Bull. Aust. Math. Soc. **113** (2026), 280–287
doi:10.1017/S0004972725100452

AN EFFECTIVE VERSION OF THE PRIMITIVE ELEMENT THEOREM

SUDIPA DAS✉, **R. THANGADURAI** and **A. TRIPATHI**

(Received 10 May 2025; accepted 10 July 2025; first published online 13 October 2025)

Abstract

Let K be an infinite field. If α and β are algebraic and separable elements over K, then by the primitive element theorem, it is well known that $\alpha + u\beta$ is a primitive element for $K(\alpha,\beta)$ for all but finitely many elements $u \in K$. If we let

$$\xi_K(\alpha,\beta) = \{u \in K : K(\alpha,\beta) \neq K(\alpha + u\beta)\}$$

be the exceptional set, then by the primitive element theorem, $|\xi_K(\alpha,\beta)| < \infty$. Dubickas ['An effective version of the primitive element theorem', *Indian J. Pure Appl. Math.* **53**(3) (2022), 720–726] estimated the size of this set when $K = \mathbb{Q}$. We take K to be a finite extension over $\mathbb{Q}$ or $\mathbb{Q}_p$, the field of p-adic numbers for some prime p, and estimate the size of the exceptional set.

2020 *Mathematics subject classification*: primary 11R32; secondary 12F10.

Keywords and phrases: primitive elements, number fields, Galois theory.

1. Introduction

In any book on field theory and Galois theory, we first encounter the primitive element theorem (see, for instance, [6, Theorem 4.6]) which states: '*If L/K is a finite separable extension of fields such that K contains infinitely many elements, and $\alpha, \beta \in L$, then for all but finitely many $u \in K$, we have $K(\alpha,\beta) = K(\alpha + u\beta)$. That is, for all but finitely many $u \in K$, the element $\alpha + u\beta$ is a primitive element for $K(\alpha,\beta)$ over K*'.

Let K be a given field which contains infinitely many elements. If α and β are algebraic and separable elements over K, we define

$$\xi_K(\alpha,\beta) = \{u \in K : K(\alpha,\beta) \neq K(\alpha + u\beta)\}$$

as the exceptional set. By the primitive element theorem, $|\xi_K(\alpha,\beta)| < \infty$. In the following theorem, we estimate the size of this set. We denote the degree of the extension field F over K by $[F : K]$.

THEOREM 1.1. *Let K be an arbitrary field which has infinitely many elements. Let α and β be distinct algebraic and separable elements over K. If the degree of β is*

© The Author(s), 2025. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc.

https://doi.org/10.1017/S0004972725100452 Published online by Cambridge University Press

at least 3 *and* $(\beta-\beta_1)/(\beta-\beta_2) \notin K$ *for any two distinct Galois conjugates of* β *with* $\beta_i \neq \beta$ *for* $i = 1, 2$, *then*

$$|\xi_K(\alpha,\beta)| \leq [K(\alpha) : K].$$

If L/K is a finite Galois extension of fields with Galois group G, then by the normal basis theorem, there exists $\alpha \in L$ such that the set $\{\sigma(\alpha) : \sigma \in G\}$ forms a K-basis for L. Such an element $\alpha \in L$ is called a *normal basis generator* for L/K. Also, for a given number field K, an algebraic element β over K is said to be *totally real*, if all its Galois conjugates are real.

Let K be a number field and $f(x) \in K[x]$ be an irreducible polynomial of degree d. Let $\Omega_f = \{\alpha_1, \ldots, \alpha_d\}$ be the set of all complex roots of $f(x)$. We say that Ω_f is *K-trivial*, if $c_1\alpha_1 + \cdots + c_d\alpha_d = 0$ for some $c_i \in K$, implies $c_1 = c_2 = \cdots = c_d$. In 1977, V. A. Kurbatov [5] proved: '*Let* L/K *be a finite Galois extension of number fields of degree* p, *for some prime number* $p \geq 3$ *with* $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$. *If* $L = K(\beta)$ *for some* β *whose minimal polynomial is* $f(x) \in K[x]$, *then* Ω_f *is K-trivial*'. In 1997, Dixon [1] proved: '*Let* L/K *be a finite Galois extension of number fields with Galois group* G *and let* $L = K(\beta)$. *If* $f(x) \in K[X]$ *is the minimal polynomial of* β *and* G *acts on* Ω_f 2*-transitively, then* Ω_f *is K-trivial*'. We prove the following corollary.

