, N-1\}$. Then we have*

$$\begin{aligned}\Big|\sum_{n=0}^{N-1} \log|f(n)| - \int_0^N \log|f(x)|\ dx\Big| \\ \leq M(2 + \log N) + (L + \tfrac{1}{2}) \log\|f\|_\infty + M \log\|q\|_\infty.\end{aligned} \tag{3.13}$$

Proof. From a standard application of Stieltjes integration we obtain the identity

$$\begin{aligned}\sum_{n=0}^{N-1} \log|f(n)| &= \sum_{n=0}^{N-1} \log^+|f(n)| \\ &= \int_{0-}^{N-} \log^+|f(x)|\ d\{[x] + \tfrac{1}{2}\} \\ &= \int_0^N \log^+|f(x)|\ dx - \tfrac{1}{2}\log^+|f(N)| + \tfrac{1}{2}\log^+|f(0)| \\ &\quad + \int_0^N B_1(x) \frac{d}{dx} \log^+|f(x)|\ dx.\end{aligned} \tag{3.14}$$

Here

$$B_1(x) = x - [x] - \tfrac{1}{2} \text{ when } x \notin \mathbb{Z}, \text{ and } B_1(x) = 0 \text{ when } x \in \mathbb{Z},$$

is the first periodic Bernoulli polynomial. We use the bound $|B_1(x)| \leq \frac{1}{2}$, the estimate (3.5) from the previous lemma, (3.11) and (3.14). In this way we arrive at the inequality

$$\begin{aligned}&\Big|\sum_{n=0}^{N-1} \log|f(n)| - \int_0^N \log^+|f(x)|\ dx\Big| \\ &\leq \tfrac{1}{2}\max\big\{\log^+|f(0)|,\ \log^+|f(N)|\big\} + \tfrac{1}{2}\int_0^N \Big|\frac{d}{dx}\log^+|f(x)|\Big|\ dx \\ &\leq M\log N + (L + \tfrac{1}{2})\log^+\|f\|_\infty + M\log^+\|q\|_\infty.\end{aligned} \tag{3.15}$$

Next we observe that

$$\begin{aligned}\Big|\int_0^N \log|f(x)|\ dx - &\int_0^N \log^+|f(x)|\ dx\Big| \\ &= \int_0^N \log^-|f(x)|\ dx \\ &\le \sum_{l=1}^{L} e(l) \int_{\mathbb{R}} \log^-|x-\alpha_l|\ dx \\ &\le \sum_{l=1}^{L} e(l) \int_{\mathbb{R}} \log^-|x-\Re(\alpha_l)|\ dx \\ &= \sum_{l=1}^{L} e(l) \int_{\mathbb{R}} \log^-|x|\ dx \\ &= 2M.\end{aligned} \tag{3.16}$$

Then we combine (3.15) and (3.16). We find that

$$\begin{aligned}\Big|\sum_{n=0}^{N-1} \log|f(n)| - &\int_0^N \log|f(x)|\ dx\Big| \\ &\le M(2+\log N) + (L+\tfrac{1}{2})\log^+\|f\|_\infty + M\log^+\|q\|_\infty.\end{aligned} \tag{3.17}$$

To complete the proof we note that $1 \le \|f\|_\infty$ and $1 \le \|q\|_\infty$, because both f and q belong to $\mathbb{Z}[x]$.

We define $\rho : \mathbb{C} \to \mathbb{R}$ by

$$\rho(z) = \tfrac{1}{2}\int_{-1}^{1} \log|t-z|\ dt + 1. \tag{3.18}$$

If follows from the basic theory of logarithmic potential functions (see [3, Appendix 4, §1.]) that ρ is nonnegative, continuous, subharmonic, and the restriction of ρ to $\mathbb{C} \setminus [-1,1]$ is harmonic. For our purposes we require information about ρ in the closed unit disc.

