Minimal degree of an algebraic number with respect to a number field containing it

Artūras Dubickas (Vilnius University)

Liege, 2023

Definition

Let β be an algebraic number of degree $d \geqslant 2$ over the field of rational numbers $\mathbb{Q}$, and let L be a number field containing β,

Definition

Let β be an algebraic number of degree $d \geqslant 2$ over the field of rational numbers $\mathbb{Q}$, and let L be a number field containing β, so that

$$\mathbb{Q}(\beta) \subseteq L.$$

Definition

Let β be an algebraic number of degree $d \geqslant 2$ over the field of rational numbers $\mathbb{Q}$, and let L be a number field containing β, so that

$$\mathbb{Q}(\beta) \subseteq L.$$

In the recent paper

- C.-M. Park and S. W. Park, Minimal degrees of algebraic numbers with respect to primitive elements, *Int. J. Number Theory* **18** (2022), 485–500

Definition

Let β be an algebraic number of degree $d \geqslant 2$ over the field of rational numbers $\mathbb{Q}$, and let L be a number field containing β, so that

$$\mathbb{Q}(\beta) \subseteq L.$$

In the recent paper

- C.-M. Park and S. W. Park, Minimal degrees of algebraic numbers with respect to primitive elements, *Int. J. Number Theory* **18** (2022), 485–500

the *minimal degree of β with respect to the field L*

Definition

Let β be an algebraic number of degree $d \geqslant 2$ over the field of rational numbers $\mathbb{Q}$, and let L be a number field containing β, so that

$$\mathbb{Q}(\beta) \subseteq L.$$

In the recent paper

- C.-M. Park and S. W. Park, Minimal degrees of algebraic numbers with respect to primitive elements, *Int. J. Number Theory* **18** (2022), 485–500

the *minimal degree of β with respect to the field L* is defined as the smallest degree of a polynomial $f \in \mathbb{Q}[x]$ such that $\beta = f(\alpha)$ for some $\alpha \in L$

Definition

Let β be an algebraic number of degree $d \geqslant 2$ over the field of rational numbers $\mathbb{Q}$, and let L be a number field containing β, so that

$$\mathbb{Q}(\beta) \subseteq L.$$

In the recent paper

- C.-M. Park and S. W. Park, Minimal degrees of algebraic numbers with respect to primitive elements, *Int. J. Number Theory* **18** (2022), 485–500

the *minimal degree of* β *with respect to the field* L is defined as the smallest degree of a polynomial $f \in \mathbb{Q}[x]$ such that $\beta = f(\alpha)$ for some $\alpha \in L$ which is the primitive element of L over $\mathbb{Q}$, i.e. $L = \mathbb{Q}(\alpha)$.

Some simple observations

Throughout, we denote the minimal degree of β with respect to the field L by $\deg_L(\beta)$.

Some simple observations

Throughout, we denote the minimal degree of β with respect to the field L by $\deg_L(\beta)$. By the definition, it is clear that

$$\deg_L(\beta) = \deg_L(a + b\beta) \tag{1}$$

for any rational numbers a and $b \neq 0$.

Some simple observations

Throughout, we denote the minimal degree of β with respect to the field L by $\deg_L(\beta)$. By the definition, it is clear that

$$\deg_L(\beta) = \deg_L(a + b\beta) \tag{1}$$

for any rational numbers a and $b \neq 0$.
As indicated in Park & Park, the minimal degree of β with respect to L in some sense represents the *shortest representation* of an algebraic number in a field.

Example

For example, if $\beta = \sqrt{2}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ then,

Example

For example, if $\beta = \sqrt{2}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ then, by the inequality which we show below,

$$\deg_L(\beta) \geqslant [L : \mathbb{Q}(\beta)] = 4.$$

Example

For example, if $\beta = \sqrt{2}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ then, by the inequality which we show below,

$$\deg_L(\beta) \geqslant [L : \mathbb{Q}(\beta)] = 4.$$

The example of the generator

$$\alpha = \sqrt{3} + 3\sqrt{5} - 5\sqrt{6} + \sqrt{10}$$

of L

Example

For example, if $\beta = \sqrt{2}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ then, by the inequality which we show below,

$$\deg_L(\beta) \geqslant [L : \mathbb{Q}(\beta)] = 4.$$

The example of the generator

$$\alpha = \sqrt{3} + 3\sqrt{5} - 5\sqrt{6} + \sqrt{10}$$

of L and the representation

$$\sqrt{2} = \frac{1}{11760}(\alpha^4 - 416\alpha^2 + 16804)$$

Example

For example, if $\beta = \sqrt{2}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ then, by the inequality which we show below,

$$\deg_L(\beta) \geqslant [L : \mathbb{Q}(\beta)] = 4.$$

The example of the generator

$$\alpha = \sqrt{3} + 3\sqrt{5} - 5\sqrt{6} + \sqrt{10}$$

of L and the representation

$$\sqrt{2} = \frac{1}{11760}(\alpha^4 - 416\alpha^2 + 16804)$$

with polynomial of degree 4 shows that

$$\deg_L(\beta) = 4.$$

Some simple observations

Apparently, the quantity $\deg_L(\beta)$ as such was not considered before this paper,

Some simple observations

Apparently, the quantity $\deg_L(\beta)$ as such was not considered before this paper, although in

- P. Drungilas and A. Dubickas, Reducibility of polynomials after a polynomial substitution, *Publ. Math. Debrecen* **96** (2020), 185–194.

Some simple observations

Apparently, the quantity $\deg_L(\beta)$ as such was not considered before this paper, although in

- P. Drungilas and A. Dubickas, Reducibility of polynomials after a polynomial substitution, *Publ. Math. Debrecen* **96** (2020), 185–194.

we investigated a problem raised by Ulas (2019) and used the methods that can be useful in studying the minimal degree of an algebraic number with respect to the field containing it.

Basic inequality

Set

$$D = [L : \mathbb{Q}(\beta)].$$

Basic inequality

Set

$$D = [L : \mathbb{Q}(\beta)].$$

We trivially have $\deg_L(\beta) = 1$ if $D = 1$, since then β itself is a generator of L over $\mathbb{Q}$, Set

$$D = [L : \mathbb{Q}(\beta)].$$

We trivially have $\deg_L(\beta) = 1$ if $D = 1$, since then β itself is a generator of L over $\mathbb{Q}$, so $\beta = \beta$ with $f(x) = x$, which is a polynomial of degree 1.

Basic inequality

Set

$$D = [L : \mathbb{Q}(\beta)].$$

We trivially have $\deg_L(\beta) = 1$ if $D = 1$, since then β itself is a generator of L over $\mathbb{Q}$, so $\beta = \beta$ with $f(x) = x$, which is a polynomial of degree 1.
We claim that for any $D \geqslant 2$ we must have

$$\deg_L(\beta) \geqslant D. \quad (2)$$

Its proof

Indeed, suppose $\beta = f(\alpha)$ for some $f \in \mathbb{Q}[x]$ and some $\alpha \in L$ satisfying $L = \mathbb{Q}(\alpha)$.

