Monatsh Math (2011) 163:415–443
DOI 10.1007/s00605-010-0241-9

Irreducibility criteria of Schur-type and Pólya-type

K. Győry · L. Hajdu · R. Tijdeman

Received: 12 November 2009 / Accepted: 2 September 2010 / Published online: 24 September 2010

Abstract Let $f(x) = (x - a_1) \cdots (x - a_m)$, where $a_1, \ldots, a_m$ are distinct rational integers. In 1908 Schur raised the question whether $f(x) \pm 1$ is irreducible over the rationals. One year later he asked whether $(f(x))^{2^k} + 1$ is irreducible for every $k \geq 1$. In 1919 Pólya proved that if $P(x) \in \mathbb{Z}[x]$ is of degree m and there are m rational integer values a for which $0 < |P(a)| < 2^{-N} N!$ where $N = \lceil m/2 \rceil$, then $P(x)$ is irreducible. A great number of authors have published results of Schur-type or Pólya-type afterwards. Our paper contains various extensions, generalizations and improvements of results from the literature. To indicate some of them, in Theorem 3.1

To the memory of Professor E. Hlawka.

Communicated by Umberto Zannier.

K. Győry and L. Hajdu are supported in part by the Hungarian Academy of Sciences and by the OTKA grants K67580 and K75566. L. Hajdu's work was further supported in part by the TÁMOP 4.2.1./B-09/1/KONV-2010-0007 project. The project is implemented through the New Hungary Development Plan, co-financed by the European Social Fund and the European Regional Development Fund.

Part of the research for this paper was done in Bonn by K. Győry and R. Tijdeman as visitors of the Hausdorff Research Institute for Mathematics and the Max-Planck-Institut für Mathematik, respectively.

K. Győry · L. Hajdu
Institute of Mathematics, University of Debrecen, P.O.Box 12, Debrecen 4010, Hungary
e-mail: gyory@math.klte.hu

L. Hajdu
e-mail: hajdul@math.klte.hu

R. Tijdeman (✉)
Mathematical Institute, Leiden University, P.O.Box 9512, 2300 RA Leiden, The Netherlands
e-mail: tijdeman@math.leidenuniv.nl

a Pólya-type result is established when the ground ring is the ring of integers of an arbitrary imaginary quadratic number field. In Theorem 4.1 we describe the form of the factors of polynomials of the shape $h(x)f(x)+c$, where $h(x)$ is a polynomial and c is a constant such that $|c|$ is small with respect to the degree of $h(x)f(x)$. We obtain irreducibility results for polynomials of the form $g(f(x))$ where $g(x)$ is a monic irreducible polynomial of degree ≤ 3 or of CM-type. Besides elementary arguments we apply methods and results from algebraic number theory, interpolation theory and diophantine approximation.

Keywords Irreducibility · Factors · Polynomials · Schur-type · Pólya-type

Mathematics Subject Classification (2000) 11R09 · 11C08

1 Introduction

In 1908 Schur [33] raised the question of the irreducibility of polynomials of the form

$$P_{\pm}(x) := (x-a_1)(x-a_2)\cdots(x-a_m) \pm 1$$

where $a_1, a_2, \ldots, a_m$ are distinct rational integers. One year later Westlund [47] and Flügel [16] found that $P_-(x)$ is always irreducible over $\mathbb{Q}$, and that $P_+(x)$ can be reducible only if, for some $c \in \mathbb{Z}$,

$$P_+(x-c) = x(x-2)+1 = (x-1)^2$$

or

$$P_+(x-c) = x(x-1)(x-2)(x-3)+1 = (x(x-3)+1)^2\,.$$

We call polynomials $P_1(x)$ and $P_2(x)$ with integral coefficients *equivalent* if $P_1(x) = P_2(x-c)$ for some integer c. Clearly, equivalent polynomials are either both reducible or both irreducible in $\mathbb{Z}[x]$.

In 1919 Pólya [30] found the following irreducibility criterion. If $P(x) \in \mathbb{Z}[x]$ is of degree m and there are m values $a \in \mathbb{Z}$ for which

$$0 < |P(a)| < 2^{-N}N!$$

where $N := \lceil m/2 \rceil$, then $P(x)$ is irreducible over $\mathbb{Q}$. This result implies that $P_{\pm}(x)$ is irreducible over $\mathbb{Q}$ for $m > 6$. By a different method Pólya proved that a polynomial $P(x) \in \mathbb{Z}[x]$ of odd degree m is irreducible if $m \geq 17$ and $|P(x)| = p$ for m different integral arguments, where p is a rational prime.

Write

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_m) \tag{1}$$

where the integers $a_1, a_2, \ldots, a_m$ are distinct. Schur [34] (see also [6]) also asked whether $(f(x))^{2^k} + 1$ is irreducible for $k \geq 1$. In 1926 Brauer, et al. [7] answered the question in the affirmative for $k = 1$ and 2, and treated many other polynomials of the type $g(f(x))$ where $g(x)$ is an irreducible polynomial of low degree. For example, they treated the irreducibility of $g(f(x))$ for $g(x) = ax^2 + 1, ax^4 + 1, ax^6 + 1$ where $a \in \mathbb{Z}_{>0}$ and $g(x) = x^8 + 1$. See also Ille [26]. Similarly Wegner [45] proved the irreducibility of $(f(x))^4 + d$ where $m > 5, d > 0, d \not\equiv 3 \mod 4$.

