S. Das, R. Thangadurai *Res Math Sci_####################_*
https://doi.org/10.1007/s40687-026-00616-z

Research in the Mathematical Sciences

RESEARCH

PV number as a completely normal basis generator of finite abelian extensions or dihedral extensions of number fields

Sudipa Das and R. Thangadurai

*Correspondence:
sudipadas@hri.res.in
Harish-Chandra Research Institute, A CI of Homi Bhabha National Institute, Chhatnag Road, Jhunsi, Prayagraj 211019, India

Abstract

For a given finite extension K over $\mathbb{Q}$, let L/K be a finite Galois extension with Galois group G. Then, by the normal basis theorem, there exists $\alpha \in L$ such that $L = K[G] \cdot \alpha$, where $K[G]$ is the group ring. Such an element α is called a normal basis generator. We say $\alpha \in L$ is a completely normal basis generator, if α is a normal basis generator for L/F for every intermediate field F such that $K \subset F \subset L$. In this article, we prove the following result. Let L/K be a finite Galois extension of number fields with Galois group G. If $L \subset \mathbb{R}$ and G is an abelian group or dihedral group, then there exists a Pisot–Vijayaraghavan number $\alpha \in L$ such that for any natural number m, α^m is a primitive element as well as a completely normal basis generator of L/K. As an application of our result, we prove the following upper bound for the index, when $L = K$ and $K = \mathbb{Q}$ in the above result, to get

$$[\mathcal{O}_K : \mathbb{Z}[G] \cdot \alpha] \leq \left(\tau^{n-1} |d_K|^{\frac{1}{2}-\frac{1}{2n}} + 1\right)^n$$

where $n = [K : \mathbb{Q}]$, $\tau = \phi(n)n > 1$ when G is abelian and $\tau = n + 1$ when G is dihedral group of order n. We also classify the extension of prime degree related to this. We use resolvents and technique from geometry of numbers.

Keywords: Normal basis generator, Pisot–Vijayaraghavan numbers, Primitive elements, Galois theory

Mathematics Subject Classification: Primary 11R32, Secondary 12F10

1 introduction

For a finite Galois extension L/K of number fields with Galois group G, consider the group ring $K[G]$. It is well known that there exists an element $\alpha \in L$ such that $L = K[G] \cdot \alpha$; in other words, $\{\sigma(\alpha) : \sigma \in G\}$ form a K-basis for L and such an element α is called a *normal basis generator* of L/K. This is known as *normal basis theorem* and can be seen in any Galois theory textbook. This theorem was first proved by E. Noether and Deuring in 1932. For more information, we shall refer [18] and [23]. For example, if $L = \mathbb{Q}(\zeta_n)$, the n-th cyclotomic field for an odd square-free natural number $n \geq 3$, then $L = \mathbb{Q}[(\mathbb{Z}/n\mathbb{Z})^*] \cdot \zeta_n$, and hence, ζ_n is a normal basis generator of L.

© The Author(s), under exclusive licence to Springer Nature Switzerland AG 2026.

Journal: 40687 Article No.: 0616 TYPESET DISK LE CP Disp.:2026/3/16 Pages: 15 Layout: BMC-OneCol

An element $\alpha \in L$ is said to be a *completely normal basis generator* for L/K, if it is a normal basis generator of L/F for every intermediate field F such that $K \subset F \subset L$. So, it is still an interesting problem to know whether some special type of algebraic number (or algebraic integer) can be a completely normal basis generator for a given finite Galois extension L/K. In 1957, C. C. Faith [9] proved that every finite Galois extension L of an infinite field K contains a completely normal basis generator. D. Hachenberger [15] provided explicit constructions of completely normal elements in prime power cyclotomic fields over $\mathbb{Q}$.

A real algebraic integer $\alpha > 1$ is said to be a *Pisot–Vijayaraghavan* number (or, in short, PV number), if $\beta \neq \alpha$ is a Galois conjugate of α, then $|\beta| < 1$. For example, any integer $m > 1$ is a PV number of degree 1, and it is known that there exists a PV number of degree d for any given natural number $d \geq 1$. For more information, we refer to [8] and [25]. The PV numbers are the only class of algebraic numbers whose powers go very close to an integer. This can be seen in the results of P. Corvaja and U. Zannier [5] and P. Philippon and P. Rath [24]. In the following results, we shall give a class of number fields that admits a PV number as its primitive element and as a completely normal basis generator.

Theorem 1.1 *Let L/K be a finite Galois extension of number fields with Galois group G and $L \subset \mathbb{R}$. If G is an abelian group, then there exists a Pisot–Vijayaraghavan number $\alpha \in L$ such that for any natural number m, α^m is a primitive element as well as a completely normal basis generator of L/K.*

Theorem 1.2 *Let L/K be a finite Galois extension of number fields with Galois group G, dihedral group of order $2n$ for some natural number n. Suppose $L \subset \mathbb{R}$ and $L \cap K(\zeta_n) = K$, where ζ_n is a primitive n-root of unity. Then, there exists a Pisot–Vijayaraghavan number $\alpha \in L$ such that for any natural number m, α^m is a primitive element as well as a completely normal basis generator of L/K.*

In order to prove Theorems 1.1 and 1.2, we first prove a characterization for a normal basis generator in terms of resolvent (idempotents for G is abelian), which we discuss in §2.1. When we specialize resolvent for a trivial character, we get the trace element. So, a related question is as follows. *For what finite Galois extensions L/K of fields, an element $\alpha \in L$ of degree $[L : K]$ is a normal basis generator of L/K if and only if its trace $\mathrm{Tr}_{L/K}(\alpha) \neq 0$?*. When K is a field of characteristic p, for a prime number p, in 1981, Childs and Orzech [2] proved that for a Galois extension L/K of degree p^n, *an element $\alpha \in L$ is a normal basis generator if and only if* $\mathrm{Tr}_{L/K}(\alpha) \neq 0$. For the number field set up, we prove the following.

Theorem 1.3 *Let $K/\mathbb{Q}$ be a number field and L/K be a finite Galois extension of degree p for a prime number $p \geq 3$ with Galois group G such that $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$. If $\alpha \in L$ such that $L = K(\alpha)$ and $\mathrm{Tr}_{L/K}(\alpha) \neq 0$, then $L = K[G] \cdot \alpha$.*

In order to prove Theorem 1.3, we take the following approach.

Definition 1.1 Let K be a number field and α be an algebraic element over K. Let $f(X) \in K[X]$ be the minimal polynomial of α over K. Let $\Omega_\alpha = \{\alpha_1, \ldots, \alpha_n\}$ be the set of all Galois conjugates of α over K. We say that Ω_α is K-trivial, if $c_1\alpha_1 + \cdots + c_n\alpha_n = 0$ for some $c_i \in K$, we necessarily have $c_1 = c_2 = \cdots = c_n$.

uncorrected proof

Then we prove the following.

