WEIL NUMBERS IN FINITE EXTENSIONS OF $\mathbb{Q}^{ab}$: THE LOXTON-KEDLAYA PHENOMENON

FLORIN STAN AND ALEXANDRU ZAHARESCU,
 WITH AN APPENDIX BY KIRAN S. KEDLAYA

ABSTRACT. A finiteness phenomenon described by Loxton and later by Kedlaya states that, for any fixed m , there exist (modulo multiplication by roots of unity) only finitely many m -Weil numbers in $\mathbb{Q}^{ab}$. In the present paper we show that this phenomenon extends to all finite extensions of $\mathbb{Q}^{ab}$.

CONTENTS

1. Introduction	4359
2. Preliminary results	4361
3. The length function	4363
4. Representations as sums of roots of unity	4364
5. p -adic bounds on the degree	4367
6. Proof of Theorem 1	4368
Appendix A. A combinatorial lemma (by Kiran S. Kedlaya)	4374
Acknowledgement	4375
References	4375

1. INTRODUCTION

Let $\mathbb{Q}$ be the field of rational numbers and let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Fix a positive integer m . An m -Weil number is an algebraic integer α such that $|\sigma(\alpha)|^2 = m$, for any $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. A classical theorem of Kronecker ([10]) shows that the 1-Weil numbers are the roots of unity. Weil numbers naturally appear in the study of various mathematical objects. For some of these aspects, the reader is referred to the work of Mumford [14], Deligne [5], Odoni [17], Deninger [6], Kowalski [9], and Anglès and Baliaeva [2]. Various connections between Weil numbers and classical Gauss or Jacobi sums, Galois Gauss sums, character tables of finite groups and inverses of zeros of zeta functions are presented by Greaves and Odoni in [15]. If ρ is a geometric representation of the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and l is a prime at which ρ is unramified, results of Deligne and de Jong imply that the eigenvalues of $\rho(\text{Frob}_l)$ are Weil numbers (see [4]). In the particular case $m = q$ (a prime power), a well-known theorem of Honda, Serre and Tate shows that there is a bijection between the set of $\mathbb{F}_q$ -isogeny classes of $\mathbb{F}_q$ -simple abelian

---

Received by the editors September 18, 2012 and, in revised form, August 21, 2013.

2010 *Mathematics Subject Classification*. Primary 11R18, 11R06.

Key words and phrases. Weil numbers, cyclotomic fields.

The research of the second author was supported by the NSF grant DMS-0901621.

varieties defined over $\mathbb{F}_q$ and the set of conjugacy classes of q -Weil numbers (see [7] and [25]). Weil numbers are also related to CM fields. For instance, if α is a totally complex m -Weil number, then $\mathbb{Q}(\alpha)$ is a CM field (see [15]). Recently, an l -adic version of classical Weil numbers was studied by Jaulent ([8]). There is also an earlier work of Robinson on algebraic integers that have all their Galois conjugates on a circle centred at the origin (see [18]).

While, as seen above, Weil numbers appear in various contexts, there is also much interest in the study of cyclotomic Weil numbers in particular. For instance, Gauss and Jacobi sums are cyclotomic, as are examples coming from character tables of finite groups. In [13], Loxton proved that modulo multiplication by roots of unity, there are only finitely many cyclotomic m -Weil numbers. Moreover, Lemma 7 of [13] gives an effective method for finding them all. Another approach, describing the same phenomenon, was provided more recently in an unpublished manuscript by Kedlaya. In the present paper we canonically associate to a pair (m, K) , where m is a positive integer and K a finite extension of $\mathbb{Q}^{ab}$, a certain group, and investigate its properties. For any positive integer m , and any finite extension K of $\mathbb{Q}^{ab}$, let $H_{m,K}$ denote the set of elements x of the form $x = x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$, where $x_1, \dots, x_n$ are m -Weil numbers in K , and the exponents $e_1, \dots, e_n$ are in $\mathbb{Z}$, and satisfy $e_1 + \dots + e_n = 0$. Then $H_{m,K}$ is a multiplicative subgroup of $K^\times$. Let us remark that μ_∞ , the group of all roots of unity in $\mathbb{Q}^{ab}$, is a subgroup of $H_{m,K}$. From Loxton's work it follows that when K coincides with $\mathbb{Q}^{ab}$, the quotient group $H_{m,\mathbb{Q}^{ab}}/\mu_\infty$ is free, of finite rank. The main result of this paper is the following extension of this result.

Theorem 1. *For any $m \geq 1$, and any finite extension K of $\mathbb{Q}^{ab}$, the quotient group $H_{m,K}/\mu_\infty$ is isomorphic to $\mathbb{Z}^r$, for some nonnegative integer $r = r_{m,K}$.*

Thus the theorem identifies μ_∞ as the torsion part of $H_{m,K}$, and also shows that the free part has finite rank. We call the number $r_{m,K}$ the *Loxton-Kedlaya rank* associated to the given positive integer m and the given finite field extension K of $\mathbb{Q}^{ab}$.

Our approach to proving Theorem 1 relies heavily on the method devised by Kedlaya, including a key combinatorial lemma, to whose reproduction in Appendix A below he has kindly agreed. We combine his method with two new ingredients. One of them is a certain norm defined on the set of algebraic numbers. Its square, which we denote by $A(\cdot)$, plays an important role in recent investigations on the classical trace problem of Siegel ([23]). Siegel's trace problem asks for the best possible constant λ_0 for which, given $\lambda < \lambda_0$, the trace of a totally real and positive algebraic integer β is at least λ times its degree, except for finitely many β 's. Schur [19] showed that $\lambda_0 \geq e^{1/2} \approx 1.649$. Siegel [20] refined Schur's arguments to show that $\lambda_0 \geq e^{11/20} \approx 1.734$. Later, Smyth [21], [22] obtained $\lambda_0 \geq 1.7719$. Recently, McKee and Smyth [16] proved that $\lambda_0 \geq 1.7783786$, and Aguirre and Peral [1] showed that $\lambda_0 \geq 1.784109$. The best result to date, $\lambda_0 \geq 1.79193$, was obtained by Liang and Wu (see [11]). Another key tool in our approach is a quantitative p -adic lemma which enables us to obtain lower bounds for the p -adic valuation of the degrees of m -Weil numbers. By combining these methods, and then extending the argument so that it applies to any finite field extension K of $\mathbb{Q}^{ab}$, we prove that for any positive integer m , the Loxton-Kedlaya rank $r_{m,K}$ associated to m and K is finite.

2. PRELIMINARY RESULTS

For any positive integer q we let ζ_q denote a primitive q^{th} root of unity. We denote by $\mathbb{Q}^{ab}$ the maximal abelian extension of $\mathbb{Q}$, and for any algebraic number field K , we denote by O_K its ring of integers.

We consider the map $A : \overline{\mathbb{Q}} \rightarrow [0, \infty)$ given by

$$A(\alpha) = \frac{1}{[K : \mathbb{Q}]} \sum_{\sigma} |\sigma(\alpha)|^2,$$

where σ runs over all the embeddings of K into $\mathbb{C}$. Here $A(\alpha)$ depends only on α and not on the field K containing α .

Clearly, for any nonzero algebraic integer α , if we denote by n its degree over $\mathbb{Q}$, and by $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ its conjugates over $\mathbb{Q}$, we have

$$A(\alpha) = \frac{|\alpha_1|^2 + \dots + |\alpha_n|^2}{n} \geq \left(\frac{|\alpha_1| + \dots + |\alpha_n|}{n} \right)^2 \geq \left(|\alpha_1| \dots |\alpha_n| \right)^{\frac{2}{n}} \geq 1.$$

In this section we collect several lemmas which will be used in the subsequent sections.

Lemma 1. *For any $\alpha, \beta \in \overline{\mathbb{Q}}$ one has $\sqrt{A(\alpha + \beta)} \leq \sqrt{A(\alpha)} + \sqrt{A(\beta)}$.*

Proof. Let $\alpha, \beta \in \overline{\mathbb{Q}}$. Let K be a number field such that $\alpha, \beta \in K$. Then

$$\sum_{\sigma} |\sigma(\alpha) + \sigma(\beta)|^2 \leq \sum_{\sigma} |\sigma(\alpha)|^2 + \sum_{\sigma} |\sigma(\beta)|^2 + \left| \sum_{\sigma} \sigma(\alpha) \overline{\sigma(\beta)} \right| + \left| \sum_{\sigma} \overline{\sigma(\alpha)} \sigma(\beta) \right|.$$

Employing Cauchy's inequality, we derive that:

$$\left| \sum_{\sigma} \sigma(\alpha) \overline{\sigma(\beta)} \right| = \left| \sum_{\sigma} \overline{\sigma(\alpha)} \sigma(\beta) \right| \leq \left(\sum_{\sigma} |\sigma(\alpha)|^2 \right)^{\frac{1}{2}} \left(\sum_{\sigma} |\sigma(\beta)|^2 \right)^{\frac{1}{2}}.$$

Hence $A(\alpha + \beta) \leq A(\alpha) + A(\beta) + 2\sqrt{A(\alpha)}\sqrt{A(\beta)}$, so $\sqrt{A(\alpha + \beta)} \leq \sqrt{A(\alpha)} + \sqrt{A(\beta)}$. $\square$

Further related properties of the map A are discussed in [24].

Lemma 2. *Let $K \subset L$ be algebraic extensions of $\mathbb{Q}$, let ρ be an algebraic integer, and let E be a field such that $K \subset E \subset L$ and $\deg_L(\rho) = \deg_E(\rho)$. Then $\deg_L(\rho) \leq \deg_K(\rho)$, and for any intermediate extension F , $E \subset F \subset L$, one has $\deg_F(\rho) = \deg_E(\rho)$, and $[F : E] = [F(\rho) : E(\rho)]$.*

Proof. Let E be such that $K \subset E \subset F$ and $\deg_L(\rho) = \deg_E(\rho)$. Then for any intermediate extension F with $E \subset F \subset L$, one has $\deg_E(\rho) \geq \deg_F(\rho) \geq \deg_L(\rho) = \deg_E(\rho)$. Hence $\deg_F(\rho) = \deg_E(\rho)$, i.e. $[F(\rho) : F] = [E(\rho) : E]$.

