SUFFICIENT CONDITIONS FOR CLASSIFYING ALGEBRAIC INTEGERS

ABHISHEK BHARADWAJ, VEEKESH KUMAR, APRAMEYO PAL, AND R. THANGADURAI

ABSTRACT. Let $\lambda_1,\dots,\lambda_k$ and $\alpha_1,\dots,\alpha_k$ be nonzero algebraic numbers for some integer $k\geq 1$ and let $L=\mathbb{Q}(\lambda_1,\dots,\lambda_k,\alpha_1,\dots,\alpha_k)$ be the number field. In this article, we classify the tuples $(\alpha_1,\dots,\alpha_k)$ such that the sum $\lambda_1\alpha_1^n+\cdots+\lambda_k\alpha_k^n$ takes values inside $\mathcal{O}_L$ for n in a finite set or an infinite set. In another interesting result, we prove that for rational functions f_i with algebraic coefficients, if the sum $\sum_{i=1}^{k}\lambda_i(f_i(x))^n\in\overline{\mathbb{Z}}[x]$ for infinitely many values of $n\in\mathbb{N}$, then via the subspace theorem, we prove that $f_i(x)\in\overline{\mathbb{Z}}[x]$. Our approach generalizes the classical question of sufficient conditions for algebraic integers using trace operators. We also give a different proof of Fatou's Lemma over number fields.

1. Introduction

It is a well-known fact [6, Pg 23-24] in invariant theory that the power sums $m_j=\sum_{i=1}^{k}X_i^j, j\geq 0$ generate the space of symmetric functions over the rational numbers. Perhaps motivated by this, Polya had proved if $\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^n)$ are integers for all natural numbers n, then α is an algebraic integer. The connection of the trace operator with power sum/symmetric functions can be seen as follows:

To determine if α is an algebraic integer, it suffices to show that the minimal polynomial of α over $\mathbb{Q}$ has integer values. However, the coefficients of the minimal polynomial are formed by elementary symmetric polynomials evaluated at the Galois conjugates of α and these values are generated by power sums. Therefore, Polya's observation can be thought of imposing a particular restriction on the power sums evaluated at a point to conclude that the same restriction holds for the elementary symmetric polynomials. One of the difficulties in showing that α is an algebraic integer by elementary manipulations is that the ring $\mathbb{Z}$ generated by power sums do not contain the elementary symmetric polynomials (but contains an integer multiple of the same. In fact, the relations between the elementary symmetric polynomials and power sums are given by Newton's identities). In the proof provided by Polya [9], he uses Fatou's lemma. Alternative proofs were given by H. Lenstra and P. Ponomarev [4] independently using complementary modules.

The result of Polya was refined further by Bart de Smit [4] who concluded that it is enough if we compute the trace of the power sums for finitely many values. This result depends on the degree of α. We expect this because we need to compute only finitely many elementary symmetric functions to determine if the given value is an algebraic integer.

In [2], P. Corvaja and U. Zannier, using the subspace theorem, proved the following. *Suppose α is an algebraic number and let E be an infinite subset of $\mathbb{N}$. For each $n\in E$, suppose there exists a positive integer q_n such that $\lim_{n\in E}(\log q_n)/n=0$ and $\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(q_n\alpha^n)\in\mathbb{Z}\backslash\{0\}$. Then α is either the h-th root of a rational number for some positive integer h or an algebraic integer.* By following

2010 *Mathematics Subject Classification.* Primary 11J87; Secondary 11S99 .
Key words and phrases. Trace, Schmidt Subspace Theorem, Skolem-Mahler-Lech Theorem.

the ideas in [2], P. Philippon and P. Rath [7] proved that *if α and λ are algebraic numbers such that $\mathrm{Tr}_{\mathbb{Q}(\alpha,\lambda)/\mathbb{Q}}(\lambda\alpha^n) \in \mathbb{Z}\backslash\{0\}$ for infinitely many natural numbers n, then α must be an algebraic integer.*

Here, we need to ensure that the trace doesn't vanish. The vanishing of the trace function can happen when the conjugates of α differ by a root of unity (*i.e.,* $\sigma(\alpha)/\alpha$ is a root of unity), thereby giving rise to vanishing sums of roots of unity. We can view $\mathrm{Tr}(\alpha^n)$ as a linear recurrence sequence, and if it vanishes for infinitely many n, then two elements in the recurrence relation differ by the root of unity by appealing to the Skolem-Mahler-Lech Theorem. This theme of vanishing of trace powers has been studied in detail in the paper [7].

In this paper, we study two problems, namely,

(1) Generalised power sums of the form
$$m_i := \sum_{j=1}^{k} \lambda_j \alpha_j^i,$$
and try to find conditions for which α_j is an algebraic integer, given that m_i is an algebraic integer for infinitely many i. As applications of this result (Theorem 2.1), we consider the analogues over polynomials, group rings, function fields and a linear combination of trace powers.

(2) Some special cases wherein, we can restrict i to a finite (effective) set for generalised power sums.

2. Our Results

Given a set of algebraic numbers $\alpha_1, \dots, \alpha_k$, we partition them into equivalence classes by the following relation :
$$\alpha_i \sim \alpha_j \text{ if and only if their ratio is a root of unity.} \tag{2.1}$$
The algebraic numbers $\alpha_1, \dots, \alpha_k$ are said to be *non-degenerate* if they have k-equivalence classes.

We denote the field of all algebraic numbers by $\overline{\mathbb{Q}}$ and the ring of all algebraic integers by $\overline{\mathbb{Z}}$. Now we state one of the main theorems as follows.

Theorem 2.1. *Let $\mathcal{L}(X_1, \dots, X_k) = \sum_{i=1}^{k} \lambda_i X_i$ be a linear form with coefficients λ_i in $\overline{\mathbb{Q}}^*$. Furthermore suppose that for $\overline{\alpha} = (\alpha_1, \dots, \alpha_k) \in \overline{\mathbb{Q}}^{*k}$, we have*
$$\mathcal{L}(\overline{\alpha^n}) \in \overline{\mathbb{Z}}\backslash\{0\},$$
for n in an infinite set $\mathfrak{S}$ where $\overline{\alpha^n} = (\alpha_1^n, \dots, \alpha_k^n)$ for any natural number n. Then corresponding to every equivalence class (defined by (2.1)), we have a partition I_j of $\{1, \dots, k\}$ such that one of the following holds true :

(1) *There exists a positive even integer h and integers ω_a for $a \in I_j$ satisfying the following:*
$$\sum_{a \in I_j} \lambda_a \zeta_h^{\omega_a n} = 0$$
for all but finitely many $n \in \mathfrak{S}$. Moreover for $a, b \in I_j$, the numbers α_a, α_b and the integers ω_a, ω_b satisfy the following relation:
$$\frac{\alpha_b}{\alpha_a} = \zeta_h^{\omega_b - \omega_a}.$$

Thus this condition is equivalent to saying that $\sum_{a \in I_j} \lambda_a \alpha_a^n = 0$ *for all but finitely many values of* n.

(2) *The numbers* α_i *are algebraic integers for all* $i \in I_j$.

Remark 2.1. In particular, Theorem 2.1 states that if $\alpha_1, \ldots, \alpha_k$ is a non-degenerate collection satisfying the above, then these are algebraic integers.

Now we proceed to provide some consequences of Theorem 2.1:

2.1. **Polynomial Values.** It is natural to ask the polynomial analogue of Theorem 2.1. We prove the following.

Theorem 2.2. *Let* $P(X_1, \ldots, X_k)$ *be a polynomial with algebraic coefficients and for some integer* m *with* $1 \leq m \leq k$, *assume that* $P(0, \ldots, 0, X_m, 0, \ldots 0)$ *is a non-constant polynomial. Let* $\alpha_1, \ldots, \alpha_k$ *be multiplicatively independent non-zero algebraic numbers such that* $P(\alpha_1^n, \ldots, \alpha_k^n) \in \overline{\mathbb{Z}} \backslash \{0\}$ *for infinitely many positive integers* n. *Then the number* α_m *is an algebraic integer.*

We have the following immediate corollary.