Theorem 1.4 *Let L/K be a finite Galois extension of number fields of degree n for some natural number n such that $L = K(\alpha)$ and $f(X) \in K[X]$ is the minimal polynomial of α. Then Ω_α is K-trivial if and only if $n = p$ a prime number and $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$.*

The converse of Theorem 1.4 was proved by V. A. Kurbatov [21] in 1977. We give a representation theoretic proof of his result and prove the other implication.

Since $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$ in the hypothesis of Theorem 1.3, by Theorem 1.4, we see that Ω_α is K-trivial. Since by hypothesis $\mathrm{Tr}(\alpha) \neq 0$, we get $L = K[G] \cdot \alpha$, which proves Theorem 1.3.

Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group G and $\mathcal{O}_K$ be its ring of integers. An element $\alpha \in \mathcal{O}_K$ is said to be a *normal integral basis generator* if α is a free generator of $\mathcal{O}_K$ as a $\mathbb{Z}[G]$ module, that is, $\mathcal{O}_K = \mathbb{Z}[G] \cdot \alpha$. By Hilbert–Speiser theorem (see, for instance, [16]), it is known that if G is abelian, then $K/\mathbb{Q}$ admits a normal integral basis if and only if it is a tamely ramified extension. If G is non-abelian, and $K/\mathbb{Q}$ admits a normal integral basis, then it must be tamely ramified extension. However, tameness is not sufficient.

Suppose $K = \mathbb{Q}[G] \cdot \alpha$ for some $\alpha \in K$ (by normal basis theorem). We need to know the ring of integers $\mathcal{O}_K$ is how far away being from a normal integral basis generator, that is, $\mathcal{O}_K = \mathbb{Z}[G] \cdot \alpha$. One way to measure this is to calculate the index $[\mathcal{O}_K : \mathbb{Z}[G] \cdot \alpha]$. By the application of Theorem 1.1, we observe the following.

Theorem 1.5 *Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group G and $K \subset \mathbb{R}$ such that G is abelian, or dihedral group. Let a PV number $\alpha \in \mathcal{O}_K$ be a normal basis generator of $K/\mathbb{Q}$. Let d_K be the discriminant of K such that $|d_K| \geq (1+\phi(n)^{-1})^{2n}$ where $n = [K : \mathbb{Q}]$. Then, the index*

$$[\mathcal{O}_K : \mathbb{Z}[G] \cdot \alpha] \leq \left(\tau^{n-1}|d_K|^{\frac{1}{2}-\frac{1}{2n}} + 1\right)^n$$

where

$$\tau = \begin{cases} \phi(n)n, & \text{when } G \text{ is abelian} \\ n+1, & \text{when } G = D_n \end{cases}.$$

Corollary 1.1 *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field where $d > 1$ is a square-free integer. Let $\alpha \in \mathcal{O}_K$ be normal basis generator of $K/\mathbb{Q}$ such that α is a PV number. If $d_K \geq 2^4$, then the index*

$$[\mathcal{O}_K : \mathbb{Z}[G] \cdot \alpha] \leq (2|d_K|^{\frac{1}{4}} + 1)^2.$$

For example, if $d > 1$ is a square-free integer and $K = \mathbb{Q}(\sqrt{d})$. Then, $\alpha = [\sqrt{d}]+1+\sqrt{d}$ and its Galois conjugate $[\sqrt{d}] + 1 - \sqrt{d}$. Thus, both are positive real numbers and α is a normal basis generator of K over $\mathbb{Q}$ (and hence α is a PV number). Therefore, by Corollary 1.1, we conclude that

$$[\mathcal{O}_K : \mathbb{Z}[G] \cdot \alpha] \leq (2d_K^{\frac{1}{4}} + 1)^2.$$

uncorrected proof

In the literature, the following results are dealing with group index. In 2022, Del Corso et al., ([4]) proved the following. *Let $K/\mathbb{Q}$ be a finite abelian extension and p be any given prime. Let $p^n d$ be the ramification index of a prime ideal lying above p where $n \geq 0$ is an integer and d is an integer coprime to p. Then, exact power of the prime p dividing (denoted by v_p) the index*

$$v_p\left(\min_{\alpha\in\mathcal{O}_K}[\mathcal{O}_K : \mathbb{Z}[G]\cdot\alpha]\right) = \frac{[K:\mathbb{Q}](p^n-1)}{p^n(p-1)}.$$

In 2024, H. Johnston and A. Torzewski [19] proved an upper bound for the index in a general setting and a particular case is as follows. *Let K be a finite Galois extension over $\mathbb{Q}$ with Galois group G, and let k be a positive integer. Then, there exists a positive integer i that is coprime to k satisfies the following property: There exists $\alpha \in \mathcal{O}_K$ such that the index $[\mathcal{O}_K : \mathbb{Z}[G]\cdot\alpha]$ divides*

$$i \cdot |G|^{\lceil 3|G|/2\rceil}.$$

In the same paper [19], they also prove the following result. *Let K be a finite Galois extension over $\mathbb{Q}$ with Galois group G. Suppose $n_1, n_2, \ldots, n_t$ are positive integers such that $\mathbb{Q}[G] \simeq \prod_{i=1}^{t} \mathrm{Mat}_{n_i}(\mathbb{Q})$. Then, there exists $\alpha \in \mathcal{O}_K$ such that the index $[\mathcal{O}_K : \mathbb{Z}[G]\cdot\alpha]$ divides*

$$\left(|G|^{|G|}\prod_{i=1}^{t} n_i^{-n_i^2}\right)^{3/2}.$$

2 Preliminaries

2.1 Criterion for a normal basis generator

Let L/K be a finite Galois extension of number fields with Galois group G of cardinality n. Let $\chi : G \to \mathbb{C}^\times$ be an complex irreducible character of G. Then, for a given number field K, we have $\chi : G \to K(\zeta_n)$ where ζ_n is a primitive n-th root of unity.