Its proof

Indeed, suppose $\beta = f(\alpha)$ for some $f \in \mathbb{Q}[x]$ and some $\alpha \in L$ satisfying $L = \mathbb{Q}(\alpha)$. Since

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = Dd,$$

Its proof

Indeed, suppose $\beta = f(\alpha)$ for some $f \in \mathbb{Q}[x]$ and some $\alpha \in L$ satisfying $L = \mathbb{Q}(\alpha)$. Since

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = Dd,$$

α is of degree dD over $\mathbb{Q}$.

Its proof

Indeed, suppose $\beta = f(\alpha)$ for some $f \in \mathbb{Q}[x]$ and some $\alpha \in L$ satisfying $L = \mathbb{Q}(\alpha)$. Since

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = Dd,$$

α is of degree dD over $\mathbb{Q}$.
Then, the conjugates of β are all of the form $f(\alpha_j)$, where α_j, $j = 1, \dots, dD$, are the conjugates of $\alpha_1 = \alpha$ over $\mathbb{Q}$.

Its proof

Indeed, suppose $\beta = f(\alpha)$ for some $f \in \mathbb{Q}[x]$ and some $\alpha \in L$ satisfying $L = \mathbb{Q}(\alpha)$. Since

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = Dd,$$

α is of degree dD over $\mathbb{Q}$.
Then, the conjugates of β are all of the form $f(\alpha_j)$, where α_j, $j = 1, \ldots, dD$, are the conjugates of $\alpha_1 = \alpha$ over $\mathbb{Q}$. Since β is of degree d over $\mathbb{Q}$, the list $f(\alpha_j)$, $j = 1, \ldots, dD$, contains exactly d distinct elements and each of them occurs exactly D times.

Its proof

Indeed, suppose $\beta = f(\alpha)$ for some $f \in \mathbb{Q}[x]$ and some $\alpha \in L$ satisfying $L = \mathbb{Q}(\alpha)$. Since

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = Dd,$$

α is of degree dD over $\mathbb{Q}$.
Then, the conjugates of β are all of the form $f(\alpha_j)$, where α_j, $j = 1, \dots, dD$, are the conjugates of $\alpha_1 = \alpha$ over $\mathbb{Q}$. Since β is of degree d over $\mathbb{Q}$, the list $f(\alpha_j)$, $j = 1, \dots, dD$, contains exactly d distinct elements and each of them occurs exactly D times. By the fundamental theorem of algebra, at most $\deg f$ numbers $f(c_j)$ for distinct $c_j \in \mathbb{C}$ can be equal.

Its proof

Indeed, suppose $\beta = f(\alpha)$ for some $f \in \mathbb{Q}[x]$ and some $\alpha \in L$ satisfying $L = \mathbb{Q}(\alpha)$. Since

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = Dd,$$

α is of degree dD over $\mathbb{Q}$.
Then, the conjugates of β are all of the form $f(\alpha_j)$, where α_j, $j = 1, \dots, dD$, are the conjugates of $\alpha_1 = \alpha$ over $\mathbb{Q}$. Since β is of degree d over $\mathbb{Q}$, the list $f(\alpha_j)$, $j = 1, \dots, dD$, contains exactly d distinct elements and each of them occurs exactly D times. By the fundamental theorem of algebra, at most $\deg f$ numbers $f(c_j)$ for distinct $c_j \in \mathbb{C}$ can be equal. Thus, $D \leqslant \deg f$, which completes the proof of (2).
(A slightly different proof of (2) is given in Park & Park.)

First result

Our first result shows that equality in (2) always holds for $d = D = 2$.

First result

Our first result shows that equality in (2) always holds for $d = D = 2$.

Theorem 1

Let K be a quadratic extension of $\mathbb{Q}$ and let L be a quadratic extension of K.

First result

Our first result shows that equality in (2) always holds for $d = D = 2$.

Theorem 1

Let K be a quadratic extension of $\mathbb{Q}$ and let L be a quadratic extension of K. Then, for each quadratic element $\beta \in K$, we have $\deg_L(\beta) = 2$.

Explanation

In Park & Park, Theorem 1 has been established in the case when $L/\mathbb{Q}$ is a Galois extension.

Explanation

In Park & Park, Theorem 1 has been established in the case when $L/\mathbb{Q}$ is a Galois extension.

In general, for a quartic extension L of $\mathbb{Q}$ the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ can be C_4, V_4, D_8, A_4 or S_4.

Explanation

In Park & Park, Theorem 1 has been established in the case when $L/\mathbb{Q}$ is a Galois extension.

In general, for a quartic extension L of $\mathbb{Q}$ the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ can be C_4, V_4, D_8, A_4 or S_4. However, for $\mathrm{Gal}(L/\mathbb{Q}) \in \{A_4, S_4\}$ the quartic field L does not contain a quadratic subfield K.

Explanation

In Park & Park, Theorem 1 has been established in the case when $L/\mathbb{Q}$ is a Galois extension.

In general, for a quartic extension L of $\mathbb{Q}$ the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ can be C_4, V_4, D_8, A_4 or S_4. However, for $\mathrm{Gal}(L/\mathbb{Q}) \in \{A_4, S_4\}$ the quartic field L does not contain a quadratic subfield K.
Indeed, if it does, then L is generated by the root of $g(x^2)$, where $g \in \mathbb{Q}[x]$ is quadratic, and hence $\mathrm{Gal}(L/\mathbb{Q}) \in \{C_4, V_4, D_8\}$; see, e.g., Awtray and Jakes (2020).

Explanation (continuation)

Consequently, C_4, A_4, D_8 are the three possibilities that may occur for $\mathrm{Gal}(L/\mathbb{Q})$ under assumptions of Theorem 1.

Explanation (continuation)

Consequently, C_4, A_4, D_8 are the three possibilities that may occur for $\mathrm{Gal}(L/\mathbb{Q})$ under assumptions of Theorem 1.

The previous result (when $L/\mathbb{Q}$ is a Galois extension) covers the cases $\mathrm{Gal}(L/\mathbb{Q}) = C_4$ (the cyclic group of order 4)

Consequently, C_4, A_4, D_8 are the three possibilities that may occur for $\mathrm{Gal}(L/\mathbb{Q})$ under assumptions of Theorem 1.

The previous result (when $L/\mathbb{Q}$ is a Galois extension) covers the cases $\mathrm{Gal}(L/\mathbb{Q}) = C_4$ (the cyclic group of order 4) and $\mathrm{Gal}(L/\mathbb{Q}) = V_4$ (the Klein 4-group).

Explanation (continuation)

Consequently, C_4, A_4, D_8 are the three possibilities that may occur for $\mathrm{Gal}(L/\mathbb{Q})$ under assumptions of Theorem 1.

The previous result (when $L/\mathbb{Q}$ is a Galois extension) covers the cases $\mathrm{Gal}(L/\mathbb{Q}) = C_4$ (the cyclic group of order 4) and $\mathrm{Gal}(L/\mathbb{Q}) = V_4$ (the Klein 4-group).

In addition to those two cases, Theorem 1 covers the only remaining possible case when L is not a Galois extension of $\mathbb{Q}$ and $\mathrm{Gal}(L/\mathbb{Q}) = D_8$ (the dihedral group of order 8, which in some literature is denoted by D_4).