In 1933 Dorwart and Ore [12] generalized various of the above mentioned results. They showed that a polynomial $P(x) \in \mathbb{Z}[x]$ of degree n taking the values ± 1 at points $a_1, \ldots, a_m \in \mathbb{Z}$ where $4 < m \leq n$ can have factors only of the form $h(x)f(x) \pm 1$ for some $h(x) \in \mathbb{Z}[x]$. The degree of a nonconstant factor of $P(x)$ is therefore never less than m, and when $m > n/2$, $P(x)$ is irreducible over $\mathbb{Q}$. They derived a similar result for polynomials taking many values $\pm p$ with p prime. They further proved that $g(f(x))$ is irreducible if $g(x) = b_0x^2 + b_1x + 1 \in \mathbb{Z}[x]$ is irreducible and $m \geq 5$, and gave all exceptions for $m \leq 4$. Furthermore, they obtained results for polynomials over fields $K = \mathbb{Q}(\sqrt{-d})$ where $d \in \mathbb{Z}_{>0}$, squarefree. For example, they proved that polynomials of the form $af(x) \pm 1$, with $a \in O_K \setminus \{0\}$ and distinct $a_1, \ldots, a_m \in O_K$, are irreducible for $m > 8$, where O_K denotes the ring of integers of K.

Seres [35–37] answered the question of Schur [34] in full generality, proving the irreducibility of the polynomials $g(f(x))$ for all $g(x) = x^{2^k} + 1$ with $k \geq 3$ and, more generally for all cyclotomic polynomials $g(x)$, except for the case $g(x) = x^4 - x^2 + 1$, $f(x) = (x + a)(x + a + 1)(x + a + 2), a \in \mathbb{Z}$. Further, he extended his results (cf. [38]) to every irreducible $g(x)$ of degree > 5 whose zeros are nonreal units of a cyclotomic field. Later, Győry [17–20] generalized Seres' results to the even more general case when the zeros of $f(x)$ are distinct integers from a fixed totally real number field and the splitting field of $g(x)$ is a CM field, i.e. a totally imaginary quadratic extension of a totally real number field.

In the present paper we want to add some new results to the investigations mentioned above. We distinguish two types of results and present them in two parts. In both parts we study the irreducibility of polynomials with coefficients in $\mathbb{Z}$ or, more generally, in the ring of integers of an imaginary number field. More precisely, in some cases we investigate as well for which k the polynomials under consideration can have a factor of degree k.

In Part I we study so-called Pólya-type results in which we consider polynomials with integer coefficients which at many integer points take small, nonzero absolute values. In Sect. 2 we derive the above mentioned result of Pólya and some refinements (essentially) due to Levit [27]. In Sect. 3 we extend these results to the case that the coefficients and the integer points come from a quadratic imaginary number field.

In Part II we obtain so-called Schur-type results by which we mean irreducibility criteria for polynomials of the form $g(h(x)f(x))$ where $f(x), g(x), h(x) \in \mathbb{Z}[x]$, $f(x)$ has only simple zeros from some algebraic number field, and $g(x)$ is an irreducible polynomial. In Sects. 4–6 we assume that $g(x)$ is linear. In Sect. 7 the degree of $g(x)$ is 2 or 3. The degree of $g(x)$ in Sect. 8 is unrestricted, but here $g(x)$ is of CM-type.

Theorems 4.1 and 4.2 extend the above mentioned results of Dorwart and Ore to polynomials $P(x) \in \mathbb{Z}[x]$ taking the same value c, or dividing the same value c,

respectively, for many integral values x. Theorem 5.1 presents a generalization to polynomials

$$P(x) = (x - a_1) \cdots (x - a_m) g_1(x) \cdots g_t(x) \pm 1$$

where $a_1, \ldots, a_m \in \mathbb{Z}$ are distinct and $g_1(x), \ldots, g_t(x) \in \mathbb{Z}[x]$ are of degree 2 and have negative discriminants. Such polynomials occur in relation with so-called ABC-fields.

In Sect. 6 Corollary 6.1 gives an upper bound for $|c|$ for which the polynomial $h(x)f(x) + c$ is irreducible if $f(x)$ is given by (1) and $h(x)f(x)$ has only simple zeros, where the upper bound depends only on the degrees of $f(x)$ and $h(x)$ and the minimal distance between the zeros of $h(x)f(x)$.

In Theorems 7.1 and 7.2 we deal with the case when the degree of $g(x)$ equals 2 or 3 and $g(f(x))$ is reducible. Finally Theorem 8.1 is a quantitative version of the main result of [20]. It gives an upper bound for the number of equivalence classes of monic polynomials $f(x) \in \mathbb{Z}[x]$ of degree m with distinct zeros in a fixed totally real algebraic number field K of degree d for which $g(f(x))$ is reducible over $\mathbb{Q}$, where $g(x) \in \mathbb{Z}[x]$ is a fixed monic irreducible polynomial having splitting field of CM-type. This upper bound depends only on $d, m, g(0)$, the degree of g and the discriminant of K.

Part I: Pólya-type results

2 The rational case: results of Levit

Pólya's irreducibility result on integral polynomials $P(x)$ having small nonzero absolute values at many distinct integers was based on a lemma proved by interpolation theory (cf. the proof of Lemma 3.1). The lemma has been sharpened by several authors, see Tatuzawa [42], Brauer and Ehrlich [8], and Levit [27]. We note that Tverberg [43,44] has given asymptotic results which are asymptotically better than Proposition 2.1 below. We write $(a)_k$ for $a(a+1)\cdots(a+k-1)$.