Let $\mathcal{G}$ be the Galois group of $K(\zeta_n)/K$. If $\sigma \in \mathcal{G}$, then $\sigma \circ \chi : G \to K(\zeta_n)$ is called *K-conjugate character* of χ. Then, it is known (see, for instance, [17], Page 546 and [13]), there is a unique character $\hat{\chi} = \kappa(\chi_1 + \cdots + \chi_c)$ of G, which is K-irreducible (a character which takes values in K and indecomposable as a character over K is called K-irreducible) containing χ where χ_i's are K-conjugate characters of χ, and κ is the Schur index of χ (We recall the definition of Schur index (see [6] and [17], Page 546) as follows. *Let L/K be a finite Galois extension of number fields with Galois group G. Let ρ be a complex irreducible representation of G and χ be its associated character. Then, the Schur index of ρ is the minimum of the degrees $[F : K(\chi)]$, where $K(\chi)$ is the field extension of K generated by all the values of χ and F varies over all the field extensions of $K(\chi)$ such that ρ is realizable in F*). Note that when G is abelian, all the complex irreducible representations of G are one dimensional, and hence, the associated characters are same as their representations. Therefore, the representation corresponding to character χ can be realized in $K(\chi)$ itself. Hence, the Schur index is one.

uncorrected proof

Let Ψ be the set of all K-irreducible characters of G. Then, it is known that the induced character (or left regular character of $K[G]$-module $K[G]$) $\mathrm{Ind}_{\{id\}}^{G}(1) = \sum_{\psi\in\Psi} n_\psi \psi$ where $n_\psi \geq 1$.

Abelian Case. Let L/K be a finite Galois extension of number fields with Galois group G. Then, the group ring $K[G]$ is semisimple, by Maschke's Theorem (see Theorem 10.8, Page 41 in [6]). If G is abelian, then $n_\psi = 1$ for all $\psi \in \Psi$, and hence, it has a unique decomposition into simple $K[G]$-submodules, namely

$$K[G] = \bigoplus_{\psi\in\Psi} K[G]\cdot\varepsilon_\psi, \tag{2.1}$$

where ε_ψ is the idempotent element in $K[G]$ and defined as

$$\varepsilon_\psi = \frac{1}{|G|}\sum_{\sigma\in G}\psi(\sigma^{-1})\sigma \in K[G].$$

It is known that for $\psi \neq \psi'$ two K-irreducible characters of G, the idempotents ε_ψ and $\varepsilon_{\psi'}$ are mutually orthogonal. We shall prove the following. (K. Girstmair [14] stated this without proof. Compare a similar result in [20]).

Proposition 2.1 *Let L/K be a finite Galois extension of number fields with abelian Galois group G. If $\alpha \in L$ such that*

$$\varepsilon_\psi(\alpha) \neq 0 \text{ for all } \psi \in \Psi,$$

then $L = K[G]\cdot\alpha$.

Proof Let $\alpha \in L$ such that $\varepsilon_\psi(\alpha) \neq 0$ for all $\psi \in \Psi$. Since L/K is a finite Galois extension with abelian group G of number fields, by the normal basis theorem and by (2.1), there exists $\beta \in L$ such that

$$L = K[G]\cdot\beta = \bigoplus_{\psi\in\Psi} K[G]\cdot\varepsilon_\psi(\beta). \tag{2.2}$$

Let $\Psi = \{\psi_1, \ldots, \psi_h\}$, by assuming $|\Psi| = h$ and let $\varepsilon_i = \varepsilon_{\psi_i}$ for all $i = 1, 2, \ldots, h$. Then for any $i = 1, 2, \ldots, h$, since $K[G]\cdot\varepsilon_i(\alpha) \subset L$, by (2.2), we have $\varepsilon_i(\alpha) = \sum_{j=1}^{h}\lambda_j\varepsilon_j(\beta)$ where $\lambda_j \in K[G]$. Then, by applying ε_i on both sides, we get $\varepsilon_i^2(\alpha) = \sum_{j=1}^{h}\lambda_j\varepsilon_i\varepsilon_j(\beta)$. Since ε_i is an idempotent and for $i \neq j$, ε_i is orthogonal to ε_j, we arrive at $\varepsilon_i(\alpha) = \lambda_i\varepsilon_i(\beta)$. Therefore, $K[G]\cdot\varepsilon_\psi(\alpha) \subset K[G]\cdot\varepsilon_\psi(\beta)$ for every $\psi \in \Psi$. Since $K[G]\cdot\varepsilon_\psi(\beta)$ is a simple $K[G]$-module and $\varepsilon_\psi(\alpha) \neq 0$ for all $\psi \in \Psi$, we must have $K[G]\cdot\varepsilon_\psi(\alpha) = K[G]\cdot\varepsilon_\psi(\beta)$ for all $\psi \in \Psi$, and hence, we conclude that $L = K[G]\cdot\alpha$. Thus, α is a normal basis generator of L. □

General Case. When G is a non-abelian group, we consider the following approach.

uncorrected proof

Let L/K be a finite Galois extension of number fields with Galois group G. For any complex representation ρ on G with its associated character χ, the *Fröhlich-Lagrange resolvent* (see Page 29 of [12], or/and Page 575 of [1]) of $\alpha \in L$ attached χ as

$$\langle \alpha | \chi \rangle_{L/K} = \det\left(\sum_{\sigma \in G} \sigma^{-1}(\alpha)\rho(\sigma)\right),$$

where $\det(A)$ denotes the determinant of a square matrix A. For more clarity, for each $\sigma \in G$ we write the matrix representation of $\rho(\sigma)$ as

$$\rho(\sigma) = (\rho_{ij}^{\sigma})_{1 \le i,j \le n}.$$

Then, $\sum_{\sigma \in G} \sigma^{-1}(\alpha)\rho(\sigma)$ is a matrix whose ij-th entry is $\sum_{\sigma \in G} \sigma^{-1}(\alpha)\rho_{ij}^{\sigma}$ for all $1 \le i, j \le n$. Hence, the resolvent is the determinant of the following matrix:

$$\langle \alpha | \chi \rangle_{L/K} = \det \begin{pmatrix} \sum_{\sigma \in G} \sigma^{-1}(\alpha)\rho_{11}^{\sigma} & \sum_{\sigma \in G} \sigma^{-1}(\alpha)\rho_{12}^{\sigma} & \cdots & \sum_{\sigma \in G} \sigma^{-1}(\alpha)\rho_{1n}^{\sigma} \\ \sum_{\sigma \in G} \sigma^{-1}(\alpha)\rho_{21}^{\sigma} & \sum_{\sigma \in G} \sigma^{-1}(\alpha)\rho_{22}^{\sigma} & \cdots & \sum_{\sigma \in G} \sigma^{-1}(\alpha)\rho_{2n}^{\sigma} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{\sigma \in G} \sigma^{-1}(\alpha)\rho_{n1}^{\sigma} & \sum_{\sigma \in G} \sigma^{-1}(\alpha)\rho_{n2}^{\sigma} & \cdots & \sum_{\sigma \in G} \sigma^{-1}(\alpha)\rho_{nn}^{\sigma} \end{pmatrix}.$$

Then we have the following result (see, for instance, A. Fröhlich [10], Corollary 3.2., [11], Page 187 and [12]).