COROLLARY 1.2. *Let* K *be a given number field. Let* α *and* β *be algebraic numbers over* K *such that* $\alpha, \beta \notin K$ *and* $\beta \notin K(\alpha)$. *Suppose one of* α *and* β *is of degree* ≥ 3.

(1) *If* $K \subset \mathbb{R}$, *then* $|\xi_K(\alpha,\beta)| \leq \min\{[K(\alpha) : K], [K(\beta) : K]\}$.
(2) *If* $K \not\subset \mathbb{R}$ *and* β *is a totally real algebraic number of degree at least* 3, *then*

$$|\xi_K(\alpha,\beta)| \leq [K(\alpha) : K].$$

(3) *If* $K \not\subset \mathbb{R}$ *and* $\beta \in \bar{\mathbb{Q}}$ *is such that* β *and at least two of its Galois conjugates are purely imaginary, then* $|\xi_K(\alpha,\beta)| \leq [K(\alpha) : K]$.
(4) *If* $K(\beta)/K$ *is a finite Galois extension of degree at least* 3 *and* β *is a normal basis generator of* $K(\beta)/K$, *then* $|\xi_K(\alpha,\beta)| \leq [K(\alpha) : K]$.
(5) *If* $f(x) \in K[x]$ *is the minimal polynomial of* β *and* Ω_f *is K-trivial, then*

$$|\xi_K(\alpha,\beta)| \leq [K(\alpha) : K].$$

It is easy to see that $|\xi_K(\alpha,\beta)| \leq (d-1)^2$, where $d = [K(\alpha,\beta) : K]$. In 2022, Dubickas [3] gave an argument for the upper bound $|\xi_K(\alpha,\beta)| \leq e(e+1)/2$, where $e = d/p$ and p is the least prime dividing d. For earlier results of this kind, we refer to [3]. Then, he proved $|\xi_K(\alpha,\beta)| \leq \min\{[\mathbb{Q}(\alpha) : \mathbb{Q}], [\mathbb{Q}(\beta) : \mathbb{Q}]\} \leq d$ (as in Corollary 1.2(1), when $K = \mathbb{Q}$) and noted that the bound for $|\xi_K(\alpha,\beta)|$ as a function of d is far from optimal. However, in the same paper, he also proved that the bound obtained in Corollary 1.2(1) cannot be improved, in general. This is applied to our situation in Corollaries 1.2 and 1.3.

https://doi.org/10.1017/S0004972725100452 Published online by Cambridge University Press

Now, we consider K as a finite extension of $\mathbb{Q}_p$, the field of p-adic numbers. If β is an algebraic element over K of degree d, then the discriminant $D(\beta)$ of β is defined by

$$D(\beta) = \prod_{1 \le i < j \le d} (\beta_i - \beta_j)^2,$$

where $\beta_1 = \beta$ and the β_j are the other Galois conjugates of β for $j \ge 2$. We say that the square root of $D(\beta)$ is *square-free* if $\sqrt{D(\beta)}$ does not contain a term $(\beta_i - \beta_j)^2$ for any $i < j$.

