Rational quotients of two linear forms in roots of a polynomial

By Artūras DUBICKAS

Institute of Mathematics, Faculty of Mathematics and Informatics, Vilnius University,
Naugarduko 24, Vilnius LT-03225, Lithuania

(Communicated by Masaki KASHIWARA, M.J.A., Jan. 12, 2018)

Abstract: Let f and g be two linear forms with non-zero rational coefficients in k and ℓ variables, respectively. We describe all separable polynomials P with the property that for any choice of (not necessarily distinct) roots $\lambda_1, \dots, \lambda_{k+\ell}$ of P the quotient between $f(\lambda_1, \dots, \lambda_k)$ and $g(\lambda_{k+1}, \dots, \lambda_{k+\ell}) \neq 0$ belongs to $\mathbf{Q}$. It turns out that each such polynomial has all of its roots in a quadratic extension of $\mathbf{Q}$. This is a continuation of a recent work of Luca who considered the case when $k = \ell = 2$, $f(x_1, x_2)$ and $g(x_1, x_2)$ are both $x_1 - x_2$, solved it, and raised the above problem as an open question.

Key words: Conjugate algebraic numbers; quadratic extensions of $\mathbf{Q}$.

1. Introduction. Consider a class of polynomials $\mathcal{P}$ of degree at least 2 such that $P(x) \in \mathcal{P}$ iff (which throughout means if and only if)

$$P(x) = x^{\delta} \prod_{j=1}^{t} (x^2 - e_j^2 D)$$

for some square-free integer $D \notin \{0, 1\}$, some $\delta \in \{0, 1\}$, and some distinct rational numbers $e_1, \dots, e_t > 0$. Here, $t = \lfloor n/2 \rfloor$, where $n := \deg P$. Throughout, by $Z(P)$ we will denote the set of all roots of $P \in \mathbf{Q}[x]$.

Recently, Luca [5, Theorem 1.2] has shown the following:

Theorem 1. *Let $P \in \mathbf{Q}[x]$ be a monic separable polynomial of degree at least 2 with at least one irrational root. Then, for any $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ in $Z(P)$, where $\lambda_3 \neq \lambda_4$, we have*

$$\frac{\lambda_1 - \lambda_2}{\lambda_3 - \lambda_4} \in \mathbf{Q}$$

iff $P(x + a) \in \mathcal{P}$ for some rational number a.

His motivation comes from some earlier papers [4] and [6]. In this direction, we first prove the following slightly more general theorem:

Theorem 2. *Let $P \in \mathbf{Q}[x]$ be a monic separable polynomial of degree at least 4 with at least one irrational root. Then, for any distinct $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in Z(P)$ we have*

$$\frac{\lambda_1 - \lambda_2}{\lambda_3 - \lambda_4} \in \mathbf{Q}$$

iff $P(x + a) \in \mathcal{P}$ for some rational number a.

Note that the condition of Theorem 2 is weaker than that of Theorem 1: it does not allow the quotients like $(\lambda_1 - \lambda_2)/(\lambda_1 - \lambda_3)$, where $\lambda_1, \lambda_2, \lambda_3$ are distinct, which have been used in the proof of [5, Theorem 1.2]. Nevertheless, the conclusion is the same. It is clear that Theorem 2 immediately implies Theorem 1 in case $n = \deg P \geqslant 4$. For $n = 2$ the statement of Theorem 1 is trivial, whereas for $n = 3$ it follows from Lemma 6 below.

Let k and ℓ be two positive integers, and let

$$f(x_1, \dots, x_k) := a_1 x_1 + \cdots + a_k x_k$$

and

$$g(x_1, \dots, x_\ell) := b_1 x_1 + \cdots + b_\ell x_\ell$$

be two linear forms with some non-zero rational coefficients $a_1, \dots, a_k, b_1, \dots, b_\ell$. In [5, Theorem 1.3], it was shown that if for some monic separable polynomial P and any $\lambda_1, \dots, \lambda_{k+\ell} \in Z(P)$, where $g(\lambda_{k+1}, \dots, \lambda_{k+\ell}) \neq 0$, one has

$$\frac{f(\lambda_1, \dots, \lambda_k)}{g(\lambda_{k+1}, \dots, \lambda_{k+\ell})} \in \mathbf{Q},$$

then the Galois group G_P of the splitting field of $P(x)$ over $\mathbf{Q}$ is of order at most 132.

