Bull. Malays. Math. Sci. Soc. (2022) 45:793–805
https://doi.org/10.1007/s40840-021-01219-3

BULLETIN *of the*
MALAYSIAN MATHEMATICAL
SCIENCES SOCIETY
http://www.springer.com/mathematics/journal/40840

# A Game with Two Players Choosing the Coefficients of a Polynomial

**Artūras Dubickas**[1]

Received: 12 February 2021 / Revised: 30 September 2021 / Accepted: 22 November 2021 /
Published online: 9 January 2022


**Abstract**
We consider some versions of a game when two players Nora and Wanda in some order are choosing the coefficients of a degree $d$ polynomial. The aim of Nora is to get a polynomial which has no roots in some field or, more generally, is irreducible over that field or, even more generally, has the largest possible Galois group $S_{\mathrm{d}}$, while the aim Wanda is the opposite. We show that in order to obtain an irreducible polynomial for Nora it suffices to have the last move. However, to ensure that the splitting field of the resulting polynomial with integer coefficients has Galois group $S_{\mathrm{d}}$ Nora needs to have at least three moves for each even $d \geq 4$. For $d = 4$ we show that Nora can always get the Galois group $S_4$ if Nora starts and they play alternately.

**Keywords** Roots of polynomials · Hilbert's irreducibility theorem · Galois group

**Mathematics Subject Classification** 11C08 · 11R09 · 11S05 · 91A46

## 1 Introduction

In this paper we study some versions of a game proposed by Gasarch, Washington and Zbarsky in [9]. Given a positive integer $d \geq 2$ and two sets $R$ and $S$, two players Nora and Wanda in some predetermined order are selecting the coefficients of a degree $d$ polynomial

$$g(x) = a_d x^d + \cdots + a_1 x + a_0$$

Communicated by Rosihan M. Ali.

✉ Artūras Dubickas
arturas.dubickas@mif.vu.lt

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

by choosing an index $j \in \{0, 1, \ldots, d\}$ which was not chosen before and assigning to the coefficient $a_j$ any value from $R$ with restriction $a_0 \neq 0$ and $a_d \neq 0$. The aim of Nora ("no root") is to ensure that the resulting polynomial $g$ has no root in $S$, while the aim of Wanda ("wants root") is to ensure that the resulting polynomial has a root in $S$. Unlike as in [9], we do not assume that the players make their moves alternately but in some predetermined order which is known to both of them in advance.

If $R$ is an integral domain and $S$ is the field of fractions of $R$, then, by Lemma 1 in [9],

**Theorem 1** *Wanda wins if she has the last move.*

The proof is elementary. On the other hand, if $R$ is a subring of a finite extension $K$ of $\mathbb{Q}$ and $S$ is the field of fractions of $R$ (so that $S \subseteq K$), then Nora wins if she has the last move. The proof of the corresponding result [9, Theorem 4] is nontrivial. As an ingredient it contains a so-called $S$-unit theorem [7,8,15], which itself is based on Schmidt's subspace theorem. Below, in Theorem 2 we will give a new proof of this result. Although it is not elementary (finding an elementary proof is left as an open problem in [9]), our proof is almost immediate. We use Hilbert's irreducibility theorem which was not used either in [9] or in a subsequent paper [16]. This approach implies a stronger conclusion asserting that the resulting polynomial not only does not have a root in the number field $K$ but is also irreducible over $K$.

**Theorem 2** *If Nora and Wanda in some order are choosing the coefficients of a degree $d \geq 2$ polynomial in a number field $K$, with Nora's move being last, then Nora can always choose the last coefficient in $\mathbb{N}$ so that the resulting polynomial is irreducible over $K$.*

***Proof*** Let $j \in \{0, 1, \ldots, d\}$ be the last index to be chosen by the last move of Nora. Suppose $f(x) = \sum_{i=0,\, i\neq j}^{d} a_i x^i$, where $a_i \in K$ for each $i \in \{0, 1, \ldots, d\} \setminus \{j\}$. Here, $a_d \neq 0$ if $j \neq d$ and $a_0 \neq 0$ if $j \neq 0$. Then, the polynomial in two variables

$$F(x, y) = f(x) + yx^j \in K[x, y]$$

is linear in $y$, and so is irreducible over $K$, since $f(x)$ and $x^j$ are coprime. So, by Hilbert's irreducibility theorem (see [14, p. 298]), there are infinitely many $t \in \mathbb{N}$ for which the polynomial $F(x, t) = f(x) + tx^j$ is irreducible over $K$. Nora can choose any of those $t$. □

Recently, Sharma and Singhal in [16] studied some other questions raised in [9]. If $K$ is an infinite extension of $\mathbb{Q}$, then the result as in Theorem 2 does not necessarily hold. So the questions with $K$ being $\overline{\mathbb{Q}}^{\text{solv}}$ (the compositum of all finite extensions of $\mathbb{Q}$ with solvable Galois group) as in [9] or $K$ being $\overline{\mathbb{Q}}^{\text{ab}}$ (the maximal abelian extension of $\mathbb{Q}$) as in [16] cannot be treated in the same manner as above.