Proposition 2.1 [27, Theorem 1] *Let $Q(x)$ be a monic polynomial of degree k with real coefficients, and let $a_1 < \cdots < a_m$ be integers. If $m > k > 0$ then, for some $r \in \{1, \ldots, m\}$,*

$$|Q(a_r)| \geq 2^{1-k} ((m-k)/2)_k.$$

The original lower bound of Pólya was $2^{-k}k!$. Pólya's argument combined with Proposition 2.1 leads immediately to the following result.

Proposition 2.2 *Let $P(x) \in \mathbb{Z}[x]$ be a polynomial of degree $m > 1$. Let $0 < k < m$. Suppose there are $k+1$ distinct integers a such that*

$$0 < |P(a)| < 2^{1-k}((m-k)/2)_k.$$

Then $P(x)$ has no factor of degree k over $\mathbb{Q}$.

Proof If $P(x)$ has a factor $Q(x) \in \mathbb{Z}[x]$ of degree k, then $0 < |Q(a)| < 2^{1-k}((m-k)/2)_k$ for $k+1$ distinct integers a, in contradiction to Proposition 2.1. □

Put $N := \lceil m/2 \rceil$. A straightforward extension of Levit's argument yields the following result in which the upper bound for $|P(a)|$ is independent of k in contrast to Proposition 2.2.

Theorem 2.1 *Let $P(x) \in \mathbb{Z}[x]$ be a polynomial of degree $m \geq 8$. Let $N \leq l < m$ and $m - l \leq k \leq l$. Suppose there are $l+1$ distinct integers a such that*

$$0 < |P(a)| < 2^{1-N}((m-N)/2)_N.$$

Then $P(x)$ has no factor of degree k over $\mathbb{Q}$.

Proof If $P(x)$ has a factor $Q(x) \in \mathbb{Z}[x]$ of degree k, then it has a factor of degree $m-k$. In view of Proposition 2.2 it therefore suffices to prove that

$$2^{1-N}((m-N)/2)_N \leq 2^{1-k}((m-k)/2)_k$$

for $N \leq k \leq l$. Let $k - N$ be even. Then it suffices to prove that

$$4^{k-N} \leq (m-k)(m-k+2)\cdots(m-N-2)(m+N)(m+N+2)\cdots(m+k-2).$$

This inequality is valid if $(m-k)(m+k-2) \geq 16$, thus for $m \geq 10$. If $k-N$ is odd, then it suffices to prove that

$$4^{k-N} \leq (m-k)(m-k+2)\cdots(m-N-1)(m+N+1)(m+N+3)\cdots(m+k-2).$$

This is satisfied if both $(m-k)(m+k-2) \geq 16$ and $m-N-1 \geq 4$, so if $m \geq 10$. The remaining cases (m,k) can be checked one by one. □

Levit [27], Theorem 3, obtained a similar result in case $l = m-2$. Besides, his Theorem 4 (and its proof) says that, for $m - N \leq l < m-2$, if there are $l+1$ distinct integers a such that $0 < |P(a)| < \lfloor (l^2+4)/8 \rfloor$, then $P(x)$ has no factor of degree k with $2 \leq k \leq m-2$, and that this upper bound for $|P(a)|$ cannot be improved upon.

By applying Theorem 2.1 for $l = m-1$ we obtain the following irreducibility result due to Levit.

Corollary 2.1 [27, Theorem 2] *Let $P(x) \in \mathbb{Z}[x]$ be a polynomial of degree m. If there are m distinct integers a such that*

$$0 < |P(a)| < 2^{1-N}((m-N)/2)_N,$$

then $P(x)$ is irreducible over $\mathbb{Q}$.

3 The imaginary quadratic case

We extend the results to imaginary quadratic fields. In what follows, we write, for a positive integer m,

$$T_m = \prod_{r=5}^{m}(\sqrt{r}-1), \quad T_m^* = 2^{\min(9-m,0)} \prod_{r=10}^{m}(\sqrt{r}-1).$$

Here we define the empty product to be 1.

Theorem 3.1 *Let $K = \mathbb{Q}(\sqrt{-d})$ where d is a positive squarefree integer, and write O_K for the ring of integers of K. Let again $N := \lceil m/2 \rceil$ and $0 < m - l \le k \le l$. Let $P(x) \in O_K[x]$ of degree m. Suppose there are $l+1$ distinct integers $a \in O_K$ such that*

$$0 < |P(a)| < (N+1)^{-1} T_{N+1}^*.$$

Then $P(x)$ cannot have a factor of degree k in $O_K[x]$.

Remark 3.1 Note that for $m < 27$ we have

$$(N+1)^{-1} T_{N+1}^* \le 1.$$

Hence in this case the statement of Theorem 3.1 is empty.

As an immediate consequence of the above theorem we obtain the following statement.

Corollary 3.1 *Using the notation of Theorem 3.1, assume that*

$$0 < |P(a)| < (N+1)^{-1} T_{N+1}^*$$

holds for m distinct integers $a \in O_K$. Then $P(x)$ is irreducible in $O_K[x]$.