LEMMA 9. *For all complex $z = x+iy$ with $|z| \le 1$ we have*

$$\rho(z) \le \frac{\pi|y|}{2} + (\log 2)|z|^2.$$

Proof. Let $\psi(z)$ be defined in the closed unit disc by

$$\psi(z) = \sum_{n=1}^{\infty} \frac{z^{2n}}{2n(2n-1)}.$$

In the upper half-disc $\{z \in \mathbb{C} : 0 < \Im(z),\ |z| < 1\}$ we find that

$$\begin{aligned} \tfrac{1}{2}\int_{-1}^{1} \log(z-t)\ dt + 1 &= \tfrac{1}{2}(1-z)\log(z-1) + \tfrac{1}{2}(1+z)\log(z+1) \\ &= \frac{\pi i}{2} - \frac{\pi i z}{2} + \sum_{n=1}^{\infty} \frac{z^{2n}}{2n(2n-1)} \\ &= \frac{\pi i}{2} - \frac{\pi i z}{2} + \psi(z), \end{aligned} \tag{3.19}$$

where we have used the principal branch of the logarithm. In the lower half-disc $\{z \in \mathbb{C} : 0 > \Im(z),\ |z| < 1\}$ the corresponding identity is

$$\tfrac{1}{2}\int_{-1}^{1} \log(z-t)\ dt + 1 = \frac{-\pi i}{2} + \frac{\pi i z}{2} + \psi(z). \tag{3.20}$$

Then (3.19), (3.20) and the continuity of ρ imply that

$$\rho(z) = \Re\Big\{\tfrac{1}{2}\int_{-1}^{1} \log(z-t)\ dt + 1\Big\} = \frac{\pi|y|}{2} + \Re\big\{\psi(z)\big\}, \tag{3.21}$$

at all points z in the closed unit disc. By the maximum modulus theorem

$$|\psi(z)| = |z|^2\Big|\frac{\psi(z)}{z^2}\Big| \le |z|^2\|\psi\|_\infty = (\log 2)|z|^2 \tag{3.22}$$

for all z in the closed unit disc. The lemma plainly follows from (3.21) and (3.22).

4. The existence of special numbers

Here we assume that k is an algebraic number field having degree $d \ge 2$ over $\mathbb{Q}$. Let $\sigma_1, \sigma_2, \dots, \sigma_d$ be the distinct embeddings of k into $\mathbb{C}$. We assume that $\sigma_1, \sigma_2, \dots, \sigma_r$ are real, that $\sigma_{r+1}, \sigma_{r+2}, \dots, \sigma_{r+s}$ are complex and not real, and that $\overline{\sigma}_{r+j} = \sigma_{r+s+j}$ for $j = 1, 2, \dots, s$. We write O_k for the ring of integers in k and Δ_k for the discriminant.

THEOREM 10. *There exists a nonzero algebraic integer α in k such that*

$$\operatorname{Trace}_{k/\mathbb{Q}}(\alpha) = 0 \quad \textit{and} \quad \max_{1\le i\le d} |\sigma_i(\alpha)| \le 4|\Delta_k|^{1/2(d-1)}. \tag{4.1}$$

Moreover, if $[\mathbb{Q}(\alpha):\mathbb{Q}] = \delta$ and f in $\mathbb{Z}[x]$ is the minimal polynomial of α over $\mathbb{Q}$, then

$$\|f\|_\infty \le 8^\delta |\Delta_k|^{\delta/2(d-1)}. \tag{4.2}$$

Proof. To begin with we observe that the set of algebraic integers in O_k which satisfy

$$\max_{1\le i\le d} |\sigma_i(\alpha)| \le T$$

is finite for every positive T. Thus it suffices to prove that for every $\epsilon > 0$ there exists an algebraic integer α in k such that

$$\operatorname{Trace}_{k/\mathbb{Q}}(\alpha) = 0 \quad \text{and} \quad \max_{1\le i\le d} |\sigma_i(\alpha)| \le (4+\epsilon)|\Delta_k|^{1/2(d-1)}.$$

Let $\omega_1, \omega_2, \ldots, \omega_d$ be an integral basis for O_k. We write Ω for the $d \times d$ matrix $\Omega = (\sigma_i(\omega_j))$, where $i = 1, 2, \ldots, d$ indexes rows and $j = 1, 2, \ldots, d$ indexes columns. Then we define W to be the $d \times d$ matrix which is organized into blocks as

$$W = \begin{pmatrix} \mathbf{1}_r & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \frac{1}{2}\mathbf{1}_s & \frac{1}{2}\mathbf{1}_s \\ \mathbf{0} & \frac{1}{2i}\mathbf{1}_s & \frac{-1}{2i}\mathbf{1}_s \end{pmatrix},$$

where $\mathbf{1}_r$ and $\mathbf{1}_s$ are identity matrices. We note that $(\det \Omega)^2 = \Delta_k$, $\det W = (-2i)^{-s}$ and the product $W\Omega$ is a $d \times d$ matrix with real entries. Next we define

$$\Lambda_k = \big\{\boldsymbol{\lambda} \in \mathbb{Z}^d : \sum_{j=1}^{d} \operatorname{Trace}_{k/\mathbb{Q}}(\omega_j)\lambda_j \equiv 0 \mod d\big\}.$$