In this paper we will prove the following:

**Theorem 3** *If Nora and Wanda in some order are choosing the coefficients of a degree $d \geq 4$ polynomial in $\mathbb{Z}$, then Nora can play so that the splitting field of the resulting*

*polynomial has the Galois group $S_d$ if she has at least four moves including at least one of the first two moves and both of the last two moves. On the other hand, if Nora has only two moves, then Wanda can achieve the opposite goal for each even $d \geq 4$.*

It is well known that the full symmetric group $S_d$ is not abelian for $d \geq 3$ and not solvable for $d \geq 5$. Hence, Theorems 2 and 3 imply the following:

**Corollary 4** *Nora wins if she has*

*(i) The last move in the game $(R, K)$, where $d \geq 2$, $K$ is a number field and $R$ is a subring of $K$;*

*(ii) At least four moves including at least one of the first two moves and both of the last two moves in the game $(R, S) = (\mathbb{Z}, \overline{\mathbb{Q}}^{\mathrm{ab}})$, where $d \geq 4$, and $(R, S) = (\mathbb{Z}, \overline{\mathbb{Q}}^{\mathrm{solv}})$, where $d \geq 5$;*

Note that for $d \in \{2, 3\}$ Nora can get the polynomial with Galois group $S_d$ if she plays last by choosing the last coefficient in $\mathbb{Z}$ so that the discriminant of the resulting polynomial is not a square in $\mathbb{Z}$. For $d = 4$ she cannot attain this goal even if she has the last three last moves, since Wanda having the first two moves can choose the first two coefficients zeros $a_1 = a_3 = 0$. Then, by Lemma 9, the Galois group of the splitting field of the resulting polynomial will be of order at most 8, so it is not $S_4$. By the same lemma, for each $d \geq 4$ Wanda can attain the same goal by restricting the order of Galois group to at most $(p-1)p^{d/p}(d/p)! < d!$ (where $p$ is the smallest prime divisor of $d$) if she has the first $d(1-1/p)$ moves by choosing $a_k = 0$ for each $k$ not divisible by $p$.

It seems very likely that for each $d \geq 4$ in a standard version of a game when Nora and Wanda make their moves alternately in $\mathbb{Z}$ with Nora's move being last Nora can always play so that the Galois group of the resulting polynomial is $S_d$. We will prove this for $d = 4$.

**Theorem 5** *If Nora and Wanda are choosing the coefficients of a degree 4 polynomial in $\mathbb{Z}$ alternately with Nora first, then Nora can always play so that the splitting field of the resulting polynomial has the Galois group $S_4$.*

In the next section we give some auxiliary results that come from various sources and then prove Theorems 3 and 5 in Sects. 3 and 4, respectively. Some further observations are given in Sect. 5.

## 2 Auxiliary Results

We first state the main result of Hering [10] as a lemma:

**Lemma 6** *Let $d \geq 2$, $j, k \in \{0, 1, \ldots, d-1\}$, $j \neq k$, $q \in \{1, \ldots, d\}$, and let*

$$f(x) = \sum_{i=0,\, i \neq j}^{d} a_i x^i \in \mathbb{Q}[x]$$

*be a polynomial satisfying* $a_d = 1$, $a_{d-q} \neq 0$, $a_{d-i} = 0$ *for each* $i \in \{1, \dots, q-1\} \setminus \{j, k\}$, *and* $a_0 \neq 0$ *if* $j, k \neq 0$. *If*

$$\gcd(d, d-q, j, k) = 1, \tag{1}$$

*then for all but at most finitely many rational numbers* $a_k$ *the splitting field of the polynomial* $f(x) + tx^j \in \mathbb{Q}[x, t]$ *has Galois group* $S_d$ *over the field* $\mathbb{Q}(t)$.

We also need some statement related to an old result of van der Waerden [17] asserting that "almost all" polynomials of degree $d$ have Galois group $S_d$. See, e.g., [4] for some precise estimates on the number of monic integer polynomials with bounded coefficients and prescribed Galois group when $d \in \{3, 4\}$ and [5] for some further progress on this problem and more references. In particular, the next lemma follows from [3, Theorem 1]:

**Lemma 7** *Suppose* $F(x, t) \in \mathbb{Z}[x, t]$ *of degree* $d$ *in* $x$ *is irreducible over* $\mathbb{Q}(t)$ *and its splitting field over* $\mathbb{Q}(t)$ *has Galois group* $S_d$. *Then, for each* $\varepsilon > 0$ *the number of* $t_0 \in \mathbb{Z} \cap [-H, H]$ *for which the splitting field of* $F(x, t_0)$ *has Galois group other than* $S_d$ *is bounded above by* $cH^{1/2+\varepsilon}$, *where* $c$ *is a positive constant that depends only on* $\varepsilon$ *and the coefficients of* $F$.

Recall that a polynomial $f$ of degree $d$ is called *reciprocal* if it satisfies the identity $f(x) = \pm x^d f(1/x)$. From [18] we borrow the following observation:

**Lemma 8** *Let* $f \in \mathbb{Z}[x]$ *be a degree* $d \geq 4$ *reciprocal polynomial. Then, the order of the Galois group of the splitting field of the polynomial* $f$ *is at most* $2^{d/2}(d/2)!$.