The next theorem completely describes all such polynomials P. As one can see, Theorem 3 implies that the Galois group G_P has order either 2 (if P

2010 Mathematics Subject Classification. Primary 11R04, 11R11.

doi: 10.3792/pjaa.94.17

has at least one irrational root) or 1 (otherwise). For brevity, let us denote

$$S(f) := f(\underbrace{1,\dots,1}_{k}) \quad \text{and} \quad S(g) := g(\underbrace{1,\dots,1}_{\ell}).$$

Theorem 3. *Let $P \in \mathbf{Q}[x]$ be a monic separable polynomial of degree at least 2 with at least one irrational root. Then, for any (not necessarily distinct) $\lambda_1, \dots, \lambda_{k+\ell} \in Z(P)$, where $g(\lambda_{k+1}, \dots, \lambda_{k+\ell}) \neq 0$, we have*

$$\frac{f(\lambda_1, \dots, \lambda_k)}{g(\lambda_{k+1}, \dots, \lambda_{k+\ell})} \in \mathbf{Q}$$

iff one of the following is true:

(i) *$S(f) = S(g) = 0$ and $P(x+a) \in \mathcal{P}$ for some rational number a;*

(ii) *at least one of the numbers $S(f)$, $S(g)$ is nonzero and $P(x) \in \mathcal{P}$.*

The proofs of the theorems are completely self-contained except for several simple observations which follow from some earlier results on additive and multiplicative relations with conjugate algebraic numbers. Specifically, we shall use the fact that, e.g., by [1, Theorem 4], for any $n \geqslant 3$ distinct algebraic numbers $\alpha_1, \dots, \alpha_n$ conjugate over $\mathbf{Q}$ we have

$$(1) \quad c_1\alpha_1 + \cdots + c_n\alpha_n \notin \mathbf{Q} \quad \text{if} \quad c_1, \dots, c_n \in \mathbf{Q}^*$$

satisfy $|c_1| \geqslant |c_2| + \cdots + |c_n|$. Also, if α_1, α_2 are distinct algebraic numbers conjugate over $\mathbf{Q}$ then

$$(2) \quad \alpha_1 - \alpha_2 \notin \mathbf{Q} \quad \text{and} \quad \alpha_1/\alpha_2 \notin \mathbf{Q} \setminus \{-1\}.$$

This easily follows, by a simple trace and norm considerations, respectively. See, e.g., [2] for the description of all algebraic numbers expressible as differences or as quotients of two conjugate algebraic numbers and [3], [7] for some further work on this problem.

2. Auxiliary results.

Lemma 4. *If $\alpha_1, \alpha_2, \alpha_3$ are distinct algebraic numbers conjugate over $\mathbf{Q}$ then*

$$\frac{\alpha_1 - \alpha_2}{\alpha_1 - \alpha_3} \notin \mathbf{Q}.$$

Proof. Suppose that $\alpha_1 - \alpha_2 = r(\alpha_1 - \alpha_3)$ with $r \in \mathbf{Q}$. Clearly, $r \neq 0$ and $r \neq 1$. Writing this equality in the form

$$(1-r)\alpha_1 - \alpha_2 + r\alpha_3 = 0$$

we see that the rational coefficients $1-r, -1, r$ are all non-zero and sum to zero. Hence, the modulus of one of them equals the sum of the moduli of the other two. This is impossible, by (1). □

Lemma 5. *Suppose that $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ are distinct algebraic numbers, and three of them (or all four) are conjugate over $\mathbf{Q}$. Then, at least one of the following three quotients*

$$\frac{\alpha_1 - \alpha_2}{\alpha_3 - \alpha_4}, \quad \frac{\alpha_1 - \alpha_3}{\alpha_2 - \alpha_4}, \quad \frac{\alpha_1 - \alpha_4}{\alpha_2 - \alpha_3}$$

is irrational.

Proof. Without restriction of generality we may assume that the numbers $\alpha_2, \alpha_3, \alpha_4$ are conjugate over $\mathbf{Q}$. Suppose the quotients considered in the lemma are $q_1, q_2, q_3 \in \mathbf{Q}^*$, respectively. Then, $\alpha_1 - \alpha_2 = q_1(\alpha_3 - \alpha_4)$, $\alpha_1 - \alpha_3 = q_2(\alpha_2 - \alpha_4)$ and $\alpha_1 - \alpha_4 = q_3(\alpha_2 - \alpha_3)$. Subtracting the second equality from the first we obtain