Since $[F(\rho) : F][F : E] = [F(\rho) : E(\rho)][E(\rho) : E]$, we deduce $[F(\rho) : E(\rho)] = [F : E]$. $\square$

Lemma 3. *Let N, N_1 be integers ≥ 1 , let p be a prime such that $N = pN_1$ and $p \nmid N_1$. Any $\alpha \in \mathbb{Q}(\zeta_N)$ can be written (not uniquely) as*

$$\alpha = \sum_{j=0}^{p-1} \alpha_j \zeta_N^j,$$

where ζ is a primitive p^{th} root of 1 and $\alpha_j \in \mathbb{Q}(\zeta_{N_1})$. If α is an algebraic integer, the α_j can be chosen to be algebraic integers. Moreover,

$$(p-1)A(\alpha) = \sum_{0 \leq i < j \leq p-1} A(\alpha_i - \alpha_j).$$

Proof. This is proved in Cassels [3], relations (3.1) and (3.4). $\square$

Lemma 4. Let $N \geq 1$ be an integer, let p be a prime, let r be the exponent of p in N , and assume that $r \geq 2$. Denote $N_1 = \frac{N}{p}$ and let $\zeta = \zeta_{p^r}$. Any $\alpha \in \mathbb{Q}(\zeta_N)$ can be written uniquely as

$$\alpha = \sum_{j=0}^{p-1} \alpha_j \zeta^j,$$

where $\alpha_j \in \mathbb{Q}(\zeta_{N_1})$, and if α is an algebraic integer, then the α_j are algebraic integers. Moreover,

$$A(\alpha) = \sum_{j=0}^{p-1} A(\alpha_j).$$

Proof. This is proved in Cassels [3], relations (3.14) and (3.16). $\square$

Since any cyclotomic integer $\alpha \in O_{\mathbb{Q}^{\text{ab}}}$ is a sum of roots of unity, we can define the length $l(\alpha)$ of α to be the smallest number l such that α can be written as a sum of l roots of unity.

Lemma 5. Let $p_1, p_2, \dots, p_n$ be distinct primes. Then $A(\alpha) \geq \frac{l(\alpha)}{2^n}$, for any $\alpha \in O_{\mathbb{Q}(\zeta_{p_1 p_2 \dots p_n})}$.

Proof. This inequality is proved in [12, Lemma 9]. $\square$

Lemma 6. Let $q \geq 2$ be an integer, let p be a prime, and let $r \geq 2$ be such that $p^r \parallel q$. Then one has a tower of extensions

$$\mathbb{Q}(\zeta_{\frac{q}{p^r}}) \subset \mathbb{Q}(\zeta_{\frac{q}{p^{r-1}}}) \subset \mathbb{Q}(\zeta_{\frac{q}{p^{r-2}}}) \dots \subset \mathbb{Q}(\zeta_{\frac{q}{p}}) \subset \mathbb{Q}(\zeta_q),$$

and the set $\{1, \zeta, \dots, \zeta^{p^d-1}\}$, where $\zeta = \zeta_{p^r}$, is an integral basis of $\mathbb{Q}(\zeta_q)$ over $\mathbb{Q}(\zeta_{\frac{q}{p^d}})$ for any $1 \leq d \leq r-1$. Moreover, for any $\alpha \in \mathbb{Q}(\zeta_q)$,

$$\alpha = \sum_{j=0}^{p^d-1} \alpha_j \zeta^j,$$

with $\alpha_j \in \mathbb{Q}(\zeta_{\frac{q}{p^d}})$, one has

$$A(\alpha) = \sum_{j=0}^{p^d-1} A(\alpha_j).$$

Proof. This follows by successively applying Lemma 4 and using the fact that ζ^{p^d} is a primitive root of unity of order p^{r-d} , for any $1 \leq d \leq r-1$. $\square$

Lemma 7. Let $k \geq 2$ be an integer, and let V be a $\mathbb{Q}$ -vector subspace of $\mathbb{Q}^k$. For any $x = (x_1, x_2, \dots, x_k) \in V$, set $S(x) = \{(i, j) : 1 \leq i < j \leq k, x_i \neq x_j\}$. Then for any $x, y \in V$, there exists $z \in V$ such that $S(z) \supseteq S(x) \cup S(y)$.

Proof. Let $x, y \in V$, $x = (x_1, x_2, \dots, x_k)$ and $y = (y_1, y_2, \dots, y_k)$. Let $z = x + ty = (x_1 + ty_1, x_2 + ty_2, \dots, x_k + ty_k)$, with $t \in \mathbb{Q}$, to be chosen later. Let $i, j \in \{1, 2, \dots, k\}$, with $(i, j) \in S(x) \cup S(y)$. Then $x_i \neq x_j$ or $y_i \neq y_j$, and the equality $x_i + ty_i = x_j + ty_j$ can occur for at most one number $t \in \mathbb{Q}$. Hence one can choose $t \in \mathbb{Q}$ such that $(i, j) \in S(z)$, for any $(i, j) \in S(x) \cup S(y)$. This shows there is a $z \in V$ such that $S(z) \supseteq S(x) \cup S(y)$, which proves the lemma. $\square$

Lemma 8. *Let $k \geq 2$ and let V be a $\mathbb{Q}$ -vector subspace of $\mathbb{Q}^k$. For every $1 \leq i < j \leq k$ denote $H_{i,j} = \{(x_1, x_2, \dots, x_k) \in \mathbb{Q}^k : x_i = x_j\}$. Suppose that $V \not\subseteq H_{i,j}$ for any i, j . Then $V \not\subseteq \bigcup_{i < j} H_{i,j}$.*

Proof. With $S(x)$ defined as in Lemma 7, note that $(i, j) \in S(x)$ if and only if $x \notin H_{i,j}$. By hypothesis, for any i, j with $i < j$ there exists $v_{ij} \in V$ such that $v_{ij} \notin H_{i,j}$. So $(i, j) \in S(v_{ij})$ for any $i < j$. Applying Lemma 7 successively, there exists $z \in V$ such that $S(z) \supseteq \bigcup_{i < j} S(v_{ij})$. For any $i < j$ one has $(i, j) \in S(v_{ij}) \subseteq S(z)$, hence $z \notin H_{i,j}$. Therefore $z \notin \bigcup_{i < j} H_{i,j}$, which completes the proof of the lemma. $\square$

We end this section by recalling an elementary result that will be used in the proof of Proposition 1.

Lemma 9. *Let a, b be positive integers, and let $d = \gcd(a, b)$, $l = \text{lcm}(a, b)$ be their greatest, respectively lowest common multiple. Also let $(x, y) \in \mathbb{Z}^2$ be a solution of the equation $ax + by = d$ and denote $\zeta_k = \exp(2\pi i/k)$ for $k \geq 1$. Then*

$$i) \zeta_l = \zeta_a^y \zeta_b^x.$$

ii) If (x, y) is a solution of the equation, then $(x + \frac{kb}{d}, y - \frac{ka}{d})$ is also a solution for any $k \in \mathbb{Z}$ (and in fact any other solution is of this form).

Proof. Since ii) is a standard result, we will only prove i). Let a, b, d, l, x and y be as in the statement of the lemma. Dividing both sides of the equality $ax + by = d$ by ab , we obtain $x \frac{1}{b} + y \frac{1}{a} = \frac{d}{ab} = \frac{1}{l}$. If we multiply the previous equality by $2\pi i$, and exponentiate it, we obtain the desired equality. $\square$

3. THE LENGTH FUNCTION

Let $\overline{\mathbb{Z}}$ denote the set of algebraic integers. Let S be a finite subset of $\overline{\mathbb{Z}}$, and let $A(S)$ be the set of all elements $z \in \overline{\mathbb{Q}}$ which can be written as $z = x_1 w_1 + \dots + x_n w_n$, with $x_1, \dots, x_n \in S$ not necessarily distinct and $w_1, \dots, w_n$ roots of unity. In fact, $A(S)$ is the $O_{\mathbb{Q}^{ab}}$ -module generated by the elements of S .

We define a length function $l_S : A(S) \rightarrow \mathbb{N}$ as follows. For any $z \in A(S)$, $l_S(z)$ is the least n for which there exist $x_1, \dots, x_n \in S$ and $w_1, \dots, w_n \in \mu_\infty$ roots of unity such that $z = x_1 w_1 + \dots + x_n w_n$.

For example, if $S = \{1\}$, then $A(S) = O_{\mathbb{Q}^{ab}}$ and l_S is the function l defined before Lemma 5.

We collect several useful properties of the length function in the next lemma.