Inequality becomes equality for some extensions

Note that for each algebraic number β of degree $d \geqslant 2$ there is a number field L satisfying $[L : \mathbb{Q}(\beta)] = D$ for which equality in (2) holds.

Inequality becomes equality for some extensions

Note that for each algebraic number β of degree $d \geqslant 2$ there is a number field L satisfying $[L : \mathbb{Q}(\beta)] = D$ for which equality in (2) holds.

Indeed, since $\beta \neq 0$, by Hilbert's irreducibility theorem, there are infinitely many $m \in \mathbb{Z}$ for which $x^D - m\beta$ is irreducible over the field $\mathbb{Q}(\beta)$.

Inequality becomes equality for some extensions

Note that for each algebraic number β of degree $d \geqslant 2$ there is a number field L satisfying $[L : \mathbb{Q}(\beta)] = D$ for which equality in (2) holds.

Indeed, since $\beta \neq 0$, by Hilbert's irreducibility theorem, there are infinitely many $m \in \mathbb{Z}$ for which $x^D - m\beta$ is irreducible over the field $\mathbb{Q}(\beta)$. For any of those $m \neq 0$ it follows that $\alpha = (m\beta)^{1/D}$ is a generator of the field

$$L = \mathbb{Q}(\beta, \alpha) = \mathbb{Q}(\alpha),$$

Inequality becomes equality for some extensions

Note that for each algebraic number β of degree $d \geqslant 2$ there is a number field L satisfying $[L : \mathbb{Q}(\beta)] = D$ for which equality in (2) holds.

Indeed, since $\beta \neq 0$, by Hilbert's irreducibility theorem, there are infinitely many $m \in \mathbb{Z}$ for which $x^D - m\beta$ is irreducible over the field $\mathbb{Q}(\beta)$. For any of those $m \neq 0$ it follows that $\alpha = (m\beta)^{1/D}$ is a generator of the field

$$L = \mathbb{Q}(\beta, \alpha) = \mathbb{Q}(\alpha),$$

and hence $\beta = \frac{1}{m}\alpha^D$ (so $f(x) = x^D/m$), which implies $\deg_L(\beta) = D$ by (2).

In general the inequality should be strict?

However, it seems very likely that for a ‘random’ β of degree $d \geqslant 3$ and a ‘random’ degree D extension L of $\mathbb{Q}(\beta)$ one should expect the strict inequality $\deg_L(\beta) > D$.

In general the inequality should be strict?

However, it seems very likely that for a 'random' β of degree $d \geqslant 3$ and a 'random' degree D extension L of $\mathbb{Q}(\beta)$ one should expect the strict inequality $\deg_L(\beta) > D$.

The problem is difficult, since even in simplest cases it gives some complicated diophantine equations, which apparently have no solutions, but there are no methods to treat them.

In general the inequality should be strict?

However, it seems very likely that for a 'random' β of degree $d \geqslant 3$ and a 'random' degree D extension L of $\mathbb{Q}(\beta)$ one should expect the strict inequality $\deg_L(\beta) > D$.

The problem is difficult, since even in simplest cases it gives some complicated diophantine equations, which apparently have no solutions, but there are no methods to treat them. In Park & Park for some special extensions they used elliptic curves, but the results are very special and very limited.

From now on, we will consider the case $D = 2$ only. We first investigate the pair $(d, D) = (3, 2)$ and show the existence of many cubic numbers β for which there are infinitely many quadratic extensions L of $\mathbb{Q}(\beta)$ such that $\deg_L(\beta) > 2$.

Cubic number in a quadratic extension

From now on, we will consider the case $D = 2$ only. We first investigate the pair $(d, D) = (3, 2)$ and show the existence of many cubic numbers β for which there are infinitely many quadratic extensions L of $\mathbb{Q}(\beta)$ such that $\deg_L(\beta) > 2$.

Recall that the *trace* of an algebraic number is the sum of its algebraic conjugates over $\mathbb{Q}$.

Cubic number in a quadratic extension

From now on, we will consider the case $D = 2$ only. We first investigate the pair $(d, D) = (3, 2)$ and show the existence of many cubic numbers β for which there are infinitely many quadratic extensions L of $\mathbb{Q}(\beta)$ such that $\deg_L(\beta) > 2$.

Recall that the *trace* of an algebraic number is the sum of its algebraic conjugates over $\mathbb{Q}$.

In view of (1) it suffices to consider algebraic integers β of trace zero.

Cubic number in a quadratic extension

Theorem 2

Let β be a cubic algebraic integer with trace zero and minimal polynomial $x^3 - kx - q$, where $k \in \mathbb{Z}$ and $q \in \mathbb{Z}^*$.

Cubic number in a quadratic extension

Theorem 2

Let β be a cubic algebraic integer with trace zero and minimal polynomial $x^3 - kx - q$, where $k \in \mathbb{Z}$ and $q \in \mathbb{Z}^*$. Assume that at least one of the following conditions holds:

Cubic number in a quadratic extension

Theorem 2

Let β be a cubic algebraic integer with trace zero and minimal polynomial $x^3 - kx - q$, where $k \in \mathbb{Z}$ and $q \in \mathbb{Z}^*$. Assume that at least one of the following conditions holds:

(i) $4k^3 - 27q^2 > 0$;

Theorem 2

Let β be a cubic algebraic integer with trace zero and minimal polynomial $x^3 - kx - q$, where $k \in \mathbb{Z}$ and $q \in \mathbb{Z}^*$. Assume that at least one of the following conditions holds:

(i) $4k^3 - 27q^2 > 0$;

(ii) *k is odd and $q \not\equiv 2 \pmod 4$;*

Cubic number in a quadratic extension

Theorem 2

Let β be a cubic algebraic integer with trace zero and minimal polynomial $x^3 - kx - q$, where $k \in \mathbb{Z}$ and $q \in \mathbb{Z}^*$. Assume that at least one of the following conditions holds:

(i) $4k^3 - 27q^2 > 0$;

(ii) k *is odd and* $q \not\equiv 2 \pmod 4$;

(iii) k, q *are both even and* $k \equiv 2 \pmod 4$ *or* $q \equiv 2 \pmod 4$;

Theorem 2

Let β be a cubic algebraic integer with trace zero and minimal polynomial $x^3 - kx - q$, where $k \in \mathbb{Z}$ and $q \in \mathbb{Z}^*$. Assume that at least one of the following conditions holds:

(i) $4k^3 - 27q^2 > 0$;

(ii) k *is odd and* $q \not\equiv 2 \pmod 4$;

(iii) k, q *are both even and* $k \equiv 2 \pmod 4$ *or* $q \equiv 2 \pmod 4$;

(iv) k *is divisible by* 4 *and* q *is odd;*

Cubic number in a quadratic extension

Theorem 2

Let β be a cubic algebraic integer with trace zero and minimal polynomial $x^3 - kx - q$, where $k \in \mathbb{Z}$ and $q \in \mathbb{Z}^*$. Assume that at least one of the following conditions holds:

(i) $4k^3 - 27q^2 > 0$;

(ii) k *is odd and* $q \not\equiv 2 \pmod 4$;

(iii) k, q *are both even and* $k \equiv 2 \pmod 4$ *or* $q \equiv 2 \pmod 4$;

(iv) k *is divisible by* 4 *and* q *is odd;*

(v) $k \equiv 1 \pmod 4$ *and* $q \equiv 2 \pmod 4$;

Cubic number in a quadratic extension

Theorem 2

Let β be a cubic algebraic integer with trace zero and minimal polynomial $x^3 - kx - q$, where $k \in \mathbb{Z}$ and $q \in \mathbb{Z}^*$. Assume that at least one of the following conditions holds:

(i) $4k^3 - 27q^2 > 0$;

(ii) k *is odd and* $q \not\equiv 2 \pmod 4$;

(iii) k, q *are both even and* $k \equiv 2 \pmod 4$ *or* $q \equiv 2 \pmod 4$;

(iv) k *is divisible by* 4 *and* q *is odd;*

(v) $k \equiv 1 \pmod 4$ *and* $q \equiv 2 \pmod 4$;

Then, there are infinitely many quadratic extensions L of $\mathbb{Q}(\beta)$ such that $\deg_L(\beta) > 2$.

Totally real algebraic numbers

Recall that an algebraic number β is called *totally real* if its all conjugates over $\mathbb{Q}$ are real.

Totally real algebraic numbers

Recall that an algebraic number β is called *totally real* if its all conjugates over $\mathbb{Q}$ are real. The condition (i) of Theorem 2 means that the discriminant of the polynomial $x^3 - kx - q$ is positive, which is the case if and only if all three of its roots are real.

Totally real algebraic numbers

Recall that an algebraic number β is called *totally real* if its all conjugates over $\mathbb{Q}$ are real. The condition (i) of Theorem 2 means that the discriminant of the polynomial $x^3 - kx - q$ is positive, which is the case if and only if all three of its roots are real. Thus, part (i) combined with (1) implies that for each totally real cubic algebraic number β there are infinitely many quadratic extensions L of $\mathbb{Q}(\beta)$ for which $\deg_L(\beta) > 2$.

Totally real algebraic numbers

Recall that an algebraic number β is called *totally real* if its all conjugates over $\mathbb{Q}$ are real. The condition (i) of Theorem 2 means that the discriminant of the polynomial $x^3 - kx - q$ is positive, which is the case if and only if all three of its roots are real. Thus, part (i) combined with (1) implies that for each totally real cubic algebraic number β there are infinitely many quadratic extensions L of $\mathbb{Q}(\beta)$ for which $\deg_L(\beta) > 2$.

The same is true for *all* totally real algebraic numbers β of degree $d \geqslant 3$:

Totally real algebraic numbers

Recall that an algebraic number β is called *totally real* if its all conjugates over $\mathbb{Q}$ are real. The condition (i) of Theorem 2 means that the discriminant of the polynomial $x^3 - kx - q$ is positive, which is the case if and only if all three of its roots are real. Thus, part (i) combined with (1) implies that for each totally real cubic algebraic number β there are infinitely many quadratic extensions L of $\mathbb{Q}(\beta)$ for which $\deg_L(\beta) > 2$.

The same is true for *all* totally real algebraic numbers β of degree $d \geqslant 3$:

Theorem 3

For each totally real algebraic number β of degree $d \geqslant 3$ there are infinitely many quadratic extensions L of $\mathbb{Q}(\beta)$ such that $\deg_L(\beta) > 2$.

Cubic algebraic numbers

It seems very likely that Theorem 3 holds for every algebraic number of degree $d \geqslant 3$, but our approach in the case $d \geqslant 4$ leads to some complicated diophantine equations that are very difficult to treat.

Cubic algebraic numbers

It seems very likely that Theorem 3 holds for every algebraic number of degree $d \geqslant 3$, but our approach in the case $d \geqslant 4$ leads to some complicated diophantine equations that are very difficult to treat.

Towards completing the cubic case we will also show the following.

Cubic algebraic numbers

It seems very likely that Theorem 3 holds for every algebraic number of degree $d \geqslant 3$, but our approach in the case $d \geqslant 4$ leads to some complicated diophantine equations that are very difficult to treat.

Towards completing the cubic case we will also show the following.

Theorem 4

For each cubic algebraic integer β satisfying $\beta^3 = k\beta + q$ with $k, q \in \mathbb{Z}$ the conclusion of Theorem 2 is true

Cubic algebraic numbers

It seems very likely that Theorem 3 holds for every algebraic number of degree $d \geqslant 3$, but our approach in the case $d \geqslant 4$ leads to some complicated diophantine equations that are very difficult to treat.

Towards completing the cubic case we will also show the following.

Theorem 4

For each cubic algebraic integer β satisfying $\beta^3 = k\beta + q$ with $k, q \in \mathbb{Z}$ the conclusion of Theorem 2 is true except possibly for some pairs $(k, q) \in \mathbb{Z}^2$ for which there is an integer $m \geqslant 0$ such that

It seems very likely that Theorem 3 holds for every algebraic number of degree $d \geqslant 3$, but our approach in the case $d \geqslant 4$ leads to some complicated diophantine equations that are very difficult to treat.

Towards completing the cubic case we will also show the following.

Theorem 4

For each cubic algebraic integer β satisfying $\beta^3 = k\beta + q$ with $k, q \in \mathbb{Z}$ the conclusion of Theorem 2 is true except possibly for some pairs $(k, q) \in \mathbb{Z}^2$ for which there is an integer $m \geqslant 0$ such that

$$k^* = k2^{-2m} \equiv 3 \pmod 4 \text{ and } q^* = q2^{-3m} \equiv 2 \pmod 4. \quad (3)$$

Explanation

So far, some examples of irrational algebraic numbers β and quadratic extensions L of $K = \mathbb{Q}(\beta)$ for which $\deg_L(\beta) > 2$ only appear in Park & Park and only for some special quartic fields K.

Explanation

So far, some examples of irrational algebraic numbers β and quadratic extensions L of $K = \mathbb{Q}(\beta)$ for which $\deg_L(\beta) > 2$ only appear in Park & Park and only for some special quartic fields K.

For instance, this is the case for $\beta = \sqrt{2} + \sqrt{3}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

Explanation

So far, some examples of irrational algebraic numbers β and quadratic extensions L of $K = \mathbb{Q}(\beta)$ for which $\deg_L(\beta) > 2$ only appear in Park & Park and only for some special quartic fields K.

For instance, this is the case for $\beta = \sqrt{2} + \sqrt{3}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

Our Theorem 1 shows that there are no such quadratic β, while Theorems 2, 3 and 4 provide a large class of such examples.

Relation to other work

In fact, one can derive the existence of such β of degree $d \geqslant 3$ in the case when

$$\mathbb{Q} + \beta\mathbb{Q}^* \cap \mathbb{Q}(\beta)^2 = \emptyset, \qquad (4)$$

Relation to other work

In fact, one can derive the existence of such β of degree $d \geqslant 3$ in the case when

$$\mathbb{Q} + \beta\mathbb{Q}^* \cap \mathbb{Q}(\beta)^2 = \emptyset, \tag{4}$$

where $\mathbb{Q} + \beta\mathbb{Q}^*$ consists of all possible sums $a + b\beta$ with rational numbers a and $b \neq 0$.