As Λ_k is the kernel of the group homomorphism $\boldsymbol{\lambda} \to \sum_{j=1}^{d} \operatorname{Trace}_{k/\mathbb{Q}}(\omega_j)\lambda_j$ from $\mathbb{Z}^d$ into $\mathbb{Z}/d\mathbb{Z}$, it follows that $\Lambda_k \subseteq \mathbb{Z}^d$ is a sublattice of index at most d.

We now assume that $1 \le r$ and let t denote a positive parameter. Then we define

$$C_{r,s}(t) = \Big\{\mathbf{y} \in \mathbb{R}^d : |y_1| < 1, |y_i| \le t \ \text{ if } \ 2 \le i \le r, \\ \text{and } \ (y_{r+j})^2 + (y_{r+s+j})^2 \le t^2 \ \text{ if } \ 1 \le j \le s\Big\}. \tag{4.3}$$

It is clear that $C_{r,s}(t)$ is a convex, symmetric subset of $\mathbb{R}^d$, and a simple computation shows that

$$\mathrm{Vol}_d\{C_{r,s}(t)\} = 2^d(\pi/4)^s t^{d-1}. \tag{4.4}$$

Hence the linear image

$$K_{r,s}(t) = (W\Omega)^{-1}C_{r,s}(t) = \big\{\mathbf{x} \in \mathbb{R}^d : W\Omega\mathbf{x} \in C_{r,s}(t)\big\},$$

is also a convex, symmetric subset. And using (4.4) we find that

$$\begin{aligned} \mathrm{Vol}_d\big\{K_{r,s}(t)\big\} &= \mathrm{Vol}_d\big\{(W\Omega)^{-1}C_{r,s}(t)\big\} \\ &= |\det W\Omega|^{-1}\mathrm{Vol}_d\{C_{r,s}(t)\} = 2^d(\pi/2)^s t^{d-1}|\Delta_k|^{-1/2}. \end{aligned} \tag{4.5}$$

Let $0 < \eta$ and set $t = (2+\eta)|\Delta_k|^{1/2(d-1)}$. Then

$$\mathrm{Vol}_d\big\{K_{r,s}(t)\big\} = 2^d(2+\eta)^{d-1}(\pi/2)^s > [\mathbb{Z}^d : \Lambda_k]2^d,$$

and so by Minkowski's convex body theorem there exists a nonzero point $\boldsymbol{\xi}$ in $K_{r,s}(t) \cap \Lambda_k$. Using $\boldsymbol{\xi}$ we define $\beta = \sum_{j=1}^d \xi_j\omega_j$, so that β is a nonzero point in O_k. ¿From the definitions of W, Ω and $C_{r,s}(t)$ we find that

$$|\sigma_1(\beta)| < 1 \ \text{ and } \ |\sigma_i(\beta)| \le (2+\eta)|\Delta_k|^{1/2(d-1)} \ \text{ for } \ i = 2, 3, \ldots, d. \tag{4.6}$$

It is clear from the first inequality on the left of (4.6) that $\beta \in O_k \setminus \mathbb{Z}$. ¿From the definition of Λ_k we learn that

$$\mathrm{Trace}_{k/\mathbb{Q}}(\beta) = md \quad \text{with} \quad m \in \mathbb{Z}.$$

We conclude that $\alpha = \beta - m$ also belongs to $O_k \setminus \mathbb{Z}$ and $\mathrm{Trace}_{k/\mathbb{Q}}(\alpha) = 0$. We also get the estimate

$$|m| = \Big|d^{-1}\sum_{i=1}^d \sigma_i(\beta)\Big| \le \max_{1\le i\le d}|\sigma_i(\beta)| \le (2+\eta)|\Delta_k|^{1/2(d-1)}$$

and therefore

$$\max_{1\le i\le d} |\sigma_i(\alpha)| \le (4+2\eta)|\Delta_k|^{1/2(d-1)}.$$

In view of our previous remarks, this verifies the inequality on the right of (4.1).