Corollary 2.1. *Let* $P(X_1, \ldots, X_k)$ *be a polynomial with algebraic coefficients and for each integer* m *with* $1 \leq m \leq k$, *assume that* $P(0, \ldots, 0, X_m, 0, \ldots 0)$ *is a non-constant polynomial. Let* $\alpha_1, \ldots, \alpha_k$ *be multiplicatively independent non-zero algebraic numbers such that* $P(\alpha_1^n, \ldots, \alpha_k^n) \in \overline{\mathbb{Z}} \backslash \{0\}$ *for infinitely many positive integers* n. *Then the number* α_m *is an algebraic integer for each integer* m.

Remark 2.2. This theorem is no longer true when we remove the condition on the polynomial P. For instance, we can consider $P(X, Y) = XY + 1$. Fix a prime p. We can choose $\alpha_1 = 1/p$ and $\alpha_2 = 2p$ and we note that $P(\alpha_1^n, \alpha_2^n) = 2^n + 1 \in \mathbb{Z} \backslash \{0\}$ for all natural numbers n. This gives a simple counterexample.

2.2. **Group Rings.** Let α be a non-zero algebraic number and let $G = \mathrm{Gal}(K/\mathbb{Q})$ where K is the Galois closure of $\mathbb{Q}(\alpha)$. We identify the index set I of Theorem 2.1 as the elements of G for convenience and consider the group ring $\bar{\mathbb{Q}}[G]$.

Theorem 2.3. *Let* $f \in \overline{\mathbb{Q}}[G]$ *be a non-zero element and suppose that* $f(\alpha^n) \in \overline{\mathbb{Z}} \backslash \{0\}$ *for* n *in an infinite subset* $\mathfrak{S}$. *Then* $\alpha \in \overline{\mathbb{Z}}$.

Remark 2.3. In particular, Theorem 2.3 proves the following: If $\sigma(\alpha^n) - \alpha^n$ is a non-zero algebraic integer for infinitely many n, then α is an algebraic integer. Note that we cannot conclude that α is an algebraic integer by applying the trace operator because $\mathrm{Tr}_{K/\mathbb{Q}}(\sigma(\alpha^n) - \alpha^n) = 0$.

2.2.1. *Action under the trace map.*

Theorem 2.4. *Let* α *be a non-zero algebraic number and let* $P(X) = a_k X^k + \cdots + a_0 \in \bar{\mathbb{Q}}[X]$ *be a non-constant polynomial of degree* d *where* $a_i \in \overline{\mathbb{Q}}$ *for all* $i = 0, \ldots, k$. *Let* $L = \mathbb{Q}(a_0, \ldots, a_d, \alpha)$ *be the number field. If* $\mathrm{Tr}_{L/\mathbb{Q}}(P(\alpha^n)) \in \mathbb{Z} \backslash \{0\}$ *for infinitely many natural numbers* n, *then either* α *is an algebraic integer or* $\mathrm{Tr}_{L/\mathbb{Q}}(a_i \alpha^{in}) = 0$ *for infinitely many values of* n *and each* $i = 1, \ldots, k$.

In the above result, we had considered only a polynomial of one variable and we observed that each sum has to be zero under the action of the trace operator. In a multivariable case, we may have that the trace operator vanishes for a subsum for trivial reasons. For simplicity, we consider a linear form in several variables.

Theorem 2.5. *Suppose $\alpha_1, \dots, \alpha_k, \lambda_1, \dots \lambda_k$ be distinct non-zero algebraic numbers and let $L = \mathbb{Q}(\alpha_i, \lambda_i \mid 1 \le i \le k)$ and h be the order of the torsion subgroup of the Galois closure of L over $\mathbb{Q}$. Assume that the following condition is satisfied:*

$$\mathrm{Tr}_{L/\mathbb{Q}}(\lambda_1\alpha_1^n + \cdots + \lambda_k\alpha_k^n) \in \mathbb{Z}\backslash\{0\}$$

for n in an infinite subset $\mathfrak{S}$. If α_1 is not an algebraic integer, then there exists an integer $a \in \{0, \dots, h-1\}$ and a proper subset P of $\{1, \dots, k\}$ containing 1 such that

$$\mathrm{Tr}_{L/\mathbb{Q}}\left(\sum_{i \in P} \lambda_i \alpha_i^a\right) = 0$$

where for each $i \in P$ there exists $\sigma_i \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma_i(\alpha_i)/\alpha_1$ is a root of unity.

We have the following interesting corollary as a consequence of this result.

Corollary 2.2. *Let $\alpha_1, \dots, \alpha_k, \lambda_1, \dots, \lambda_k$ be non-zero algebraic numbers. Let $L = \mathbb{Q}(\alpha_i, \lambda_i \mid 1 \le i \le k)$ be the number field and K be its Galois closure. Let h be the order of the torsion subgroup of the multiplicative group $K^\times$ and assume that no proper subsum of $\lambda_1\alpha_1^a + \cdots + \lambda_k\alpha_k^a$ under the trace map vanishes for each $a \in \{0, 1, \dots, h-1\}$. If $\mathrm{Tr}_{L/\mathbb{Q}}(\lambda_1\alpha_1^n + \cdots + \lambda_k\alpha_k^n) \in \mathbb{Z}\backslash\{0\}$ for infinitely many natural numbers n, then each α_i is an algebraic integer for all $i = 1, \dots, k$.*

When $k = 1$, the above corollary recovers the result of P. Philippon and P. Rath in [7].

2.3. **Determining the nature of rational functions from values.** We now consider a situation where we can deduce about nature of certain rational functions under some assumptions.

Theorem 2.6. *Let $f_1, \dots, f_k$ be non-constant rational functions with algebraic coefficients and $\lambda_1, \dots, \lambda_k$ be non-zero algebraic numbers. Assume that the ratio f_i/f_j is not a constant function for $i \neq j$. If*

$$\sum_{i=1}^{k} \lambda_i (f_i(x))^n \in \overline{\mathbb{Z}}[x] \tag{2.2}$$

for n in an infinite set $\mathfrak{S}$, then each $f_i(x) \in \overline{\mathbb{Z}}[x]$.

It may possible to show that the functions f_i are polynomial functions without appealing to the subspace theorem. However, the approach here is to deduce the nature of rational function via its specialisations. After the application of the subspace theorem, we have only used valuation arguments throughout to prove the theorem.

2.4. **Determining Algebraic integers in Finite iteration.** In the work of B. de Smit, a finite bound on i in $\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^i)$ was given in order to determine whether α is an algebraic integer.

Using some elementary properties, we address the following question :

$$\text{Does there exist a bound on } i \text{ for which } m_i := \sum_{j=1}^{k} \lambda_j \alpha_j^i \in \mathcal{O}_K \implies \alpha_j \in \mathcal{O}_K \text{ for all } 1 \le j \le k?$$

We answer this question for $k = 2$ and highlight some difficulties for arbitrary k. We state the following theorem :

Theorem 2.7. *Let $\alpha_1, \alpha_2, \lambda_1, \lambda_2$ be non-zero algebraic numbers. Let $K = \mathbb{Q}(\lambda_i, \alpha_i \mid 1 \le i \le 2)$ be a number field. Then there exists a constant C depending on $m_0, m_1, m_2, m_3, \lambda_1, \lambda_2$ such that if*

$$m_i = \lambda_1\alpha_1^i + \lambda_2\alpha_2^i \in \mathcal{O}_K \text{ for all } 1 \le i \le C \implies \alpha_i \in \mathcal{O}_K.$$

Our next theorem is another generalization of a result of B. de Smit.

Theorem 2.8. *Let α_1 be a nonzero algebraic number and $\alpha_2, \ldots, \alpha_k$ be all the other Galois conjugates of α_1 for some integer $k \geq 2$. Let K be the Galois closure of $\mathbb{Q}(\alpha_1)$ and $[K : \mathbb{Q}] = d \geq k$. For any integers $b_1, \ldots, b_k$ (not necessarily distinct) such that $b_1 + \cdots + b_k = n \neq 0$, if $\mathrm{Tr}_{K/\mathbb{Q}}(b_1\alpha_1^j + \cdots + b_k\alpha_k^j) \in \mathbb{Z}$ for all $j = 1, 2, \ldots, d + d[\log_2(nd)] + 1$, then α is an algebraic integer and so are α_j for all $j \geq 2$.*

By taking $b_1 = q$, any positive integer q and $b_i = 0$ for all $i = 2, \ldots, k$ in Theorem 2.8, we get a natural result as follows.