Lemma 10. *Let $S \subset \overline{\mathbb{Z}}$ be a finite set, stable under the Galois action. Then the following statements are true:*

$$i) l_S(z\zeta) = l_S(z), \forall z \in A(S), \forall \zeta \in \mu_\infty.$$

$$ii) l_S(z) = l_S(y), \forall z \in A(S) \text{ and for any } \mathbb{Q}\text{-conjugate } y \text{ of } z.$$

$$iii) l_S(y + z) \leq l_S(y) + l_S(z), \forall y, z \in A(S).$$

Proof. i) Let $z \in A(S)$, and $\zeta \in \mu_\infty$. Write $z = x_1 w_1 + \dots + x_n w_n$, with $n = l_S(z)$, $x_1, \dots, x_n \in S$ and $w_1, \dots, w_n \in \mu_\infty$. Then $z\zeta = x_1(w_1\zeta) + \dots + x_n(w_n\zeta)$, which implies that $l_S(z\zeta) \leq l_S(z)$. Repeating the above argument with z replaced by $z\zeta$ and ζ replaced by ζ^{-1} , we obtain $l_S(z) \leq l_S(z\zeta)$, which completes the proof of i).

ii) Let $z \in A(S)$, and let y be a conjugate of z . Write $z = x_1 w_1 + \dots + x_n w_n$, with $n = l_S(z)$, $x_1, \dots, x_n \in S$ and $w_1, \dots, w_n \in \mu_\infty$. Let σ be an embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$ with $y = \sigma(z)$. Then $y = \sigma(z) = \sigma(x_1) v_1 + \dots + \sigma(x_n) v_n$, where $v_i = \sigma(w_i) \in \mu_\infty$. This implies $l_S(y) \leq n = l_S(z)$. As above, by symmetry, we obtain $l_S(z) \leq l_S(y)$, hence $l_S(y) = l_S(z)$.

iii) Let $y, z \in A(S)$, and write $y = a_1 w_1 + \dots + a_n w_n$, $z = b_1 v_1 + \dots + b_m v_m$, with $n = l_S(y)$, $m = l_S(z)$, $a_1, \dots, a_n, b_1, \dots, b_m \in S$ and $w_1, \dots, w_n, v_1, \dots, v_m \in \mu_\infty$. Then $y + z = a_1 w_1 + \dots + a_n w_n + b_1 v_1 + \dots + b_m v_m$, hence $l_S(y + z) \leq n + m = l_S(y) + l_S(z)$. $\square$

Lemma 11. *For any positive numbers D and M , there exist only a finite number of algebraic integers $\alpha \in \overline{\mathbb{Z}}$ with $\deg_{\mathbb{Q}}(\alpha) < D$ and such that, for any embedding σ of $\overline{\mathbb{Q}}$ in $\mathbb{C}$, $|\sigma(\alpha)| < M$.*

Proof. Let D, M be positive numbers, and let α be as in the statement of the lemma. Let $d = \deg_{\mathbb{Q}}(\alpha)$ and let $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_d$ be the conjugates of α over $\mathbb{Q}$. One has

$$\left| \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq d} \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_k} \right| \leq \binom{d}{k} M^k < 2^d M^k < 2^D M^D,$$

for any $1 \leq k \leq d$.

Employing Viète's relations, we see that each coefficient in the minimal polynomial of α over $\mathbb{Q}$ is bounded in terms of D and M . So there exist only a finite number of such polynomials, hence there are only finitely many algebraic integers α in $\overline{\mathbb{Q}}$ such that $|\sigma(\alpha)| < M$, for any embedding σ of $\overline{\mathbb{Q}}$ in $\mathbb{C}$. $\square$

Lemma 12. *For any finite set $S \subset \overline{\mathbb{Z}}$ and for any positive numbers D and M there exist only a finite number of elements $z \in A(S)$ with $\deg_{\mathbb{Q}}(z) < D$ and $l_S(z) < M$.*

Proof. Let S be a finite set of algebraic integers, and let D, M be positive numbers. Let $z \in A(S)$ such that $\deg_{\mathbb{Q}}(z) < D$ and $l_S(z) < M$. Write z as $z = x_1 w_1 + \dots + x_k w_k$, with $k = l_S(z) < M$, where $x_1, \dots, x_k \in S$, and $w_1, \dots, w_k$ roots of unity. Then for any embedding σ of $\overline{\mathbb{Q}}$ in $\mathbb{C}$, $|\sigma(z)| \leq |\sigma(x_1 w_1)| + \dots + |\sigma(x_k w_k)| = |\sigma(x_1)| + \dots + |\sigma(x_k)| \leq k||S|| < M||S||$, where $||S|| = \max |\sigma(x)|$, the maximum being taken over all the elements $x \in S$ and over all the embeddings σ of $\overline{\mathbb{Q}}$ in $\mathbb{C}$. We now apply Lemma 11 to conclude that there are only finitely many such elements z in $A(S)$. $\square$

4. REPRESENTATIONS AS SUMS OF ROOTS OF UNITY

Lemma 13. *For any positive integer $n \geq 1$ there is an integer k_n such that any $\alpha \in O_{\mathbb{Q}^{ab}}$ with $A(\alpha) \leq \frac{n}{2}$ has $l(\alpha) \leq k_n$.*

Proof. We prove the above statement by induction on $n \geq 1$. For $n = 1$, or $n = 2$, we can take $k_1 = k_2 = 1$. Indeed, we have seen in Section 2 that $A(\alpha) \geq 1$, for any nonzero algebraic integer α . Thus, $A(\alpha) \leq \frac{1}{2}$ implies $\alpha = 0$, so we can take $k_1 = 1$. Similarly, $A(\alpha) \leq 1$ implies that α is 0 or a root of unity, which shows that we can take $k_2 = 1$ as well.

Assume that for any $1 \leq t \leq n$, there exists a $k_t \geq 1$ such that any $\alpha \in O_{\mathbb{Q}^{ab}}$ with $A(\alpha) \leq \frac{t}{2}$ has $l(\alpha) \leq k_t$.

Let $\alpha \in O_{\mathbb{Q}^{ab}}$ such that $A(\alpha) \leq \frac{n+1}{2}$. Let $\beta \in \{\alpha\eta : \eta \text{ root of unity}\}$ of minimal conductor q , in the sense that $\beta \in \mathbb{Q}(\zeta_q)$ and q is minimal with this property, where ζ_q is a primitive q^{th} root of unity.

Note that $A(\alpha) = A(\beta)$ and $l(\alpha) = l(\beta)$. We distinguish two cases.

Case 1. There exists a prime p such that $p^2 | q$. Then let ζ be a primitive root of unity of order $p^r || q$, where $r \geq 2$. Using Lemma 4 we write

$$(1) \quad \beta = \beta_1 \zeta^{i_1} + \beta_2 \zeta^{i_2} + \dots + \beta_k \zeta^{i_k}$$

with $0 \leq i_1 < i_2 < \dots < i_k \leq p-1$, and $\beta_j \in O_{\mathbb{Q}(\zeta_{\frac{q}{p}})} \setminus \{0\}$. Moreover, it follows from the minimality of q that $k \geq 2$, since for $k=1$, $\beta = \beta_1 \zeta^{i_1}$, hence $\beta \zeta^{-i_1}$ would belong to the smaller field $\mathbb{Q}(\zeta_{\frac{q}{p}})$.

Since $A(x) \geq 1$, for any nonzero algebraic integer x , using Lemma 4 we derive

$$\frac{n+1}{2} \geq A(\alpha) = A(\beta) = A(\beta_1) + A(\beta_2) + \dots + A(\beta_k) \geq A(\beta_j) + k - 1 \geq A(\beta_j) + 1,$$

for any $1 \leq j \leq k$. Hence $A(\beta_j) \leq \frac{n+1}{2} - 1 = \frac{n-1}{2}$. By the inductive hypothesis $l(\beta_j) \leq k_{n-1}$, for any $1 \leq j \leq k$. We derive that

$$l(\alpha) = l(\beta) \leq \sum_{j=1}^k l(\beta_j) \leq k k_{n-1} \leq \frac{n+1}{2} k_{n-1}.$$

Case 2. q is square-free. Let $p | q$ be a prime and let ζ be a primitive root of unity of order p . Using Lemma 3 we can write $\beta = a_0 + a_1 \zeta + a_2 \zeta^2 + \dots + a_{p-1} \zeta^{p-1}$, with $a_j \in \mathbb{Z}[\zeta_{\frac{q}{p}}]$.

Let r be the largest number of equal coefficients among $a_0, a_1, \dots, a_{p-1}$. Then

$$\begin{aligned} A(\beta) &\geq \frac{1}{2(p-1)} \sum_{0 \leq i \leq p-1} \#\{0 \leq j \leq p-1 : a_j \neq a_i\} \\ &\geq \frac{1}{2(p-1)} \sum_{0 \leq i \leq p-1} (p-r) = \frac{p(p-r)}{2(p-1)}. \end{aligned}$$

Thus $\frac{n+1}{2} \geq \frac{p(p-r)}{2(p-1)}$, which implies $r \geq p - (n+1) + \frac{n+1}{p} > p - (n+1)$, hence $r \geq p - n$. Subtracting $s(1 + \zeta + \dots + \zeta^{p-1}) = 0$ from β , where s is the common value of the r equal coefficients, we may assume in what follows that

$$(2) \quad \beta = \beta_1 \zeta^{j_1} + \beta_2 \zeta^{j_2} + \dots + \beta_k \zeta^{j_k},$$

with $k \leq n$, $0 \leq j_1 < j_2 < \dots < j_k \leq p-1$ and all the coefficients $\beta_1, \beta_2, \dots, \beta_k$ are nonzero elements of $\mathbb{Z}[\zeta_{\frac{q}{p}}]$.

On the other hand, using Lemma 3, we see that

$$\begin{aligned} \frac{n+1}{2} \geq A(\alpha) = A(\beta) &= \frac{1}{p-1} (A(\beta_1 - \beta_2) + A(\beta_1 - \beta_3) + \dots + A(\beta_{k-1} - \beta_k)) \\ &\quad + \frac{p-k}{p-1} (A(\beta_1) + A(\beta_2) + \dots + A(\beta_k)). \end{aligned}$$

This implies

$$\frac{n+1}{2} \geq \frac{p-k}{p-1} \sum_{j=1}^k A(\beta_j) \geq \frac{p-n}{p-1} \sum_{j=1}^k A(\beta_j),$$

hence

$$\sum_{j=1}^k A(\beta_j) \leq \frac{(p-1)(n+1)}{2(p-n)}.$$

Fix $j \in \{1, 2, \dots, k\}$. Since each β_i is a nonzero algebraic integer, we have $A(\beta_i) \geq 1$, and we obtain

$$k-1 + A(\beta_j) \leq \sum_{i \neq j} A(\beta_i) + A(\beta_j) \leq \frac{(p-1)(n+1)}{2(p-n)}.$$

Therefore

$$A(\beta_j) \leq \frac{(p-1)(n+1)}{2(p-n)} - k + 1.$$

Since $k \geq 2$, this further implies

$$(3) \quad A(\beta_j) \leq \frac{p(n-1) + n - 1}{2(p-n)}.$$

Subcase 2.1. There exists a prime $p|q$ such that $p \geq n^2 + n - 1$. In this case from (3) we have $A(\beta_j) \leq \frac{n}{2}$, for any $1 \leq j \leq k$. Then the inductive hypothesis implies $l(\beta_j) \leq k_n$, and from (2) we obtain

$$l(\alpha) = l(\beta) \leq \sum_{j=1}^k l(\beta_j) \leq k k_n \leq n k_n.$$

Subcase 2.2. All the primes p in the decomposition of q are $\leq n^2 + n - 2$.