We next prove the following simple lemma:

**Lemma 9** *Let* $f \in \mathbb{Z}[x]$ *be a degree* $d \geq 4$ *polynomial which is expressible in the form* $g(x^m)$ *for some* $g \in \mathbb{Z}[x]$ *and some integer* $m \geq 2$. *Then, the order of the Galois group of the splitting field of* $f$ *is at most* $\varphi(m)m^{d/m}(d/m)!$, *where* $\varphi$ *is the Euler function.*

***Proof*** It is clear that $m|d$. Set $s = d/m$. Let $K = \mathbb{Q}(\beta_1, \dots, \beta_s)$ be the splitting field of $g(x)$, whose roots are $\beta_1, \dots, \beta_s$. The splitting field of $f$ is contained in $L = \mathbb{Q}(\beta_1^{1/m}, \dots, \beta_s^{1/m}, e^{2\pi i/m})$. Since $K \subseteq L$, the degree of $\beta_i^{1/m}$ over $L$ is at most $m$ for $i = 1, \dots, s$, and $e^{2\pi i/m}$ is of degree $\varphi(m)$ over $\mathbb{Q}$ (and so of degree at most $\varphi(m)$ over $K$), we obtain

$$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] \leq \varphi(m)m^s s!,$$

which gives the required bound. □

Next, we recall a version of Hilbert's irreducibility theorem (see [14, p. 298]):

**Lemma 10** *Let* $F(x, y) \in \mathbb{Q}[x, y]$ *be an irreducible over* $\mathbb{Q}$ *polynomial. Then, there is an infinite arithmetic progression of positive integers* $\mathcal{A}$ *such that for each* $y_0 \in \mathcal{A}$ *the polynomial* $F(x, y_0) \in \mathbb{Q}[x]$ *is irreducible over* $\mathbb{Q}$.

The following result will be used in the proof of Theorem 5 (see, for instance, the paper of Davenport, Lewis and Schinzel [6] for a more general result):

**Lemma 11** *Let $k \geq 2$ be an integer and let $f \in \mathbb{Z}[x]$ be a polynomial such that for each $x \in \mathbb{N}$ the number $f(x)$ is a $k$th power of an integer. Then, there exists $h \in \mathbb{Z}[x]$ such that $f(x) = h(x)^k$.*

This lemma implies the following corollary:

**Corollary 12** *If $f \in \mathbb{Z}[x]$ is a polynomial of odd degree, then $f(x)$ is not a perfect square for infinitely many $x \in \mathbb{N}$.*

Finally, by a result of Kappe and Warren [13], we have the following:

**Lemma 13** *Let*

$$f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$$

*be a quartic irreducible polynomial with discriminant $\Delta(f)$ and splitting field $F$. Then,* $\mathrm{Gal}(F/\mathbb{Q}) = S_4$ *if and only if its cubic resolvent*

$$r_f(x) = x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2)$$

*is irreducible over $\mathbb{Q}$ and $\Delta(f)$ is not a square in $\mathbb{Q}$.*

In fact, the discriminants of $f$ and $r_f$ are equal

$$\Delta(f) = \Delta(r_f) \tag{2}$$

(see, e. g., [11, p. 251]). We stress that there are several definitions of *cubic resolvents* of a quartic polynomial that define different polynomials. (It can be also a resolvent of degree 6 as in [1].) The one we use here is from [12].

## 3 Proof of Theorem 3

For the first part of the theorem, we assume that Nora has four moves including at least one of the first two and both last two moves. We first consider the case when she has the first move and the last two moves. Then, on her first move she chooses $a_{d-1} = 1$. On Nora's second move she chooses $a_d = 1$ if Wanda has not chosen $a_d$. If Wanda has chosen $a_d = a \neq 0$, then Nora makes her second move arbitrarily. Thus, if the last two coefficients to be chosen by Nora are $a_j$ and $a_k$, then we must have $j \neq k$ and $j, k \notin \{d-1, d\}$. Hence, the polynomial before the last two moves of Nora is

$$g(x) = ax^d + x^{d-1} + a_j x^j + a_k x^k + f(x),$$

where $f(x) = \sum_{i \in S} a_i x^i$ with $S = \{0, 1, \ldots, d\} \setminus \{j, k, d-1, d\}$.

Note that condition (1) of Lemma 6 for monic $g(x)/a \in \mathbb{Q}[x]$ is satisfied, because $q = 1$. Then, by Lemma 6, Nora can select $a_k \in \mathbb{N}$ (being outside some finite set of rational numbers) so that the splitting field of the polynomial

$$G(x,t) = x^d + x^{d-1}/a + tx^j/a + a_k x^k/a + f(x)/a \in \mathbb{Q}[x,t]$$

has Galois group $S_d$ over the field $\mathbb{Q}(t)$. Then, so is the Galois group of $aG(x,t) \in \mathbb{Z}[x,t]$ over $\mathbb{Q}(t)$. Hence, by Lemma 7, there exists $t_0 \in \mathbb{N}$ such that the Galois group of $G(x,t_0)$ is $S_d$, and the aim of Nora is achieved by selecting $a_k = t_0$.