Corollary 2.3. *Let α be a nonzero algebraic number of degree $k \geq 2$ and K be the Galois closure of $\mathbb{Q}(\alpha)$ of degree $[K : \mathbb{Q}] = d$. If $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^j) \in \frac{1}{q}\mathbb{Z}$ for all $j = 1, 2, \ldots, d + d[\log_2(qd)] + 1$ and for some positive integer q, then α is an algebraic integer.*

Corollary 2.3 motivated us to prove the following general result whose proof is similar to the proof of Theorem 2.8 and hence we omit the proof.

Theorem 2.9. *Let α be given nonzero algebraic number of degree $k \geq 2$ and K be the Galois closure of $\mathbb{Q}(\alpha)$ of degree $[K : \mathbb{Q}] = d$. Let λ be a nonzero element of K and $\mathrm{Tr}_{K/\mathbb{Q}}(\lambda) = a/b$ for some coprime integers a and b. If $\mathrm{Tr}_{K/\mathbb{Q}}(\lambda\alpha^j) \in \frac{1}{q}\mathbb{Z}$ for all $j = 1, 2, \ldots, d + d[\log_2(dq|ab|)] + 1$ for some integer $q \geq 1$, then α is an algebraic integer.*

2.5. **Diophantine type result.** We also prove a Diophantine type result as follows.

Theorem 2.10. *Let $\alpha_1, \ldots, \alpha_k$ be non-zero algebraic numbers such that none of the α_i's is root of unity and let $\lambda_1, \ldots, \lambda_k$ be non-zero algebraic numbers. Let $L = \mathbb{Q}(\lambda_1, \ldots, \lambda_k, \alpha_1, \ldots, \alpha_k)$ be the number field. Then, for any given non-zero rational number p/q, there are at most finitely many $n \in \mathbb{N}$ satisfying $\mathrm{Tr}_{L/\mathbb{Q}}(\lambda_1\alpha_1^n + \cdots + \lambda_k\alpha_k^n) = \frac{p}{q}$.*

3. Preliminaries

In this section, we state the propositions/theorems required for the proof of our theorems. We also need some results which are applications of the Schmidt Subspace Theorem, formulated by Evertse and Schlickewei. For a reference, see ([1, Chapter 7], [10, Chapter V, Theorem $1D'$], and [11, Page 16, Theorem II.2]).

Let $K \subset \mathbb{C}$ be a number field which is Galois over $\mathbb{Q}$ with Galois group $\mathrm{Gal}(K/\mathbb{Q})$. Let M_K be the set of all inequivalent places of K and M_∞ be the set of all archimedean places of K. For each place $v \in M_K$, we denote $|\cdot|_v$ the absolute value corresponding to v, normalized with respect to K. Indeed if $v \in M_\infty$, then there exists an automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ of K such that for all $x \in K$,

$$|x|_v = |\sigma(x)|^{d(\sigma)/[K:\mathbb{Q}]},$$

where $d(\sigma) = 1$, if $\sigma(K) = K \subset \mathbb{R}$; and $d(\sigma) = 2$ otherwise. Note that since K is Galois over $\mathbb{Q}$, the function $d(\sigma)$ is constant. Non-archimedean absolute values are normalized accordingly so that the product formula $\prod_{\omega \in M_K} |x|_\omega = 1$ holds true for any $x \in K^\times$.

For all $x \in K$, the *absolute Weil height*, $H(x)$, is defined as

$$H(x) := \prod_{\omega \in M_K} \max\{1, |x|_\omega\}.$$

We define the logarithmic Weil height $h(x) := \log(H(x))$.

For a vector $\mathbf{x} = (x_1, \ldots, x_n) \in K^n$ and for a place $\omega \in M_K$, the ω-norm for $\mathbf{x}$ denote by $||\mathbf{x}||_\omega$ and defined by

$$||\mathbf{x}||_\omega := \max\{|x_1|_\omega, \ldots, |x_n|_\omega\}$$

and the *projective height*, $H(\mathbf{x})$, is defined by

$$H(\mathbf{x}) = \prod_{\omega \in M_K} ||\mathbf{x}||_\omega \text{ for all } \mathbf{x} \in K^n.$$

Proposition 3.1. (A. Kulkarni *et al.* [5]) *Let $\alpha_1, \ldots, \alpha_k$ be non-degenerate non-zero algebraic numbers and let $\lambda_1, \ldots, \lambda_k$ be non-zero algebraic numbers. Then there are at most finitely many natural numbers n satisfying*

$$\lambda_1 \alpha_1^n + \cdots + \lambda_k \alpha_k^n = 0.$$

We shall use the following theorem as an alternative of the subspace theorem (though derived from it) :

Theorem 3.1. (A. Kulkarni *et al.* [5]) *Let K be a number field which is Galois over $\mathbb{Q}$ and S be a finite set of places, containing all the archimedean places. Let $\lambda_1, \ldots, \lambda_k$ be non-zero elements of K. Let $\varepsilon > 0$ be a positive real number and $\omega \in S$ be a distinguished place. Let $\mathfrak{E}$ be the set of all $(u_1, \ldots, u_k) \in (\mathcal{O}_S^\times)^k$ which satisfies the inequality*

$$0 < \left| \sum_{j=1}^{k} \lambda_j u_j \right|_\omega \leq \frac{\max\{|u_1|_\omega, \ldots, |u_k|_\omega\}}{H(u_1, \ldots, u_k, 1)^\epsilon}, \tag{3.1}$$

where $\mathcal{O}_S^\times$ is the ring S-units in K. If $\mathfrak{E}$ is an infinite subset, then there exist $c_1, \ldots, c_k \in K$, not all zero, such that

$$c_1 u_1 + \cdots + c_k u_k = 0$$

holds true for infinitely many elements $(u_1, \ldots, u_k)$ of $\mathfrak{E}$.

We prove the following proposition regarding the elements of Galois group fixing the equivalence class of a non zero algebraic element α (given by (2.1)). This is of independent interest.

Proposition 3.2. *Let α be a non-zero algebraic number, and L be any Galois extension of $\mathbb{Q}$ containing α with $G = \mathrm{Gal}(L/\mathbb{Q})$. Let*

$$H = \{\sigma \in G \ : \ \sigma(\alpha) \sim \alpha\}$$

be a subset of G. Then the following statements are true.

1. *H is a subgroup of G.*
2. *For any given $\tau \in G$, we have, $\{\sigma \in G \mid \sigma(\tau(\alpha)) \sim \tau(\alpha)\} = \tau H \tau^{-1}$.*

Proof. If $\sigma_a \in H$ then we have $\sigma_a(\alpha) = \zeta_h^{w_a}\alpha$. Since G permutes the roots of unity, so does H. This shows that H is closed under inversion and composition of automorphisms in G. Hence H is a subgroup of G. This proves (1).

Let $\sigma \in H$ be any element. Then we have

$$\sigma(\alpha) \sim \alpha \Leftrightarrow \tau(\sigma(\alpha)) \sim \tau(\alpha) \Leftrightarrow (\tau\sigma\tau^{-1})(\tau\alpha) \sim \tau(\alpha),$$

proving the second statement. □

We shall state the following basic and well-known lemma that roughly says 'integrality' is a local phenomenon.

Lemma 3.1. *Let $\alpha \in \bar{\mathbb{Q}}$ be an algebraic number. Then α is an algebraic integer if and only if α is integral over $\mathbb{Z}_p$ for every prime number p where $\mathbb{Z}_p$ is the ring of p-adic integers.*

The following lemma is also basic and well-known and omitted the proof here.

Lemma 3.2. *Let K be a finite extension over $\mathbb{Q}_p$ of degree d where $\mathbb{Q}_p$ is the field of p-adic integers. Let $\alpha \in K$ be an element such that $\alpha \notin \mathcal{O}_K$, the local ring of K. Then $\beta = \alpha^{-1} \in \mathcal{O}_K$. Furthermore, if the characteristic polynomial of β is*

$$f_{K|\mathbb{Q}_p}(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x],$$

then $a_d = 1$ and $a_i \in p\mathbb{Z}_p$ for all $i = 0, 1, \ldots, d-1$ where $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Z}_p$.