Let $p_1 < p_2 < \dots < p_{\pi(n^2+n-2)}$ be the primes $\leq n^2 + n - 2$, and let $N_0(n)$ be their product. Then $\beta \in \mathbb{Q}(\zeta_{N_0(n)})$ and Lemma 5 implies that

$$l(\beta) \leq 2^{\pi(n^2+n-2)} A(\beta) \leq 2^{\pi(n^2+n-2)} \frac{n+1}{2}.$$

We may now take $k_{n+1} = \max \left\{ \frac{n+1}{2} k_{n-1}, n k_n, \frac{n+1}{2} 2^{\pi(n^2+n-2)} \right\}$, and then in all cases we have $l(\alpha) = l(\beta) \leq k_{n+1}$. $\square$

Lemma 14. Fix an algebraic integer η . Then for any positive integer $n \geq 1$ there exists an integer $t_n = t_n(\eta)$ such that any $\alpha \in O_{\mathbb{Q}^{ab}}[\eta]$ with $A(\alpha) \leq n$ has $l(\alpha) \leq t_n$.

Proof. Denote $d = \deg_{\mathbb{Q}^{ab}}(\eta)$, and let $\alpha \in O_{\mathbb{Q}^{ab}}[\eta]$. Write $\alpha = b_0 + b_1\eta + \dots + b_{d-1}\eta^{d-1}$, with $b_j \in O_{\mathbb{Q}^{ab}}$, for each $0 \leq j \leq d-1$.

Let $\{w_0, w_1, \dots, w_{d-1}\}$ be the dual basis of $\{1, \eta, \eta^2, \dots, \eta^{d-1}\}$. Then $b_j = \text{Tr}_{\mathbb{Q}^{ab}(\eta)/\mathbb{Q}^{ab}}(\alpha w_j) = z_0^{(j)} + z_1^{(j)} + \dots + z_{d-1}^{(j)}$, where $z_0^{(j)}, z_1^{(j)}, \dots, z_{d-1}^{(j)}$ are the conjugates of αw_j over $\mathbb{Q}^{ab}$.

Since $A(\alpha) \leq n$, and the w_j 's are fixed, we have $A(\alpha w_j) < M_1$, for some positive number $M_1 = M_1(n, \eta)$. Hence $A(z_i^{(j)}) < M_1$, for each i (in fact, $A(z_0^{(j)}) = A(z_1^{(j)}) = \dots = A(z_{d-1}^{(j)})$, since $z_0^{(j)}, \dots, z_{d-1}^{(j)}$ are conjugate over $\mathbb{Q}^{ab}$, hence over $\mathbb{Q}$).

Now Lemma 1 and the relation $A(b_j) = A(z_0^{(j)} + z_1^{(j)} + \dots + z_{d-1}^{(j)})$ show that there exists $M_2 = M_2(n, \eta)$ such that $A(b_j) < M_2$, for each j .

Lastly, Lemma 13 implies that $l(b_j)$ is bounded in terms of M_2 (which depends only on n and η), say $l(b_j) < M_3$, for some $M_3 = M_3(n, \eta)$. Hence $l(\alpha) \leq l(b_0) + l(b_1) + \dots + l(b_{d-1}) < M_4$, where $M_4 = M_4(n, \eta) = dM_3$, and this completes the proof of Lemma 14. $\square$

5. p -ADIC BOUNDS ON THE DEGREE

Let $\mathbb{Q}_p$ be the field of p -adic numbers and $|\cdot|_p$ be the usual p -adic absolute value on $\mathbb{Q}_p$. Let $\mathbb{Z}_p$ denote the ring of p -adic integers.

Lemma 15. *For any $k \geq 2$, for any prime p , there is a number $\rho_{k,p} > 0$ such that for any $a_1, a_2, \dots, a_k \in \mathbb{Q}_p$, we have:*

$$\max_{i,j} \min_{(l,s) \neq (i,j)} |(a_i - a_j) - (a_l - a_s)|_p \geq \rho_{k,p} \min_{i \neq j} |a_i - a_j|_p.$$

Proof. Let us assume that the conclusion of the lemma is false. Then there is an integer $k \geq 2$ and a prime p such that for any sequence $(\epsilon_n)_{n \geq 1}$ of positive numbers such that $\lim_{n \rightarrow \infty} \epsilon_n = 0$, there exist $a_1^{(n)}, a_2^{(n)}, \dots, a_k^{(n)} \in \mathbb{Q}_p$ such that

$$(4) \quad \max_{i,j} \min_{(l,s) \neq (i,j)} |(a_i^{(n)} - a_j^{(n)}) - (a_l^{(n)} - a_s^{(n)})|_p < \epsilon_n \min_{i \neq j} |a_i^{(n)} - a_j^{(n)}|_p.$$

Multiplying, if necessary, the above inequality by $|p^{v_n}|_p$, for a suitable integer v_n , we may assume, without loss of generality, that all $a_j^{(n)} \in \mathbb{Z}_p$, for any $j, n \geq 1$.

$$\text{Let } \eta_n = \eta_n(a_1^{(n)}, a_2^{(n)}, \dots, a_k^{(n)}) = \min_{i \neq j} |a_i^{(n)} - a_j^{(n)}|_p.$$

It follows that

$$\max_{i,j} \min_{(l,s) \neq (i,j)} |(a_i^{(n)} - a_j^{(n)}) - (a_l^{(n)} - a_s^{(n)})|_p < \epsilon_n \eta_n.$$

If $\eta_n = 0$, we obtain a contradiction with (4), and the proof of the lemma is complete.

Hence we can assume $\eta_n > 0$. For any i, j

$$\min_{(l,s) \neq (i,j)} |(a_i^{(n)} - a_j^{(n)}) - (a_l^{(n)} - a_s^{(n)})|_p \leq \epsilon_n \eta_n.$$

Hence for any $1 \leq i < j \leq k$, there exist l, s such that

$$(5) \quad |(a_i^{(n)} - a_j^{(n)}) - (a_l^{(n)} - a_s^{(n)})|_p \leq \epsilon_n \eta_n.$$

Let $b_{i,j,l,s}^{(n)} := (a_i^{(n)} - a_j^{(n)}) - (a_l^{(n)} - a_s^{(n)}) \in \mathbb{Z}_p$. Then

$$|b_{i,j,l,s}^{(n)}|_p \leq \epsilon_n \eta_n.$$

For any n , we construct a matrix $A^{(n)} = (A_{\alpha,\beta}^{(n)})_{\alpha,\beta}$ with $m := \binom{k}{2}$ rows and k columns defined as follows: for each $1 \leq r \leq m$, the r^{th} row contains two elements equal to 1, $A_{ri}^{(n)} = A_{rs}^{(n)} = 1$, two elements equal to -1 , $A_{rj}^{(n)} = A_{rl}^{(n)} = -1$, and all the other elements on this row are 0. Since $A_{\alpha,\beta}^{(n)} \in \{-1, 0, 1\}$ for any $1 \leq \alpha \leq m$, $1 \leq \beta \leq k$ and any $n \geq 1$, there exists a subsequence t_n for which $A^{(t_n)}$ is constant, say $A^{(t_n)} = A = (A_{\alpha,\beta})_{\alpha,\beta}$.

Let $i_0, j_0 \in \{1, 2, \dots, k\}$ such that $i_0 < j_0$, and $v_0 = (0, \dots, 0, 1, 0, \dots, 0, -1, 0, \dots, 0) \in \mathbb{Q}^k$ be the vector with 1 on the i_0^{th} component, -1 on the j_0^{th} component,

and all the other components 0. Next, we show that $v_0 \notin \langle l_1, l_2, \dots, l_m \rangle$, the vector space generated by the rows $l_1, l_2, \dots, l_m$ of the matrix A . For, suppose that $v_0 \in \langle l_1, l_2, \dots, l_m \rangle$. Then there exist $c_i \in \mathbb{Q}$, $1 \leq i \leq m$ such that

$$v_0 = c_1 l_1 + c_2 l_2 + \dots + c_m l_m.$$

Multiplying the above equality on the right by the column vector $(a_1^{(n)}, a_2^{(n)}, \dots, a_k^{(n)})^t$, we obtain

$$a_{i_0}^{(n)} - a_{j_0}^{(n)} = \sum_{i,j,l,s} c_{i,j,l,s} b_{i,j,l,s}^{(n)},$$

where $(c_{i,j,l,s})_{i,j,l,s}$ is a permutation of the set $\{c_1, c_2, \dots, c_m\}$. It follows that

$$\begin{aligned} (6) \quad 0 < \eta_n &\leq |a_{i_0}^{(n)} - a_{j_0}^{(n)}|_p = \left| \sum_{i,j,l,s} c_{i,j,l,s} b_{i,j,l,s}^{(n)} \right|_p \\ &\leq \max_{i,j,l,s} |c_{i,j,l,s}|_p |b_{i,j,l,s}^{(n)}|_p \leq \epsilon_n \eta_n \left(\max_{1 \leq i \leq m} |c_i|_p \right). \end{aligned}$$

Then (6) implies

$$1 \leq \epsilon_n \max_{1 \leq i \leq m} |c_i|_p,$$

which contradicts the fact that $\lim_{n \rightarrow \infty} \epsilon_n = 0$. Hence $v_0 \notin \langle l_1, l_2, \dots, l_m \rangle$.