Proposition 2.2 *Let L/K be a finite Galois extension of number fields with Galois group G. Then, an element $\alpha \in L$ is a normal basis generator of L over K if and only if the resolvant $(\alpha|\chi)_{L/K} \neq 0$ for all K-irreducible character χ of G.*

When G is abelian, $\langle \alpha | \psi \rangle_{L/K} \neq 0$ implies $\varepsilon_{\psi}(\alpha) \neq 0$ for every K-irreducible character ψ of G and hence Proposition 2.2 implies Proposition 2.1.

Suppose G is dihedral group of order $2n$ for some natural number n. It is well known that (we refer to J. P. Serre [26]) the complex irreducible representations of D_{2n} are either dimension 1 or of dimension 2. We assume the presentation of

$$G = \langle r, s \mid r^n = s^2 = 1, srs = r^{-1} \rangle.$$

Case 1. Representations of dimension 1.

Suppose n is even. There are 4 representations ψ_i of dimension 1, which are given by the table.

	r^k	sr^k
ψ_1	1	1
ψ_2	1	-1
ψ_3	$(-1)^k$	$(-1)^k$
ψ_4	$(-1)^k$	$(-1)^{k+1}$

Uncorrected Proof

Suppose n is odd. Then, there are two representations ψ as follows.

	r^k	sr^k
ψ_1	1	1
ψ_2	1	-1

Case 2. Irreducible representations of dimension 2

The irreducible representations of dimension 2 are as follows. All the non-isomorphic representations of dimension 2 are given by φ_h for each integer h satisfying $1 \leq h < n/2$ and defined by

$$\varphi_h(r^k) = \begin{pmatrix} \omega^{hk} & 0 \\ 0 & \omega^{-hk} \end{pmatrix}$$

and

$$\varphi_h(sr^k) = \begin{pmatrix} 0 & \omega^{-hk} \\ \omega^{hk} & 0 \end{pmatrix}$$

where ω is a primitive n-th root of unity.

We need the following result due to K. Girstmair.

Theorem 2.1 (K. Girstmair [13]) *Let $K(\alpha)$ be a finite Galois extension of K with Galois group G. Let $f(X) \in K[X]$ be the minimal polynomial of α over K. Then, Ω_α is K-trivial if and only if the character $\psi = \rho - 1$ of G is K-irreducible, where ρ is the character associated with the left regular $K[G]$-module $K[G]$.*

2.2 Existence of PV number as a primitive element

Let $K/\mathbb{Q}$ be a number field of degree n and $\mathcal{O}_K$ be the ring of integers of K. Then it is well known that there are precisely $n = r_1 + 2r_2$ embeddings of K into $\mathbb{C}$. Among them, there are precisely r_1 number of real embeddings of K, say, $\sigma_1, \ldots, \sigma_{r_1}$ and r_2 number of complex embeddings, say, $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$, up to conjugation. Note that $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$ for all $j = 1, 2, \ldots, r_2$. For a nonzero fractional ideal $\mathcal{I}$ of K, we denote the norm of the fractional ideal as $N(\mathcal{I})$ and note that $N(\mathcal{O}_K) = 1$; the discriminant of $K/\mathbb{Q}$ by d_K. We need the following theorem of Minkowski [23].

Theorem 2.2 *Let $K/\mathbb{Q}$ be a number field of degree $n = r_1 + 2r_2$ where r_1 is the number of real embeddings of K and r_2 is the number of distinct complex embeddings of K. Let $\mathcal{I}$ be a nonzero fractional ideal in K. Suppose there are positive constants $c_1, \ldots, c_{r_1+r_2}$ satisfying*

$$\prod_{i=1}^{r_1+r_2} c_i > \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d_K|} N(\mathcal{I}).$$

Then, there exists a nonzero element $\alpha \in \mathcal{I}$ satisfying

$$|\sigma_i(\alpha)| < c_i \text{ for } 1 \leq i \leq r_1, \text{ and } |\sigma_{r_1+j}(\alpha)|^2 < c_{r_1+j} \text{ for } 1 \leq j \leq r_2.$$

We first prove the following general theorem.

uncorrected proof

Theorem 2.3 *Let $K/\mathbb{Q}$ be a number field such that $K \subset \mathbb{R}$ and $\tau > 1$ be a given real number. Then, there exists a PV number $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$ and for any non-trivial embedding $\sigma : K \to \mathbb{C}$, we have $|\sigma(\alpha)| < \tau^{-1}$.*

Proof Given that $K \subset \mathbb{R}$ is a number field of degree $n = r_1 + 2r_2$. Therefore, the identity embedding of K is a real embedding and we denote it by σ_1. Choose positive real numbers $c_1, c_2, \ldots, c_{r_1+r_2}$ such that $c_1 > 1$, $c_j < \frac{1}{\tau}$ for $j = 2, 3, \ldots, r_1$, $c_{r_1+j} < \frac{1}{\tau^2}$ for $j = 1, 2, \ldots, r_2$ and satisfying

$$\prod_{i=1}^{r_1+r_2} c_i > \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d_K|} N(\mathcal{O}_K) = \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d_K|}.$$

Then by Theorem 2.2, there exists a nonzero element $\beta \in \mathcal{O}_K$ satisfying

$$|\sigma_i(\beta)| < c_i \text{ for } 1 \le i \le r_1, \text{ and } |\sigma_{r_1+j}(\beta)|^2 < c_{r_1+j} \text{ for } 1 \le j \le r_2.$$

Since $\beta \in \mathcal{O}_K \backslash \{0\}$, we conclude that $N(\beta) \in \mathbb{Z}\backslash\{0\}$. Thus, we get

$$1 \le |N(\beta)| = \prod_{i=1}^{r_1+2r_2} |\sigma_i(\beta)| = |\sigma_1(\beta)| \prod_{i=2}^{r_1} |\sigma_i(\beta)| \prod_{i=1}^{r_2} |\sigma_{r_1+i}(\beta)|^2,$$

Since $|\sigma_i(\beta)| < 1/\tau$ for all $i = 2, 3, \ldots, r_1$ and $|\sigma_{r_1+j}(\beta)|^2 < 1/\tau^2$ for all $j = 1, 2, \ldots, r_2$, we must have $|\sigma_1(\beta)| = |\beta| > 1$ as $N(\beta) \ge 1$. Rest of the Galois conjugates of β satisfies $|\sigma_j(\beta)| < 1/\tau < 1$. Therefore, we conclude that $\beta \in \mathcal{O}_K$ is of degree n. Let

$$\alpha = \begin{cases} \beta & ; \text{ if } \beta > 0 \\ -\beta & ; \text{ if } \beta < 0. \end{cases}$$