We need the following lemma in the proof of Theorem 2.8.

Lemma 3.3. *Let p be a given prime number and let K be a finite Galois extension over $\mathbb{Q}_p$ of degree d. Let $\alpha \in K$ be an element such that $\alpha \notin \mathcal{O}_K$ and β be a Galois conjugate of α. Let b_1 and b_2 be given p-adic integers such that $b_1 + b_2 \neq 0$. Then for each integer $\ell \geq 0$, there exists an integer $i \in \{1, 2, \ldots, d\}$ such that $b_1\alpha^{\ell+i} + b_2\beta^{\ell+i} \neq 0$.*

Proof. Since $\alpha \notin \mathcal{O}_K$, it is clear that $\alpha^{-1} \in \mathcal{O}_K$ and let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0 \in \mathbb{Z}_p[x]$ be the characteristic polynomial of α^{-1}. Since β is a Galois conjugate of α, it is clear that $f(\alpha^{-1}) = 0 = f(\beta^{-1})$. we see that for every integer $m \geq 0$, we have

$$\alpha^m = -a_{d-1}\alpha^{m+1} - \cdots - a_0\alpha^{m+d} \text{ and } \beta^m = -a_{d-1}\beta^{m+1} - \cdots - a_0\beta^{m+d}.$$

Therefore, we get

$$b_1\alpha^m + b_2\beta^m = -a_{d-1}(b_1\alpha^{m+1} + b_2\beta^{m+1}) - \cdots - a_0(b_1\alpha^{m+d} + b_2\beta^{m+d}). \tag{3.2}$$

Now we prove the assertion by induction on ℓ.

We put $m = 0$ in (3.2), we get

$$0 \neq b_1 + b_2 = -a_{d-1}(b_1\alpha^1 + b_2\beta^1) - \cdots - a_0(b_1\alpha^d + b_2\beta^d)$$

which implies the assertion when $\ell = 0$. Assume the assertion is true for some integer $\ell > 0$. That is, there exists an integer $i \in \{1, 2, \ldots, d\}$ such that $b_1\alpha^{\ell+i} + b_2\beta^{\ell+i} \neq 0$. If $i \geq 2$, then $\ell + i = \ell + 1 + j$ for some integer $j \in \{1, 2, \ldots, d\}$ and then we are done. Hence we assume that $i = 1$. That is, $b_1\alpha^{\ell+1} + b_2\beta^{\ell+1} \neq 0$. Now, put $m = \ell + 1$ in (3.2) to get the assertion in this case as well. Hence the lemma. □

We conclude this section by discussing a proof of Fatou's Lemma. This was proved by Pisot [8] for number fields and the proof was adapted based on Fatou's work [3]. We provide a different proof of the same as mentioned in the abstract.

Proposition 3.3 (Fatou's lemma)**.** *Let K be a number field and $f \in K(x) \cap \mathcal{O}_K[[x]]$ such that $f(x) = g(x)/h(x)$ with $g(x), h(x) \in K[x]$, $h(0) = 1$ and coprime in $K[x]$. Then $g(x), h(x) \in \mathcal{O}_K[x]$.*

Proof. We write $f(x) = g(x)/h(x)$ where $g, h \in K[x]$ coprime and $h(0) = 1$. Then there exist two polynomials $r, s \in \mathcal{O}_K[x]$ such that $r(x)g(x) + s(x)h(x) = c$ for some non zero constant $c \in \mathcal{O}_K$. Therefore we have

$$\frac{c}{h(x)} \in \mathcal{O}_K[[x]]. \tag{3.3}$$

Now let $h(x) = \prod_{i=1}^{k}(1 - a_ix)^{c_i}$ in $\overline{\mathbb{Q}}[x]$ with each $c_i \geq 1$ and $a_i \in \overline{\mathbb{Q}}$ distinct. For each i, multiplying (3.3), by the factor

$$\left[\prod_{\substack{j=1\\ j\neq i}}^{k} \mathrm{den}(a_j)^{c_j}(1 - a_jx)^{c_j}\right] \left[\mathrm{den}(a_i)^{c_i-1}(1 - a_ix)^{c_i-1}\right],$$

we define a new formal power series $\widetilde{f}_i(x) := c'(1-a_ix)^{-1}$ with c' depending on $\text{den}(a_j)$ and c_j for $1 \le j \le k$. Here $\text{den}(\alpha)$ denotes the denominator of algebraic number α. Since we are multiplying by a polynomial with entries in algebraic integers, we have $\widetilde{f}_i(x) \in \mathcal{O}_L[[x]]$ for some finite extension L of K where $h(x)$ splits completely. Therefore for any prime $\mathfrak{P}$ in $\mathcal{O}_L$ we have

$$v_{\mathfrak{P}}(c'a_i^n) \ge 0 \text{ for all } n \implies v_{\mathfrak{P}}(a_i) \ge 0$$

This proves that a_i is an algebraic integer and repeats the same process for all i. Therefore $h(x) \in K[x] \cap \mathcal{O}_L[x] = \mathcal{O}_K[x]$ and consequently $g(x) = f(x)h(x) \in \mathcal{O}_K[x]$ as both f, h take values in $\mathcal{O}_K$. □

Remark 3.1. It is possible to simultaneously prove that the numbers a_i are algebraic integers by considering the function $c'/\prod_{i=1}^{k}(1-a_ix)$ and apply Theorem 2.1 for different linear forms $\mathcal{L}_m$.

4. Proofs of Theorems 2.1 to 2.6

Proof of Theorem 2.1. Let $K = \mathbb{Q}(\alpha_1, \dots \alpha_k)$ and h be the order of the torsion subgroup of K^*. We write $\mathfrak{S} = \bigcup_m \mathfrak{S}_{\mathfrak{m}} \cup \mathfrak{T}$, where each $\mathfrak{S}_{\mathfrak{m}}$ is a subset of $\mathfrak{S}$ consisting of positive integers n' such that $n' \equiv m \mod h$ and $\mathfrak{T}$ is a finite set. Since $\mathfrak{S}$ is infinite, we note that there exists an integer m such that for infinitely many integers n of $\mathfrak{S}$ we have that $n \equiv m \mod h$. This ensures there exists at least one m for which $\mathfrak{S}_m$ is infinite.

We partition $\{\alpha_1, \dots, \alpha_k\} = \bigcup_j S_j$ where each S_j denotes an equivalence class given by (2.1). Furthermore, for each S_j, we correspondingly define an index set I_j consisting of the indices a such that $\alpha_a \in S_j$. We select $\beta_j \in S_j$ to be a representative of this class. Therefore for $\alpha_a \in S_j$, we write $\alpha_a = \beta_j\zeta_h^{\omega_a}$ for some integer ω_a where ζ_h is a primitive h-th root of unity.

Note that for $n \in \mathfrak{S}_m$, we have:

$$\mathcal{L}(\alpha_1^n, \dots, \alpha_k^n) = \sum_{i=1}^{k} \lambda_i\alpha_i^n = \sum_j \sum_{a\in I_j} \lambda_a\alpha_a^n = \sum_j \sum_{a\in I_j} \lambda_a\zeta_h^{\omega_a n}\beta_j^n = \sum_j \kappa_{j,m}\beta_j^n,$$

where the sum over j runs over the finite number of equivalence classes and $\kappa_{j,m} = \sum_{a\in I_j} \lambda_a\zeta_h^{\omega_a m}$, as $n \equiv m \mod h$. Therefore, for each residue class $m \mod h$ which appears infinitely many times in $\mathfrak{S}$, we have a new linear form

$$\mathcal{L}_m(X_1, \dots, X_d) = \sum_{j=1}^{d} \kappa_{j,m}X_j$$

with d depending on α_i, λ_i and m.

By assuming the assertion (1) is not true, we consider that there are infinitely many natural numbers n for which $\sum_{a\in I_j} \lambda_a\zeta_h^{\omega_a n}$ is non-zero and we label this set as $\mathfrak{S}'$. Choosing m as above for which we have $\mathfrak{S}_m$, we arrive at a reduced linear form $\mathcal{L}_m(X_1, \dots, X_d) = \sum_{i=1}^{d} \kappa_{i,m}X_i$ where we assume that each of the coefficients is non-zero and in particular $\kappa_{j,m} \neq 0$.

