Bull. Aust. Math. Soc. **96** (2017), 185–190
doi:10.1017/S0004972717000508

ON POLYNOMIALS WHOSE ROOTS HAVE RATIONAL QUOTIENT OF DIFFERENCES

FLORIAN LUCA

(Received 14 March 2017; accepted 11 April 2017; first published online 5 July 2017)

Abstract

We classify all polynomials $P(X) \in \mathbb{Q}[X]$ with rational coefficients having the property that the quotient $(\lambda_i - \lambda_j)/(\lambda_k - \lambda_\ell)$ is a rational number for all quadruples of roots $(\lambda_i, \lambda_j, \lambda_k, \lambda_\ell)$ with $\lambda_k \neq \lambda_\ell$.

2010 *Mathematics subject classification*: primary 11C08; secondary 11R04, 11R32.

Keywords and phrases: roots of polynomials.

1. Introduction

In this paper, we address the following question.

Question 1.1. Let $P(X) \in \mathbb{Q}[X]$ be a monic squarefree nonconstant polynomial. Let $Z(P)$ be the set of roots of $P(X)$. Is it true that if

$$(\lambda_i - \lambda_j)/(\lambda_k - \lambda_\ell) \in \mathbb{Q} \quad \text{for all } \{\lambda_i, \lambda_j, \lambda_k, \lambda_\ell\} \subset Z(P)^4, \lambda_k \neq \lambda_\ell, \tag{1.1}$$

then $Z(P) \subset \mathbb{Q}$?

Neither of the conditions ‘monic’ or ‘squarefree’ is essential in the above question. We have only imposed them for simplicity.

Condition (1.1) is not so unusual. Characteristic polynomials of certain graphs satisfy condition (1.1) (see [3]). In [2], it is shown that if $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ are roots of unity with $\lambda_3 \neq \lambda_4$ and $(\lambda_1 - \lambda_2)/(\lambda_3 - \lambda_4) \in \mathbb{Q}$ then there exist $i, j \in \{1, 2, 3, 4\}$ such that $\lambda_i = -\lambda_j$.

The example

$$P(X) = X^n \prod_{j=1}^{k} (X^2 - de_j^2) \quad \text{for } n \in \{0, 1\}, \tag{1.2}$$

where d is a squarefree integer (not 0 or 1), $k \geq 1$ is a positive integer and $e_1, \ldots, e_k$ are distinct positive rational numbers, shows that the answer to Question 1.1 is no.

The author is supported by grant CPRR160325161141 from the NRF of South Africa, an A-rated scientist award from the NRF of South Africa and the grant no. 17-02804S of the Czech Granting Agency.

We first show that every polynomial $P(X) \in \mathbb{Q}[X]$ satisfying condition (1.1) is given, up to a translation in the variable X, by (1.2) for suitable values of $d, k, e_1, \dots, e_k$.

Theorem 1.2. *If $P(X) \in \mathbb{Q}[X]$ is a monic polynomial with simple roots and satisfies (1.1) but $Z(P) \not\subset \mathbb{Q}$, then there is a rational number a such that $Q(X) := P(X - a)$ is given by (1.2) for suitable values of $d, k, e_1, \dots, e_k$.*

Note that in this case the splitting field of $P(X)$ is $\mathbb{Q}(\sqrt{d})$, so the Galois group of $f(X)$ is $\mathbb{Z}/2\mathbb{Z}$. This suggests that, instead of asking that the ratios $(\lambda_i - \lambda_j)/(\lambda_k - \lambda_\ell)$ are rational numbers, we could take

$$f(X_1, \dots, X_{m+k}) = \frac{F(X_1, \dots, X_k)}{G(X_{k+1}, \dots, X_{m+k})},$$

where $F(X_1, \dots, X_k)$ and $G(Y_1, \dots, Y_m)$ are homogeneous polynomials of degree D in $\mathbb{Q}[X_1, \dots, X_k]$ and $\mathbb{Q}[Y_1, \dots, Y_m]$, respectively, and impose the condition that

$$f(\lambda_1, \dots, \lambda_{k+m}) \in \mathbb{Q} \quad \text{for all } (\lambda_1, \dots, \lambda_{k+m}) \in Z(P)^{k+m} \tag{1.3}$$

whenever $G(\lambda_{k+1}, \dots, \lambda_{k+m}) \neq 0$. Can we say anything special about the roots of $P(X)$? For example, if $k = m = 2$, $F(X_1, X_2) = X_1 - X_2$ and $G(Y_1, Y_2) = Y_1 - Y_2$, then

$$f(X_1, X_2, X_3, X_4) = \frac{F(X_1, X_2)}{G(X_3, X_4)}.$$

By Theorem 1.2, the condition (1.3) for this example implies that the splitting field of $P(X)$ over $\mathbb{Q}$ has degree at most 2.