$$(3) \quad (q_2 - 1)\alpha_2 + (1 - q_1)\alpha_3 + (q_1 - q_2)\alpha_4 = 0.$$

Similarly, subtracting the third equality from the first we find that

$$(4) \quad (q_3 - 1)\alpha_2 - (q_1 + q_3)\alpha_3 + (q_1 + 1)\alpha_4 = 0.$$

Let us analyze (3) first. Note that $q_1 = 1$ yields $q_2 = 1$, since otherwise $\alpha_2 = \alpha_4$, which is not the case. Similarly, $q_2 = 1$ leads to $q_1 = 1$ and $q_1 = q_2$ leads to $q_1 = q_2 = 1$. (This happens precisely when $\alpha_1 + \alpha_4 = \alpha_2 + \alpha_3$.) Hence, in case $q_1 \neq 1$, we must have $q_2 \neq 1$ and $q_1 \neq q_2$. However, since the coefficients $q_2 - 1, 1 - q_1, q_1 - q_2$ of (3) sum to zero, this is impossible, by the same argument as in the proof of Lemma 4. Consequently, we must have $q_1 = q_2 = 1$. By exactly the same argument, as the coefficients $q_3 - 1, -q_1 - q_3, q_1 + 1$ of (4) sum to zero, we deduce that $q_3 = 1$ and $q_1 = -1$. This contradicts to $q_1 = 1$. □

Lemma 6. *Let $P \in \mathbf{Q}[x]$ be a monic separable polynomial of degree at least 3 with at least one irrational root. If*

$$\frac{\lambda_1 - \lambda_2}{\lambda_1 - \lambda_3} \in \mathbf{Q}$$

for any three distinct $\lambda_1, \lambda_2, \lambda_3 \in Z(P)$ then $P(x+a) \in \mathcal{P}$ for some rational a.

Proof. By Lemma 4, none of the irreducible factors of P has degree at least 3. Hence, P is a product of linear and quadratic polynomials, with at least one factor being quadratic. Suppose $\alpha_{1,2} = -a \pm e_1\sqrt{D}$ are the roots of some quadratic factor.

(Here, $e_1 > 0$ and a are rational numbers, and $D \neq 0, 1$ is a square-free integer.) Let $\alpha \notin \{\alpha_1, \alpha_2\}$ be any root of P. From

$$\frac{\alpha_1 - \alpha_2}{\alpha_1 - \alpha} = \frac{2e_1\sqrt{D}}{-a + e\sqrt{D} - \alpha} \in \mathbf{Q}$$

it follows that $(\alpha + a)/\ \sqrt{D} \in \mathbf{Q}$. Now, using $\deg \alpha \leqslant 2$, we will show that this is only possible when $\alpha = -a + e\sqrt{D}$ with some rational $e \neq e_1$.

Indeed, if $\deg \alpha = 1$ then $\alpha = -a$. If otherwise $\deg \alpha = 2$ then $\alpha = -b + e\sqrt{D_1}$, where b and $e \neq 0$ are rational numbers and $D_1 \notin \{0, 1\}$ is a square-free integer. Then,

$$\frac{\alpha_1 - \alpha}{\alpha_1 - \alpha_2} = \frac{a - b + e\sqrt{D_1}}{2e_1\sqrt{D}} \in \mathbf{Q}.$$

For $a = b$ we obtain $\sqrt{D_1/D} \in \mathbf{Q}$ which implies that $D = D_1$, and hence $\alpha = -a + e\sqrt{D}$.

Assume that $a \neq b$. Then,

$$e\sqrt{D_1} + e'\sqrt{D} = b - a \tag{5}$$

for some $e' \in \mathbf{Q}$. To show that (5) is impossible we observe that, by (5), the numbers D and D_1 both must be positive. Squaring (5) we deduce that $ee'\sqrt{DD_1} \in \mathbf{Q}$. So $ee' = 0$ or DD_1 is a perfect square. The case $e = 0$ combined with (5) leads to $e' = 0$, which is impossible. Similarly, $e' = 0$ gives the same contradiction. Finally, since $D > 0$ and $D_1 > 0$ are square-free, their product DD_1 is a perfect square only if $D = D_1$. Combined with (5) this yields that $(e + e')\sqrt{D} = b - a \neq 0$, which is impossible.