Let $\tilde{A}_{i_0, j_0}$ be the matrix obtained by adding one more row (the vector v_0) to the matrix A (i.e. the vector v_0 is the $m+1$ st row of $\tilde{A}_{i_0, j_0}$).

Let $V = \{x \in \mathbb{Q}^k : Ax = 0\}$ and let $\tilde{V} = \{x \in \mathbb{Q}^k : \tilde{A}_{i_0, j_0} x = 0\}$.

One has

$$\text{rank } A + \dim V = k = \text{rank } \tilde{A} + \dim \tilde{V},$$

and since $\text{rank } A < \text{rank } \tilde{A}$, we have that $\dim V > \dim \tilde{V}$. Hence $V \neq \tilde{V}$.

Let $H_{i_0, j_0} = \{x = (x_1, x_2, \dots, x_k) \in \mathbb{Q}^k : x_{i_0} = x_{j_0}\}$. One has $\tilde{V} = V \cap H_{i_0, j_0}$. Since $V \neq \tilde{V}$, we obtain $V \not\subseteq H_{i_0, j_0}$. Applying Lemma 8, we deduce that $V \not\subseteq \bigcup_{i < j} H_{i,j}$.

Let $w = (w_1, w_2, \dots, w_k)$ be an element of V which does not belong to $\bigcup_{i < j} H_{i,j}$. We may assume, without loss of generality, that $w_1 < w_j < w_k$, for any $1 < j < k$. Then $w_k - w_1 > w_i - w_j$, for any $1 < i, j < k$. So for the pair $(k, 1)$ there is no pair (i, j) for which $b_{k,1,i,j}$ exists, contradicting (5). This completes the proof of Lemma 15. $\square$

6. PROOF OF THEOREM 1

We first prove the following proposition.

Proposition 1. *Let K be a finite extension of $\mathbb{Q}^{ab}$. For any positive integer m , there is a finite set $T_{m,K}$ such that the set $S_{m,K}$ of all m -Weil numbers in K satisfies $S_{m,K} = T_{m,K} \mu_\infty$.*

Proof. Let K be a finite extension of $\mathbb{Q}^{ab}$. We can assume, on replacing K by a larger finite extension, that the extension $K/\mathbb{Q}^{ab}$ is Galois, so that in particular complex conjugation sends K to itself. Fix $\eta \in \overline{\mathbb{Z}}$ such that $K = \mathbb{Q}^{ab}(\eta)$ and let $d = \deg_{\mathbb{Q}^{ab}}(\eta) \geq 1$.

Before embarking on the actual proof of Proposition 1, we first outline our general strategy. We first show that it is enough to prove that for any positive integer m , modulo roots of unity, there are only finitely many m -Weil numbers in the ring

$O_{\mathbb{Q}^{ab}}[\eta]$. Then we employ a variation of Kedlaya's method (which successfully bounds q in the case q is a prime), to provide in our case of a general q a uniform upper bound for the size of each prime factor dividing q . This part of the proof also makes use of some ideas from our proof of Lemma 13. After completing this first step, we proceed with the second stage of the proof. This consists in providing, for each fixed prime factor p of q/q_0 , an upper bound for the exponent of p in q/q_0 . Intuitively, this step is a type of descent, via a tower of subfields of $L_q(\eta)$, where the key tool is provided by the quantitative p -adic Lemma 15. With the completion of this step, which entirely bounds q , we will be in a position where we can view β inside a large, but fixed, extension of L_{q_0} . This will then immediately conclude the proof of Proposition 1, since on the one hand by Lemma 14 we will have a uniform upper bound for the length of all m -Weil numbers β , and on the other hand by Lemma 12 there are only finitely many such β 's in the above fixed field.

Indeed, let $\alpha \in K$ be an m -Weil number. Write $\alpha = u_0 + u_1\eta + \dots + u_{d-1}\eta^{d-1}$, with $u_i \in \mathbb{Q}^{ab}$, for any $0 \leq i \leq d-1$. Let $\{w_0, w_1, \dots, w_{d-1}\}$ be the dual basis of the basis $\{1, \eta, \eta^2, \dots, \eta^{d-1}\}$ of K over $\mathbb{Q}^{ab}$. Then $u_i = \text{Tr}_{K/\mathbb{Q}^{ab}}(\alpha w_i)$, $\forall 0 \leq i \leq d-1$. Choose $m_1 \geq 1$ such that $m_1 w_i \in \overline{\mathbb{Z}}$, $\forall i$. Then $m_1 u_i \in \overline{\mathbb{Z}}$, for any i , and hence $m_1 \alpha \in O_{\mathbb{Q}^{ab}}[\eta]$. Since α is an m -Weil number, $m_1 \alpha$ is an $(m_1 m)$ -Weil number, and $m_1 \alpha$ (modulo multiplication by roots of unity) belongs to a finite set. Hence (again modulo multiplication by roots of unity) α would belong to a finite set.

Let m be a positive integer. Next, we will prove that modulo roots of unity, there are only finitely many m -Weil numbers in $O_{\mathbb{Q}^{ab}}[\eta]$.

Using the definitions we introduced in Section 3, if we put $S = \{1, \eta, \eta^2, \dots, \eta^{d-1}\}$, Lemma 14 shows that there exists a positive number $M = M(m, \eta)$ such that any m -Weil number α in $A(S) = O_{\mathbb{Q}^{ab}}[\eta]$ has length $l(\alpha) < M$.

For a positive integer n , we denote by $L_n = \mathbb{Q}(\zeta_n)$ the cyclotomic extension of $\mathbb{Q}$ generated by a primitive n^{th} root of unity. Write the complex conjugate of η in the basis $1, \eta, \eta^2, \dots, \eta^{d-1}$ (recall that we assumed that complex conjugation maps K to itself) with coefficients $c_1, c_2, \dots, c_d \in \mathbb{Q}^{ab}$. Fix a finite cyclotomic extension $F = L_{q_0}$ of $\mathbb{Q}$ that contains all the coefficients $c_1, c_2, \dots, c_d$, (large enough) such that $\deg_{\mathbb{Q}^{ab}}(\eta) = \deg_F(\eta)$, and such that $4n_0|q_0$, where n_0 is the product of all primes less than M .

Then using Lemma 2 we obtain that $[K : \mathbb{Q}^{ab}] = [F(\eta) : F] = [L(\eta) : L]$, and $[L : F] = [L(\eta) : F(\eta)]$ for any finite extension L of F contained in $\mathbb{Q}^{ab}$. As a consequence, any basis of L/F is a basis for $L(\eta)/F(\eta)$.

Let $\alpha \in A(S) = O_{\mathbb{Q}^{ab}}[\eta]$ be an m -Weil number, and let

$$q = \min\{n > 1 : \exists \zeta \in \mu_\infty \text{ such that } \alpha\zeta \in L_n(\eta) \text{ and } q_0|n\}.$$

Let ζ be a root of unity such that $\beta := \alpha\zeta \in L_q(\eta)$. Note that β is also an m -Weil number.

From the proof of Lemma 14 we know that there exists a positive number $M = M(m, \eta)$ such that any m -Weil number in $O_{\mathbb{Q}^{ab}}[\eta]$, in particular β , can be written as

$$(7) \quad \beta = (\zeta_{1,1} + \dots + \zeta_{1,m_1}) + (\zeta_{2,1} + \dots + \zeta_{2,m_2})\eta + (\zeta_{3,1} + \dots + \zeta_{3,m_3})\eta^2 + \dots,$$

with $m_1 + m_2 + m_3 + \dots < M$, where $\zeta_{i,j}$ are roots of unity in L_q .

Claim 1. Next, we will show that for any prime divisor p of $\frac{q}{q_0}$, there exists a basis of $L_q/L_{q/p}$ in which β can be written as a sum of less than M (nonzero) terms.

Proof of Claim 1. Let p be a prime with $p|\frac{q}{q_0}$. We distinguish two cases:

Case 1. $p||q$. In this case $B_j := \{1, \zeta_p, \dots, \hat{\zeta}_p^j, \dots, \zeta_p^{p-1}\}$ is a basis in $L_q/L_{q/p}$, for any $0 \leq j \leq p-1$ (the $\hat{}$ means that the corresponding term is omitted). Since $q = \text{lcm}(p, \frac{q}{p})$, we can write $\zeta_q = \zeta_p^a \zeta_{\frac{q}{p}}^b$, with a, b integers and $0 \leq a \leq p-1$.

Hence each term $\zeta_{i,j}$ in the sum (7) can be written in the form $\zeta_{i,j} = \zeta_p^{a_{i,j}} \zeta_{\frac{q}{p}}^{b_{i,j}}$, with $a_{i,j}, b_{i,j} \in \mathbb{Z}$, and $0 \leq a_{i,j} \leq p-1$. From the definition of q_0 , and the fact that $p|\frac{q}{q_0}$, and $p||q$, we deduce that $p > M$. Thus there exists $j_0 \in \{0, 1, \dots, p-1\}$ such that $j_0 \neq a_{i,j}$, for any i, j . Denote the elements of the basis B_{j_0} by $u_1, u_2, \dots, u_{p-1}$. Note that $\zeta_{\frac{q}{p}}^{b_{i,j}} \in L_{q/p}$, so we can write all elements $\zeta_{i,j}$ in the basis B_{j_0} , with only one nonzero term. As we noted above, B_{j_0} is also a basis for $L_q(\eta)/L_{q/p}(\eta)$ and we write $\beta \in L_q(\eta)$ in this basis as $\beta = b_1 u_1 + \dots + b_k u_k$, where $b_1, \dots, b_k$ are nonzero elements of $L_{q/p}(\eta)$, and $u_1, \dots, u_k$ are some of the basis elements (we retain only the nonzero terms in the representation of β in this basis).