Now, let us consider the case when Nora has the second move (but the first has Wanda) and the last two moves. If Wanda has not chosen $a_{d-1}$ on her first move, then Nora takes $a_{d-1} = 1$ and uses exactly the same strategy as that above. Otherwise, on her first move Nora selects $a_1 = 1$. With her second move she can choose $a_0 = 1$ if $a_0$ was not chosen before by Wanda. Otherwise, if $a_0$ is already chosen by Wanda, say as $a \neq 0$, then Nora makes her second move arbitrarily. This time, the polynomial before the last two moves of Nora is

$$g(x) = a + x + a_j x^j + a_k x^k + f(x),$$

where $f(x) = \sum_{i \in S} a_i x^i$ with $S = \{0, 1, \ldots, d\} \setminus \{0, 1, j, k\}$. Consider its reciprocal polynomial

$$g^*(x) = x^d g(1/x) = ax^d + x^{d-1} + a_j x^{d-j} + a_k x^{d-k} + x^d f(1/x).$$

By the argument as above, Nora can choose $a_j, a_k \in \mathbb{N}$ so that the Galois group of $g^*(x)$ is $S_d$. If the roots of $g^*$ are $\beta_1, \ldots, \beta_d$, then the roots of $g$ are $\beta_1^{-1}, \ldots, \beta_d^{-1}$. From

$$\mathbb{Q}(\beta_1, \ldots, \beta_d) = \mathbb{Q}(\beta_1^{-1}, \ldots, \beta_d^{-1})$$

we conclude that the Galois group of $g$ is $S_d$, as required.

For the second part of the theorem we assume, for a contradiction, that some two moves of Nora are sufficient to obtain the polynomial $g$ with Galois group $S_d$.

Firstly, by Theorem 1, one of those two moves must be the last one. Suppose that the other one is, say, $\ell$th move, where $\ell \in \{1, \ldots, d\}$. If $\ell > d/2$, then using the first $d/2$ moves Wanda can select $a_k = 0$ for each odd $k$. Hence, no matter how the two players will play, the splitting field of the resulting polynomial $g(x) = h(x^2)$, where $h \in \mathbb{Z}[x]$ is of degree $d/2$, will be of order at most $2^{d/2}(d/2)!$ by Lemma 9 with $m = 2$. Since $2^{d/2}(d/2)! < d!$ for $d \geq 4$, this shows that the Galois group of $g$ is not $S_d$.

Assume that $\ell \leq d/2$. We will consider two cases depending on the parity of $\ell$. For $\ell$ odd Wanda sets $a_k = 0$ for each $k$ in the set

$$\{1, 3, \ldots, \ell - 2\} \cup \{d - (\ell - 2), \ldots, d - 3, d - 1\}.$$

This set is empty for $\ell = 1$; otherwise, it contains $\ell - 1$ distinct elements. Now, in case if Nora takes the coefficient $a_k$ with $k \in \{0, d/2, d\}$, then Wanda can select all zeros for $a_k$ with $k \neq 0, d$, and leave the last coefficient for Nora either $a_0$ or $a_d$. The resulting polynomial will be of the form $g(x) = a_d x^d + a_{d/2} x^d/2 + a_0$, where $a_d a_0 \neq 0$ (but possibly $a_{d/2} = 0$). By Lemma 9 with $m = d/2$, the Galois group of $g$ is of order at most

$$\varphi(d/2)(d/2)^2 2! = \varphi(d/2) d^2/2 < d^3/4 < d!$$

for $d \geq 4$, and we conclude as above. If Nora sets $a_k = t$ for $k \notin \{0, d/2, d\}$, then Wanda can select $a_{d-k} = t$, $a_d = a_0 = 1$, choose other coefficients zeros and leave $a_{d/2}$ to be determined by Nora. The resulting polynomial will be reciprocal, so, by Lemma 8, its Galois group will be of order at most $2^{d/2}(d/2)! < d!$.

Finally, suppose that $\ell$ is even. Then, Wanda can select $a_d = 1$ and $a_k = 0$ for each $k$ in the set

$$\{1, 3, \ldots, \ell - 3\} \cup \{d - (\ell - 3), \ldots, d - 3, d - 1\}.$$

This set is empty for $\ell = 2$; otherwise, it contains $\ell - 2$ distinct elements. This time, if Nora takes the coefficient $a_k$ with $k \in \{0, d/2\}$, then Wanda can set all zeros for the remaining coefficients $a_k$ with $k \neq 0, d/2$ and leave the last coefficient for Nora $a_0$ or $a_{d/2}$. The Galois group of the resulting polynomial $g(x) = x^d + a_{d/2} x^{d/2} + a_0$ will be of order at most $2^{d/2}(d/2)!^2$ by Lemma 9. If Nora takes $a_k = t$ for some $k \notin \{0, d/2\}$, then Wanda can select $a_{d-k} = t$, $a_0 = 1$, choose zeros for other coefficients and leave $a_{d/2}$ to be determined by Nora. The polynomial

$$x^d + t x^{d-k} + a_{d/2} x^{d/2} + t x^k + 1$$

is reciprocal no matter which value Wanda assigns to $a_{d/2}$, so the Galois group of this polynomial will be of order at most $2^{d/2}(d/2)!$ by Lemma 8. This completes the proof of the second claim of the theorem.