It follows that all the roots of P of degree $n = \deg P$ must be of the form $-a \pm e_j\sqrt{D}$, where e_j are distinct positive rational numbers for $j = 1, \dots, \lfloor n/2 \rfloor$, plus, in addition, $e_0 = 0$ if n is odd. This means that $P(x + a) = x^\delta \prod_{j=1}^{\lfloor n/2 \rfloor} (x^2 - e_j^2 D) \in \mathcal{P}$. (Here, $\delta = 0$ if n is even, and $\delta = 1$ if n is odd.) □

Lemma 7. *Let $P \in \mathbf{Q}[x]$ be a monic separable polynomial of degree at least 2 with at least one irrational root. If $\lambda_2/\lambda_1 \in \mathbf{Q}$ for any $\lambda_1, \lambda_2 \in Z(P)$, where $\lambda_1 \neq 0$, then $P(x) \in \mathcal{P}$.*

Proof. For $n = \deg P = 2$ the only possibility is $P(x) = x^2 - e^2D$, where $D \neq 0, 1$ is a square-free integer and $e \in \mathbf{Q}^*$. Thus, $P \in \mathcal{P}$.

Suppose that $n \geqslant 3$. Then, P cannot have a rational root other than 0. Write $P(x) = x^\delta Q(x)$, where $\delta \in \{0, 1\}$ and $\delta = 1$ iff 0 is a root of P. Take any two roots of Q which are conjugate over $\mathbf{Q}$, say α_1 and α_2 ($\alpha_2 \neq \alpha_1$). Then $\alpha_2 = q\alpha_1$ for some rational $q \neq 0$. By (2), we deduce that $q = -1$ is the only possibility. Hence, $\alpha_1, -\alpha_1$ are all conjugates of α_1 over $\mathbf{Q}$. This means that each irreducible factor of the polynomial Q must be quadratic and of the form $x^2 - D_i$, where $D_i \neq u^2$ for $u = 0, 1, 2, \dots$. Furthermore, the condition of the lemma implies that $\sqrt{D_i/D_j} \in \mathbf{Q}$. Write any fixed irrational root of Q in the form $e\sqrt{D}$, with $e \in \mathbf{Q}^*$ a square-free integer $D \neq 0, 1$. Then, in view of $\sqrt{D_i/D_j} \in \mathbf{Q}$ all the roots of Q must be of the form $e_i\sqrt{D}$ with $e_i \in \mathbf{Q}$. This implies the required result. □

3. Proofs of Theorems 2 and 3.

Proof of Theorem 2. By Lemma 5, each irreducible factor of P must be either linear or quadratic. If P has at least two linear factors, say $\lambda_1, \lambda_2 \in \mathbf{Q}$ are two distinct roots of P, then the condition of the theorem implies that $\lambda_3 - \lambda_4 \in \mathbf{Q}$ for any $\lambda_3, \lambda_4 \in Z(P)$. Selecting λ_3 and λ_4 as two roots of the same quadratic factor, we arrive at a contradiction. Consequently, P has at most one linear factor.

Take an irrational root of P of the form $-a + e\sqrt{D}$, where $D \neq 0, 1$ is a square-free integer, $a, e \in \mathbf{Q}$ and $e > 0$. Since $-a - e\sqrt{D}$ is also the root of P, we must have $(\lambda_1 - \lambda_2)/\sqrt{D} \in \mathbf{Q}$ for any $\lambda_1, \lambda_2 \in Z(P) \setminus \{-a + e\sqrt{D}, -a - e\sqrt{D}\}$. Selecting any other pair of quadratic conjugate roots, we see that they should be $-b \pm e'\sqrt{D}$ with rational b and $e' > 0$. Moreover, the quotient between $-a + e\sqrt{D} - (-b + e'\sqrt{D}) = b - a + (e - e')\sqrt{D}$ and $-a - e\sqrt{D} - (-b - e'\sqrt{D}) = b - a - (e - e')\sqrt{D}$ must be rational. Hence, $a = b$ or $e = e'$. However, in case $e = e'$ and $a \neq b$ the quotient

$$\frac{-a + e\sqrt{D} - (-b - e\sqrt{D})}{-a - e\sqrt{D} - (-b + e\sqrt{D})} = \frac{b - a + 2e\sqrt{D}}{b - a - 2e\sqrt{D}}$$

equals

$$\frac{(b - a)^2 + 4e^2D + 4e(b - a)\sqrt{D}}{(b - a)^2 - 4e^2D},$$

and so is irrational, which is a contradiction. Hence, $a = b$ is the only possibility.