COROLLARY 1.3. *Let K be a finite extension over $\mathbb{Q}_p$, the field of p-adic numbers. Let α and β be algebraic over K.*

(1) *If $K(\beta)$ is a finite Galois extension over K of degree ≥ 3 and β is a normal basis generator of $K(\beta)/K$, then $|\xi_K(\alpha, \beta)| \le [K(\alpha) : K]$.*
(2) *If $K(\beta)$ is a finite Galois extension over K of degree ≥ 3 and if the square root of the discriminant of β over K is square-free, then $|\xi_K(\alpha, \beta)| \le [K(\alpha) : K]$.*
(3) *Suppose L is the splitting field of β and L/K is unramified. Let $\bar{L}$ and $\bar{K}$ be the residue fields of L and K. If β is an integral element which is the pre-image of a normal basis generator of the residue field $\bar{L}/\bar{K}$ of degree ≥ 3, then*

$$|\xi_K(\alpha, \beta)| \le [K(\alpha) : K].$$

2. Preliminaries

We first prove some lemmas and then we prove the theorem and its corollaries. The first lemma provides a criterion for an element to be a primitive element.

LEMMA 2.1 [3]. *Let K/F be a finite separable extension over a field F and let L be the Galois closure of K whose Galois group is $G = \mathrm{Gal}(L/F)$. Let H be the subgroup of G which fixes K and let $\{H, \sigma_1 H, \ldots, \sigma_{d-1} H\}$ be a complete set of left coset representatives of H where $d = [K : F] = [G : H]$. Then, $\alpha \in K$ is a primitive element, that is, $K = F(\alpha)$ if and only if $\sigma_i(\alpha) \ne \alpha$ for every $i = 1, 2, \ldots, d-1$.*

LEMMA 2.2. *Let K be a field with infinitely many elements. Let α_1, α_2 and α_3 be distinct algebraic and separable elements over K. Then, the following statements are equivalent:*

(1) *$(\alpha_1 - \alpha_2)/(\alpha_1 - \alpha_3) \notin K$;*
(2) *for any $x_1, x_2, x_3 \in K \backslash \{0\}$ with $x_1 + x_2 + x_3 = 0$, we have $x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3 \ne 0$.*

PROOF. Observe that

$$\frac{\alpha_1 - \alpha_2}{\alpha_1 - \alpha_3} = x \in K \iff (x-1)\alpha_1 + \alpha_2 - x\alpha_3 = 0,$$

https://doi.org/10.1017/S0004972725100452 Published online by Cambridge University Press

with $x_1 = x - 1$, $x_2 = 1$ and $x_3 = -x$ satisfying $x_1 + x_2 + x_3 = 0$. Note that $x \neq 0$ as $\alpha_1 \neq \alpha_2$. Hence, $x_1, x_2, x_3 \in K\backslash\{0\}$. Conversely, if $x_1, x_2, x_3 \in K\backslash\{0\}$ are such that $x_1 + x_2 + x_3 = 0$ and $x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3 = 0$, then

$$\begin{aligned} 0 &= (-x_2 - x_3)\alpha_1 + x_2\alpha_2 + x_3\alpha_3 \\ &= x_2(\alpha_2 - \alpha_1) + x_3(\alpha_3 - \alpha_1) \iff \frac{\alpha_1 - \alpha_2}{\alpha_1 - \alpha_3} = -\frac{x_3}{x_2} \in K. \end{aligned}$$

This proves the lemma. □

The proof of the following lemma follows easily from [2, Theorem 4] (see also [3, Lemma 4]). Hence, we omit the proof.

LEMMA 2.3 [2]. *Let $K \subset \mathbb{R}$ be a given number field and let α_1, α_2 and α_3 be distinct algebraic numbers over K which are Galois conjugates of each other. If x_1, x_2 and x_3 are nonzero elements of K such that $x_1 + x_2 + x_3 = 0$, then $x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3 \neq 0$.*

LEMMA 2.4. *Let K be a finite extension over $\mathbb{Q}_p$ for some prime p. Let α be an algebraic element over K of degree $d \geq 3$ and let L/K be a finite Galois extension which contains α. Suppose there are nonzero elements $x_1, x_2, x_3 \in K$ with $x_1 + x_2 + x_3 = 0$ and distinct Galois conjugates $\alpha_1 = \alpha, \alpha_2, \alpha_3$ of α such that $x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3 = 0$. Then, the square root of $D(\alpha)$ is not square-free.*