## 4 Proof of Theorem 5

The strategy of Nora can be described as follows. She starts with, say, $a_3 = 1$. Then, with her second move she sets $a_1 = 0$ if $a_1$ is not yet chosen by Wanda and $a_2 = -a_1$ otherwise, where $a_1 = u$ was chosen by Wanda in her first move. Let $t$ be the last coefficient to be chosen by Nora's final move, and let $u, v \in \mathbb{Z}$ be the coefficients chosen by Wanda. Then, there are five possibilities:

(i) $g(x) = ux^4 + x^3 + vx^2 + t$,
(ii) $g(x) = ux^4 + x^3 + tx^2 + v$,
(iii) $g(x) = tx^4 + x^3 + ux^2 + v$,
(iv) $g(x) = vx^4 + x^3 - ux^2 + ux + t$,
(v) $g(x) = tx^4 + x^3 - ux^2 + ux + v$.

In each case we will show that Nora can choose $t \in \mathbb{Z}$ so that the corresponding polynomial $g$ is irreducible over $\mathbb{Q}$ and has Galois group $S_4$.

In case (i), by Lemma 13, the cubic resolvent of the monic polynomial

$$f(x) = g(x)/u = x^4 + x^3/u + vx^2/u + t/u \in \mathbb{Q}[x],$$

where $u \neq 0$, is equal to

$$r_f(x) = x^3 - vx^2/u - 4tx/u - (1 - 4uv)t/u^3. \tag{3}$$

By Lemma 10, there is an arithmetic progression of positive integers $\mathcal{A} = p_1 y + q_1$, where $p_1, q_1 \in \mathbb{N}$ and $y = 1, 2, 3, \ldots$, such that for each $t = p_1 y + q_1$, $y \in \mathbb{N}$, the polynomial $g(x)$ as in (i) is irreducible over $\mathbb{Q}$. We will show that for some of those $y \in \mathbb{N}$ the polynomial $r_f$ as in (3) is irreducible over $\mathbb{Q}$. Write $r_f$ in the form

$$r_f(x) = x^2(x - v/u) - (p_1 y + q_1)(4x/u + (1 - 4uv)/u^3).$$

It is irreducible as a polynomial in two variables $x$, $y$, unless the polynomials $x^2(x - v/u)$ and $4x/u + (1 - 4uv)/u^3$ have a common root. The second polynomial vanishes at $x_0 = v/u - 1/(4u^2) \neq 0$, while neither $x$ nor $x - v/u$ vanish at $x = x_0$. Thus, $x^2(x - v/u)$ and $4x/u + (1 - 4uv)/u^3$ are coprime, and hence $r_f$ as a polynomial in two variables $x$, $y$ is irreducible over $\mathbb{Q}$. By Lemma 10 again, there are $p_2, q_2 \in \mathbb{N}$ such that for each $y = p_2 z + q_2$, where $z \in \mathbb{N}$, the polynomial $r_f$ is irreducible over $\mathbb{Q}$. Setting $p = p_1 p_2$ and $q = p_1 q_2 + q_1$, we obtain

$$t = p_1 y + q_1 = p_1(p_2 z + q_2) + q_1 = pz + q$$

and so (3) for $t = pz + q$, namely,

$$r_f(x) = x^3 - vx^2/u - 4(pz + q)x/u - (1 - 4uv)(pz + q)/u^3, \tag{4}$$

is irreducible over $\mathbb{Q}$ for each $z \in \mathbb{N}$.

It is well known that the discriminant of a monic cubic polynomial

$$f(x) = x^3 + Ax^2 + Bx + C$$

equals

$$\Delta(f) = A^2B^2 - 4B^3 - 4A^3C - 27C^2 + 18ABC. \tag{5}$$

Hence, the discriminant $\Delta(r_f)$ for $r_f$ as in (4) multiplied by $u^6$ is a cubic polynomial in $z$ with integer coefficients and the leading coefficient $4^4 u^3 p^3 \neq 0$. So, by Corollary 12, for infinitely many $z \in \mathbb{N}$ the number $u^6 \Delta(r_f)$ is not a perfect square. Now, Nora can choose any of those $z$. To see that this completes the proof of the theorem in case (i), we observe that then, by (2), $\Delta(f)$ is not a square in $\mathbb{Q}$, and so the splitting field of

$f$ over $\mathbb{Q}$ (and hence that of $g$ considered in (i)) has Galois group $S_4$ according to Lemma 13.