Relation to other work

In fact, one can derive the existence of such β of degree $d \geqslant 3$ in the case when

$$\mathbb{Q} + \beta\mathbb{Q}^* \cap \mathbb{Q}(\beta)^2 = \emptyset, \tag{4}$$

where $\mathbb{Q} + \beta\mathbb{Q}^*$ consists of all possible sums $a + b\beta$ with rational numbers a and $b \neq 0$.
This question has been considered in Drungilas & Dubickas (2020) in a completely different context:

Relation to other work

In fact, one can derive the existence of such β of degree $d \geqslant 3$ in the case when

$$\mathbb{Q} + \beta\mathbb{Q}^* \cap \mathbb{Q}(\beta)^2 = \emptyset, \qquad (4)$$

where $\mathbb{Q} + \beta\mathbb{Q}^*$ consists of all possible sums $a + b\beta$ with rational numbers a and $b \neq 0$.

This question has been considered in Drungilas & Dubickas (2020) in a completely different context: for a given polynomial $f \in \mathbb{Q}[x]$ which is irreducible over $\mathbb{Q}$ find $g \in \mathbb{Q}[x]$ of smallest possible degree such that the composition polynomial $f(g(x))$ is reducible over $\mathbb{Q}$.

Relation to other work

In fact, one can derive the existence of such β of degree $d \geqslant 3$ in the case when

$$\mathbb{Q} + \beta\mathbb{Q}^* \cap \mathbb{Q}(\beta)^2 = \emptyset, \tag{4}$$

where $\mathbb{Q} + \beta\mathbb{Q}^*$ consists of all possible sums $a + b\beta$ with rational numbers a and $b \neq 0$.

This question has been considered in Drungilas & Dubickas (2020) in a completely different context: for a given polynomial $f \in \mathbb{Q}[x]$ which is irreducible over $\mathbb{Q}$ find $g \in \mathbb{Q}[x]$ of smallest possible degree such that the composition polynomial $f(g(x))$ is reducible over $\mathbb{Q}$. This trivially holds for $g(x) = f(x) + x$, since $f(f(x) + x)$ is divisible by $f(x)$; see, e.g.,

Relation to other work: some literature

- F. Lemmermeyer, Composite values of irreducible polynomials, *Elem. Math.* **74** (2019), 36–37.
- M. Ulas, Is every irreducible polynomial reducible after a polynomial substitution? *J. Number Theory* **202** (2019), 37–59.

Relation to other work: some literature

- F. Lemmermeyer, Composite values of irreducible polynomials, *Elem. Math.* **74** (2019), 36–37.
- M. Ulas, Is every irreducible polynomial reducible after a polynomial substitution? *J. Number Theory* **202** (2019), 37–59.

A similar question on whether, for a fixed rational $a \neq 0$ and cubic algebraic number β, the set

$$\mathbb{Q} + a\beta \cap \mathbb{Q}(\beta)^2$$

is empty or not has been considered in

Relation to other work: some literature

- F. Lemmermeyer, Composite values of irreducible polynomials, *Elem. Math.* **74** (2019), 36–37.
- M. Ulas, Is every irreducible polynomial reducible after a polynomial substitution? *J. Number Theory* **202** (2019), 37–59.

A similar question on whether, for a fixed rational $a \neq 0$ and cubic algebraic number β, the set

$$\mathbb{Q} + a\beta \cap \mathbb{Q}(\beta)^2$$

is empty or not has been considered in

- F. Lemmermeyer, Binomial squares in pure cubic number fields, *J. Théor. Nombres Bordeaux*, **24** (2012), 691–704.

Relation to other work

In particular, we have shown in Drungilas & Dubickas (2020) that (4) does not hold for all β of degree at most 3.

Relation to other work

In particular, we have shown in Drungilas & Dubickas (2020) that (4) does not hold for all β of degree at most 3.

Observe that for any $d \geqslant 4$ there exist β of degree d for which (4) does not hold.

In particular, we have shown in Drungilas & Dubickas (2020) that (4) does not hold for all β of degree at most 3.

Observe that for any $d \geqslant 4$ there exist β of degree d for which (4) does not hold.

For instance, for d even we can take β satisfying $\beta^d = \beta + 1$, since then $1 + \beta$ is the square of $\beta^{d/2} \in \mathbb{Q}(\beta)$,

Relation to other work

In particular, we have shown in Drungilas & Dubickas (2020) that (4) does not hold for all β of degree at most 3.

Observe that for any $d \geqslant 4$ there exist β of degree d for which (4) does not hold.

For instance, for d even we can take β satisfying $\beta^d = \beta + 1$, since then $1 + \beta$ is the square of $\beta^{d/2} \in \mathbb{Q}(\beta)$, while for d odd we can take $\beta = 2^{1/d}$, since then 2β is the square of $\beta^{(d+1)/2} \in \mathbb{Q}(\beta)$.

Relation to other work

On the other hand, we showed in that (4) holds, e.g., for $\beta = (1+i)/\sqrt{2}$ of degree 4.

Relation to other work

On the other hand, we showed in that (4) holds, e.g., for $\beta = (1+i)/\sqrt{2}$ of degree 4. By the next proposition, this implies that $\deg_L((1+i)/\sqrt{2}) > 2$ for each

$$L = \mathbb{Q}(\beta, \sqrt{B}) = \mathbb{Q}(i, \sqrt{2}, \sqrt{B}),$$

where B is a square-free integer such that $\sqrt{B} \notin \mathbb{Q}(\beta)$.

Relation to other work

On the other hand, we showed in that (4) holds, e.g., for $\beta = (1+i)/\sqrt{2}$ of degree 4. By the next proposition, this implies that $\deg_L((1+i)/\sqrt{2}) > 2$ for each

$$L = \mathbb{Q}(\beta, \sqrt{B}) = \mathbb{Q}(i, \sqrt{2}, \sqrt{B}),$$

where B is a square-free integer such that $\sqrt{B} \notin \mathbb{Q}(\beta)$.

Proposition 1

Let β be an algebraic number of degree $d \geqslant 4$ satisfying (4). Then, for each square-free integer B such that $\sqrt{B} \notin \mathbb{Q}(\beta)$ the field $L = \mathbb{Q}(\beta, \sqrt{B})$ is a quadratic extension of $\mathbb{Q}(\beta)$ and $\deg_L(\beta) > 2$.

Construction of a class of non-squares

The important element in the proofs of Theorems 2, 3 and 4 is the next proposition which is slightly more general than that above:

Construction of a class of non-squares

The important element in the proofs of Theorems 2, 3 and 4 is the next proposition which is slightly more general than that above:

Proposition 2

Let β *be an algebraic number of degree* $d \geqslant 3$*. Suppose that there exists* $\gamma \in \mathbb{Q}(\beta)$ *such that*

Construction of a class of non-squares

The important element in the proofs of Theorems 2, 3 and 4 is the next proposition which is slightly more general than that above:

Proposition 2

Let β be an algebraic number of degree $d \geqslant 3$. Suppose that there exists $\gamma \in \mathbb{Q}(\beta)$ such that

$$(a + b\beta)\gamma \notin \mathbb{Q}(\beta)^2 \tag{5}$$

for all rational numbers a, b, not both zeroes.