PROOF. Assume that $x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3 = 0$ for some nonzero elements $x_i \in K$ and for some distinct Galois conjugates $\alpha_1 = \alpha, \alpha_2$ and α_3. We consider the valuation in L and denote it by $v_L(\gamma)$ for $\gamma \in L$. Since $x_1 + x_2 + x_3 = 0$, we must have $v_L(x_i) = v_L(x_j)$ for some i, j with $1 \leq i < j \leq 3$. Without loss of generality, we assume that $v_L(x_1) = v_L(x_2)$. Since

$$\begin{aligned} x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3 = 0 &\iff x_1\alpha_1 + x_2\alpha_2 + (-x_1 - x_2)\alpha_3 = 0 \\ &\iff \alpha_1 - \alpha_3 = -\frac{x_2}{x_1}(\alpha_2 - \alpha_3), \end{aligned}$$

it follows that $v_L(\alpha_1 - \alpha_3) = v_L(x_2/x_1) + v_L(\alpha_2 - \alpha_3) = v_L(\alpha_2 - \alpha_3)$. Therefore, $(\alpha_1 - \alpha_3)^2$ divides $\sqrt{D(\alpha)}$. This proves the lemma. □

LEMMA 2.5 (Nakayama lemma, [4]). *Suppose M is a finitely generated module over a commutative ring R and $J(R)$ is the intersection of all the maximal ideals of R. If $M = J(R)M$, then $M = 0$.*

LEMMA 2.6. *Let K be a finite extension of $\mathbb{Q}_p$ for some prime p and let β be an integral element over K of degree ≥ 3. Let L be the splitting field of β over K such that L/K is unramified. Let $\bar{L}$ and $\bar{K}$ be the residue fields of L and K, respectively. If β is a pre-image of a normal basis generator of $\bar{L}/\bar{K}$, then for any other distinct Galois conjugates β' and β'' of β, if $c_1\beta + c_2\beta' + c_3\beta'' = 0$ for some $c_1, c_2, c_3 \in K$, then $c_1 = c_2 = c_3 = 0$.*

PROOF. Put $\beta = \beta_1$ and label the other given distinct conjugates β_2 and β_3. Assume that $c_1\beta_1 + c_2\beta_2 + c_3\beta_3 = 0$ for some $c_1, c_2, c_3 \in K$, not all zero. Let G be the Galois group of the unramified extension L/K which is the splitting field of $\beta = \beta_1$. Let O_K

https://doi.org/10.1017/S0004972725100452 Published online by Cambridge University Press

be the local ring of K and $\mathfrak{m}_L$ be the unique maximal ideal in L. Let σ_1, σ_2 and σ_3 be the automorphisms of L such that $\sigma_i(\beta) = \beta_i$ for $i = 1, 2, 3$.

Since $\beta = \beta_1$ is a pre-image of a normal basis generator γ of the residue field $\bar{L}/\bar{K}$, under reduction modulo $\mathfrak{m}_L$, we can write $\beta_i + \mathfrak{m}_L = \bar{\beta}_i$ for $i = 1, 2, 3$. Under the reduction modulo $\mathfrak{m}_L$, the automorphisms σ_i are automorphisms $\bar{\sigma}_i$ of $\bar{L}$ over $\bar{K}$. Note that $\mathfrak{m}_L \cap O_K = \mathfrak{m}_K$ is the maximal ideal of K.