In the remaining cases (ii)-(v) the proof is similar although there are some details that should be treated differently (especially in case (ii)). For this reason, when the situation is similar, we sometimes give less details, in particular, for the part leading from (3) to (4) and for the final part of the proof. We stress that the most important ingredient in the strategy of Nora is to have the terms with $t$ in the analogues of (3) we consider so that $r_f$ is linear in terms of the variable $y$ in each of the cases, and the irreducibility of $r_f$ as a two variable polynomial can be confirmed easily.

In case (ii), by Lemma 13, the cubic resolvent of the monic polynomial

$$f(x) = g(x)/u = x^4 + x^3/u + tx^2/u + v/u \in \mathbb{Q}[x],$$

where $u \neq 0$, is

$$\begin{aligned} r_f(x) &= x^3 - tx^2/u - 4vx/u - (1 - 4ut)v/u^3 \\ &= x^3 - 4vx/u - v/u^3 - t(x^2/u - 4v/u^2). \end{aligned}$$

As above we choose $p_1, q_1 \in \mathbb{N}$ so that for $t = p_1 y + q_1$ the polynomial $f(x)$ is irreducible for each $y \in \mathbb{N}$. Note that $r_f$ as a polynomial in $x$, $y$, where $t = p_1 y + q_1$, is irreducible, unless $x(x^2 - 4v/u) - v/u^3$ and $x^2 - 4v/u$ have a common root. Since $v \neq 0$, this is not the case, so $r_f$ as a polynomial in $x$, $y$ is irreducible in $\mathbb{Q}$. Hence, by Lemma 10, as in (4), there are $p, q \in \mathbb{N}$ such that for $t = p + qz$, where $z \in \mathbb{N}$, the polynomial

$$r_f(x) = x^3 - (pz + q)x^2/u - 4vx/u - (1 - 4u(pz + q))v/u^3 \tag{6}$$

is irreducible over $\mathbb{Q}$ for each $z \in \mathbb{N}$.

This time, by (5) and (6), the discriminant of $r_f$ multiplied by $u^6$ and written as a polynomial in $pz + q$ equals

$$u^6 \Delta(r_f) = 16uv(pz + q)^4 + \cdots + 4^4(uv)^3 - 27v^2,$$

where the terms for $(pz + q)^3$, $(pz + q)^2$, $pz + q$ are integers. If this is a square for each $z \in \mathbb{N}$, then, by Lemma 11,

$$u^6 \Delta(r_f) = h(z)^2 = h((pz + q)/p - q/p)^2$$

identically for some quadratic $h \in \mathbb{Z}[z]$. In particular, this implies that $uv$ is a perfect square, say, $uv = w^2$ with $w \in \mathbb{Z} \setminus \{0\}$. Furthermore, inserting $z = -q/p$ we see that

$$4^4(uv)^3 - 27v^2 = v^2(4^4 u^3 v - 27) = v^2(16^2 u^2 w^2 - 27) = h(-q/p)^2$$

is a perfect square as well. Then, $(16uw)^2 - 27 = (16|uw|)^2 - 27$ must be a perfect square. However, this is not the case in view of

$$(16|uw|)^2 - (16|uw| - 1)^2 \geq 16^2 - 15^2 = 31 > 27.$$

Consequently, for some $z \in \mathbb{N}$ the discriminant $\Delta(f) = \Delta(r_f)$ is not a square in $\mathbb{Q}$. This completes the proof for $g$ as in (ii) the same manner as before.

Now, we turn to the case (iii). It more convenient to consider the reciprocal polynomial $g^*(x) = vx^4 + ux^2 + x + t$ which has the same splitting field as $g$. Then, by Lemma 13, the cubic resolvent of

$$f(x) = g^*(x)/v = x^4 + ux^2/v + x/v + t/v$$

is

$$\begin{aligned} r_f(x) &= x^3 - ux^2/v - 4tx/v - (1 - 4ut)/v^2 \\ &= x^3 - ux^2/v - 1/v^2 - 4t(x/v - u/v^2). \end{aligned}$$

The polynomials $x^3 - ux^2/v - 1/v^2 = x^2(x - u/v) - 1/v^2$ and $x - u/v$ are coprime, so arguing as above we conclude that for some $p, q \in \mathbb{N}$ the polynomial

$$r_f(x) = x^3 - ux^2/v - 4(pz + q)x/v - (1 - 4(pz + q)t)/v^2$$

is irreducible over $\mathbb{Q}$ for each $z \in \mathbb{N}$. As in case (i), the discriminant $v^6\Delta(r_f)$ is a cubic polynomial in $z$ with integer coefficients and the leading coefficient $4^4v^3p^3 \neq 0$. So, by Corollary 12, for infinitely many $z \in \mathbb{N}$ the number $v^6\Delta(r_f)$ is not a perfect square. This completes the proof of the theorem in the case (iii) by Lemma 13.