To prove Theorem 3.1 we need the following lemma similar to Proposition 2.1.

Lemma 3.1 *Using the notation of Theorem 3.1, if $P(x) \in O_K[x]$ is of degree m and $a_0, a_1, \ldots, a_m$ are elements of O_K, then for some $t \in \{0, 1, \ldots, m\}$ we have $|P(a_t)| \ge (m+1)^{-1} T_{m+1}^*$.*

The proof of this lemma is based on the following assertion which will also be used later on.

Lemma 3.2 *Let $\alpha_1, \ldots, \alpha_m$ $(m \ge 2)$ be complex numbers such that $|\alpha_r - \alpha_s| \ge \delta$ for all $1 \le r < s \le m$ with some $\delta > 0$. Suppose that $z \in \mathbb{C}$ such that $|z - \alpha_1| \le |z - \alpha_r|$ for all $r = 2, \ldots, m$. Then we have*

$$\prod_{r=2}^{m} |z - \alpha_r| \ge \left(\frac{\delta}{2}\right)^{m-1} T_m,$$

where the right-hand side can be replaced by $\delta^{m-1}T_m^*$ *if* $z = \alpha_1$.

Proof Let $\alpha_1 = \gamma_1, \gamma_2, \ldots, \gamma_m$ be a rearrangement of $\alpha_1, \alpha_2, \ldots, \alpha_m$ such that

$$|z - \gamma_1| \le |z - \gamma_2| \le \cdots \le |z - \gamma_m|$$

and let $d_r = |z - \gamma_r|$ for $r = 2, \ldots, m$. By the definition of δ, the open discs with centers α_r $(r = 1, \ldots, m)$ of radius $\delta/2$ are pairwise disjoint. Thus for $r = 2, \ldots, m$ we have

$$r \cdot \pi \left(\frac{\delta}{2}\right)^2 \le \pi \left(d_r + \frac{\delta}{2}\right)^2.$$

Hence we immediately obtain that

$$d_r \ge \frac{\delta}{2}\left(\sqrt{r} - 1\right) \quad \text{for } r = 2, \ldots, m. \tag{2}$$

Further, for every $r > 1$ we clearly have $d_r \ge \frac{\delta}{2}$, and even $d_r \ge \delta$ if $z = \alpha_1$. This yields

$$\prod_{r=2}^{m} |z - \alpha_r| \ge \left(\frac{\delta}{2}\right)^{m-1} T_m$$

where the right-hand side can be replaced by $\delta^{m-1}T_N^*$ if $z = \alpha_1$. □

Proof of Lemma 3.1 By the interpolation formula of Lagrange we have

$$P(x) = \sum_{r=0}^{m} P(a_r) \prod_{\substack{s=0 \\ s \ne r}}^{m} \frac{x - a_s}{a_r - a_s}.$$

Since the absolute value of the leading coefficient of $P(x)$ is at least 1, we get

$$\left| \sum_{r=0}^{m} P(a_r) \prod_{\substack{s=0 \\ s \ne r}}^{m} \frac{1}{a_r - a_s} \right| \ge 1.$$

Let t be an index such that

$$|P(a_t)| = \max_{s=0,1,\ldots,m} |P(a_s)|.$$

Then we have

$$|P(a_t)| \geq \left(\sum_{r=0}^{m} \prod_{\substack{s=0 \\ s \neq r}}^{m} \frac{1}{|a_r - a_s|} \right)^{-1}.$$

Using that $|a_r - a_s| \geq 1$ for all $r \neq s$ and taking $z = a_s$ in Lemma 3.2, we get

$$\prod_{\substack{s=0 \\ s \neq r}}^{m} |a_r - a_s| \geq T^*_{m+1}.$$

Hence the statement follows by a simple calculation. □

Proof of Theorem 3.1 Suppose that $P(x)$ has a factor in $O_K[x]$ of degree k with $m - l \leq k \leq l$. Then it has a factor $Q(x)$ of degree k with $N \leq k \leq l$. Since $Q(a) \mid P(a)$ in O_K, there are $l + 1$ integers $a \in O_K$ such that

$$0 < |Q(a)| \leq |P(a)| < (N+1)^{-1} T^*_{N+1}.$$

One can easily check that $m^{-1} T^*_m$ is a monotone increasing function of m for $m \geq 10$. Hence, as $m \geq 27$ and $Q(a) \neq 0$, we get that

$$0 < |Q(a)| < (l+1)^{-1} T^*_{l+1}$$

is valid for $l + 1$ distinct integers a. However, this contradicts Lemma 3.1, and the statement follows. □

Part II: Schur-type results

4 Polynomials with many rational integer zeros

By $\tau(c)$ we denote the number of positive divisors of a nonzero integer c. Further, for $\alpha \in \mathbb{R}$ we define the integers $\lfloor \alpha \rfloor$ and $\lceil \alpha \rceil$ by $\alpha - 1 < \lfloor \alpha \rfloor \leq \alpha \leq \lceil \alpha \rceil < \alpha + 1$.

Theorem 4.1 *Let c and m be nonzero integers with*

$$m > 2\tau(c)(2 + \lfloor \log_2 |c| \rfloor).$$

Let $f(x)$ be given by (1), $h(x)$ a polynomial with integral coefficients and put $P(x) = h(x) f(x) + c$. Then every divisor of $P(x)$ in $\mathbb{Z}[x]$ is of the shape $h(x) f(x) + c_1$ where $h(x)$ is a polynomial with integral coefficients and c_1 is an integer dividing c.