Consequently, all irrational roots of P have the form $-a \pm e_i\sqrt{D}$, $i = 1, \dots, t$, where e_i are distinct positive rational numbers. If P is of odd degree, it has a rational root α. Then, from

$$\frac{-a + e_1\sqrt{D} - \alpha}{2e_1\sqrt{D}} = \frac{1}{2} - \frac{a + \alpha}{2e_1\sqrt{D}} \in \mathbf{Q}$$

and $\alpha \in \mathbf{Q}$, we conclude that $\alpha = -a$. This implies that $P(x + a) \in \mathcal{P}$. The converse is clear. □

Proof of Theorem 3. Suppose first that $S(f) = S(g) = 0$. Then, $k, \ell \geqslant 2$. Selecting $x_i = \lambda_1$ for each $i \in \{1, \dots, k\}$ with $a_i > 0$ and $x_i = \lambda_2$ for each i with $a_i < 0$, we find that $f(x_1, \dots, x_k) = a\lambda_1 - a\lambda_2$, where a is a positive rational number. Similarly, we select $x_i = \lambda_3$ for each $i \in \{1, \dots, \ell\}$ with $b_i > 0$ and $x_i = \lambda_4$ for each i with $b_i < 0$. Then, $g(x_1, \dots, x_\ell) = b\lambda_3 - b\lambda_4$ for some rational $b > 0$. This yields $(\lambda_1 - \lambda_2)/(\lambda_3 - \lambda_4) \in \mathbf{Q}$. The result now follows, by Theorem 1. The converse is clear.

Suppose that $S(f), S(g) \neq 0$. Then, we can select $x_1 = \dots = x_k = \lambda_2$ in f and $x_1 = \dots = x_\ell = \lambda_1 \neq 0$ in g. This yields $\lambda_2/\lambda_1 \in \mathbf{Q}$ for any $\lambda_1 \neq 0$, and the required result follows from Lemma 7. The converse is also clear.

Suppose next that $S(f) \neq 0$ and $S(g) = 0$. Then, we select $x_1 = \dots = x_k = \lambda_1 \neq 0$ in f and $x_i = \lambda_2$ for each $i \in \{1, \dots, \ell\}$ with $b_i > 0$ and $x_i = \lambda_1$ for each i with $b_i < 0$ in g. This yields $f(x_1, \dots, x_k) = a\lambda_1$ and $g(x_1, \dots, x_\ell) = b\lambda_2 - b\lambda_1$ for some rational $a \neq 0$ and $b > 0$. Consequently, $\lambda_1/(\lambda_2 - \lambda_1) \in \mathbf{Q}$ for any pair of roots λ_1, λ_2 satisfying $\lambda_2 \neq \lambda_1$ and $\lambda_1 \neq 0$. Equivalently, $\lambda_2/\lambda_1 \in \mathbf{Q}$, so that in view of Lemma 7 we find again that $P(x) \in \mathcal{P}$. The proof in the case $S(f) = 0$ and $S(g) \neq 0$ is exactly the same. The converse in both cases is clear. □

In conclusion, we observe that the same result as in Theorem 3 also holds under assumption that the roots $\lambda_1, \dots, \lambda_{k+\ell} \in Z(P)$ are distinct and $n = \deg P \geqslant k + \ell$ except that in addition to (i), (ii) we will have one more option (iii) when $n = k + \ell$, all the coefficients a_i of $f(x_1, \dots, x_k) = a_1x_1 + \dots + a_kx_k$ are equal, $a_1 = \dots = a_k$, all the coefficients b_j of $g(x_1, \dots, x_\ell) = b_1x_1 + \dots + b_\ell x_\ell$ are equal, $b_1 = \dots = b_\ell$, and the sum of the roots of P is zero. The proof is essentially the same as that of the present version of Theorem 3. (It is based on the above lemmas, but contains more technical details, so we omit it.)

Acknowledgement. This research was funded by a grant (No. S-MIP-17-66/LSS-110000-1274) from the Research Council of Lithuania.

References

[1] A. Dubickas, On the degree of a linear form in conjugates of an algebraic number, Illinois J. Math. **46** (2002), no. 2, 571–585.

[2] A. Dubickas and C. J. Smyth, Variations on the theme of Hilbert's Theorem 90, Glasg. Math. J. **44** (2002), no. 3, 435–441.

[3] A. Dubickas, Additive Hilbert's Theorem 90 in the ring of algebraic integers, Indag. Math. (N.S.) **17** (2006), no. 1, 31–36.

[4] P. Habegger, The norm of Gaussian periods. (to appear in Q. J. Math.).

[5] F. Luca, On polynomials whose roots have rational quotient of differences, Bull. Aust. Math. Soc. **96** (2017), no. 2, 185–190.

[6] N. Saxena, S. Severini and I. E. Shparlinski, Parameters of integral circulant graphs and periodic quantum dynamics, Int. J. Quantum Inf. **5** (2007), 417–430.

[7] T. Zaïmi, On the integer form of the additive Hilbert's Theorem 90, Linear Algebra Appl. **390** (2004), 175–181.