In case (iv) for

$$f(x) = g(x)/v = x^4 + x^3/v - ux^2/v + ux/v + t/v$$

we obtain

$$\begin{aligned} r_f(x) &= x^3 + ux^2/v + (u/v^2 - 4t/v)x - (t/v^3 + 4ut/v^2 + u^2/v^2) \\ &= x^3 + ux^2/v + ux/v^2 - u^2/v^2 - t(4x/v + 1/v^3 + 4u/v^2). \end{aligned}$$

The polynomials $x^3 + ux^2/v + ux/v^2 - u^2/v^2$ and $x + u/v + 1/(4v^2)$ have the same root only if the polynomial

$$x^2(x + u/v) + ux/v^2 - u^2/v^2$$

vanishes at $x_0 = -u/v - 1/(4v^2)$. This happens if and only if

$$-\frac{x_0^2}{4v^2} + \frac{ux_0}{v^2} - \frac{u^2}{v^2} = -\frac{(x_0 - 2u)^2}{4v^2} = 0,$$

that is, $x_0 = 2u = -u/v - 1/(4v^2)$. Consequently, $8uv^2 = -4uv - 1$, which is impossible by different parity of both sides. Therefore, by the same argument as above, it follows that there are $p, q \in \mathbb{N}$ such that the polynomial

$$r_f(x) = x^3 + ux^2/v + (u/v^2 - 4(pz+q)/v)x - (u^2v + (pz+q)(4uv+1))/v^3$$

is irreducible over $\mathbb{Q}$ for each $z \in \mathbb{N}$. This time, as $v^6\Delta(r_f)$ is a cubic polynomial in $z$ with integer coefficients and nonzero leading coefficient, we conclude in the same fashion as before.

Finally, in case (v) we consider the reciprocal polynomial again. The cubic resolvent of

$$f(x) = g^*(x)/v = x^4 + ux^3/v - ux^2/v + x/v + t/v,$$

is

$$\begin{aligned} r_f(x) &= x^3 + ux^2/v + (u - 4tv)x/v^2 - (tu(u+4v) + v)/v^3 \\ &= x^3 + ux^2/v + ux/v^2 - 1/v^2 - t(4x/v + u(u+4v)/v^3). \end{aligned}$$

The polynomials $x^3 + ux^2/v + ux/v^2 - 1/v^2$ and $4x + u(u+4v)/v^2$ have the same root only if

$$x^2(x + u/v) + ux/v^2 - 1/v^2$$

vanishes at $x_0 = -u/v - u^2/(4v^2)$. This happens if and only if

$$-\frac{x_0^2u^2}{4v^2} + \frac{ux_0}{v^2} - \frac{1}{v^2} = -\frac{(ux_0 - 2)^2}{4v^2} = 0,$$

that is, $ux_0 = 2$. This is impossible for $u = 0$. For $u \neq 0$ we obtain $2 = ux_0 = -u^2/v - u^3/(4v^2)$. Consequently, $8v^2 + 4vu^2 + u^3 = 0$. However, this is also impossible, because the discriminant of this quadratic equation is $v$ equals

$$16u^4 - 32u^3 = 16u^2(u^2 - 2u) = 16u^2((u-1)^2 - 1),$$

which is not a square in $\mathbb{Z}$ for $u \neq 0$, since $(u-1)^2 - 1$ is not a square. Consequently, there exist $p, q \in \mathbb{N}$ for which the polynomial

$$r_f(x) = x^3 + ux^2/v + (u - 4v(pz+q))x/v^2 - ((pz+q)u(u+4v) + v)/v^3$$

is irreducible over $\mathbb{Q}$ for each $z \in \mathbb{N}$. Again, as $v^6\Delta(r_f)$ is a cubic polynomial in $z$ with integer coefficients and nonzero leading coefficient, we conclude the argument for (v) as before.

## 5 Concluding Remarks

In Theorem 5, since $d = 4$ is even, Nora has three moves the first, the third and the last one, while Wanda's two moves are the second and the fourth. By Theorems 1 and 3, to get the Galois group $S_4$ Nora needs at least three moves, including the last move and at least one of the first two moves. So, except for the case 1, 3, 5 (as in Theorem 5), other possible three moves of Nora satisfying this condition are 2, 3, 5 or 1, 4, 5 or 2, 4, 5 or 1, 2, 5. Using a strategy similar to that of Nora described in the proof of Theorem 5, one can derive that Nora also wins if she has the moves as described above. For instance, if her moves are 1, 2, 5, then Nora can set $a_3 = 1$ and $a_1 = 0$. Then, no matter which moves 3, 4 of Wanda are, before the last move Nora will be in one the situations described in (i), (ii) or (iii). Other cases can be treated similarly.