Corollary 4.1 *Suppose the conditions of the theorem hold. Then $P(x)$ is reducible over $\mathbb{Q}$ if and only if $h(x)$ can be written as*

$$h(x) = h_1(x)h_2(x)f(x) + c_2h_1(x) + c_1h_2(x)$$

where $h_1(x), h_2(x)$ are nonzero polynomials with integral coefficients and c_1, c_2 are integers with $c_1c_2 = c$.

Proof It is easy to see that with the above choice of $h(x)$ we have

$$P(x) = (h_1(x)f(x) + c_1)(h_2(x)f(x) + c_2).$$

On the other hand, if $P(x)$ is reducible, then by Theorem 4.1 it has a factorization of the above shape with $c_1c_2 = c$ and it follows that $h(x)$ is as in the statement of Corollary 4.1. □

Corollary 4.2 [12], cf. [29,39] *Suppose the conditions of the theorem hold.*

(i) *If $\deg(h) < m$, then $P(x)$ is irreducible.*

(ii) *If $\deg(h) = m$ and $P(x)$ is reducible over $\mathbb{Q}$ then $h(x) = af(x) + b$ where a and b are nonzero integers.*

Proof In case (i) $h(x)$ cannot be written in the way displayed in Corollary 4.1. In case (ii) it follows from Corollary 4.1 that both h_1 and h_2 are constants. □

Remark 4.1 If $c = \pm 1$, then the condition on m in Theorem 4.1 becomes $m > 4$. The condition is necessary, even if $\deg(h) = m$, as is demonstrated by the following example. Let $m = 4$ and

$$f(x) = x(x-1)(x-2)(x-3) \quad \text{and} \quad h(x) = x^4 - 8x^3 + 20x^2 - 14x - 3.$$

Then we have

$$h(x)f(x) + 1 = (x(x-1)(x-3)^2 - 1)^2.$$

However, $x(x-1)(x-3)^2 - 1$ is not of the form given in the theorem.

Dorwart also classified all polynomials which take the values ± 1 at more places than their degrees, see [11, p. 378].

Remark 4.2 In case c is a prime p, Dorwart and Ore [12], Theorem 14, obtained an absolute lower bound for m. Let $P(x)$ take the values $\pm p$ at $m > 5$ integral points $a_1, \ldots, a_m$. They proved that if $f(x)$ is defined by (1), then $P(x) = h(x)f(x) \pm p$ for some $h(x) \in \mathbb{Z}[x]$. Consequently, $P(x)$ can have only factors of degree $\geq m$ if $m > 5$. They further showed that a polynomial $af(x) \pm p$ is irreducible if m is odd

and $m \neq 3$, and when m is even it may have only two factors of the degree $m/2$. The exceptions for $m = 3$ are given by

$$P(x) = (x-1)(x+1)(x+p) + p = x(x^2 + px - 1),$$
$$P(x) = 4x(x-1)(2x+p-1) + p = (2x-1)(4x^2 + 2px - 4x - p).$$

Brauer [5] and Dorwart [10] have investigated the situation more closely, see Dorwart [11] for more information. Weisner [46] studied for general nonzero integer c the polynomials of degree n which assume the value c for n distinct integral values of x.

Remark 4.3 Corollary 4.2 (i) can be compared with the following result of Győry and Rimán [24, Theorem 2]. If $c \neq 0$, $m \geq 2$ are integers, $h(x) \in \mathbb{Z}[x]$ is of degree $< m$, and $f(x)$ is given by (1) such that

$$\max_{r,s} |a_r - a_s| > \begin{cases} |c| + 1 & \text{if } m = 2, \\ |c| + 2 & \text{if } m \geq 3, \end{cases}$$

then $P(x) = h(x)f(x) + c$ is irreducible over $\mathbb{Q}$. A similar result is proved in [24, Theorem 1], with a smaller lower bound when $h(x)$ is constant.

The argument in the proof below is an extension of proofs given by Dorwart and Ore [12].

Proof of Theorem 4.1 Put $S = \tau(c)$, $T = 2 + \lfloor \log_2 |c| \rfloor$. Assume that

$$P(x) = h(x)f(x) + c = H_1(x)H_2(x)$$

for nonconstant polynomials $H_1(x)$, $H_2(x) \in \mathbb{Z}[x]$. (The statement is clearly true if any of $H_1(x)$, $H_2(x)$ is constant.) For each $r = 1, \ldots, m$ we have $H_1(a_r) | c$.

Suppose that there exists a c_1 such that $H_1(a_r) = c_1$ for more than $T + 1$ integers a_r, say $a_1, \ldots, a_{T+2}$. Since $H_1(x)$ is nonconstant, it follows that $\deg(H_1) \geq T + 2$ and

$$H_1(x) - c_1 = (x - a_1) \cdots (x - a_{T+2}) H_3(x) \tag{3}$$

for some polynomial $H_3(x)$ with integral coefficients. If now $H_1(a_r) = c_2 \neq c_1$ for some $r > T + 2$, then $H_1(x) - c_2 = (x - a_r)H_4(x)$ for some $H_4(x)$ with integral coefficients, and hence, by (3),

$$(a_r - a_1) \cdots (a_r - a_{T+2}) \mid c_2 - c_1. \tag{4}$$

At most two factors on the left-hand side are ± 1. Each other factor contributes at least one prime factor to the product. Hence the number of prime factors of $c_2 - c_1$ counted according to multiplicities is at least T which contradicts that $|c_2 - c_1| \leq 2|c| < 2^T$. Thus $H_1(a_r) = c_1$ for each $r = 1, \ldots, m$, i.e.

$$H_1(x) = h_1(x)f(x) + c_1 \tag{5}$$

for some $h_1(x) \in \mathbb{Z}[x]$. Further $H_2(a_r) = c_2$ with $c_2 = c/c_1$ for each $r = 1, \ldots, m$ whence

$$H_2(x) = h_2(x) f(x) + c_2 \tag{6}$$

where $h_2(x) \in \mathbb{Z}[x]$.