We have reduced our question to the following :

$$\mathcal{L}_m(\overline{\beta}^n) \in \overline{\mathbb{Z}}\backslash\{0\},$$

where $\overline{\beta} = (\beta_1, \ldots, \beta_d)$. We note that the numbers $\beta_1, \ldots, \beta_d$ are non-degenerate as they correspond to disjoint equivalence classes. We proceed to prove that β_j is an algebraic integer by Theorem 3.1 and thereby all elements of S_j are algebraic integers.

Let S be a suitable finite subset of M_K containing all the archimedean places such that α_i is an S-unit for each $i = 1, 2, \ldots, k$. Assume that β_j is not an algebraic integer. Then there exists a finite place $\omega \in S$ such that $|\beta_j|_\omega > 1$. Choose $\epsilon > 0$ such that $\epsilon < \dfrac{\log|\beta_j|_\omega}{\log H(\beta_1, \ldots, \beta_d, 1)}$. Since $\mathfrak{S}_m$ is an infinite set, for all large enough $n \in \mathfrak{S}_m$, we have $|\beta_j|_\omega^{hn} H(\beta_1^{hn}, \ldots, \beta_d^{hn}, 1)^{-\epsilon} > 1$. This is possible by the choice of ϵ and $|\beta_j|_\omega > 1$. Then Theorem 3.1 yields the following

$$\sum_{i=1}^{d} b_i \beta_i^n = 0$$

holds true for infinitely many natural numbers n where $b_i \in K$ and not all zero, which is a contradiction as the numbers β_i for $1 \leq i \leq d$ are non-degenerate. Therefore β_j is an algebraic integer. $\square$

Proof of Theorem 2.2. Suppose $P(X_1, \ldots X_k) = \sum_{\mathbf{i}} a_{\mathbf{i}} X_{\mathbf{i}}$ where we denote $\mathbf{i}$ to be a multi-index and $X_{\mathbf{i}} = \prod_{j=1}^{k} X_j^{b_j}$ where $\mathbf{i} = (b_1, \ldots, b_k)$. Note that the condition on P implies that we have at least one monomial consisting only of X_m for some integer $1 \leq m \leq k$. Now, consider the linear form $\mathcal{L}((X_{\mathbf{i}})) = \sum_{\mathbf{i}} a_{\mathbf{i}} X_{\mathbf{i}}$. We naturally apply this linear form on the tuple $(\alpha_{\mathbf{i}}^n)$, where we define $\alpha_{\mathbf{i}} = \prod_{j=1}^{k} \alpha_j^{b_j}$.

By Theorem 2.1, for every equivalence class in (2.1), we have a corresponding partition satisfying one of the two properties. By hypothesis, there exists an integer m with $1 \leq m \leq k$ such that the partition I_m contains $(0, \ldots, b_m, \ldots 0)$. This corresponds to the equivalence class of the element $\alpha_m^{b_m}$. We consider both possibilities below:

(1) Suppose we assume that Condition 1 of Theorem 2.1 is satisfied for the partition I_m. We have
$$\sum_{\mathbf{i} \in I_m} a_{\mathbf{i}} \alpha^{\mathbf{i}n} = 0,$$
for infinitely many n. Then for $\mathbf{i}, \mathbf{j} \in I_m$, we note that $\alpha^{\mathbf{i}}/\alpha^{\mathbf{j}} = \alpha^{\mathbf{i}-\mathbf{j}}$ is a root of unity. Since $\alpha_1, \ldots, \alpha_k$ are multiplicatively independent, this implies that exactly one of the coordinates in the tuple $\mathbf{i} = (i_1, \ldots, i_k)$ and $\mathbf{j} = (j_1, \ldots j_k)$ are distinct. Since the tuple $(0, \ldots, b_m, \ldots, 0) \in I_m$, we have $i_r = j_r = 0$ for $r \neq m$. Therefore $\alpha^{\mathbf{i}-\mathbf{j}} = \alpha_m^{i_m - j_m}$ is a root of unity, and hence α_m is a root of unity.

(2) If Condition 1 is not satisfied for I_m, then $\alpha_m^{b_m}$ is an algebraic integer. Consequently, α_m is an algebraic integer. $\square$

Proof of Theorem 2.3. Let $f = \sum_i \lambda_i \sigma_i$. We have

$$f(\alpha^n) = \sum_i \lambda_i \sigma_i(\alpha^n) = \sum_i \lambda_i \sigma_i(\alpha)^n.$$

Therefore, we can take $\overline{\alpha} = (\sigma_1(\alpha), \dots, \sigma_i(\alpha), \dots)$. Suppose α is not an algebraic integer. We apply Theorem 2.1 and immediately deduce that for each partition I_j, there exists a proper vanishing subsum for all but finitely values of n. We enumerate the elements of G as $\sigma_1, \sigma_2, \dots$. We have,

$$\sum_{i\in I_j} \lambda_i \sigma_i(\alpha)^n = 0 \text{ for all partitions } I_j.$$

Therefore, for all but finitely many values of $n \in \mathfrak{S}$, we have

$$f(\alpha^n) = \sum_{I_j} \sum_{\sigma_i \in I_j} \lambda_i \sigma_i(\alpha)^n = 0.$$

This is a contradiction. $\square$

Proof of Theorem 2.4. If α is a root of unity, there is nothing to prove, and therefore we assume that α is not a root of unity. Furthermore, we can reduce our computations to the field $F = \mathbb{Q}(\alpha)$. This is because we can write $\mathrm{Tr}_{\mathbb{Q}(a_0,\dots,a_d,\alpha)/\mathbb{Q}}(a_i\alpha^n) = \mathrm{Tr}_{F/\mathbb{Q}}(c_i\alpha^n)$ where $c_i = \mathrm{Tr}_{\mathbb{Q}(a_0,\dots,a_d,\alpha)/F}(a_i)$. Henceforth we assume $a_i \in F$. Thus, by the hypothesis, we have $\mathrm{Tr}_{F/\mathbb{Q}}(P(\alpha^n)) \in \mathbb{Z}\backslash\{0\}$ for infinitely many n. Therefore $\sum_{i=0}^{d} \mathrm{Tr}_{F/\mathbb{Q}}(a_i\alpha^{in}) \in \mathbb{Z}\backslash\{0\}$ for infinitely many n.

Assume that α is not an algebraic integer. Expanding the trace operator, by Theorem 2.1, we have a partition I_j such that

$$\sum_{i\in I_j} b_i \alpha_i^n = 0,$$

for all but finitely many n. Here b_i denote the conjugates of a_l for some finite collection and α_i denotes some conjugate of α^l for $l \le d$ appropriately. We claim the following:

$$\text{If } \alpha^l \sim \sigma(\alpha)^k \text{ for some } 1 \le l, k \le d, \text{ then } l = k.$$

We can conclude this from the properties of logarithmic Weil height $h(x)$. We have

$$|l| h(\alpha) = h(\alpha^l) = h(\zeta\sigma(\alpha)^k) = h(\alpha^k) = |k| h(\alpha)$$

implying $l = k$ as both are positive. Suppose $a_l\alpha^l$ is one of the terms in the summand. We have,

$$\sum_{i\in I_j} \sigma_i(a_l\alpha^{ln}) = 0$$

for all but finitely many n. Applying the trace operator both sides, we get $|I_j|\mathrm{Tr}_{F/\mathbb{Q}}(a_l\alpha^{ln}) = 0$ for infinitely many n. We prove the theorem as we can repeat the same process for all the partitions I_j (note that none of the powers or conjugates of α is an algebraic integer). $\square$

Proof of Theorem 2.5. We write the index set $I = \{(i, \sigma) \mid 1 \le i \le k, \sigma \in \mathrm{Gal}(L/\mathbb{Q})\}$. Let the linear form corresponding to the trace operator as follows:

$$\sum_{i=1}^{k} \sum_{\sigma\in \mathrm{Gal}(L/\mathbb{Q})} \sigma(\lambda_i) X_{i,\sigma}.$$