Construction of a class of non-squares

The important element in the proofs of Theorems 2, 3 and 4 is the next proposition which is slightly more general than that above:

Proposition 2

Let β be an algebraic number of degree $d \geqslant 3$. Suppose that there exists $\gamma \in \mathbb{Q}(\beta)$ such that

$$(a + b\beta)\gamma \notin \mathbb{Q}(\beta)^2 \tag{5}$$

for all rational numbers a, b, not both zeroes. Then, there is an infinite sequence of prime numbers

$$p_1 < p_2 < p_3 < \dots$$

Construction of a class of non-squares

The important element in the proofs of Theorems 2, 3 and 4 is the next proposition which is slightly more general than that above:

Proposition 2

Let β be an algebraic number of degree $d \geqslant 3$. Suppose that there exists $\gamma \in \mathbb{Q}(\beta)$ such that

$$(a + b\beta)\gamma \notin \mathbb{Q}(\beta)^2 \tag{5}$$

for all rational numbers a, b, not both zeroes. Then, there is an infinite sequence of prime numbers

$$p_1 < p_2 < p_3 < \dots$$

such that the fields $L_i = \mathbb{Q}(\beta, \sqrt{p_i\gamma})$, $i = 1, 2, 3, \dots,$ are pairwise distinct quadratic extensions of $\mathbb{Q}(\beta)$ and $\deg_{L_i}(\beta) > 2$.

An ingredient for the proofs of Theorems 2 and 4

In the proofs of Theorems 2 and 4 we used a classical result of Legendre:

An ingredient for the proofs of Theorems 2 and 4

In the proofs of Theorems 2 and 4 we used a classical result of Legendre:

Lemma 5

Let a, b, c be three nonzero integers, not all of the same sign, and such that abc is square-free.

An ingredient for the proofs of Theorems 2 and 4

In the proofs of Theorems 2 and 4 we used a classical result of Legendre:

Lemma 5

Let a, b, c be three nonzero integers, not all of the same sign, and such that abc is square-free. Then, the Diophantine equation

$$ax^2 + by^2 + cz^2 = 0$$

is solvable in integers x, y, z, not all zero,

An ingredient for the proofs of Theorems 2 and 4

In the proofs of Theorems 2 and 4 we used a classical result of Legendre:

Lemma 5

Let a, b, c be three nonzero integers, not all of the same sign, and such that abc is square-free. Then, the Diophantine equation

$$ax^2 + by^2 + cz^2 = 0$$

is solvable in integers x, y, z, not all zero, if and only if $-bc$, $-ca$, $-ab$ are quadratic residues of a, b, c, respectively.

Proof of Theorem 3 (when β is totally real)

The main ingredient is the next lemma.

Proof of Theorem 3 (when β is totally real)

The main ingredient is the next lemma.

Lemma 6

Let β be a totally real algebraic number of degree $d \geqslant 3$.

Proof of Theorem 3 (when β is totally real)

The main ingredient is the next lemma.

Lemma 6

Let β be a totally real algebraic number of degree $d \geqslant 3$. Then, there is $\gamma \in \mathbb{Q}(\beta)$ of degree d

Proof of Theorem 3 (when β is totally real)

The main ingredient is the next lemma.

Lemma 6

Let β be a totally real algebraic number of degree $d \geqslant 3$. Then, there is $\gamma \in \mathbb{Q}(\beta)$ of degree d such that for any rational numbers a, b, not both zeroes, the number $(a + b\beta)\gamma$ is not a square in the field $\mathbb{Q}(\beta)$.

Proof of Lemma 6

Fix β of degree d. By shifting β by a rational number, if necessary, we can assume without restriction of generality that its trace is zero.

Proof of Lemma 6

Fix β of degree d. By shifting β by a rational number, if necessary, we can assume without restriction of generality that its trace is zero. Let $\sigma_1, \dots, \sigma_d$ be the d distinct embeddings of the field $K = \mathbb{Q}(\beta)$ into $\mathbb{C}$.

Proof of Lemma 6

Fix β of degree d. By shifting β by a rational number, if necessary, we can assume without restriction of generality that its trace is zero. Let $\sigma_1, \dots, \sigma_d$ be the d distinct embeddings of the field $K = \mathbb{Q}(\beta)$ into $\mathbb{C}$. For each $\alpha \in K$ we define

$$\mathrm{Trace}(\alpha) := \sum_{j=1}^{n} \sigma_j(\alpha).$$

Proof of Lemma 6

Fix β of degree d. By shifting β by a rational number, if necessary, we can assume without restriction of generality that its trace is zero. Let $\sigma_1, \dots, \sigma_d$ be the d distinct embeddings of the field $K = \mathbb{Q}(\beta)$ into $\mathbb{C}$. For each $\alpha \in K$ we define

$$\mathrm{Trace}(\alpha) := \sum_{j=1}^{n} \sigma_j(\alpha).$$

This trace function satisfies the property of the linear mapping

$$\mathrm{Trace}(u_1\alpha_1 + \cdots + u_m\alpha_m) = u_1\mathrm{Trace}(\alpha_1) + \cdots + u_m\mathrm{Trace}(\alpha_m) \quad (6)$$

for $u_i \in \mathbb{Q}$ and $\alpha_i \in K$.

Proof of Lemma 6

Fix β of degree d. By shifting β by a rational number, if necessary, we can assume without restriction of generality that its trace is zero. Let $\sigma_1, \dots, \sigma_d$ be the d distinct embeddings of the field $K = \mathbb{Q}(\beta)$ into $\mathbb{C}$. For each $\alpha \in K$ we define

$$\mathrm{Trace}(\alpha) := \sum_{j=1}^{n} \sigma_j(\alpha).$$

This trace function satisfies the property of the linear mapping

$$\mathrm{Trace}(u_1\alpha_1 + \cdots + u_m\alpha_m) = u_1\mathrm{Trace}(\alpha_1) + \cdots + u_m\mathrm{Trace}(\alpha_m) \quad (6)$$

for $u_i \in \mathbb{Q}$ and $\alpha_i \in K$. If α lies in a proper subfield of K, then $\mathrm{Trace}(\alpha)$ is equal to $[K : \mathbb{Q}(\alpha)]$ multiplied by the trace of α.

Proof of Lemma 6 (continuation)

Now, for each $k \in \mathbb{N}$ we set

$$t_k := \mathrm{Trace}(\beta^k) \in \mathbb{Q}.$$

Proof of Lemma 6 (continuation)

Now, for each $k \in \mathbb{N}$ we set

$$t_k := \mathrm{Trace}(\beta^k) \in \mathbb{Q}.$$

Let $f \in \mathbb{Q}[x]$ be the minimal (monic) polynomial of β over $\mathbb{Q}$.