Suppose next that for every divisor c_1 of c the number of a_r with $H_1(a_r) = c_1$ is at most $T + 1$. Then $m \le 2S(T + 1)$. Since the total number of divisors of c is $2S$ and $m > 2ST$, there exists some c_1 such that $H_1(a_r) = c_1$ for exactly $T + 1$ integers a_r, say $a_1, \ldots, a_{T+1}$. We distinguish between the cases $S = 1$ and $S > 1$.

If $S = 1$, then $c_1 \in \{-1, 1\}$, $T = 2$ and m is 5 or 6. We get that the only possibility is that $H_1(a_r) = c_1$ for $r = 1, 2, 3$ say, and $H_1(a_r) = -c_1$ for $r = 4, 5$ (and also for $r = 6$ if $m = 6$). Then by a similar argument as before we deduce that

$$(a_4 - a_1)(a_4 - a_2)(a_4 - a_3) \mid 2 \quad \text{and} \quad (a_5 - a_1)(a_5 - a_2)(a_5 - a_3) \mid 2.$$

The first relation gives that two out of the numbers $|a_4 - a_1|$, $|a_4 - a_2|$ and $|a_4 - a_3|$ equal 1 and the third one is 2, while the second one yields the same conclusion for the numbers $|a_5 - a_1|$, $|a_5 - a_2|$, $|a_5 - a_3|$. However, since $a_r \ne a_s$ for $r \ne s$, this is impossible. Hence we get that (5) is valid anyhow, and the same is true for (6).

If $S > 1$ then $m > ST + T + 1$. Hence either there exists some c_2 such that $c_1 c_2 > 0$ and $H_1(a_r) = c_2$ for some $r > T + 1$ or there exist a c_1^* and $c_2^* \ne c_1^*$ with $c_1 c_1^* < 0$ and $c_1^* c_2^* > 0$ such that $H_1(a_r) = c_1^*$ for exactly $T + 1$ integers r and $H_1(a_r) = c_2^*$ for another r. In the latter case, after renaming, we also have $T + 1$ integers $a_1, \ldots, a_{T+1}$ such that $H_1(a_s) = c_1$ for $s = 1, \ldots, T + 1$ and integers c_2 and $r > T + 1$ with $c_1 c_2 > 0$ such that $H_1(a_r) = c_2$. Reasoning as for (4) we derive

$$(a_r - a_1) \cdots (a_r - a_{T+1}) \mid c_2 - c_1.$$

Using that $|c_2 - c_1| < 2^{T-1}$ we obtain (5) and (6) in this case too. □

Remark 4.4 The condition on m in Theorem 4.1 and Corollary 4.1 can be improved upon when c is large. In the first place in (4) the left-hand side can be bounded from below by $(\lfloor \frac{T+2}{2} \rfloor)!(\lfloor \frac{T+3}{2} \rfloor)!$ by using that at most two factors are ± 2, at most two are ± 3, and so on. The result is an improvement of order $\log \log |c|$ for large $|c|$. Another improvement is obtained by replacing the upper bound $2|c|$ in the above proof by $|c| + 1$: If $|c_1| = |c|$, $|c_2| > 1$ or $|c_2| = |c|$, $|c_1| > 1$, then we consider the corresponding expression for H_2. We find instead of (4) that

$$(a_r - a_1) \cdots (a_r - a_{T+2}) \mid \left(\frac{c}{c_1} - \frac{c}{c_2} \right)$$

and use that $|\frac{c}{c_1} - \frac{c}{c_2}| \le |c| + 1$. Otherwise either $|c_1| = |c|$, $|c_2| = 1$ or $|c_2| = |c|$, $|c_1| = 1$ or $|c_1| \le \frac{|c|}{2}$, $|c_2| \le \frac{|c|}{2}$, and in each case $|c_1 - c_2| \le |c| + 1$.

In the following variant of Theorem 4.1 we only require that $P(a_r) | c$ for $r = 1, \ldots, m$.

Theorem 4.2 *Let c and m be positive integers with*

$$m > 2\tau(c)(3 + \lfloor \log_2 |c| \rfloor). \tag{7}$$

Let $P(x) \in \mathbb{Z}[x]$ such that there exist integers $a_1, \ldots, a_m$ for which $P(a_r)$ divides c for $r = 1, \ldots, m$. Then every divisor of $P(x)$ is of the shape $h(x)f(x) + c_1$ where $f(x)$ is given by (1), $h(x) \in \mathbb{Z}[x]$ and c_1 is an integer dividing c.

As in Remark 4.4 the lower bound on m can be improved if $|c|$ is large.