We prove that the splitting field of $P(X)$ has bounded degree under the more general condition given by (1.3) when $D = 1$ and that the bound is independent both of the numbers k and m and of the two forms F and G.

Theorem 1.3. *Assume that $D = 1$ and that condition (1.3) holds. Then the Galois group of $P(X)$ over $\mathbb{Q}$ is of order at most 132.*

Almost surely, 132 is not optimal in Theorem 1.3. We leave it as a challenge to find the optimal bound and give an example of when it is attained.

2. The proofs

2.1. The proof of Theorem 1.2. We start by observing that if $P(X)$ has two roots in $\mathbb{Q}$, then all the roots are in $\mathbb{Q}$. Indeed, assuming, say, $\lambda_1 \neq \lambda_2$ are in $\mathbb{Q}$ and using

$$\frac{\lambda_1 - \lambda}{\lambda_1 - \lambda_2} \in \mathbb{Q} \quad \text{for all } \lambda \in Z(P),$$

we see that $\lambda \in \mathbb{Q}$ for all $\lambda \in Z(P)$, and therefore $Z(P) \subset \mathbb{Q}$. From now on, we assume that $P(X)$ has at most one root in $\mathbb{Q}$. Let λ_1 be any irrational root of $P(X)$ of degree $m \geq 2$ and let $\lambda_2, \dots, \lambda_m$ be the remaining conjugates of λ_1. Condition (1.1) shows that

$$\lambda_1 - \lambda_k = q_k(\lambda_1 - \lambda_2) \quad \text{for all } k = 1, 2, \dots, m, \tag{2.1}$$

https://doi.org/10.1017/S0004972717000508 Published online by Cambridge University Press

where $q_k \in \mathbb{Q}$ for $k = 1, \ldots, m$. (We can take $q_1 = 0$ and $q_2 = 1$.) Sum up (2.1) for $k = 1, \ldots, m$ to give

$$m\lambda_1 - S = Q\lambda_1 - Q\lambda_2,$$

where $S := \sum_{k=1}^{m} \lambda_k \in \mathbb{Q}$ and $Q := \sum_{k=1}^{m} q_k$. This gives

$$(m - Q)\lambda_1 + Q\lambda_2 = S. \tag{2.2}$$

If $Q = 0$, we find $\lambda_1 = S/m \in \mathbb{Q}$ which is false. A similar contradiction is obtained from (2.2) if $m - Q = 0$, namely $\lambda_2 = S/m \in \mathbb{Q}$, contrary to the hypothesis. Thus, putting $\alpha = Q/(m - Q)$,

$$\lambda_1 + \alpha\lambda_2 \in \mathbb{Q}. \tag{2.3}$$

Let σ be an automorphism of the Galois group of the splitting field of $P(X)$ over $\mathbb{Q}$ such that $\lambda_2 = \lambda_1^{\sigma}$ and assume that the orbit of λ_1 under σ is $(\lambda_1, \lambda_2, \ldots, \lambda_i)$. That is, $\lambda_j^{\sigma} = \lambda_{j+1 \text{ (mod } i)}$. Applying σ successively to (2.3),

$$\lambda_j + \alpha\lambda_{j+1 \text{ (mod } i)} \in \mathbb{Q},$$

for $j = 1, \ldots, i$. Thus,

$$\lambda_1 \equiv (-\alpha)\lambda_2 \text{ (mod } \mathbb{Q}) \equiv (-\alpha)^2\lambda_3 \text{ (mod } \mathbb{Q}) \equiv \cdots \equiv (-\alpha)^i\lambda_1 \text{ (mod } \mathbb{Q}).$$

Thus, $(1 - (-\alpha)^i)\lambda_1 \in \mathbb{Q}$. Since $\lambda_1 \notin \mathbb{Q}$, this is only possible if $\alpha = \pm 1$.

If $\alpha = +1$, $\lambda_1 - \lambda_2 \in \mathbb{Q}$. Condition (1.1) implies that

$$\lambda_1 - \lambda_i = q_i(\lambda_1 - \lambda_2) \in \mathbb{Q}$$

for $i = 1, \ldots, m$. Summing up the above relations $m\lambda_1 - S \in \mathbb{Q}$, and therefore $\lambda_1 \in \mathbb{Q}$ a contradiction. Thus, $\lambda_1 + \lambda_2 \in \mathbb{Q}$. This is indeed true if $m = 2$.