Next we assume that $r = 0$ and define

$$\begin{aligned} C_{0,s}(t) = \Big\{\mathbf{y}\in\mathbb{R}^d : (y_1)^2 + t^{-2}(y_{s+1})^2 < 1, \\ \text{and} \quad (y_j)^2 + (y_{s+j})^2 \le t^2 \quad \text{if} \quad 2\le j\le s\Big\}. \end{aligned} \tag{4.7}$$

Clearly $C_{0,s}(t)$ is also a convex, symmetric subset of $\mathbb{R}^d$, and again we have

$$\mathrm{Vol}_d\{C_{0,s}(t)\} = 2^d(\pi/4)^s t^{d-1}. \tag{4.8}$$

We set $t = (2+\eta)|\Delta_k|^{1/2(d-1)}$ and proceed as before to determine a nonzero point β in O_k. In this case we find that

$$\begin{aligned} (\Re(\sigma_1(\beta))^2 + t^{-2}(\Im(\sigma_1(\beta))^2 < 1, \\ \text{and} \quad |\sigma_j(\beta)| \le (2+\eta)|\Delta_k|^{1/2(d-1)} \quad \text{for} \quad 2\le j\le s. \end{aligned} \tag{4.9}$$

The first inequality on the left of (4.9) shows that $\beta \in O_k \setminus \mathbb{Z}$. The rest of the argument verifying (4.1) is essentially the same.

To complete the proof, let f in $\mathbb{Z}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. Then (4.1) implies that the Mahler measure $\mu(f)$ satisfies the bound

$$\mu(f) \le 4^\delta |\Delta_k|^{\delta/2(d-1)}, \quad \text{where} \quad [\mathbb{Q}(\alpha):\mathbb{Q}] = \delta.$$

And from the inequality on the left of (3.1) we conclude that

$$\|f\|_\infty \le 2^\delta \mu(f) \le 8^\delta |\Delta_k|^{\delta/2(d-1)}.$$

5 Proof of Theorem 1

Let k be a Galois extension of $\mathbb{Q}$ with $[k:\mathbb{Q}] = d \geq 2$. As in section 2 we assume that all primes $p \leq dN(d-1)^{-1}$ split in k, where $N \geq d$ is a positive integer parameter. By Theorem 10 there exists an algebraic integer α in $O_k \setminus \mathbb{Z}$ with $\mathrm{Trace}_{k/\mathbb{Q}}(\alpha) = 0$ and

$$\max_{1\leq i\leq \delta} |\alpha_i| \leq 4|\Delta_k|^{1/2(d-1)}, \tag{5.1}$$

where $[\mathbb{Q}(\alpha):\mathbb{Q}] = \delta$ and $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_\delta$ are the conjugates of α in k. We assume that

$$\exp(\max\{105, 25(\log d)^2\}) \leq 8|\Delta_k|^{1/2(d-1)} \leq N. \tag{5.2}$$

Then the minimal polynomial f of α over $\mathbb{Q}$ satisfies the bound (4.2) and therefore $\|f\|_\infty \leq N^\delta$. Let $A_N(\alpha)$ be defined as in (2.1). Then Theorem 5 and the product formula imply that

$$0 = \log|A_N(\alpha)| + \sum_p \log|A_N(\alpha)|_p \leq \log|A_N(\alpha)| - N\delta^{-1}. \tag{5.3}$$

And from Lemma 8 we get the estimate

$$\begin{aligned}
\log|A_N(\alpha)| &= d\delta^{-1}\sum_{n=0}^{N-1}\log|f(n)| - d\log N! \\
&\leq d\delta^{-1}\Big\{\int_0^N \log|f(x)|\,dx + \delta(2+\log N) + (2\delta+\tfrac{1}{2})\log\|f\|_\infty\Big\} \\
&\qquad\qquad - d\{N\log N - N\} \\
&\leq dN\delta^{-1}\Big\{\int_0^1 \log|N^{-\delta}f(Nx)|\,dx + \delta\Big\} + 6d^2\log N
\end{aligned} \tag{5.4}$$