We now write each term $\zeta_{i,j} \eta^{i-1}$ in the basis $\{u_1, u_2, \dots, u_{p-1}\}$ of $L_q(\eta)/L_{q/p}(\eta)$. Multiplying by η^{i-1} (which is in $L_{q/p}(\eta)$), we obtain that $\zeta_{i,j} \eta^{i-1}$ is of the form $b u_l$, with $b \in L_{q/p}(\eta)$ and u_l is one of the elements of the basis $u_1, u_2, \dots, u_{p-1}$ of $L_q(\eta)/L_{q/p}(\eta)$.

Adding up all the terms $\zeta_{i,j} \eta^{i-1}$ written in the above form, we conclude that β can be written in the basis $u_1, u_2, \dots, u_{p-1}$ using at most $m_1 + m_2 + m_3 + \dots < M$ nonzero terms. From the uniqueness of writing a vector in a basis, we infer that it will coincide with the one above, $\beta = b_1 u_1 + \dots + b_k u_k$. Hence $k < M$.

Case 2. $p^2|q$. Let $r \geq 2$ be such that $p^r||q$. In this case $C := \{1, \zeta_{p^r}, \dots, \zeta_{p^r}^{p^r-1}\}$ is a basis in $L_q/L_{q/p}$. Denote, for simplicity, the elements of the basis C by $v_1, v_2, \dots, v_p$. Then C is also a basis for $L_q(\eta)/L_{q/p}(\eta)$ and we write $\beta \in L_q(\eta)$ in this basis as $\beta = b_1 v_1 + \dots + b_k v_k$, where $b_1, \dots, b_k$ are nonzero elements of $L_{q/p}(\eta)$, and $v_1, \dots, v_k$ are some of the basis elements (we retain only the nonzero terms in the representation of β in this basis).

Since $q = \text{lcm}(p^r, \frac{q}{p})$, we can write $\zeta_q = \zeta_{p^r}^a \zeta_{\frac{q}{p}}^b$, with a, b integers and $0 \leq a \leq p^r - 1$. In fact, using Lemma 9, we can choose a in the set $\{0, 1, \dots, p-1\}$, and this shows, as in Case 1, that each term $\zeta_{i,j} \eta^{i-1}$ in relation (7) is of the form $b v_l$, with $b := \zeta_{\frac{q}{p}}^b \eta^{i-1} \in L_{q/p}(\eta)$ and $v_l := \zeta_{p^r}^a$ is one of the elements of the basis $1, \zeta_{p^r}, \dots, \zeta_{p^r}^{p^r-1}$ of $L(\eta)/L_{q/p}(\eta)$.

We now add up all the terms $\zeta_{i,j} \eta^{i-1}$, written in the above form. We conclude, just as in Case 1 above, that β can be written in the basis $v_1, v_2, \dots, v_p$ using at most $m_1 + m_2 + m_3 + \dots < M$ nonzero terms. From the uniqueness of writing a vector in a basis, we infer that it will coincide with the one above, $\beta = b_1 u_1 + \dots + b_k u_k$. Hence $k < M$.

Claim 2. Next, we show that any prime divisor p of $\frac{q}{q_0}$ is bounded (in terms of m and η).

Proof of Claim 2. Let p be a prime, with $p|\frac{q}{q_0}$. As above, we distinguish two cases:

Case 1. $p||q$. Write β in the basis B_{j_0} constructed above as $\beta = \alpha_1 \zeta^{j_1} + \alpha_2 \zeta^{j_2} + \dots + \alpha_k \zeta^{j_k}$, with $k < M$, $\zeta = \zeta_p$, $0 \leq j_1 < j_2 < \dots < j_k \leq p-1$ and all the coefficients $\alpha_1, \alpha_2, \dots, \alpha_k$ are nonzero elements of $L_{\frac{q}{p}}(\eta)$.

Here $k \geq 1$ since β is nonzero. Moreover, we have that $k \geq 2$. Indeed, if $k = 1$, say $\alpha_1 \neq 0$, then $\beta = \alpha_1 \zeta^{j_1}$, hence $\beta \zeta^{-j_1} = \alpha_1 \in L_{\frac{q}{p}}(\eta)$, which contradicts the minimality of q .

Assume now that $p > 6^{\frac{M}{2}}$. Then $p > 6^{\frac{k}{2}}$, and we may apply Lemma 16 from Appendix A to $j_1, j_2, \dots, j_k$. It follows that there exists a pair, say (j_1, j_2) such that $j_2 - j_1 \not\equiv j_l - j_s \pmod{p}$, for any $(l, s) \neq (2, 1)$.

Let $i_0 \in \{0, 1, \dots, p-1\}$ such that $i_0 \not\equiv j_m - j_n \pmod{p}$, for any $1 \leq m, n \leq k$. Such an i_0 exists as $k^2 < p$. Then, $B_{i_0} = \{1, \zeta, \dots, \zeta^{i_0-1}, \zeta^{i_0+1}, \dots, \zeta^{p-1}\}$ is a basis of $L_q(\eta)$ over $L_{\frac{q}{p}}(\eta)$.

Note that for $0 \leq i < j \leq p-1$ we have $1 \leq p - (j - i) \leq p-1$ and

$$\zeta^{i-j} = \zeta^{-(j-i)} = \zeta^{p-(j-i)}.$$

One has

$$\begin{aligned} m &= \beta \bar{\beta} = (\alpha_1 \zeta^{j_1} + \alpha_2 \zeta^{j_2} + \dots + \alpha_k \zeta^{j_k})(\bar{\alpha}_1 \zeta^{-j_1} + \bar{\alpha}_2 \zeta^{-j_2} + \dots + \bar{\alpha}_k \zeta^{-j_k}) \\ &= \sum_{1 \leq j \leq k} |\alpha_j|^2 + \sum_{1 \leq l < s \leq k} \alpha_s \bar{\alpha}_l \zeta^{j_s - j_l} + \sum_{1 \leq u < v \leq k} \alpha_u \bar{\alpha}_v \zeta^{j_u - j_v} \\ &= \sum_{1 \leq j \leq k} |\alpha_j|^2 + \sum_{1 \leq l < s \leq k} \alpha_s \bar{\alpha}_l \zeta^{j_s - j_l} + \sum_{1 \leq u < v \leq k} \alpha_u \bar{\alpha}_v \zeta^{p-(j_v - j_u)}. \end{aligned}$$

Note that $\alpha_j \in L_{\frac{q}{p}}(\eta)$ implies $\bar{\alpha}_j \in L_{\frac{q}{p}}(\bar{\eta})$, and since $\bar{\eta} \in L_{q_0}(\eta) \subset L_{\frac{q}{p}}(\eta)$, we deduce that $\bar{\alpha}_j \in L_{\frac{q}{p}}(\eta)$.

Since $j_2 - j_1 \not\equiv j_l - j_s \pmod{p}$, for any $(l, s) \neq (2, 1)$, and because there is no ζ^{i_0} term in the above equation, the term $\alpha_2 \bar{\alpha}_1 \zeta^{j_2 - j_1}$ on the right side of the above equality cannot be canceled by any other terms. It follows that $\alpha_2 = 0$ or $\alpha_1 = 0$, a contradiction.

Hence for any prime p such that $p \nmid q$ one has $p < 6^{\frac{M}{2}}$.

Case 2. $p^2 \mid q$. Let ζ be a primitive root of unity of order p^r , where $p^r \nmid q$. Then $\gamma := \zeta^p \in L_{\frac{q}{p}}$ is a primitive root of unity of order p^{r-1} .

Write β in the basis C defined above as $\beta = \alpha_1 \zeta^{i_1} + \alpha_2 \zeta^{i_2} + \dots + \alpha_k \zeta^{i_k}$, with nonzero coefficients $\alpha_j \in L_{\frac{q}{p}}(\eta)$, for any $1 \leq j \leq k$, with $0 \leq i_1 < i_2 < \dots < i_k \leq p-1$, and $k < M$.

Note that by the same argument as in Case 1, $k \geq 2$.

If $p > 6^{\frac{M}{2}}$, then $p > 6^{\frac{k}{2}}$, and applying Lemma 16 to $i_1, i_2, \dots, i_k$, there exists a pair, say (i_1, i_2) such that $i_2 - i_1 \not\equiv i_l - i_s \pmod{p}$, for any $(l, s) \neq (2, 1)$.

Note that for $0 \leq i < j \leq p-1$ we have $1 \leq p - (j - i) \leq p-1$ and

$$\zeta^{i-j} = \zeta^{i-j+p^r} = \zeta^{p-(j-i)+p(p^{r-1}-1)} = \zeta^{p-(j-i)} \cdot \zeta^{p(p^{r-1}-1)} = \gamma^{p^{r-1}-1} \cdot \zeta^{p-(j-i)},$$

where $\gamma = \zeta^p \in L_{\frac{q}{p}}$.

We have

$$\begin{aligned} m &= \beta \bar{\beta} = (\alpha_1 \zeta^{i_1} + \alpha_2 \zeta^{i_2} + \dots + \alpha_k \zeta^{i_k})(\bar{\alpha}_1 \zeta^{-i_1} + \bar{\alpha}_2 \zeta^{-i_2} + \dots + \bar{\alpha}_k \zeta^{-i_k}) \\ &= \sum_{1 \leq j \leq k} |\alpha_j|^2 + \sum_{1 \leq l < s \leq k} \alpha_s \bar{\alpha}_l \zeta^{i_s - i_l} + \sum_{1 \leq u < v \leq k} \alpha_u \bar{\alpha}_v \zeta^{i_u - i_v} \\ &= \sum_{1 \leq j \leq k} |\alpha_j|^2 + \sum_{1 \leq l < s \leq k} \alpha_s \bar{\alpha}_l \zeta^{i_s - i_l} + \sum_{1 \leq u < v \leq k} \alpha_u \bar{\alpha}_v \gamma^{p^{r-1}-1} \zeta^{p-(i_v - i_u)}. \end{aligned}$$

Here $1, \zeta, \zeta^2, \dots, \zeta^{p-1}$ is a basis of L_q over $L_{\frac{q}{p}}$. Reasoning as above, we find that $\alpha_2 \bar{\alpha}_1 = 0$, which is a contradiction.