Therefore if we write $\overline{\alpha} = (\sigma(\alpha_i))_{1\le i\le k, \sigma\in\mathrm{Gal}(L/\mathbb{Q})}$ and apply Theorem 2.1, we note that there exists a partition I_1 containing $(1, \sigma_1)$ (σ_1 denotes the identity map) such that

$$\sum_{(i,\sigma_j)\in I_1} \sigma_j(\lambda_i)\sigma_j(\alpha_i)^n = 0 = \alpha_1^n \left(\sum_{(i,\sigma_j)} \sigma_j(\lambda_i) {\zeta_h}^{(w_{ij} - w_{11})n} \right)$$

for all but finitely many n. We set $P = \{i \mid \exists\sigma \in \mathrm{Gal}(L/\mathbb{Q}))$ such that $(i,\sigma) \in I_1\}$. For each $i \in P$, we set $\tau_i \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\alpha_1 \sim \tau_i(\alpha_i)$. We now write the above summation as

$$\sum_{i\in P}\sum_{\sigma\in H_i} \sigma(\tau_i(\lambda_i))\sigma(\tau_i(\alpha_i^n)) = 0,$$

where $H_i := \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) \mid \tau_i(\alpha_i) \sim \sigma(\tau_i(\alpha_i))\}$. By Proposition 3.2 for each $i \in P$, H_i is a subgroup of $\mathrm{Gal}(L/\mathbb{Q})$. We claim that $H_i = H_j$ for any $i, j \in P$. This is because for any $\sigma \in H_i$ we have,

$$\tau_j(\alpha_j) \sim \tau_i(\alpha_i) \sim \sigma(\tau_i(\alpha_i)) \sim \sigma(\tau_j(\alpha_j))$$

We have the first equivalence, because $(i, \tau_i) \in I_1$, the second equivalence by the definition of H_i, and finally the third equivalence by acting σ on the first equivalence. Therefore $\sigma \in H_j$ and consequently $H_i \subseteq H_j$ for any $i, j \in P$ implying that $H_i = H_j$. Thus we have

$$\sum_{\sigma\in H_1} \sigma\left(\sum_{i\in P} \tau_i\left(\lambda_i\alpha_i^n\right)\right) = 0$$

for all but finitely many values of $n \in \mathfrak{S}$.

There exists a non-negative integer $a < h$ such that there are infinitely many $n \equiv a \mod h$ with $n \in \mathfrak{S}$. For any such $n \equiv a \mod h$ in $\mathfrak{S}$, we get

$$\alpha_1^n \sum_{\sigma_j\in H_1}\sum_{i\in P} \sigma_j(\tau_i(\lambda_i))\zeta_h^{(w_{ij}-w_{11})n} = 0 \implies \sum_{\sigma\in H_1}\sum_{i\in P} \sigma(\tau_i(\lambda_i)(\tau_i(\alpha_i)^a) = 0.$$

Acting the above sum with the trace operator $\mathrm{Tr}_{L/\mathbb{Q}}$ and noting that $\mathrm{Tr}_{L/\mathbb{Q}}$ is invariant under Galois action, we obtain

$$\sum_{i\in P} \mathrm{Tr}_{L/\mathbb{Q}}(\lambda_i\alpha_i^a) = 0.$$

This proves the theorem. □

Proof of Theorem 2.6. Let $K = \mathbb{Q}(\text{conjugates of zeroes and poles of } f_i(x), \lambda_i \mid 1 \le i \le k)$. We write $f_i(x) = \dfrac{p_i(x)}{q_i(x)}$ with both $p_i(x), q_i(x) \in \mathcal{O}_K[x]$ satisfying $(p_i(x), q_i(x)) = 1$ in $K[x]$. Let h be the order of the torsion subgroup of K. We set

$$\mathfrak{V}_K := \mathcal{O}_K\backslash\{\text{Zeroes of } p_i(x), q_i(x), (q_j(x)p_i(x))^h - (q_i(x))p_j(x))^h \text{ for } 1 \le i < j \le k\}.$$

Note that this set is the complement of a finite set as $f_i(x)/f_j(x)$ is not a constant, and we are removing solutions of the equation $f_i(x)/f_j(x) = \zeta_h^a$. More generally, for any number field L, the set $\mathfrak{V}_L$ is a complement of a finite set. For any $\alpha \in \mathfrak{V}_K$ (or $\mathfrak{V}_L$), we note that the tuple $(f_1(\alpha), \ldots, f_k(\alpha))$ is a non-degenerate tuple and by Theorem 2.1, $f_i(\alpha) \in \mathcal{O}_K$ (or $\mathcal{O}_L$). We proceed to show that f_i is a polynomial.

Since $(p_i(x), q_i(x)) = 1$ in $K[x]$, there exist polynomials $r_i(x), s_i(x) \in \mathcal{O}_K[x]$ and $\beta_i \neq 0 \in \mathcal{O}_K$ such that

$$r_i(x)p_i(x) + s_i(x)q_i(x) = \beta_i,$$

and hence $r_i(x)f_i(x) + s_i(x) = \beta_i/q_i(x)$. Therefore, for $\alpha \in \mathfrak{V}_K$, the value $\beta_i/q_i(\alpha) \in \mathcal{O}_K$.

We rule out the possibility of q_i being a non-constant polynomial. We consider the problem locally, namely, by showing that there exists a prime ideal $\mathfrak{P}$ and $\alpha \in \mathfrak{V}_K$ such that $|q_i(\alpha)|_{\mathfrak{P}} < |\beta_i|_{\mathfrak{P}}$. This gives a contradiction because $\beta_i/q_i(\alpha)$ is an algebraic integer. To find such a prime $\mathfrak{P}$, we proceed as follows. We first factorise $q_i(x) = \prod_{i=0}^{d}(c_ix - a_i)$ with $c_i \neq 0$ for all i, and we can find $\mathfrak{P}$

such that $|\beta_i|_{\mathfrak{P}} = 1$, $|c_i|_{\mathfrak{P}} = 1$ and $|a_i|_{\mathfrak{P}} = 1$ provided $a_i \neq 0$. The question therefore reduces to look for $\alpha \in \mathfrak{V}_K$ such that $|q_i(\alpha)|_{\mathfrak{P}} < 1$. Since $\mathfrak{V}_K \to \mathcal{O}_K/\mathfrak{P}$ is surjective (note that $\mathfrak{V}_K$ is the complement of a finite set in $\mathcal{O}_K$), we conclude that it is enough to find a solution in $\mathcal{O}_K/\mathfrak{P}$. We can choose $\alpha \in \mathfrak{V}_K$ such that $|q_i(\alpha)|_{\mathfrak{P}} < 1$ by lifting the solution of one of the linear factors. This choice of α gives the required contradiction. Therefore, we conclude that $f_i(x) \in K[x]$.

We now proceed to show that $f_i(x) \in \mathcal{O}_K[x]$. Let $f_i(x) = p_i(x)/\beta = \dfrac{1}{\beta}\displaystyle\sum_{j=0}^{d} b_j x^j$ for some $\beta, b_j \in \mathcal{O}_K[x]$. Suppose there exists prime $\mathfrak{P}$ such that $v_{\mathfrak{P}}(b_j/\beta) < 0$ for some j. We choose a number field L containing K having a prime $\mathfrak{Q}$ above $\mathfrak{P}$ such that the ramification index (say m) is greater than $2d$. By the choice of m, we conclude that

$$m \min_i v_{\mathfrak{P}}(b_i/\beta) + d < 0. \tag{4.1}$$

Note that such L can be chosen by adjoining the appropriate root of unity to K. We remind that for any $\alpha \in K^*$, we have $v_{\mathfrak{Q}}(\alpha) = m v_{\mathfrak{P}}(\alpha)$.