Combining (5.3) and (5.4) we obtain the inequality

$$1 \leq d\Big\{\int_0^1 \log|N^{-\delta}f(Nx)|\,dx + \delta\Big\} + \Big(\frac{6d^3\log N}{N}\Big). \tag{5.5}$$

Next we derive (5.5) again but with $-\alpha$ in place of α, and then we combine the two bounds. In this way we establish the estimate

$$1 \leq d\Big\{\tfrac{1}{2}\int_{-1}^1 \log|N^{-\delta}f(Nx)|\,dx + \delta\Big\} + \Big(\frac{6d^3\log N}{N}\Big). \tag{5.6}$$

¿From Lemma 9 and (5.1) we get

$$\begin{aligned}\Big\{\tfrac{1}{2}\int_{-1}^{1}\log|N^{-\delta}f(Nx)|\ dx+\delta\Big\} &= \sum_{i=1}^{\delta}\Big\{\tfrac{1}{2}\int_{-1}^{1}\log|t-N^{-1}\alpha_i|\ dt+1\Big\}\\ &= \sum_{i=1}^{\delta}\rho(N^{-1}\alpha_i)\\ &\le 3N^{-1}\sum_{i=1}^{\delta}|\alpha_i|\\ &\le 12\delta N^{-1}|\Delta_k|^{1/2(d-1)}.\end{aligned} \tag{5.7}$$

Thus (5.2), (5.6) and (5.7) lead to the bound

$$\begin{aligned}1 &\le \Big(\frac{12d^2|\Delta_k|^{1/2(d-1)}}{N}\Big)+\Big(\frac{6d^3\log N}{N}\Big)\\ &\le \Big(\frac{12d^2|\Delta_k|^{1/2(d-1)}}{N}\Big)+\Big(\frac{6d^3\max\{105,25(\log d)^2\}}{\exp(\max\{105,25(\log d)^2\})}\Big)\\ &\le \Big(\frac{12d^2|\Delta_k|^{1/2(d-1)}}{N}\Big)+10^{-40}.\end{aligned} \tag{5.8}$$

We select

$$N=\big[13d^2|\Delta_k|^{1/2(d-1)}\big],$$

use the hypothesis (5.2), and obtain a contradiction to (5.8). We have shown that if

$$\exp(\max\{105,25(\log d)^2\})\le 8|\Delta_k|^{1/2(d-1)}, \tag{5.9}$$

then there exists a prime number p with

$$p\le dN(d-1)^{-1}\le 26d^2|\Delta_k|^{1/2(d-1)}$$

such that p does not split completely in k.

References

1. E. Bach and J. Sorenson, *Explicit bounds for primes in residue classes*, Math. Comp. **65** (1996), no. 216, 1717–1735.

2. C. F. Gauss, *Disquisitiones Arithmeticae*, (1801), English translation, Springer-Verlag, New York, 1986.
3. J. C. Lagarias, H. L. Montgomery and A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. **54** (1979), 271–296.
4. G. G. Lorentz, M. v. Golitschek and Y. Makovoz, *Constructive Approximation*, Springer-Verlag, New York, 1996.
5. K. Mahler, *An application of Jensen's formula to polynomials*, Mathematika **7** (1960), 98–100.
6. K. Mahler, *On the zeros of the derivative of a polynomial*, Proc. Roy. Soc. London, Ser. A **264** (1961), 145–154.
7. V. K. Murty, *The least prime which does not split completely*, Forum Math. **6** (1994), 555–565.
8. J. Oesterlé, *Versions effectives du Théorème de Chebotarev sous L'Hypothèse de Riemann Généralisée*, Astérisque **61** (1979), 165–167.
9. C. G. Pinner and J. D. Vaaler, *The Number of Irreducible Factors of a Polynomial, I*, Trans. Amer. Math. Soc. **339** (1993), 809–834.
10. J. B. Rosser and L. Schoenfeld, *Sharper Bounds for the Chebyshev Functions $\theta(x)$ and $\psi(x)$*, Math. Comp. **29** (1975), no. 129, 243–269.
11. J. F. Voloch, *Chebyshev's method for number fields* (1999).

Jeffrey D. Vaaler, Department of Mathematics, University of Texas, Austin, TX 78712, e-mail: `vaaler@math.utexas.edu`

José Felipe Voloch, Department of Mathematics, University of Texas, Austin, TX 78712, e-mail: `voloch@math.utexas.edu`