Hence for any prime p such that $p^2 | q$ one has $p < 6^{\frac{M}{2}}$.

Now that we have a uniform upper bound for the size of all prime factors of q , we proceed with the second stage of the proof of Proposition 1.

Claim 3. We now fix a prime divisor p of q/q_0 , and bound the exponent, call it r , of p in q/q_0 .

Proof of Claim 3. Let ζ be a primitive root of unity of order p^r , where $p^r \parallel q$. Consider the following tower of $r-1$ extensions, each of degree p :

$$L_{\frac{q}{p^{r-1}}}(\eta) \subset L_{\frac{q}{p^{r-2}}}(\eta) \subset \dots \subset L_{\frac{q}{p}}(\eta) \subset L_q(\eta).$$

We write $\beta \in L_q(\eta)$ as

$$(8) \quad \beta = \alpha_1 \zeta^{i_1} + \alpha_2 \zeta^{i_2} + \dots + \alpha_k \zeta^{i_k},$$

with $k < M$, $0 \leq i_1 < i_2 < \dots < i_k < p^{r-1}$, and with nonzero coefficients $\alpha_j \in L_{\frac{q}{p^{r-1}}}(\eta)$, for any $1 \leq j \leq k$.

Note that for $0 \leq i < j \leq p^{r-1} - 1$ we have $1 \leq p^{r-1} - (j - i) \leq p^{r-1} - 1$ and $\zeta^{i-j} = \zeta^{i-j+p^r} = \zeta^{p^{r-1}-(j-i)+p^{r-1}(p-1)} = \zeta^{p^{r-1}-(j-i)} \cdot \zeta^{p^{r-1}(p-1)} = \delta^{p-1} \cdot \zeta^{p^{r-1}-(j-i)}$, where $\delta := \zeta^{p^{r-1}} \in L_{\frac{q}{p^{r-1}}}$.

One has

$$\begin{aligned} m &= \beta \bar{\beta} = (\alpha_1 \zeta^{i_1} + \alpha_2 \zeta^{i_2} + \dots + \alpha_k \zeta^{i_k})(\bar{\alpha}_1 \zeta^{-i_1} + \bar{\alpha}_2 \zeta^{-i_2} + \dots + \bar{\alpha}_k \zeta^{-i_k}) \\ &= \sum_{1 \leq j \leq k} |\alpha_j|^2 + \sum_{1 \leq l < s \leq k} \alpha_s \bar{\alpha}_l \zeta^{i_s - i_l} + \sum_{1 \leq u < v \leq k} \alpha_u \bar{\alpha}_v \zeta^{i_u - i_v} \\ &= \sum_{1 \leq j \leq k} |\alpha_j|^2 + \sum_{1 \leq l < s \leq k} \alpha_s \bar{\alpha}_l \zeta^{i_s - i_l} + \sum_{1 \leq u < v \leq k} \alpha_u \bar{\alpha}_v \delta^{p-1} \zeta^{p^{r-1} - (i_v - i_u)}. \end{aligned}$$

Note that $1, \zeta, \dots, \zeta^{p^{r-1}-1}$ is a basis of $L_q(\eta)$ over $L_{\frac{q}{p^{r-1}}}(\eta)$.

If there exists a pair (i_a, i_b) such that $i_a - i_b \not\equiv i_l - i_s \pmod{p^r}$, for all $(l, s) \neq (a, b)$, then $\alpha_a \bar{\alpha}_b = 0$, so $\alpha_a = 0$ or $\alpha_b = 0$, a contradiction.

Hence for any $a, b \in \{1, 2, \dots, k\}$ there exist $l, s \in \{1, 2, \dots, k\}$ such that $i_a - i_b \equiv i_l - i_s \pmod{p^r}$. This means $|(i_a - i_b) - (i_l - i_s)|_p \leq \frac{1}{p^r}$. It follows that

$$\frac{1}{p^r} \geq \max_{a,b} \min_{l,s} |(i_a - i_b) - (i_l - i_s)|_p.$$

Lemma 15 implies that $\frac{1}{p^r} \geq \rho_{k,p} \min_{a \neq b} |i_a - i_b|_p$. Then there exist $a_0, b_0 \in \{1, 2, \dots, k\}$ such that $|i_{a_0} - i_{b_0}|_p \leq \frac{1}{\rho_{k,p}} \cdot \frac{1}{p^r}$.

Fix a positive integer $c_{k,p}$ such that $\frac{1}{\rho_{k,p}} < p^{c_{k,p}}$. Then

$$(9) \quad |i_{a_0} - i_{b_0}|_p < \frac{1}{p^{r-c_{k,p}}}.$$

If $r \leq c_{k,p} + 1$, we are done.

If $r > c_{k,p} + 1$, then relation (9) is equivalent to $i_{a_0} \equiv i_{b_0} \pmod{p^{r-c_{k,p}}}$. Let t be an integer such that $i_{a_0} = i_{b_0} + tp^{r-c_{k,p}}$. We may assume, without loss of generality, $a_0 = 1$, $b_0 = 2$, and thus we obtain $i_1 = i_2 + tp^{r-c_{k,p}}$. We deduce

$$\alpha_1 \zeta^{i_1} + \alpha_2 \zeta^{i_2} = \zeta^{i_2} (\alpha_2 + \alpha_1 \zeta^{i_1 - i_2}) = \zeta^{i_2} (\alpha_2 + \alpha_1 \zeta^{tp^{r-c_{k,p}}}).$$

Note that

$$\zeta^{p^{r-c_k,p}} \in L_{\frac{q}{p^{r-1}}}(\zeta^{c_k,p})(\eta) \subseteq L_{\frac{q}{p^{r-1-c_k,p}}}(\eta),$$

so

$$\gamma_2 := \alpha_2 + \alpha_1 \zeta^{tp^{r-c_k,p}} \in L_{\frac{q}{p^{r-1-c_k,p}}}(\eta).$$

Hence $\beta = \gamma_2 \zeta^{i_2} + \gamma_3 \zeta^{i_3} + \dots + \gamma_k \zeta^{i_k}$, where $\gamma_j := \alpha_j$, for any $3 \leq j \leq k$.

For each l , $2 \leq l \leq k$, we use the division algorithm to write $i_l = a_l p^{r-1-c_k,p} + b_l$ for some positive integers a_l, b_l with $0 \leq b_l < p^{r-1-c_k,p}$. It follows that

$$\gamma_l \zeta^{i_l} = \gamma_l \zeta^{a_l p^{r-1-c_k,p}} \zeta^{b_l} = \delta_l \zeta^{b_l}, \text{ where } \delta_l := \gamma_l \zeta^{a_l p^{r-1-c_k,p}} \in L_{\frac{q}{p^{r-1-c_k,p}}}(\eta).$$

Hence

$$(10) \quad \beta = \delta_2 \zeta^{b_2} + \delta_3 \zeta^{b_3} + \dots + \delta_k \zeta^{b_k}.$$

Note that (10) is the representation of β in the basis $1, \zeta, \zeta^2, \dots, \zeta^{p^{r-1-c_k,p}-1}$. In conclusion, β can be uniquely written as

$$\beta = \eta_1 \zeta^{j_1} + \eta_2 \zeta^{j_2} + \dots + \eta_s \zeta^{j_s},$$

with $0 \leq j_1 < j_2 < \dots < j_s < p^{r-1-c_k,p}$, $s < k$ and $\eta_i \in L_{\frac{q}{p^{r-1-c_k,p}}}(\eta)$, for any $1 \leq i \leq s$.

This shows that the representation of β in the basis corresponding to $L_{\frac{q}{p^{r-1-c_k,p}}}(\eta)$ is strictly shorter than the representation corresponding to $L_{\frac{q}{p^{r-1}}}(\eta)$.

Let $H_\beta(j)$ be the length of the representation of β in the basis $1, \zeta, \dots, \zeta^{p^j-1}$ of $L_q(\eta)$ over $L_{\frac{q}{p^j}}(\eta)$. We proved that $k_2 := H_\beta(r-1-c_{k_1,p}) < H_\beta(r-1) = k =: k_1$.

Repeating this argument, we obtain

$$k_3 := H_\beta(r-1-c_{k_1,p}-c_{k_2,p}) < H_\beta(r-1-c_{k_1,p}) = k_2,$$

for a certain positive integer $c_{k_2,p}$.

Continuing in this way, there are two possibilities:

Either 1. there exists a $d \geq 1$ such that $H_\beta(r-1-c_{k_1,p}-c_{k_2,p}-\dots-c_{k_d,p}) = 1$. This contradicts the minimality of q .

Or 2. there is an $e \geq 1$ such that $r-1-c_{k_1,p}-c_{k_2,p}-\dots-c_{k_e,p} < c_{k_{e+1},p}$. This implies $r_p := r \leq 1 + \sum_{i=2}^m c_{i,p}$ (where $c_{i,p} = 0$, if $i \notin \{k_1, k_2, \dots, k_e\}$).

Let $P_0(m, \eta) = \{p \text{ prime} : p|q\}$. We proved that the set $P_0(m, \eta)$ is finite.

We have $\frac{q}{q_0} = \prod_{p|\frac{q}{q_0}} p^{r_p}$, hence

$$\log \frac{q}{q_0} = \sum_{p|\frac{q}{q_0}} r_p \log p \leq \sum_{p \in P_0(m, \eta)} (1 + \sum_{i=2}^m c_{i,p}) \log p,$$

which shows that q is bounded in terms of m and η .

Applying Lemma 12 and Lemma 14 we obtain that there exist only a finite number of such β , which completes the proof of Proposition 1. $\square$

We now prove Theorem 1. Let $m \geq 1$, let K be a finite extension of $\mathbb{Q}^{ab}$, let $S_{m,K}$ denote the set of m -Weil numbers in K , and let $H_{m,K} = \{x_1^{e_1} x_2^{e_2} \dots x_n^{e_n} : n \geq 1, x_i \in S_{m,K}, e_i \in \mathbb{Z}, \forall 1 \leq i \leq n \text{ and } e_1 + e_2 + \dots + e_n = 0\}$.