Now since $\mathfrak{V}_L$ is the complement of a finite set, we choose $\alpha \in \mathfrak{V}_L$ such that $v_{\mathfrak{Q}}(\alpha) = 1$. Now, consider $v_{\mathfrak{Q}}(f_i(\alpha))$. For any two distinct numbers $i, j \leq d$, due to (4.1), we have,

$$v_{\mathfrak{Q}}(b_j\alpha^j/\beta) \neq v_{\mathfrak{Q}}(b_i\alpha^i/\beta),$$

because $m > 2d$ (If they are equal, we take absolute values and consider their difference to get a contradiction). Therefore,

$$v_{\mathfrak{Q}}(f_i(\alpha)) = \min_i (v_{\mathfrak{Q}}(b_i/\beta) + i) \leq \min_i m(v_{\mathfrak{P}}(b_i/\beta)) + d < 0.$$

This is a contradiction as we have $f_i(\alpha) \in \mathcal{O}_L$ for $\alpha \in \mathfrak{V}_L$. □

Remark 4.1. For the second part, to conclude that $f_i(x) \in \mathcal{O}_K[x]$ given that $f_i(x) \in K[x]$ it is necessary to take a ramified extension. This is because we have integer-valued polynomials that are not in $\mathcal{O}_K[x]$ (For example, if we take $f(x) = x(x-1)/2$, then $f(\mathbb{Z}) \subseteq \mathbb{Z}$).

5. Proofs of Theorems 2.7 and 2.8

Proof of Theorem 2.7. Without loss of generality, we can assume that $\lambda_i \in \mathcal{O}_K$ by multiplying with a suitable denominator. By hypothesis, $m_i = \lambda_1\alpha_1^i + \lambda_2\alpha_2^i \in \mathcal{O}_K$ for all $1 \leq i \leq C$ where C is a positive integer to be chosen later. Suppose there exists a prime ideal $\mathcal{P}$ such that $v_{\mathcal{P}}(\alpha_1) < 0$. Then for each $i > v_{\mathcal{P}}(\lambda_1)$, we have

$$v_{\mathcal{P}}(\lambda_1\alpha_1^i + \lambda_2\alpha_2^i) \geq 0.$$

However, for $i > v_{\mathcal{P}}(\lambda_1)$, we have that $v_{\mathcal{P}}(\lambda_1\alpha_1^i) = v_{\mathcal{P}}(\lambda_1) + i v_{\mathcal{P}}(\alpha_1) \leq v_{\mathcal{P}}(\lambda_1) - i < 0$. Using the fact that $v_{\mathcal{P}}(x+y) = \min\{v_{\mathcal{P}}(x), v_{\mathcal{P}}(y)\}$, when $v_{\mathcal{P}}(x) \neq v_{\mathcal{P}}(y)$, we get

$$v_{\mathcal{P}}(\lambda_1\alpha_1^i) = v_{\mathcal{P}}(\lambda_2\alpha_2^i) \implies i|v_{\mathcal{P}}(\alpha_1) - v_{\mathcal{P}}(\alpha_2)| \leq v_{\mathcal{P}}(\lambda_1\lambda_2).$$

Now if $i > v_{\mathcal{P}}(\lambda_1\lambda_2)$ and $m_i \in \mathcal{O}_K$, then we note that $v_{\mathcal{P}}(\alpha_1) = v_{\mathcal{P}}(\alpha_2)$. In particular, $v_{\mathcal{P}}(\alpha_2) < 0$. Now consider the term

$$V_n := m_n m_{n+2} - m_{n+1}^2 = \lambda_1\lambda_2\alpha_1^n\alpha_2^n(\alpha_1 - \alpha_2)^2 = V_0(\alpha_1\alpha_2)^n. \tag{5.1}$$

Assume that $m_n \in \mathcal{O}_K$ for $n \leq \frac{1}{2}\max v_{\mathcal{P}}(V_0) + 3$. Therefore $V_n \in \mathcal{O}_K$ for each $n \leq \frac{1}{2}\max v_{\mathcal{P}}(V_0) + 1$. Set $n_0 = \frac{1}{2}\max v_{\mathcal{P}}(V_0) + 1$. Then on the one hand $v_{\mathcal{P}}(V_{n_0}) > 0$ by our assumption, but on the other hand $v_{\mathcal{P}}(V_{n_0}) = v_{\mathcal{P}}(V_0) + 2n_0 v_p(\alpha_1) < 0$, a contradiction. Therefore either $v_{\mathcal{P}}(\alpha_1) > 0$ or $m_n \notin \mathcal{O}_K$ for some n in the given range.

Thus by setting $C = 1 + \frac{1}{2}\max_{\mathcal{P}} v_{\mathcal{P}}(V_0) + \max_{\mathcal{P}}(|v_{\mathcal{P}}(\lambda_1)| + |v_{\mathcal{P}}(\lambda_2)|)$ and assume that $m_n \in \mathcal{O}_K$ for all $0 \le n \le C$, then we obtain that α_1 and α_2 are algebraic integers.

Remark 5.1. One may try to generalise this argument for $k \ge 3$. There are issues with the valuation argument for more than 2 variables. We may use Hankel determinants of matrices with entries consisting only of m_i to arrive at an equation very similar to (5.1). Proceeding in the same manner from there, one may obtain that $\prod_{i=1}^{k} \alpha_i \in \mathcal{O}_K$. However, it is not possible to obtain a bound purely depending on m_i, λ_i, by induction for the following reason: When we try to do induction over k, we know the values m_i only for k terms and not for $k-1$ terms. The process will follow through but we won't be able to determine C, if we assume that $|\alpha_i|_{\mathcal{P}} \le 1$ for some i by this method.

Proof of Theorem 2.8. By Lemma 3.1, it is enough to prove the assertion for $\mathbb{Q}_p$ for every prime number p.

Let p be a given prime number. Assume that α_1 is not integral over $\mathbb{Z}_p$ and K be the Galois closure of $\mathbb{Q}_p(\alpha_1)$. All the other Galois conjugates of α_1 are $\alpha_2, \ldots, \alpha_k$ for some integer k. It is also enough to prove the case when $b_3 = b_4 = \cdots = b_k = 0$ and the proof for the general case follows verbatim.

Assume that α_1 is not integral over $\mathbb{Z}_p$ (and so is α_2). For simplicity, we write $\alpha_1 = \alpha$ and $\alpha_2 = \beta$. Then α^{-1} and β^{-1} are integral over $\mathbb{Z}_p$ and let the characteristic polynomial $f_{K|\mathbb{Q}_p}(x) := f(x)$ of α^{-1} satisfies the assertion in Lemma 3.2. Since β is a Galois conjugate of α, we see that the characteristic polynomial of β^{-1} is $f(x)$ itself. Write the unique maximal ideal $p\mathbb{Z}_p$ of $\mathbb{Z}_p$ by $\mathfrak{P}$.

If $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$, then $f(\alpha^{-1}) = 0$ and $f(\beta^{-1}) = 0$. Hence we get

$$a_0 + a_1\alpha^{-1} + \cdots + a_{d-1}\alpha^{-d+1} + \alpha^{-d} = 0 = a_0 + a_1\beta^{-1} + \cdots + a_{d-1}\beta^{-d} \tag{5.2}$$

Then, for any integer $\ell \ge 0$, multiplying by $\alpha^{d+\ell}$ both sides of (5.2), we get

$$\alpha^{\ell} = -a_{d-1}\alpha^{\ell+1} - \cdots - a_0\alpha^{d+\ell} \text{ with } a_i \in \mathfrak{P} \tag{5.3}$$

and

$$\beta^{\ell} = -a_{d-1}\beta^{\ell+1} - \cdots - a_0\beta^{d+\ell} \text{ with } a_i \in \mathfrak{P} \tag{5.4}$$

by Lemma 3.2. Now, for any integer $\ell \ge 0$, let M_ℓ be a $\mathbb{Z}_p$-submodule of K spanned by $b_1\alpha^{\ell+1} + b_2\beta^{\ell+1}, \ldots, b_1\alpha^{\ell+d} + b_2\beta^{\ell+d}$. By Lemma 3.3, it is clear that M_ℓ is a non-zero $\mathbb{Z}_p$-submodule of K. Hence, by (5.3) and (5.4), we have

$$b_1\alpha^{\ell} + b_2\beta^{\ell} \in \mathfrak{P}M_\ell \text{ for any integer } \ell \ge 0. \tag{5.5}$$

Note that for any nonnegative integers ℓ_1 and ℓ_2, we have

$$M_{\ell_1} \subset M_{\ell_2} \text{ whenever } \ell_1 < \ell_2. \tag{5.6}$$

It is enough to prove that for $\ell_1 = \ell$, $\ell_2 = \ell + 1$, we have $b_1\alpha^{\ell+1} + b_2\beta^{\ell+1} \in M_{\ell_2}$ (and then inductively we can get the general assertion). Since $f(\alpha^{-1}) = 0 = f(\beta^{-1})$, multiplying by $\alpha^{\ell+1+d}$ on both sides, similarly $\beta^{\ell+1+d}$ we get $b_1\alpha^{\ell+1} + b_2\beta^{\ell+1} \in M_{\ell_2}$, as desired.