Since the $\bar{\sigma}_i$ are automorphisms of the Galois group $\bar{L}/\bar{K}$ and $\overline{\sigma_1(\beta)} = \gamma$, the normal basis generator of $\bar{L}/\bar{K}$ along with two other Galois conjugates of γ are given by $\overline{\sigma_i(\beta)} = \gamma_i$ for $i = 2, 3$. Since L/K is an unramified extension, we have $[L : K] = [\bar{L} : \bar{K}]$ and hence $\bar{\sigma}_2 \neq \bar{\sigma}_3$. This in turn implies that $\gamma_2 \neq \gamma_3$ and both are distinct from γ. We denote the Galois group of $\bar{L}/\bar{K}$ by $\bar{G}$.

Consider the O_K-module $M = O_K[G] \cdot (c_1\sigma_1 + c_2\sigma_2 + c_3\sigma_3)$. Then,

$$M/\mathfrak{m}_L M = (O_K/\mathfrak{m}_K)[\bar{G}] \cdot [\overline{c_1\sigma_1 + c_2\sigma_2 + c_3\sigma_3}] = \bar{K}[\bar{G}] \cdot (\bar{c}_1\bar{\sigma}_1 + \bar{c}_2\bar{\sigma}_2 + \bar{c}_3\bar{\sigma}_3). \tag{2.1}$$

Since $c_1\beta_1 + c_2\beta_2 + c_3\beta_3 = 0$, we conclude that

$$\bar{c}_1\gamma + \bar{c}_2\gamma_2 + \bar{c}_3\gamma_3 = \bar{0}.$$

Since γ is a normal basis generator, we must have $\bar{c}_i = \bar{0}$ for $i = 1, 2, 3$. Together with (2.1), this implies that

$$M/\mathfrak{m}_L M = \bar{0} \iff M = \mathfrak{m}_L M.$$

Since $\mathfrak{m}_L$ is the only maximal ideal in L, by Nakayama's Lemma 2.5, we conclude that $M = 0$. However, $O_K[G]$ is a free module over O_K with generators as their elements, so we conclude that $c_1 = c_2 = c_3 = 0$. □

3. Proof of Theorem 1.1

Let K be an infinite field. We wish to prove $|\xi_K(\alpha, \beta)| \leq [K(\alpha) : K]$. In fact, we prove that whenever $u, v \in \xi_K(\alpha, \beta)$ with $u \neq v$ in K, there are two distinct Galois conjugates of α which gives the desired result.

Let $u, v \in \xi_K(\alpha, \beta)$ with $u \neq v$. Since $\alpha + u\beta$ and $\alpha + v\beta$ are not primitive elements of $L = K(\alpha, \beta)$, by Lemma 2.1, there exist embeddings $\tau_1, \tau_2 : L \to \mathbb{C}$ such that $\tau_1(\alpha + u\beta) = \alpha + u\beta$ and $\tau_2(\alpha + v\beta) = \alpha + v\beta$.

Note that if $\tau_i(\beta) = \beta$ (or $\tau_i(\alpha) = \alpha$), then these equations give $\tau_i(\alpha) = \alpha$ (respectively, $\tau_i(\beta) = \beta$) as u, v are elements of K. It follows that τ_i must be the identity, which is in contradiction to Lemma 2.1. Therefore, $\tau_i(\alpha) \neq \alpha$ and $\tau_i(\beta) \neq \beta$. Thus,

$$\tau_1(\alpha) + u\tau_1(\beta) = \alpha + u\beta \quad \text{and} \quad \tau_2(\alpha) + v\tau_2(\beta) = \alpha + v\beta,$$

with $\tau_i(\alpha) \neq \alpha$ and $\tau_i(\beta) \neq \beta$ for $i = 1, 2$. Since $\tau_1(\alpha)$ and $\tau_2(\alpha)$ are Galois conjugates distinct from α, we claim that $\tau_1(\alpha) \neq \tau_2(\alpha)$ (and the proof of the assertion follows).

https://doi.org/10.1017/S0004972725100452 Published online by Cambridge University Press

To the contrary, assume that $\tau_1(\alpha) = \tau_2(\alpha)$. Since $u \neq v$, we must have $\tau_1(\beta) \neq \tau_2(\beta)$. From these equations,

$$u(\beta - \tau_1(\beta)) = \tau_1(\alpha) - \alpha = \tau_2(\alpha) - \alpha = v(\beta - \tau_2(\beta))$$

and hence

$$\frac{\beta - \tau_1(\beta)}{\beta - \tau_2(\beta)} = \frac{v}{u} \in K,$$

which is a contradiction. This proves the theorem.