Now, for each $k \in \mathbb{N}$ we set

$$t_k := \mathrm{Trace}(\beta^k) \in \mathbb{Q}.$$

Let $f \in \mathbb{Q}[x]$ be the minimal (monic) polynomial of β over $\mathbb{Q}$. We consider two cases, first, when $f(x) = g(x)^2$ for some $g \in \mathbb{Q}[x]$, and, second, when f is not of such form.

Proof of Lemma 6 (continuation)

Now, for each $k \in \mathbb{N}$ we set

$$t_k := \mathrm{Trace}(\beta^k) \in \mathbb{Q}.$$

Let $f \in \mathbb{Q}[x]$ be the minimal (monic) polynomial of β over $\mathbb{Q}$. We consider two cases, first, when $f(x) = g(x)^2$ for some $g \in \mathbb{Q}[x]$, and, second, when f is not of such form.

We begin with the latter case. It is clear that $t_k > 0$ for k even, since the number β^k is totally positive for such k.

Now, for each $k \in \mathbb{N}$ we set

$$t_k := \mathrm{Trace}(\beta^k) \in \mathbb{Q}.$$

Let $f \in \mathbb{Q}[x]$ be the minimal (monic) polynomial of β over $\mathbb{Q}$. We consider two cases, first, when $f(x) = g(x)^2$ for some $g \in \mathbb{Q}[x]$, and, second, when f is not of such form.

We begin with the latter case. It is clear that $t_k > 0$ for k even, since the number β^k is totally positive for such k. Set

$$\gamma := -\frac{t_2}{d} - \frac{t_3}{t_2}\beta + \beta^2 \in \mathbb{Q}(\beta). \tag{7}$$

Proof of Lemma 6 (continuation)

Recall that $t_1 = 0$ by the assumption on β. With the choice of γ as in (7), by (6), we obtain $\mathrm{Trace}(\gamma) = -t_2 - 0 + t_2 = 0$.

Proof of Lemma 6 (continuation)

Recall that $t_1 = 0$ by the assumption on β. With the choice of γ as in (7), by (6), we obtain $\mathrm{Trace}(\gamma) = -t_2 - 0 + t_2 = 0$. Likewise, by (6),

$$\mathrm{Trace}(\beta\gamma) = \mathrm{Trace}\Big(-\frac{t_2}{d}\beta - \frac{t_3}{t_2}\beta^2 + \beta^3\Big) = 0 - t_3 + t_3 = 0.$$

Proof of Lemma 6 (continuation)

Recall that $t_1 = 0$ by the assumption on β. With the choice of γ as in (7), by (6), we obtain $\mathrm{Trace}(\gamma) = -t_2 - 0 + t_2 = 0$. Likewise, by (6),

$$\mathrm{Trace}(\beta\gamma) = \mathrm{Trace}\big(-\frac{t_2}{d}\beta - \frac{t_3}{t_2}\beta^2 + \beta^3\big) = 0 - t_3 + t_3 = 0.$$

By $\mathrm{Trace}(\beta) = \mathrm{Trace}(\beta\gamma) = 0$ and (6), for any $a, b \in \mathbb{Q}$ it follows that

$$\mathrm{Trace}((a + b\beta)\gamma) = a\mathrm{Trace}(\beta) + b\mathrm{Trace}(\beta\gamma) = 0.$$

Proof of Lemma 6 (continuation)

Recall that $t_1 = 0$ by the assumption on β. With the choice of γ as in (7), by (6), we obtain $\mathrm{Trace}(\gamma) = -t_2 - 0 + t_2 = 0$. Likewise, by (6),

$$\mathrm{Trace}(\beta\gamma) = \mathrm{Trace}\left(-\frac{t_2}{d}\beta - \frac{t_3}{t_2}\beta^2 + \beta^3\right) = 0 - t_3 + t_3 = 0.$$

By $\mathrm{Trace}(\beta) = \mathrm{Trace}(\beta\gamma) = 0$ and (6), for any $a, b \in \mathbb{Q}$ it follows that

$$\mathrm{Trace}((a + b\beta)\gamma) = a\mathrm{Trace}(\beta) + b\mathrm{Trace}(\beta\gamma) = 0.$$

Note that the trace of each nonzero $\alpha \in \mathbb{Q}(\beta)^2$ must be positive, because such α is totally positive.

Proof of Lemma 6 (continuation)

Recall that $t_1 = 0$ by the assumption on β. With the choice of γ as in (7), by (6), we obtain $\mathrm{Trace}(\gamma) = -t_2 - 0 + t_2 = 0$. Likewise, by (6),

$$\mathrm{Trace}(\beta\gamma) = \mathrm{Trace}\Big(-\frac{t_2}{d}\beta - \frac{t_3}{t_2}\beta^2 + \beta^3\Big) = 0 - t_3 + t_3 = 0.$$

By $\mathrm{Trace}(\beta) = \mathrm{Trace}(\beta\gamma) = 0$ and (6), for any $a, b \in \mathbb{Q}$ it follows that

$$\mathrm{Trace}((a + b\beta)\gamma) = a\mathrm{Trace}(\beta) + b\mathrm{Trace}(\beta\gamma) = 0.$$

Note that the trace of each nonzero $\alpha \in \mathbb{Q}(\beta)^2$ must be positive, because such α is totally positive. Hence, $\mathrm{Trace}(\alpha) > 0$ for each nonzero $\alpha \in \mathbb{Q}(\beta)^2$.

Proof of Lemma 6 (continuation)

Recall that $t_1 = 0$ by the assumption on β. With the choice of γ as in (7), by (6), we obtain $\mathrm{Trace}(\gamma) = -t_2 - 0 + t_2 = 0$. Likewise, by (6),

$$\mathrm{Trace}(\beta\gamma) = \mathrm{Trace}\Big(- \frac{t_2}{d}\beta - \frac{t_3}{t_2}\beta^2 + \beta^3\Big) = 0 - t_3 + t_3 = 0.$$

By $\mathrm{Trace}(\beta) = \mathrm{Trace}(\beta\gamma) = 0$ and (6), for any $a, b \in \mathbb{Q}$ it follows that

$$\mathrm{Trace}((a + b\beta)\gamma) = a\mathrm{Trace}(\beta) + b\mathrm{Trace}(\beta\gamma) = 0.$$

Note that the trace of each nonzero $\alpha \in \mathbb{Q}(\beta)^2$ must be positive, because such α is totally positive. Hence, $\mathrm{Trace}(\alpha) > 0$ for each nonzero $\alpha \in \mathbb{Q}(\beta)^2$. But we already showed that $\mathrm{Trace}((a + b\beta)\gamma) = 0$, so $(a + b\beta)\gamma \notin \mathbb{Q}(\beta)^2$, since $a + b\beta \neq 0$ and $\gamma \neq 0$ by (7).

Proof of Lemma 6 (continuation)

It remains to show that γ is of degree d.