Now we claim that for any integer $\ell \ge 0$ and any integer $m \ge 0$, we have

$$b_1\alpha^{\ell} + b_2\beta^{\ell} \in \mathfrak{P}^{m+1}M_{\ell+dm}. \tag{5.7}$$

Let ℓ be any nonnegative integer and $m = 0$. Then (5.7) is true by (5.5). Hence, we shall assume that (5.7) holds true for ℓ and for some integer $m \ge 1$. That is, we have $b_1\alpha^{\ell} + b_2\beta^{\ell} \in \mathfrak{P}^{m+1}M_{\ell+dm}$

and we prove (5.7) holds true for ℓ and $m+1$. For any integer i with $\ell+dm+1 \leq i \leq \ell+d(m+1)$, we have $b_1\alpha^i + b_2\beta^i \in M_{\ell+dm}$. By (5.5) and (5.6), we get

$$b_1\alpha^i + b_2\beta^i \in \mathfrak{P}M_i \subset \mathfrak{P}M_{\ell+d(m+1)} \text{ for all integers } i \text{ with } \ell+dm+1 \leq i \leq \ell+d(m+1)$$

and hence we get

$$M_{\ell+dm} \subset \mathfrak{P}M_{\ell+d(m+1)}. \tag{5.8}$$

Since, by the induction hypothesis, we have $b_1\alpha^\ell + b_2\beta^\ell \in \mathfrak{P}^{m+1}M_{\ell+dm}$, by (5.8), we arrive at

$$b_1\alpha^\ell + b_2\beta^\ell \in \mathfrak{P}^{m+2}M_{\ell+d(m+1)}$$

as desired.

Now to finish the proof, we take $\ell = 0$ and $m = v_p((b_1+b_2)d)$. By hypothesis, we know that $\mathrm{Tr}_{K|\mathbb{Q}_p}(M_{a-d}) \subset \mathbb{Z}_p$ for all integers $a \leq [d\log_2((b_1+b_2)d)] + 1$. Since $dm < d\log_2((b_1+b_2)d)+1$, we get $\mathrm{Tr}_{K|\mathbb{Q}_p}(M_{dm}) \subset \mathbb{Z}_p$. Therefore, since $b_1+b_2 = b_1\alpha^0 + b_2\beta^0 \in \mathfrak{P}^{m+1}M_{dm}$, we see that $(b_1+b_2)d = \mathrm{Tr}_{K|\mathbb{Q}_p}(b_1\alpha^0+b_2\beta^0) \in \mathrm{Tr}_{K|\mathbb{Q}_p}(\mathfrak{P}^{m+1}M_{dm}) \subset \mathbb{Z}_p$. Therefore, we get, $(b_1+b_2)d \in \mathfrak{P}^{m+1}$ which implies that the power of p dividing $(b_1+b_2)d$ is at least $m+1$, a contradiction. Hence the theorem. □

6. Proof of Theorem 2.10

Suppose not. Then the set $\mathfrak{S}$ of positive integers n such that

$$\mathrm{Tr}_{L/\mathbb{Q}}((q\lambda_1\alpha_1^n + \cdots + q\lambda_k\alpha_k^n)/p) = \sum_{i=1}^{k} \sum_{\sigma\in\mathrm{Gal}(L/\mathbb{Q})} (q/p)\sigma(\lambda_i)\sigma(\alpha_i) = 1 \tag{6.1}$$

is infinite. By the equivalence relation given by (2.1), we have the partition

$$\{\sigma(\alpha_i) : 1 \leq i \leq k, \sigma \in \mathrm{Gal}(L/\mathbb{Q})\} = \bigcup_{j=1}^{s} S_j.$$

Furthermore, corresponding to each S_j, we define an index set I_j consisting of the indices (j,σ) such that $\sigma(\alpha_j) \in S_j$. We select $\beta_{(j,\sigma)} \in S_j$ to be a representative of this class. Therefore for $\sigma(\alpha_j) \in S_j$, we write $\sigma(\alpha_j) = \beta_j\zeta_h^{\omega_a}$. Consequently, the above relation can be re-written as

$$\sum_{j=1}^{s} \sum_{(j,\sigma)\in T_j} (q/p)\sigma(\lambda_j)\sigma(\alpha_j)^n = 1$$

for all but finitely many n, where $\lambda_j \in L$. Therefore, for each residue class $a \mod h$ which appears infinitely many times in $\mathfrak{S}$, we have a new equation of the form

$$\sum_{i=1}^{s'} \lambda_j''\beta_j^m = 1,$$

holds for infinitely many n of the form $n = a + mh$, where $s' \leq s$ and none of λ_j'' is zero. Now we claim that each β_i is a root of unity. If not, then there exists a place ω such that

$$M = \max\{|\beta_i|_\omega : 1 \leq i \leq s'\} > 1.$$

Choose a finite subset S of places on L that contains all the archimedean places such that λ_i'' and β_i's are S-units. We apply Theorem 3.1 with an appropriate choice of ϵ (with the help of the lower bound of M), and then by Proposition 3.1, we get a contradiction. Thus we conclude that each β_i

is a root of unity, which in turn implies that α_i's are the root of unity. This leads to a contradiction and hence the theorem.

Acknowledgments. This work is part of the SERB-MATRICS project and the last author is thankful to the SERB, India.

References

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

[2] P. Corvaja and U. Zannier, On the rational approximation to the powers of an algebraic number: Solution of two problems of Mahler and Mendes France, *Acta Math.*, **193** (2004), 175–191.

[3] P. Fatou, Sur les séries entières à coefficients entiers. *C. R. Acad. Sci.*, Paris 138, 342–344 (1904).

[4] B. de Smit, Algebraic numbers with integral power traces, *J. Number Theory* **45** (1) (1993) 112–116.

[5] A. Kulkarni, N. Mavraki and K. D. Nguyen, Algebraic approximations to linear combinations of powers: An extension of results by Mahler and Corvaja-Zannier, *Trans. Amer. Math. Soc.*, **371** (6) (2019) 3787–3804.

[6] I. G. Macdonald, Symmetric functions and Hall polynomials. With contributions by A. V. Zelevinsky. *Oxford University Press* (1998)

[7] P. Philippon and P. Rath, A note on trace of powers of algebraic numbers, *J. Number Theory*, **219** (2021), 198–211.

[8] C. Pisot, La répartition modulo 1 et les nombres algébriques. *Ann. Sc. Norm. Super. Pisa, II. Ser.* 7, 205–248 (1938)

[9] G. Polya, Über ganzwertige ganze Funktionen, *Rend. Circ Mat. Palermo*, **40** (1915), 1–16.

[10] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Math., **1467**, (Springer, Berlin, 1991).

[11] U. Zannier, *Some Applications of Diophantine Approximation to Diophantine Equations* (with special emphasis on the Schmidt Subspace Theorem), (Forum, Udine, 2003).

(Abhishek Bharadwaj) Department of Mathematics, Jeffery Hall, 99 University Avenue, Queen's University, Kingston, Ontario, K7L 3N6, Canada

(Aprameyo Pal and R. Thangadurai) Harish-Chandra Research Institute, HBNI, Chhatnag Road, Jhunsi, Prayagraj 211019, India.

(Veekesh Kumar) National Institute of Science Education and Research Bhubaneswar, HBNI, P.O. Jatni, Khurda 752050, Odisha, India

Email address, Abhishek Bharadwaj: `atb4@queensu.ca`

Email address, Aprameyo Pal: `aprameyopal@hri.res.in`

Email address, Veekesh Kumar: `veekeshiitg@gmail.com`

Email address, R. Thangadurai: `thanga@hri.res.in`