4. Proof of Corollary 1.2

PROOF OF COROLLARY 1.2(1). Since either α or β is of degree ≥ 3, we can assume that β is of degree ≥ 3. Since $K \subset \mathbb{R}$, by Lemmas 2.3 and 2.2, we conclude that

$$\frac{\beta - \beta_1}{\beta - \beta_2} \notin K$$

for any distinct conjugates $\beta_i \neq \beta$ $(i = 1, 2)$. Therefore, by Theorem 1.1,

$$|\xi_K(\alpha, \beta)| \leq [K(\alpha) : K].$$

If $[K(\alpha) : K] \geq [K(\beta) : K] \geq 3$, we swap the roles of β and α giving $|\xi_K(\alpha, \beta)| \leq [K(\beta) : K]$. This proves part (1) of the corollary. □

PROOF OF COROLLARY 1.2(2). If $K \subset \mathbb{R}$, the result follows from Corollary 1.2(1). Hence, we assume that $K \subset \mathbb{C}$.

If $x_1, x_2, x_3 \in \mathbb{C}$, then we write $x_j = a_{j1} + ia_{j2}$ for $j = 1, 2, 3$ and $a_{rs} \in \mathbb{R} \cap K$. Since $x_1 + x_2 + x_3 = 0$, we have

$$a_{11} + a_{21} + a_{31} = 0 \quad \text{and} \quad a_{12} + a_{22} + a_{32} = 0.$$

Since β is of degree ≥ 3 and totally real, every Galois conjugate of β is real. Therefore, if β_1 and β_2 are any distinct Galois conjugates of β with $\beta_i \neq \beta$, then by Lemma 2.3,

$$a_{11}\beta + a_{21}\beta_1 + a_{31}\beta_2 \neq 0 \quad \text{and} \quad a_{12}\beta + a_{22}\beta_1 + a_{32}\beta_2 \neq 0.$$

Therefore, $x_1\beta + x_2\beta_1 + x_3\beta_2 \neq 0$. Part (2) of the corollary follows by Lemma 2.2 and Theorem 1.1. □

PROOF OF COROLLARY 1.2(3). Given that β and two of its Galois conjugates are purely imaginary, we have distinct conjugates $\beta = i\beta', \beta_1 = i\beta_1'$ and $\beta_2 = i\beta_2'$ with β', β_1' and β_2' distinct real numbers. With the same notation in the proof of Corollary 1.2(2),

$$i(a_{11}\beta' + a_{21}\beta_1' + a_{31}\beta_2') \neq 0 \quad \text{and} \quad -(a_{12}\beta' + a_{22}\beta_1' + a_{32}\beta_2') \neq 0,$$

by Lemma 2.3. Therefore,

$$a_{11}\beta' + a_{21}\beta_1' + a_{31}\beta_2' \neq 0 \quad \text{and} \quad a_{12}\beta' + a_{22}\beta_1' + a_{32}\beta_2' \neq 0,$$

and hence $x_1\beta + x_2\beta_1 + x_3\beta_2 \neq 0$. Part (3) of the corollary follows by Lemma 2.2 and Theorem 1.1. □

https://doi.org/10.1017/S0004972725100452 Published online by Cambridge University Press