If $m \geq 3$, then we can replace λ_2 by any λ_i for $i = 2, \ldots, m$ in the above argument, getting $\lambda_1 + \lambda_i \in \mathbb{Q}$ for $i = 2, \ldots, m$. Summing up these relations, $(m - 2)\lambda_1 + S \in \mathbb{Q}$, so $\lambda_1 \in \mathbb{Q}$ (because $m > 2$), again a contradiction. Thus, $m = 2$.

This is true for all irrational roots of $P(X)$. We now distinguish three cases.

Case 1. $\#Z(P) = 2$. In this case, $P(X) = X^2 + 2aX + b$ is irreducible in $\mathbb{Q}[X]$. We therefore obtain $P(X - a) = X^2 - \Delta$, where $\Delta = a^2 - b$ is not a square of a rational number, so it can be written in the form e^2d, where d is a squarefree integer (not equal to 0 or 1) and e is some nonzero rational number.

Case 2. $\#Z(P) = 3$. In this case, $P(X)$ has a rational root λ_3. Let us write $X^2 + 2aX + b = (X - \lambda_1)(X - \lambda_2)$. Then $\lambda_{1,2} = -a \pm \sqrt{\Delta}$, with $\Delta = a^2 - b$ not a square of a rational number, so $\lambda_1 - \lambda_2 = 2\sqrt{\Delta}$. Since $(\lambda_3 - \lambda_1)/(\lambda_1 - \lambda_2) \in \mathbb{Q}$, it follows that $\lambda_3 = -a$. Thus, in this case,

$$P(X) = (X + a)(X^2 + 2aX + b).$$

In particular, $P(X - a) = X(X^2 - \Delta)$, where again $\Delta = e^2d$, with d being an integer which is squarefree and not 0 or 1 and e is some nonzero rational number.

https://doi.org/10.1017/S0004972717000508 Published online by Cambridge University Press

Case 3. $\#Z(p) \geq 4$. In this case, $P(X)$ has at least two irreducible quadratic factors. Let any two of these irreducible factors be $X^2 + 2aX + b = (X - \lambda_1)(X - \lambda_2)$ and $X^2 + 2a'X + b' = (X - \lambda_1')(X - \lambda_2')$. Then $\lambda_1 - \lambda_2 = 2\sqrt{\Delta}$ and $\lambda_1' - \lambda_2' = 2\sqrt{\Delta'}$, where $\Delta = a^2 - b$, $\Delta' = a'^2 - b'$ are not squares of rational numbers. The condition $(\lambda_1' - \lambda_2')/(\lambda_1 - \lambda_2) \in \mathbb{Q}$ shows that $\Delta'/\Delta = u^2$ is the square of a rational number u which may be assumed positive. Thus, if we write $\Delta = e^2 d$ with d a squarefree integer and a positive rational number e, then $\Delta' = e'^2 d$, where $e' := eu$. Now looking at

$$\frac{\lambda_1' - \lambda_1}{\lambda_1 - \lambda_2} = \frac{-(a' - a) + e\sqrt{d}(\pm u \pm 1)}{2e\sqrt{d}} \in \mathbb{Q},$$

we see easily that $a = a'$. All of the above holds for any two quadratic irreducible factors of $P(X)$. Thus, $Q(X) = P(X - a)$ has the property that every quadratic factor of it is of the form $X^2 - e^2 d$, where the squarefree integer d is the same for all factors (and the positive rational number e varies with the factor). Finally, if there is a rational root of $Q(X)$ then the argument from Case 2 implies that it is zero.

Collecting all of the above gives the desired conclusion.

2.2. The proof of Theorem 1.3. We assume that

$$F(X_1, \ldots, X_k) = \sum_{i=1}^{k} f_i X_i \quad \text{and} \quad G(Y_1, \ldots, Y_m) = \sum_{i=1}^{m} g_i Y_i \quad \text{with } f_1 g_1 \neq 0.$$

Assume first that $k = m = 1$. In this case, λ_1/λ_2 is a rational number for any two roots $\lambda_1, \lambda_2 \in Z(P)$ with $\lambda_2 \neq 0$. Assuming that P has degree at least 2, condition (1.1) applies to $Z(P)$ and, by Theorem 1.2, the Galois group of $P(X)$ has order at most 2.