Proof of Lemma 6 (continuation)

It remains to show that γ is of degree d. If not, then for some conjugate $\beta' \neq \beta$ of β we must have

$$-\frac{t_2}{d} - \frac{t_3}{t_2}\beta + \beta^2 = -\frac{t_2}{d} - \frac{t_3}{t_2}\beta' + \beta'^2.$$

Proof of Lemma 6 (continuation)

It remains to show that γ is of degree d. If not, then for some conjugate $\beta' \neq \beta$ of β we must have

$$-\frac{t_2}{d} - \frac{t_3}{t_2}\beta + \beta^2 = -\frac{t_2}{d} - \frac{t_3}{t_2}\beta' + \beta'^2.$$

This is equivalent to $\beta + \beta' = t_3/t_2$. Since the trace of β is zero, this is only possible if $t_3 = 0$. Hence, $\beta + \beta' = 0$, that is, $-\beta$ is a conjugate of β, which means that $f(x) = g(x)^2$ for some $g \in \mathbb{Q}[x]$.

Proof of Lemma 6 (continuation)

It remains to show that γ is of degree d. If not, then for some conjugate $\beta' \neq \beta$ of β we must have

$$-\frac{t_2}{d} - \frac{t_3}{t_2}\beta + \beta^2 = -\frac{t_2}{d} - \frac{t_3}{t_2}\beta' + \beta'^2.$$

This is equivalent to $\beta + \beta' = t_3/t_2$. Since the trace of β is zero, this is only possible if $t_3 = 0$. Hence, $\beta + \beta' = 0$, that is, $-\beta$ is a conjugate of β, which means that $f(x) = g(x)^2$ for some $g \in \mathbb{Q}[x]$. This is not allowed by our assumption on f, which completes the proof of the lemma in the second case.

Proof of Lemma 6 (continuation)

Now, we consider the first case, when $f(x) = g(x)^2$ for some $g \in \mathbb{Q}[x]$.

Proof of Lemma 6 (continuation)

Now, we consider the first case, when $f(x) = g(x)^2$ for some $g \in \mathbb{Q}[x]$. Then, d must be even, so $d \geqslant 4$. This time, we select

$$\gamma := -\frac{t_2}{d} - \frac{g_0 t_4}{t_2}\beta + \beta^2 + g_0\beta^3, \tag{8}$$

where $g_0 \in \mathbb{N}$ will be chosen later.

Now, we consider the first case, when $f(x) = g(x)^2$ for some $g \in \mathbb{Q}[x]$. Then, d must be even, so $d \geqslant 4$. This time, we select

$$\gamma := -\frac{t_2}{d} - \frac{g_0 t_4}{t_2}\beta + \beta^2 + g_0\beta^3, \tag{8}$$

where $g_0 \in \mathbb{N}$ will be chosen later. Since $f(x) = g(x)^2$, we clearly have $t_1 = t_3 = 0$, and so $\mathrm{Trace}(\gamma) = -t_2 - 0 + t_2 + 0 = 0$.

Proof of Lemma 6 (continuation)

Now, we consider the first case, when $f(x) = g(x)^2$ for some $g \in \mathbb{Q}[x]$. Then, d must be even, so $d \geqslant 4$. This time, we select

$$\gamma := -\frac{t_2}{d} - \frac{g_0 t_4}{t_2}\beta + \beta^2 + g_0\beta^3, \tag{8}$$

where $g_0 \in \mathbb{N}$ will be chosen later. Since $f(x) = g(x)^2$, we clearly have $t_1 = t_3 = 0$, and so $\mathrm{Trace}(\gamma) = -t_2 - 0 + t_2 + 0 = 0$. Similarly,

$$\mathrm{Trace}(\beta\gamma) = \mathrm{Trace}(-\frac{t_2}{d}\beta - \frac{g_0 t_4}{t_2}\beta^2 + \beta^3 + g_0\beta^4) = 0 - g_0 t_4 + 0 + g_0 t_4 = 0.$$

Proof of Lemma 6 (continuation)

As above, we deduce that $(a + b\beta)\gamma \notin \mathbb{Q}(\beta)^2$, so it remains to show that γ is of degree d.

As above, we deduce that $(a+b\beta)\gamma \notin \mathbb{Q}(\beta)^2$, so it remains to show that γ is of degree d. If not, then for some conjugate $\beta' \neq \beta$ of β we must have

$$-\frac{t_2}{d} - \frac{g_0 t_4}{t_2}\beta + \beta^2 + g_0\beta^3 = -\frac{t_2}{d} - \frac{g_0 t_4}{t_2}\beta' + \beta'^2 + g_0\beta'^3.$$

As above, we deduce that $(a + b\beta)\gamma \notin \mathbb{Q}(\beta)^2$, so it remains to show that γ is of degree d. If not, then for some conjugate $\beta' \neq \beta$ of β we must have

$$-\frac{t_2}{d} - \frac{g_0 t_4}{t_2}\beta + \beta^2 + g_0\beta^3 = -\frac{t_2}{d} - \frac{g_0 t_4}{t_2}\beta' + \beta'^2 + g_0\beta'^3.$$

This is equivalent to

$$g_0(\beta^2 + \beta'^2 + \beta\beta' - t_4/t_2) + \beta + \beta' = 0. \qquad (9)$$

Proof of Lemma 6 (completion)

However, we can always choose $g_0 \in \mathbb{N}$ so that (9) does not hold, unless there exists a conjugate β' of β such that $\beta' \neq \beta$ and the numbers $\beta^2 + \beta'^2 + \beta\beta' - t_4/t_2$ and $\beta + \beta'$ are both equal to zero.

Proof of Lemma 6 (completion)

However, we can always choose $g_0 \in \mathbb{N}$ so that (9) does not hold, unless there exists a conjugate β' of β such that $\beta' \neq \beta$ and the numbers $\beta^2 + \beta'^2 + \beta\beta' - t_4/t_2$ and $\beta + \beta'$ are both equal to zero.

But in that case we must have $\beta' = -\beta$ and so $\beta^2 + \beta'^2 + \beta\beta' = \beta^2 = t_4/t_2$. Therefore, β is a rational or a quadratic number, which is not the case.

Proof of Lemma 6 (completion)

However, we can always choose $g_0 \in \mathbb{N}$ so that (9) does not hold, unless there exists a conjugate β' of β such that $\beta' \neq \beta$ and the numbers $\beta^2 + \beta'^2 + \beta\beta' - t_4/t_2$ and $\beta + \beta'$ are both equal to zero.

But in that case we must have $\beta' = -\beta$ and so $\beta^2 + \beta'^2 + \beta\beta' = \beta^2 = t_4/t_2$. Therefore, β is a rational or a quadratic number, which is not the case. This shows that with an appropriate choice of $g_0 \in \mathbb{N}$ the number γ defined in (8) is of degree d, and finishes the proof of the lemma.

Completion of the proof of Theorem 3

Proof of Theorem 3.

Fix a totally real β of degree $d \geqslant 3$ and select any $\gamma \in \mathbb{Q}(\beta)$ as claimed in Lemma 6. The assertion of the theorem follows by Proposition 2. $\square$

Publication

- A. DUBICKAS, Minimal degree of an element of a number field with respect to its quadratic extension, *Proc. Indian Acad. of Sciences (Math. Sci.)*, (to appear).