Then, $\alpha > 1$ and all its other conjugates $|\sigma_i(\alpha)| < 1$ for all $i > 1$. Hence, α is a PV number in K with $K = \mathbb{Q}(\alpha)$ and $|\sigma(\alpha)| < \tau^{-1}$ for every non-trivial embedding of K. □

Lemma 2.1 *Let $K/\mathbb{Q}$ be a number field and L/K be a finite Galois extension with Galois group G such that $L \subset \mathbb{R}$ and let $\tau > 1$ be a given real number. Then, there exists a PV number $\alpha \in L$ such that $L = K(\alpha^m)$ for any natural number $m \ge 1$ and for any non-trivial element $\sigma \in G$, we have $|\sigma(\alpha^m)| < \frac{1}{\tau^m}$.*

Proof By Theorem 2.3, we know that $L = \mathbb{Q}(\alpha)$, and hence, $L = K(\alpha)$ for some PV number α and $|\sigma(\alpha)| < \frac{1}{\tau}$ for any non-trivial $\sigma \in G$. Therefore, for any natural number m and for any non-trival element $\sigma \in G$, we have $|\sigma(\alpha^m)| = |\sigma(\alpha)|^m < \frac{1}{\tau^m}$. So, to finish the proof, it is enough to prove that for any natural number m, the degree of α^m is the same as that of α over K.

Let the degree of $\alpha \in L$ over K be $d = [L : K]$ and $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ be all the Galois conjugates of α. Suppose there exists m such that the degree of α^m is $< d$. Since the Galois conjugates of α^m over K are precisely $\alpha_1^m, \ldots, \alpha_d^m$ and the degree is $< d$, we must have $\alpha_i^m = \alpha_j^m$ for some $1 \le i \ne j \le d$. That means, $\alpha_i = \zeta\alpha_j$ for some m-th root of unity $\zeta \in L$. Then, by applying all $\sigma \in G$, we must get $\alpha_1 = \alpha = \zeta'\alpha_r$ for some $1 < r \le d$. Since $\alpha > 1$, we must have $|\alpha_r| > 1$, a contradiction, as α is a PV number. Hence, $\alpha_i^m \ne \alpha_j^m$ for any $i \ne j$ and hence the lemma. □

uncorrected proof

2.3 Primitive group action

For this section, we refer to a fine article by K. Conrad [3]. Let G be a finite group and let X be a non-empty set such that $|X| > 1$. We say G acts on X transitively, if for any given $x, y \in X$, there exists $g \in G$ such that $gx = y$; equivalently, this action has only one orbit.

For a given group action of G on X, we define *G-equivalence relation* on X as follows (see Definition 7.3 in [3]); $x \sim y \implies gx \sim gy$ for all $g \in G$ and $x, y \in X$.

This is an equivalence relation and the equivalence classes form a partition of X. Note that given any transitive group action of G on X, we have at least two G-equivalence relations, namely the equivalence relation having all of X as a single equivalence class and the equivalence relations whose equivalence classes are individual points of X.

A transitive action of G on X is said to be a *primitive action*, if there are no G-equivalence relations on X, other than the two equivalence relations of individual points and the whole set.

The following is a basic result that gives an equivalent criterion for an action to be primitive.

Theorem 2.4 [3] *Let G be a finite group and X be a set with $|X| > 1$. Then, the following statements are equivalent.*

(1) G acts on X primitively.
(2) For every $x \in X$, the stabilizer subgroup of x of G is a maximal subgroup of G.

We have the following observation.

Theorem 2.5 *Assume that $L = K(\alpha)$. Then, G acts on Ω_α primitively if and only if $|G| = [L : K] = |\Omega_\alpha| = n = p$, a prime number.*

Proof By Theorem 2.4, we see that G acts on Ω_α primitively if and only if the stabilizer subgroup of α of G must be a maximal subgroup of G. Since α is a primitive element of L, the only subgroup of G fixes α is the trivial subgroup. Hence, we conclude that G acts on Ω_α primitively if and only if $\{id\}$ is a maximal subgroup of G. Therefore, by Sylow's theorem, we further infer that G acts on Ω_α primitively if and only $|G| = p$, a prime number. Hence the theorem. □

3 Proof of Theorem 1.1

Given that L/K be a finite Galois extension of number fields with abelian Galois group G. Suppose $|G| = [L : K] = n$. Since $L \subset \mathbb{R}$, in Theorem 2.3 taking $\tau = \phi(n)[L : K]$, there exists a PV number $\alpha \in L$ such that $L = \mathbb{Q}(\alpha)$ and $|\sigma(\alpha)| < \dfrac{1}{\phi(n)[L : K]}$ for every non-trivial embedding of L into $\mathbb{C}$. Since $L = \mathbb{Q}(\alpha) \subset K(\alpha) \subset L$, we conclude that $L = K(\alpha)$. By Lemma 2.1, for any natural number m, we have $L = K(\alpha^m)$.

To complete the proof, it is enough to prove that $L = K[G] \cdot \alpha^m$ for any natural number m. However, it is enough to prove $m = 1$ as $\alpha^m > 1$ and $|\sigma(\alpha^m)| < \tau^{-m}$, by Lemma 2.1. By Proposition 2.1, it is enough to check that $\varepsilon_\psi(\alpha) \neq 0$ for all K-irreducible characters $\psi \in \Psi$ of G.

Uncorrected proof

Let $\psi \in \Psi$ be a K-irreducible character of G and ε_ψ be the corresponding idempotent element. To prove $\varepsilon_\psi(\alpha) \neq 0$, it is enough to prove $|G| \cdot |\varepsilon_\psi(\alpha)| \neq 0$. Let $G = \{\sigma_1, \ldots, \sigma_n\}$ with σ_1 is the trivial element and $n = [L : K]$. Consider

$$|G| \cdot |\varepsilon_\psi(\alpha)| = \left| \sum_{\sigma \in G} \psi(\sigma^{-1})\sigma(\alpha) \right| \geq |\psi(\sigma_1^{-1})| \cdot |\alpha| - |\psi(\sigma_2^{-1})| \cdot |\sigma_2(\alpha)| - \cdots - |\psi(\sigma_n^{-1})| \cdot |\sigma_n(\alpha)| \tag{3.1}$$