From now on, we assume that $\max\{k, m\} \geq 2$. We may assume that $m \geq 2$ (if not, we replace F/G by its reciprocal). We assume that $P(X)$ has n distinct roots and that $n > 5$, otherwise the Galois group of $P(X)$ is of order at most $5! = 120$. We also assume that $P(X)$ has irrational roots otherwise its Galois group is trivial. Let λ, λ' be any two distinct roots of $P(X)$. Let $\lambda_2, \ldots, \lambda_{k+m}$ be all in $\{\lambda, \lambda'\}$ such that $G(\lambda_{k+1}, \ldots, \lambda_{k+m}) \neq 0$. To see that this is possible, let $\lambda_{k+2}, \ldots, \lambda_{k+m}$ be chosen arbitrarily from $\{\lambda, \lambda'\}$ and note that since $g_1 \neq 0$ and $\lambda \neq \lambda'$, it is not possible that $G(\lambda, \lambda_{k+2}, \ldots, \lambda_{k+m})$ and $G(\lambda', \lambda_{k+2}, \ldots, \lambda_{k+m})$ are both zero. So we can choose $\lambda_{k+1} \in \{\lambda, \lambda'\}$ such that $f(x, \lambda_2, \ldots, \lambda_{k+m})$ is defined for any complex number x. Now let λ'' be any element in $Z(P) \backslash \{\lambda, \lambda'\}$. Then since

$$f(\lambda'', \lambda_2, \ldots, \lambda_{k+m}) = F(\lambda'', \lambda_2, \ldots, \lambda_k)/G(\lambda_{k+1}, \ldots, \lambda_{k+m}) \in \mathbb{Q}$$

and $f_1 \neq 0$, it follows that

$$\lambda'' \text{ is a } \mathbb{Q}\text{-linear combination of } \sum_{i=2}^{k} f_i \lambda_i \text{ and } G(\lambda_{k+1}, \ldots, \lambda_{k+m}). \tag{2.4}$$

In particular, λ, λ' and λ'' are linearly dependent over $\mathbb{Q}$. It follows, by the main result of [1], that if λ is any irrational root of $P(X)$, then its degree is at most 12. Taking λ to

https://doi.org/10.1017/S0004972717000508 Published online by Cambridge University Press

be some irrational root of $P(X)$ and λ' to be some conjugate of λ, relation (2.4) (valid for all $\lambda'' \in Z(P)\backslash\{\lambda, \lambda'\}$) shows that

$$Z(P) \subset \mathbb{Q}(\lambda, \lambda')$$

and the field on the right-hand side above has degree at most $12 \times 11 = 132$. The theorem is proved.

3. Comments

In case F and G have degree $D \geq 2$, we do not necessarily get a bound on the order of the Galois group of $P(X)$ under the condition (1.3). For example, we can take

$$F(X_1, \ldots, X_k) = \sum_{i=1}^{k} f_i X_i^2 \quad \text{and} \quad G(Y_1, \ldots, Y_m) = \sum_{i=1}^{m} g_i Y_i^2$$

for some vectors of coefficients $(f_1, \ldots, f_k) \in \mathbb{Q}^k$ and $(g_1, \ldots, g_m) \in \mathbb{Q}^m$, none of them zero, and then we can take

$$P(X) = \prod_{i=1}^{N} (X^2 - e_i)$$

for any rational numbers e_i for $i = 1, \ldots, N$. In particular, taking e_i to be distinct primes, for example, the Galois group of $P(X)$ can be $(\mathbb{Z}/2\mathbb{Z})^N$ for arbitrarily large values of N. It is perhaps true that condition (1.3) implies that the largest prime factor of the order of the Galois group of $P(X)$ is bounded by a function of D. We leave this problem as a challenge.

Acknowledgements

I thank the referee for a careful reading of the manuscript. I also thank Igor Shparlinski for suggesting the problem and Art Dubickas for providing some references. This work was done at the Fields Institute in Toronto during the workshop of *Heights and Applications to Unlikely Intersections* in February 2017. I thank this institution for its hospitality and support.

References

[1] N. Berry, A. Dubickas, N. D. Elkies, B. Poonen and C. Smyth, 'The conjugate dimension of algebraic numbers', *Q. J. Math.* **55** (2004), 237–252.

[2] P. Habegger, 'The norm of Gaussian periods', Preprint, 2016, arXiv:1611.07287v1.

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

FLORIAN LUCA, School of Mathematics,
University of the Witwatersrand, Private Bag X3,
Wits 2050, South Africa

https://doi.org/10.1017/S0004972717000508 Published online by Cambridge University Press

Max Planck Institute for Mathematics, Vivatgasse 7,
53111 Bonn, Germany
and
Department of Mathematics, Faculty of Sciences,
University of Ostrava, 30. dubna 22, 701 03 Ostrava 1,
Czech Republic
e-mail: florian.luca@wits.ac.za

https://doi.org/10.1017/S0004972717000508 Published online by Cambridge University Press