Remark 4.5 In case c is a prime p, Dorwart and Ore [12] proved Theorem 4.2 with $m > 10$ instead of (7). It follows that a polynomial from $\mathbb{Z}[x]$ taking the values dividing p at more than 10 integer points cannot have factors of degree less than $m/2$.

The method was used by Ore [28] to show that a polynomial $P(x) \in \mathbb{Z}[x]$ of degree m taking values dividing a prime at $m+5$ integer points is irreducible. The bound $m+5$ is best possible in view of the example $P(x) = ((x-1)(x-2)-1)((x-5)(x-6)-1)$ taking prime values or their opposites for $x = 0, 1, 2, 3, 4, 5, 6, 7$.

Proof of Theorem 4.2 As in the proof of Theorem 4.1 put $S = \tau(c)$ and $T = 2 + \lfloor \log_2 |c| \rfloor$. Assume that

$$P(x) = H_1(x)H_2(x)$$

for nonconstant polynomials $H_1(x), H_2(x) \in \mathbb{Z}[x]$. (If any of $H_1(x), H_2(x)$ is constant then the statement is trivial.) For each $r = 1, \ldots, m$ we have $H_1(a_r)|c$.

Using the box principle we know that there exists a c_1 such that $H_1(a_r) = c_1$ for more than $T + 1$ integers a_r. Following the proof of Theorem 4.1 we conclude that

$$H_1(x) = h(x)f(x) + c_1 \tag{8}$$

for some $h(x) \in \mathbb{Z}[x]$. Since $H_1(x)$ is an arbitrary divisor of $P(x)$, the conclusion follows. □

5 Polynomials with rational and imaginary quadratic zeros

In the formulation of Theorems 4.1 and 4.2 the condition that the zeros of f and the coefficients of g are in $\mathbb{Z}$ can be replaced by the condition that they are in the ring of integers of $\mathbb{Q}(\sqrt{-d})$ where d is some positive integer, not a square. However, in this case the lower bound on m will depend on c and d. We do not work this out as it is straightforward.

In this section we investigate the irreducibility of polynomials of the shape

$$(x - a_1) \cdots (x - a_m)g_1(x) \cdots g_t(x) \pm 1 \tag{9}$$

where $m, t \geq 0$, the a_r-s are distinct integers and the distinct monic polynomials $g_s(x) \in \mathbb{Z}[x]$ are of degree two and have negative discriminants. Under the assumption that all the zeros of the polynomials g_s $(s = 1, \ldots, t)$ belong to the same quadratic

Table 1 Factors of exceptional polynomials

No.	Polynomial	No.	Polynomial	No.	Polynomial
1	$x-1$	5	x^2+1	9	x^2-x+2
2	x	6	x^2+2	10	x^2+x+2
3	$x+1$	7	x^2-x+1	11	x^2-x+3
4	x^2-2x+2	8	x^2+x+1		

number field, Dorwart and Ore [12] have described all reducible polynomials of the form (9). Getting rid of the assumption, our next theorem yields a complete characterization of the reducible polynomials of the form (9). As a motivation of our work, we remark that irreducible polynomials of the form (9) define generalizations of so-called ABC-fields; see e.g. [1,2,40] and the references given there.

By tuple $[i_1, \ldots, i_l]$ we denote the product of the corresponding polynomials from Table 1.

Theorem 5.1 *Put*

$$P_{\pm}(x) = (x-a_1)\cdots(x-a_m)g_1(x)\cdots g_t(x) \pm 1$$

and

$$F(x) = (x-a_1)\cdots(x-a_m)g_1(x)\cdots g_t(x),$$

where $m+t > 0$, the a_r-s are distinct integers and the $g_s(x) \in \mathbb{Z}[x]$ are distinct monic quadratic polynomials with negative discriminants. Then $P_{\pm}(x)$ is irreducible over $\mathbb{Q}$ except for the following cases:

- *$P_+(x)$ is reducible if and only if either $F(x)$ is equivalent to one of the polynomials*

  $[1,5], [1,8], [2,8], [1,3,5], [1,3,7], [1,3,8], [1,5,7], [1,5,8],$
  $[1,5,9], [1,7,8], [2,3,10], [2,6,8], [1,2,4,5], [1,2,5,10],$
  $[1,2,6,9], [1,3,5,7], [1,3,5,8], [1,3,7,8], [1,5,6,7], [1,5,7,8],$
  $[2,3,5,9], [2,3,6,10], [2,5,8,10], [5,6,9,10], [1,2,4,5,9],$
  $[1,2,7,9,11], [1,3,5,7,8], [1,2,5,6,7,9], [1,2,5,7,8,9],$
  $[2,3,5,6,8,10], [2,3,5,7,8,10],$

  or $F(x)$ is of the form

  $$p(x)(p(x)+2) \quad or \quad p(x)(p(x)+1)(p(x)+2)(p(x)+3)$$

  where $p(x)$ is an arbitrary monic linear polynomial or a monic quadratic polynomial with negative discriminant.

- *$P_-(x)$ is reducible if and only if $F(x)$ is equivalent to one of the polynomials*

  [5], [8], [3, 5], [3, 7], [3, 8], [4, 5], [5, 7], [5, 8], [7, 8], [2, 6, 7], [3, 5, 7], [3, 5, 8], [3, 5, 10], [3, 7, 8], [4, 5, 9], [5, 7, 8], [6, 7, 8], [2, 5, 7, 9], [3, 5, 6, 8], [3, 5, 7, 8].