Since ψ is a K-irreducible character of G, then there exists a unique complex irreducible character χ of G such that $\psi = \chi_1 + \cdots + \chi_c$, where χ_i are the K-conjugate characters of χ and $c = [K(\zeta_n) : K]$ with $n = |G|$. Note that $\psi(\sigma_1^{-1}) = 1$ as σ_1 is the identity embedding. Therefore, for any $i \geq 2$, $\sigma_i \in G$, we see that

$$|\psi(\sigma_i^{-1})| \leq c = [K(\zeta_n) : K] \leq \phi(n) \tag{3.2}$$

where $\phi(n)$ denotes the Euler ϕ-function. Therefore by (3.1), (3.2) and $|\sigma_i(\alpha)| < 1/(\phi(n)[L : K])$ for every $i \geq 2$, we get

$$\begin{aligned} |G| \cdot |\varepsilon_\psi(\alpha)| &\geq |\alpha| - \phi(n)|\sigma_2(\alpha)| - \ldots - \phi(n)|\sigma_n(\alpha)| \\ &> \alpha - \frac{1}{[L : K]} - \ldots - \frac{1}{[L : K]} = \alpha - \frac{[L : K] - 1}{[L : K]} > 0, \end{aligned}$$

as $\alpha > 1$. Thus, $\varepsilon_\psi(\alpha) \neq 0$ for all $\psi \in \Psi$.

If F is an intermediate field such that $K \subset F \subset L$, then L/F is a Galois extension with the Galois group H (which is a subgroup of G). Then, H is abelian and $[F(\zeta_n) : F] \leq [K(\zeta_n) : K]$. Therefore, the same estimate in (3.1) holds for L/F with the same α. Hence, $L = F[H] \cdot \alpha$ and $L = F(\alpha)$ follows. □

4 Proof of Theorem 1.2

As in the proof of Theorem 1.1, it is enough to prove the assertion when $m = 1$.

By hypothesis, L/K is finite Galois extension with dihedral Galois group G of order $2n$ and $L \subset \mathbb{R}$. By choosing $\tau = 2n + 1 = |G| + 1 > 1$, by Theorem 2.3, we conclude that there exists a PV number $\alpha \in L$ such that $\alpha > 1$ and $|\sigma(\alpha)| < 1/\tau$ for every $1 \neq \sigma \in G$.

Also, by hypothesis, we know that $L \cap K(\zeta_n) = K$ for some ζ_n, a primitive n-th root of unity. Therefore, by Galois theory, the Galois group $G(LK(\zeta_n)/K(\zeta_n))$ of $LK(\zeta_n)$ is isomorphic to the Galois group of L/K through $\sigma \mapsto \sigma|_L$, restriction map, that is, $G(LK(\zeta_n)/K(\zeta_n)) \cong G(L/K) = G$, the dihedral group of order $2n$. Also, we know that if $\alpha \in L$ generates a normal basis for $LK(\zeta_n)/K(\zeta_n)$, then α is a normal basis generator for L/K. With all these reduction, it is enough to prove that the PV number $\alpha \in L$ is a normal basis generator for $LK(\zeta_n)/K(\zeta_n)$. By Proposition 2.2, it is enough to prove that

$$\langle \alpha | \chi \rangle = \langle \alpha \mid \chi \rangle_{LK(\zeta_n)/K(\zeta_n)} = \det\Big(\sum_{\sigma \in G} \sigma^{-1} \rho_h(\sigma)\Big) \neq 0$$

for every $K(\zeta_n)$-irreducible character χ associated to complex representation ρ_h of D_{2n}. Note that $\alpha \in L$ is a PV number and hence $\sigma^{-1}(\alpha) > 1$ whenever σ^{-1} is identity and otherwise $|\sigma^{-1}(\alpha)| < 1/(2n + 1)$.

uncorrected proof

Since $K(\zeta_n)$ is a character theoretic splitting field of G, we see that the complex irreducible characters of G is the same as the set of irreducible characters of G over $K(\zeta_n)$.

If ρ is a complex one-dimensional representation of G, then

$$\langle \alpha \mid \chi \rangle = \sum_{\sigma \in G} \sigma^{-1}(\alpha)\rho(\sigma)$$

with $\rho(\sigma)$ is an n-root of unity. Thus,

$$|\langle \alpha | \chi \rangle| \geq \alpha - \sum_{\sigma \in G, \sigma \neq id} |\sigma^{-1}(\alpha)| \geq 1 - \frac{2n-1}{2n+1} > 0.$$

This proves the assertion for the dimension 1 representations of G.

Now, let ρ be a complex irreducible representation of G of dimension 2. Then, $\rho = \varphi_h$ for some integer $0 < h < n/2$. Let χ be the associate character of φ_h and consider

$$\langle \alpha \mid \chi \rangle = \det\left(\sum_{\sigma \in G} \sigma^{-1}(\alpha)\varphi_h(\sigma)\right).$$

Since the presentation of G is

$$\langle r, s \mid r^n = s^2 = 1, srs = r^{-1} \rangle,$$

we see that

$$\begin{aligned} \langle \alpha \mid \chi \rangle &= \det\left(\sum_{t=1}^{n} r^{-t}(\alpha)\varphi_h(r^t) + \sum_{t=1}^{n} (sr^t)^{-1}(\alpha)\varphi_h(sr^t)\right) \\ &= \det\begin{pmatrix} \sum_{t=1}^{n} r^{-t}(\alpha)\omega^{ht} & \sum_{t=1}^{n} (sr^t)^{-1}(\alpha)\omega^{-ht} \\ \sum_{t=1}^{n} (sr^t)^{-1}(\alpha)\omega^{ht} & \sum_{t=1}^{n} r^{-t}(\alpha)\omega^{-ht} \end{pmatrix}. \end{aligned}$$

Thus, in order to prove $\langle \alpha | \chi \rangle \neq 0$, since the determinant of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $ad - bc$ and $|ad - bc| \geq |ad| - |bc|$, it is enough to compute the lower bound for $\left|\sum_{t=1}^{n} r^{-t}(\alpha)\right|$ and the upper bound for $\left|\sum_{t=1}^{n} (sr^t)^{-1}(\alpha)\right|$ as $|\omega^m| = 1$ for evey m.

Since $\alpha \in L$ is a PV number, $\alpha > 1$ and $|\sigma(\alpha)| < 1/(2n+1)$ for every $1 \neq \sigma \in G$. Therefore,

$$\left|\sum_{t=1}^{n} r^{-t}(\alpha)\right| \geq |\alpha| - \frac{n-1}{2n+1} > 1 - \frac{n-1}{2n+1} \geq \frac{n+2}{2n+1}$$

whereas for every $t = 1, 2, \ldots, n$, we see that $sr^{-t} \neq 1$, and hence

$$\left|\sum_{t=1}^{n} (sr^t)^{-1}(\alpha)\right| < \frac{n}{2n+1}.$$

uncorrected proof

Therefore, the determinant of the matrix is nonzero.