However, not every (even a quite 'random' choice) of Nora leads to her win. For example, if she has moves 1,2,5 and sets $a_3 = a$, $a_2 = b$, then Wanda can always choose $a_1$ and $a_0$ so that the splitting field of the resulting polynomial has Galois group of order at most 8 no matter which will be the final coefficient determined by Nora. Indeed, if $a = 0$, then Wanda can set $a_1 = 0$ and the resulting Galois group will be of order at most 8 by Lemma 9. If $a \neq 0$, then Wanda can choose

$$a_1 = 2\ell(b - a\ell) \quad \text{and} \quad a_0 = \ell^2(b - a\ell), \tag{7}$$

where $\ell$ is an integer not in set $\{0, b/a\}$. Then, $a_1 a_0 \neq 0$ and Nora has the polynomial

$$tx^4 + ax^3 + bx^2 + a_1 x + a_0$$

before her last move. After her last choice of $t \neq 0$, the splitting field of this polynomial is the same as that of

$$f(x) = x^4 + a_1 x^3/a_0 + bx^2/a_0 + ax/a_0 + t/a_0 \in \mathbb{Q}[x].$$

If $f$ is reducible over $\mathbb{Q}$, then the Galois group of its splitting field is of order at most 6. If it is irreducible, then, by Lemma 13, the cubic resolvent of $f$ equals

$$r_f(x) = x^3 - \frac{bx^2}{a_0} + \frac{(a_1 a - 4a_0 t)x}{a_0^2} - \frac{a_1^2 t - 4a_0 bt + a_0 a^2}{a_0^3}. \tag{8}$$

Inserting $x = 2a/a_1$ into $r_f$, we find that

$$\begin{aligned} r_f(2a/a_1) &= \frac{8a^3}{a_1^3} - \frac{4a^2 b}{a_1^2 a_0} + \frac{2a(a_1 a - 4a_0 t)}{a_1 a_0^2} - \frac{a_1^2 t - 4a_0 bt + a_0 a^2}{a_0^3} \\ &= (8aa_0^2 - 4a_1 a_0 b + a_1^3)\Big(\frac{a^2}{a_1^3 a_0^2} - \frac{t}{a_1 a_0^3}\Big). \end{aligned}$$

By (7), we derive that

$$a_1^2 - 4a_0b = (b - a\ell)(4\ell^2(b - a\ell) - 4\ell^2 b) = -4a\ell^3(b - a\ell) = -\frac{8aa_0^2}{a_1},$$

and hence

$$8aa_0^2 - 4a_1a_0b + a_1^3 = 0.$$

Consequently, $r_f(2a/a_1) = 0$, which implies that the polynomial (8) is reducible over $\mathbb{Q}$. Therefore, by the main result of [13] (see also [2] for a recent detailed exposition), the Galois group of the splitting field of $f$ is $C_4$ (cyclic group of order 4), $V_4$ (the Klein 4-group of order 4) or $D_4$ (dihedral group of order 8). In any case its order is at most 8 no matter which $t \in \mathbb{Z} \setminus \{0\}$ was chosen by Nora.

**Acknowledgements** This research has received funding from European Social Fund (Project No 09.3.3-LMT-K-712-01-0037) under grant agreement with the Research Council of Lithuania (LMTLT).

## References

1. Awtrey, C., Barkley, B., Guinn, J., McCraw, M.: Resolvents, masses, and Galois groups of irreducible quartic polynomials. Pi Mu Epsilon J. **13**, 609–618 (2014)
2. Barai, R.: On determination of Galois group of quartic polynomials. Math. Student **87**, 73–85 (2018)
3. Castillo, A., Dietmann, R.: On Hilbert's irreducibility theorem. Acta Arith. **180**, 1–14 (2017)
4. Chow, S., Dietmann, R.: Enumerative Galois theory for cubics and quartics. Adv. Math. **372**, 107282 (2020)
5. Chow, S., Dietmann, R.: Towards van der Waerden's conjecture, preprint at arXiv:2106.14593v1 (2021)
6. Davenport, H., Lewis, D.H., Schinzel, A.: Polynomials of certain special types. Acta Arith. **9**, 107–116 (1964)
7. Evertse, J.-H.: The number of solutions of decomposable form equations. Invent. Math. **122**, 559–601 (1995)
8. Evertse, J.-H., Schlickewei, H.P., Schmidt, W.M.: Linear equations in variables which lie in a multiplicative group. Ann. of Math. **155**(2), 807–836 (2002)
9. Gasarch, W., Washington, L.C., Zbarsky, S.: The coefficient-choosing game. J. Comb. Number Theory **10**, 1–17 (2018)
10. Hering, H.: Seltenheit der Gleichungen mit Affekt bei linearem Parameter. Math. Ann. **186**, 263–270 (1970)
11. Jacobson, N.: Basic algebra. I. W. H. Freeman and Co., San Francisco, Calif (1974)
12. Kaplansky, I.: Fields and rings, Chicago Lectures in Mathematics, 2nd edn. University of Chicago Press (1972)
13. Kappe, L.-C., Warren, B.: An elementary test for the Galois group of a quartic polynomial. Amer. Math. Monthly **96**, 133–137 (1989)
14. Schinzel, A.: Polynomials with special regard to reducibility. Cambridge University Press, Cambridge, UK (2000)
15. Schlickewei, H.P.: $S$-unit equations over number fields. Invent. Math. **102**, 95–107 (1990)
16. Sharma, D., Singhal, L.: On the coefficient-choosing game. Mosc. J. Comb. Number Theory **10**, 183–202 (2021)
17. van der Waerden, B.L.: Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt. Monatsh. Math. Phys. **43**, 137–147 (1936)
18. Viana, P., Veloso, P.M.: Galois theory of reciprocal polynomials. Amer. Math. Monthly **109**, 466–471 (2002)