PROOF OF COROLLARY 1.2(4). Let $K(\beta)$ be a finite Galois extension over K such that β is a normal integral basis generator over K of degree at least 3. If the Galois group of $K(\beta)/K$ is G, then the set $\{\sigma(\beta) : \sigma \in G\}$ forms a K-basis and, in particular, it is K-linearly independent. Therefore, if β_1 and β_2 are any distinct Galois conjugates of β such that $\beta_i \neq \beta$, then $x_1\beta + x_2\beta_1 + x_3\beta_2 \neq 0$ for any nonzero tuple $(x_1, x_2, x_3) \in K^3$. By Lemma 2.2, we have $(\beta - \beta_1)/(\beta - \beta_2) \notin K$. The result follows from Theorem 1.1. □

PROOF OF COROLLARY 1.2(5). Let f be the minimal polynomial of β and assume that Ω_f, the set of all roots of f over K, is K-trivial. Since Ω_f is K-trivial and the degree of β is at least 3, if $c_1\beta + c_2\beta_2 + c_3\beta_3 = 0$ for some $c_i \in K$ and for any distinct conjugates $\beta_1 \neq \beta_2$ different from β, then $c_1 = c_2 = c_3 = 0$. Therefore, for any nonzero $c_1, c_2, c_3 \in K$ with $c_1 + c_2 + c_3 = 0$, we must have $c_1\beta + c_2\beta_2 + c_3\beta_3 \neq 0$. The result now follows from Theorem 1.1. □

5. Proof of Corollary 1.3

Let $K(\beta)$ be a finite Galois extension over K. Since β is a normal basis generator, Corollary 1.3(1) follows by the same proof as Corollary 1.2(4).

To prove Corollary 1.3(2), we can assume that β is not a normal basis generator of $K(\beta)/K$. Since the square-root of the discriminant of β in $K(\beta)$ is square-free, by Lemmas 2.4 and 2.2, the element $(\beta - \beta_1)/(\beta - \beta_2) \notin K$ for any distinct Galois conjugates $\beta_i \neq \beta$. Corollary 1.3(2) now follows from Theorem 1.1.

Since β is a pre-image of a normal basis generator of $\bar{L}/\bar{K}$, by Lemma 2.6, we see that $c_1\beta + c_2\beta_1 + c_3\beta_3 \neq 0$ whenever one of the c_i is nonzero. Therefore, Corollary 1.3(3) follows from Lemma 2.2 and Theorem 1.1.

Acknowledgement

We are thankful to the referee for going through the manuscript and suggesting changes that improved the presentation. This work was finished when we were visiting the Institute of Mathematical Sciences (IMSc), Chennai. We are thankful to IMSc for the wonderful research atmosphere and their hospitality.

References

[1] J. D. Dixon, 'Polynomials with nontrival relations between their roots', *Acta Arith.* **LXXXII**(3) (1997), 293–302.
[2] A. Dubickas, 'On the degree of a linear form in conjugates of an algebraic number', *Illinois J. Math.* **46** (2002), 571–585.
[3] A. Dubickas, 'An effective version of the primitive element theorem', *Indian J. Pure Appl. Math.* **53**(3) (2022), 720–726.
[4] N. Jacobson, *Basic Algebra I* (Freeman, New York, 1980).
[5] V. A. Kurbatov, 'Galois extensions of prime degree and their primitive elements', *Soviet Math.* **21** (1977), 49–52.
[6] S. Lang, *Algebra*, 3rd edn, Graduate Texts in Mathematics, 211 (Springer, New York, 2002).

https://doi.org/10.1017/S0004972725100452 Published online by Cambridge University Press

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

R. THANGADURAI, Harish-Chandra Research Institute,
A CI of Homi Bhabha National Institute, Chhatnag Road,
Jhunsi, Prayagraj 211019, India
e-mail: thanga@hri.res.in

A. TRIPATHI, Harish-Chandra Research Institute,
A CI of Homi Bhabha National Institute, Chhatnag Road,
Jhunsi, Prayagraj 211019, India
e-mail: aparnatripathi@hri.res.in

https://doi.org/10.1017/S0004972725100452 Published online by Cambridge University Press