Now, let E be an intermediate field such that $K \subset E \subset L$. Then L/E is a Galois extension with Galois group H, a subgroup of G. Any subgroup H of G is either cyclic or dihedral group of order $2m$ satisfying $H = \langle r^{n/m}, sr^k, 0 < k < n\rangle$ with $m|n$. Since $m|n$, we see that $K(\zeta_m) \subset K(\zeta_n)$.

Using the fact that $L \cap K(\zeta_n) = K$, we get $L \cap E(\zeta_m) = E$.

If H is cyclic, then all the irreducible characters of H are one dimensional over $E(\zeta_m)$. Hence, we get

$$\langle \alpha|\chi\rangle_{LE(\zeta_m)/E(\zeta_m)} = \sum_{\sigma\in H} \chi(\sigma)\sigma^{-1}(\alpha)$$

and we get

$$\left|\langle \alpha|\chi\rangle_{LE(\zeta_m)/E(\zeta_m)}\right| \geq 1 - \frac{|H|-1}{2n+1}.$$

If H is dihedral group of order $2m$, then all the complex irreducible characters of H are irreducible characters over $K(\zeta_n)$. Using the similar calculation as above, we can complete the proof of the theorem. □

5 Proof of Theorem 1.4

Given that K is a number field and L/K is a finite Galois extension of degree n for a natural number $n \geq 2$ with Galois group G such that $L = K(\alpha)$ for some $\alpha \in L$.

Suppose Ω_α is K-trivial. Then G acts primitively on Ω_α. Therefore, by Theorem 2.5, we conclude that $n = p$ is a prime number. Hence $G \cong \mathbb{Z}/p\mathbb{Z}$, the cyclic group of order p. Now, we need to prove that $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$.

Since Ω_α is K-trivial, by Theorem 2.1, we see that the character $\mathrm{Ind}_{\{Id\}}^G(1) - 1$ is K-irreducible. Note that the group ring is decomposed as rings

$$K[G] = K[\mathbb{Z}/p\mathbb{Z}] \cong K[X]/\langle X^p - 1\rangle = K[X]/\langle X-1\rangle \oplus K[X]/\langle 1 + X + \cdots + X^{p-1}\rangle.$$

Since $\mathrm{Ind}_{\{Id\}}^G(1) - 1$ is K-irreducible, we conclude that the second component is indecomposable, and hence, we conclude that $\zeta_p \notin K$.

To prove $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$, it is enough to prove that $[K(\zeta_p) : K] = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. Suppose $[K(\zeta_p) : K] < p - 1$. Since $\mathrm{Ind}_{\{id\}}^G(1) - 1 = \sum_\psi n_\psi \psi$ where the sum is running over all the non-trivial K-irreducible characters of G and each complex irreducible character χ of G is contained in one and only ψ that appears in the above sum. The K-irreducible character ψ corresponding to the given complex irreducible character χ of G can be obtained as $\psi = \kappa(\chi_1 + \cdots + \chi_c)$ where χ_i's are running over $\{\sigma \circ \chi : \sigma \in \mathrm{Gal}(K(\zeta_p)/K)\}$ with $[K(\zeta_p) : K] = c < p - 1$ where κ is the Schur index of the character χ. Since G is the cyclic group, it is known that $\kappa = 1$ and $n_\psi = 1$ (cf. [26], Page 92). Since $c < p-1$ and the dual group $\mathrm{Hom}(G, \mathbb{C}^\times)$ of G is of cardinality p, we must have a non-trivial complex irreducible character η of G, which is not corresponding to ψ above. Hence, we conclude that there exists another K-irreducible non-trivial character ψ_1 of G other than ψ. Thereby we conclude that $\mathrm{Ind}_{\{id\}}^G(1) - 1$ cannot be K-irreducible, a contradiction. Hence, we get $[K(\zeta_p) : K] = p - 1$ and so $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$.

Uncorrected Proof

Conversely suppose $n = p \geq 3$ and $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$. Then, the Galois group $\mathrm{Gal}(K(\zeta_p)/K) \cong (\mathbb{Z}/p\mathbb{Z})^*$. If χ_1 is a non-trivial complex irreducible character of G, then the unique K-irreducible character containing χ_1 is $\psi = \chi_1 + \chi_2 + \cdots + \chi_{p-1}$ where χ_i runs over $\{\sigma \circ \chi : \sigma \in \mathrm{Gal}(K(\zeta_p)/K)\}$. Since there are only $(p-1)$ non-trivial complex irreducible characters of G, we conclude that ψ contains all the complex irreducible characters of G. Hence, $\mathrm{Ind}_{\{id\}}^{G}(1) - 1 = \psi$, which is K-irreducible. Then, by Theorem 2.1, we conclude that Ω_α is K-trivial. □

6 Proof of Theorem 1.5

Given that $K/\mathbb{Q}$ is a finite Galois extension with Galois group G which is either abelian or dihedral. Since $K \subset \mathbb{R}$, by Theorem 1.1, there exists a PV number $\alpha \in K$ such that $K = \mathbb{Q}[G] \cdot \alpha$ with $\alpha \in \mathcal{O}_K$, that is, the set $\{\sigma(\alpha) : \sigma \in G\}$ forms $\mathbb{Q}$-basis for K. Therefore, the discriminant $D(\alpha)$ of $\{\sigma(\alpha) : \sigma \in G\}$ is given by

$$|D(\alpha)| = [\mathcal{O}_K : \mathbb{Z}[G] \cdot \alpha]^2 |d_K|$$

where d_K is the absolute discriminant of K. Thus, we have

$$[\mathcal{O}_K : \mathbb{Z}[G] \cdot \alpha] = \sqrt{\frac{|D(\alpha)|}{|d_K|}}. \tag{6.1}$$

Since α is a PV number, by Theorem 1.1, we also see that if $\beta \neq \alpha$ is a Galois conjugate of α, then $|\beta| < \frac{1}{\tau}$ where $\tau = n\phi(n)$ when G is abelian and $\tau = n+1$ when G is dihedral of order $n = [K : \mathbb{Q}]$. Let $\alpha_1 = \alpha, \ldots, \alpha_n$ be all the Galois conjugates of α. Then, it is known (see, for instance, [22]) that

$$\sqrt{|D(\alpha)|} = \left| \prod_{s=1}^{n} \left(\sum_{r=1}^{n} \alpha_r e^{\frac{2\pi i r s}{n}} \right) \right|.$$