Fix $\eta \in S_{m,K}$. Then $\eta\rho \in S_{m,K}$, for all $\rho \in \mu_\infty$.

Put $x_1 = \eta\rho$, $e_1 = 1$, $x_2 = \eta$, and $e_2 = -1$. This shows that $\rho = x_1^{e_1} x_2^{e_2} \in H_{m,K}$, so μ_∞ is a subgroup of $H_{m,K}$.

Now let $\alpha \in S_{m,K}$. Then Proposition 1 shows that there are only finitely many such α (modulo multiplication by roots of unity). Denote them by $u_1, \dots, u_L$. Then the set of ratios u_i/u_j is finite, and it provides a set of generators for the quotient group $H_{m,K}/\mu_\infty$.

Lastly, $H_{m,K}/\mu_\infty$ is free (if not, there would be an element $y \in H_{m,K}/\mu_\infty$ with $y^k = 1$ for some integer $k > 1$. But then, taking a representative $x \in H_{m,K}$ of y , we would have $x^k \in \mu_\infty$, so x itself would be a root of unity). Hence $H_{m,K}/\mu_\infty$ is a finitely generated abelian group, without torsion, so it is isomorphic to $\mathbb{Z}^r$, for some nonnegative integer r .

APPENDIX A. A COMBINATORIAL LEMMA (BY KIRAN S. KEDLAYA)

In this appendix, we reproduce a combinatorial lemma from our unpublished 2001 manuscript “Weil numbers in prime cyclotomic fields” which is used in the present paper.

Lemma 16. *Let $k \geq 4$ be a positive integer, p a prime greater than $6^{k/2}$, and $a_1, \dots, a_k$ distinct elements of $\mathbb{Z}/p\mathbb{Z}$. Then at least one of the differences $a_i - a_j$ ($1 \leq i < j \leq k$) occurs only once.*

Proof. Suppose on the contrary that each difference occurs at least twice. Then for each pair i, j with $1 \leq i < j \leq k$, we have one or more linear relations of the form $a_i - a_j - a_{i'} + a_{j'} = 0$. These relations can be viewed as elements either of $(\mathbb{Q}^k)^*$ or of $(\mathbb{F}_p^k)^*$. Over $\mathbb{Q}$, any vector satisfying all of these relations must have two coordinates equal, otherwise the difference between the maximum and minimum coordinates could not equal some other difference. Thus the span of the relations lies in some hyperplane of the form $a_i - a_j$.

On the other hand, over $\mathbb{F}_p$, we are assuming there exists a vector satisfying the relations with all coordinates distinct. Thus the span of the relations has strictly smaller dimension over $\mathbb{F}_p$ than over $\mathbb{Q}$. In particular, for some $\ell \leq k$, there exists a set of ℓ relations which span an ℓ -dimensional space over $\mathbb{Q}$ but do not over $\mathbb{F}_p$. Form the matrix whose rows are these relations; the determinants of all of its $\ell \times \ell$ submatrices are divisible by p , whereas at least one of these determinants is nonzero.

Each relation, considered as a vector in $\mathbb{R}^n$, has Euclidean norm at most $\sqrt{6}$, since up to sign, its nonzero coordinates are $1, 1, -1, -1$ or $1, -2, 1$. By Hadamard’s inequality, the determinant of the chosen submatrix is at most $6^{\ell/2} \leq 6^{k/2}$, but it has a prime divisor $p > 6^{k/2}$. Contradiction. $\square$

The following example, suggested by Ernie Croot, shows that the optimal lower bound in the previous lemma is probably exponential. If p is a prime such that $2^\ell \equiv -1 \pmod{p}$, then the set $0, 1, 2, 2^2, \dots, 2^{2^\ell-1}$ has no unique differences, by virtue of the equalities

$$0 - 2^i = 2^{\ell+i} - 0, \quad 2^i - 2^j = 2^{\ell+j} - 2^{\ell-i}, \quad 2^i - 2^{\ell+i} = 2^{i+1} - 0.$$

In particular, if there are infinitely many primes of the form $(2^\ell + 1)/3$ (sometimes called *Wagstaff primes*), then there exist infinitely many k for which we can find a counterexample to the lemma for $p > c^{2^{k/2}}$. According to the Prime Pages web site (<http://primes.utm.edu>), as of the end of 2010, the largest proven prime of this form is for $\ell = 42737$, due to Morain in 2007.

ACKNOWLEDGEMENT

The authors are grateful to Kiran S. Kedlaya for Appendix A.

REFERENCES

- [1] Julián Aguirre and Juan Carlos Peral, *The trace problem for totally positive algebraic integers*, Number theory and polynomials, London Math. Soc. Lecture Note Ser., vol. 352, Cambridge Univ. Press, Cambridge, 2008, pp. 1–19, DOI 10.1017/CBO9780511721274.003. With an appendix by Jean-Pierre Serre. MR2428512 (2009k:11172)
- [2] Bruno Anglès and Tatiana Beliaeva, *On Weil numbers in cyclotomic fields*, Int. J. Number Theory **5** (2009), no. 5, 871–884, DOI 10.1142/S1793042109002432. MR2553513 (2010j:11154)
- [3] J. W. S. Cassels, *On a conjecture of R. M. Robinson about sums of roots of unity*, J. Reine Angew. Math. **238** (1969), 112–131. MR0246852 (40 #121)
- [4] A. J. de Jong, *Smoothness, semi-stability and alterations*, Inst. Hautes Études Sci. Publ. Math. **83** (1996), 51–93. MR1423020 (98e:14011)
- [5] Pierre Deligne, *La conjecture de Weil. II* (French), Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252. MR601520 (83c:14017)
- [6] Christopher Deninger, *Exchanging the places p and ∞ in the Leopoldt conjecture*, J. Number Theory **114** (2005), no. 1, 1–17, DOI 10.1016/j.jnt.2005.03.006. MR2163903 (2006f:11136)
- [7] Taira Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95. MR0229642 (37 #5216)
- [8] Jean-François Jaulent, *Plongements l -adiques et l -nombres de Weil* (French, with English and French summaries), J. Théor. Nombres Bordeaux **20** (2008), no. 2, 335–351. MR2477507 (2010c:11140)
- [9] E. Kowalski, *Weil numbers generated by other Weil numbers and torsion fields of abelian varieties*, J. London Math. Soc. (2) **74** (2006), no. 2, 273–288, DOI 10.1112/S0024610706023040. MR2269629 (2008e:11075)
- [10] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. **53** (1857), 173–175.
- [11] Yanhua Liang and Qiang Wu, *The trace problem for totally positive algebraic integers*, J. Aust. Math. Soc. **90** (2011), no. 3, 341–354, DOI 10.1017/S1446788711001030. MR2833305 (2012h:11149)
- [12] J. H. Loxton, *On the maximum modulus of cyclotomic integers*, Acta Arith. **22** (1972), 69–85. MR0309896 (46 #9000)
- [13] J. H. Loxton, *On two problems of R. W. Robinson about sums of roots of unity*, Acta Arith. **26** (1974/75), 159–174. MR0371852 (51 #8069)
- [14] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970. MR0282985 (44 #219)
- [15] A. Greaves and R. W. K. Odoni, *Weil-numbers and CM-fields. I*, J. Reine Angew. Math. **391** (1988), 198–212. MR961169 (90a:11115)
- [16] James McKee and Chris Smyth, *Salem numbers of trace -2 and traces of totally positive algebraic integers*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 327–337, DOI 10.1007/978-3-540-24847-7_25. MR2137365 (2006a:11134)
- [17] R. W. K. Odoni, *Weil numbers and CM fields. II*, J. Number Theory **38** (1991), no. 3, 366–377, DOI 10.1016/0022-314X(91)90025-7. MR1114485 (92h:11086)
- [18] Raphael M. Robinson, *Conjugate algebraic integers on a circle*, Math. Z. **110** (1969), 41–51. MR0246826 (40 #95)
- [19] I. Schur, *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten* (German), Math. Z. **1** (1918), no. 4, 377–402, DOI 10.1007/BF01465096. MR1544303
- [20] Carl Ludwig Siegel, *The trace of totally positive and real algebraic integers*, Ann. of Math. (2) **46** (1945), 302–312. MR0012092 (6,257a)
- [21] C. J. Smyth, *The mean values of totally real algebraic integers*, Math. Comp. **42** (1984), no. 166, 663–681, DOI 10.2307/2007609. MR736460 (86e:11115)

- [22] Christopher Smyth, *Totally positive algebraic integers of small trace* (English, with French summary), Ann. Inst. Fourier (Grenoble) **34** (1984), no. 3, 1–28. MR762691 (86f:11091)
- [23] Florin Stan and Alexandru Zaharescu, *Siegel's trace problem and character values of finite groups*, J. Reine Angew. Math. **637** (2009), 217–234, DOI 10.1515/CRELLE.2009.097. MR2599088 (2011d:11252)
- [24] Florin Stan and Alexandru Zaharescu, *The Siegel norm of algebraic numbers*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **55(103)** (2012), no. 1, 69–77. MR2951973
- [25] J. Tate, *Classes d'isogénie de variétés abéliennes sur un corps fini (d'après T. Honda)*, Sémin. Bourbaki, **21**, 1968/69, Exp. 352.

SIMION STOILOW INSTITUTE OF MATHEMATICS OF THE ROMANIAN ACADEMY, RESEARCH UNIT 5, PO Box 1-764, RO-014700 BUCHAREST, ROMANIA

E-mail address: `sfloringabriel@yahoo.com`

SIMION STOILOW INSTITUTE OF MATHEMATICS OF THE ROMANIAN ACADEMY, RESEARCH UNIT 5, PO Box 1-764, RO-014700 BUCHAREST, ROMANIA — AND — DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, ALTGELD HALL, 1409 W. GREEN STREET, URBANA, ILLINOIS 61801

E-mail address: `zaharesc@illinois.edu`