Therefore,

$$\sqrt{|D(\alpha)|} \leq \prod_{s=1}^{n} \left(\sum_{r=1}^{n} |\alpha_r| \right) < \left(\alpha + \frac{n-1}{\tau} \right)^n,$$

Also, by Proposition 2.2, we see that $c_1 > \tau^{n-1}\sqrt{|d_K|}$ and so, if we choose $c_1 = [\tau^{n-1}\sqrt{|d_K|}] + 1$, then we conclude that

$$\alpha < [\tau^{n-1}\sqrt{|d_K|}] + 1.$$

Thus by (6.1), we get

$$\begin{aligned}
[\mathcal{O}_K : \mathbb{Z}[G] \cdot \alpha] = \sqrt{\frac{|D(\alpha)|}{|d_K|}} &< \frac{(\alpha + \frac{n-1}{\tau})^n}{\sqrt{|d_K|}} \\
&< \frac{(\tau^{n-1}\sqrt{|d_K|} + 1 + \frac{n-1}{\tau})^n}{\sqrt{|d_K|}} = \left(\frac{\tau^{n-1}\sqrt{|d_K|} + 1 + \frac{n-1}{\tau}}{|d_K|^{1/2n}} \right)^n \\
&= \left(\tau^{n-1}|d_K|^{\frac{1}{2}-\frac{1}{2n}} + \frac{1 + \frac{n-1}{\tau}}{|d_k|^{1/2n}} \right)^n.
\end{aligned}$$

uncorrected proof

By choosing $|d_K| \geq (1+\phi(n)^{-1})^{2n}$, we see that $1+\frac{n-1}{\tau} < |d_K|^{1/2n}$, as $\tau = \phi(n)n$ or $\tau = n+1$. Hence we get

$$[\mathcal{O}_K : \mathbb{Z}[G]\cdot\alpha] < \left(\tau^{n-1}|d_K|^{\frac{1}{2}-\frac{1}{2n}}+1\right)^n$$

as desired. □

Proof of Corollary 1.1 Since $n = [K:\mathbb{Q}] = 2$, it is known that the Schur index $\kappa = 1$ for the cyclic group and $\phi(n)n = 2$. Hence, we get $\tau = 2$. Therefore, by Theorem 1.3, we get the corollary. □

Acknowledgements
We are thankful to the Institute of Mathematical Sciences, Chennai, for providing a wonderful research atmosphere where the authors were visiting while finalizing this paper. We are also thankful to Professor Sinnou David for a thought-provoking question to compute the upper bound in Theorem 1.5. We are also grateful to the referee for meticulously going through the manuscript and providing constructive suggestions to improve the presentation of the manuscript.

Data Availability
There are no data associated with the results of this manuscript.

Declarations

Conflict of interest
There is no conflict of interest in this work.

Received: 2 June 2025 Accepted: 9 March 2026

References

1. Byott, N.P., Sodaïgui, B.: Realizable Galois module classes for tetrahedral extensions. Compos. Math. **141**(3), 573–582 (2005)
2. Childs, L.N., Orzech, M.: On modular group rings, normal bases, and fixed points. Amer. Math. Monthly **88**(2), 142–145 (1981)
3. Conrad, K.: Transitive group actions. https://kconrad.math.uconn.edu/blurbs/grouptheory/transitive.pdf
4. Corso, I.D., Ferri, F., Lombardo, D.: How far is an extension of *p*-adic fields from having a normal integral basis? J. Number Theory **233**, 158–197 (2022)
5. Corvaja, P., Zannier, U.: On the rational approximation to the powers of an algebraic number: solution of two problems of Mahler and Mendés France. Acta Math. **193**, 175–191 (2004)
6. Curtis, C.W., Reiner, I.: Representation Theory of Finite Groups and Associated Algebras. Interscience Publishers, John Wiley and Sons, New York, London, Sydney (1962)
7. Curtis, C.W., Reiner, I.: Methods of Representation Theory, vol. II. Wiley, New York (1967)
8. Dubickas, A.: There are infinitely many limit points of the fractional parts of powers. Proc. Indian Acad. Sci. (Math. Sci.) **115**(4), 391–397 (2004)
9. Faith, C.C.: Extensions of normal bases and completely basic fields. Trans. Amer. Math. Soc. **85**(2), 406–427 (1957)
10. Fröhlich, A.: Resolvents, discriminants, and trace invariants. J. Algebra **4**, 173–198 (1966)
11. Fröhlich, A.: Resolvents and trace form. Math. Proc. Cambridge Philos. Soc. **78**, 185–210 (1975)
12. Fröhlich, A.: Galois module structure of algebraic integers, Ergeb. Math. Grenzgeb. (3), **1**, Springer-Verlag, Berlin (1983)
13. Girstmair, K.: Linear relations between roots of polynomials. Acta Arth. **LXXXIX**(1), 53–96 (1999)
14. Girstmair, K.: A remark on Normal bases. J. Number Theory **58**, 64–65 (1996)
15. Hachenberger, D.: Universal normal bases for an abelian closure of the field of rational numbers. Acta Arith **93**(4), 329–341 (2000)
16. Hilbert, D.: The Theory of Algebraic Number Fields. Springer-Verlag, Berlin, New York (1998)
17. Huppert, B.: Endliche grruppen I. Springer, Berlin (1967); reprint 1979
18. Jacobson, N.: Basic algebra - I. Freeman (1980)
19. Johnston, H., Torzewski, A.: On the existence of free subslattices of bounded index and arithmetic applications. J. Algebra **657**, 81–108 (2024)
20. Jung, H.Y., Koo, J.K., Shin, D.H.: Normal bases of ray class fields over imaginary quadratic fields. Math. Z. **271**(1–2), 109–116 (2012)
21. Kurbatov, V.A.: Galois extensions of prime degree and their primitive elements. Soviet Math. (Izv. VUZ) **21**, 49–52 (1977)
22. Lehmer, D.H.: Some properties of Circulants. J. Number Theory **5**, 43–54 (1973)
23. Narkiewicz, W.: Elementary and analytic theory of algebraic numbers, 3rd edn. Springer (2015)
24. Philippon, P., Rath, P.: A note on the trace of powers of algebraic numbers. J. Number Theory **219**, 198–211 (2021)
25. Pisot, C.: Répartition (mod 1) des puissances successives des nombres réels. Comment Math. Helv. **19**, 159–160 (1946)

Uncorrected proof

458 26. Serre, J.P.: Linear Representations of Finite Groups. Springer, New York (1977)
459 27. Washington, L.C.: Introduction to Cyclotomic Fields. 2nd edn. Graduate Texts in Mathematics, Vol. 83. Springer, New
460 York (1997)

461 **Publisher's Note**

462 Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

uncorrected proof