Proof of Theorem 5.1 Suppose that we have $P_\pm(x) = H_1(x)H_2(x)$ with some monic polynomials $H_1(x), H_2(x) \in \mathbb{Z}[x]$. Then we have $H_1(\beta_s)H_2(\beta_s) = \pm 1$ for all $s = 1, \ldots, t$, where β_s is a zero of g_s. Thus, using that the β_s-s are quadratic imaginary algebraic integers, we deduce that

$$H_1(\beta_s) \in U := \{\pm 1, \pm i, \pm\varepsilon, \pm(1-\varepsilon)\}, \tag{10}$$

where $\varepsilon = (1 + i\sqrt{3})/2$. Certainly, the same holds for $H_1(\overline{\beta_s})$, while $H_1(a_s)$ $(s = 1, \ldots, m)$ may assume the values ± 1 only.

We split the proof into several parts, in accordance with (10).

Case I Suppose that $H_1(\beta_s) = \pm i$ for some s. Then $H_1(\beta_s) \in \mathbb{Q}(\beta_s)$ yields that $\beta_s \in \mathbb{Q}(i)$. Since $H_1(\beta_s) = \pm i$, we get that

$$H_1(x) \mp i = (x - \beta_s)h_1(x) \tag{11}$$

holds with some $h_1(x) \in \mathbb{Z}[i][x]$. Taking complex conjugates we obtain that

$$H_1(x) \pm i = (x - \overline{\beta_s})h_2(x)$$

is also valid with the appropriate $h_2(x) \in \mathbb{Z}[i][x]$. The last two equalities give

$$(x - \beta_s)h_1(x) - (x - \overline{\beta_s})h_2(x) = \mp 2i,$$

whence

$$\beta_s - \overline{\beta_s} \mid 2 \quad \text{in the ring } \mathbb{Z}[i]. \tag{12}$$

Write $\beta_s = u + vi$ with some integers u, v with $v \neq 0$. Then $\overline{\beta_s} = u - vi$, which by (12) implies that $v = \pm 1$ (and further that $\beta_s - \overline{\beta_s} = \pm 2i$). Observe that this also implies $g_s(x + u) = x^2 + 1$. From this point on we shall always assume that $\beta_s = u + i$, which we can do without loss of generality.

Now we look at all the possible other factors of $F(x)$ in turn.

Assume first that $F(x)$ has a linear factor $x - a_r$. Then by $H_1(a_r) = \pm 1$ we have $H_1(x) \mp 1 = (x - a_r)h_3(x)$ with some $h_3(x) \in \mathbb{Z}[x]$. Hence we deduce that $\beta_s - a_r$ divides $1 + i$ in $\mathbb{Z}[i]$, whence one of $a_r = u - 1, u, u + 1$ must be valid. This clearly yields that

$$x + u - a_r \in \{x - 1, x, x + 1\}.$$

Assume next that for some β_r with $r \neq s$ we have $H_1(\beta_r) = \pm i$. Then by the previous argument we already know that $\beta_r = w \pm i$ must be valid for some $w \in \mathbb{Z}$. Further, we also get that either

$$(x - \beta_s)(x - \beta_r)h_4(x) - (x - \overline{\beta_s})(x - \overline{\beta_r})h_5(x) = \mp 2i$$

or

$$(x - \beta_s)(x - \overline{\beta_r})h_4(x) - (x - \overline{\beta_s})(x - \beta_r)h_5(x) = \mp 2i$$

with some $h_4(x), h_5(x) \in \mathbb{Z}[i][x]$. Since $\beta_s - \overline{\beta_s} = \pm 2i$, and without loss of generality we may assume that $\Re(\beta_r) \geq u$, this implies that $w = u + 1$. Hence we can write $g_r(x + u) = x^2 - 2x + 2$.

Suppose now that $H_1(\beta_r) \in \{\pm\varepsilon, \pm(1 - \varepsilon)\}$ for some r. Then we have $\beta_r \in \mathbb{Q}(\varepsilon)$, and further,

$$H_1(x) + u_0 = (x - \beta_r)h_6(x) \tag{13}$$

holds with some $u_0 \in \{\mp\varepsilon, \mp(1 - \varepsilon)\}$ and $h_6(x) \in \mathbb{Z}[\varepsilon][x]$. Taking conjugates we get that

$$H_1(x) + \overline{u_0} = (x - \overline{\beta_r})h_7(x) \tag{14}$$

is also valid with some $h_7(x) \in \mathbb{Z}[\varepsilon][x]$. Using the last two equalities we obtain

$$(x - \beta_r)h_6(x) - (x - \overline{\beta_r})h_7(x) = \pm(1 - 2\varepsilon),$$

implying $\beta_r - \overline{\beta_r} \mid 1 - 2\varepsilon$ in $\mathbb{Z}[\varepsilon]$. Let $\beta_r = w + z\varepsilon$ with $w, z \in \mathbb{Z}, z \neq 0$. Then as $\overline{\varepsilon} = 1 - \varepsilon$, we get $\overline{\beta_r} = w + z - z\varepsilon$, whence $z = \pm 1$. Obviously, without loss of generality we may assume that $\beta_r = w + \varepsilon$. Now a similar argument as before yields that $u - w + i - \varepsilon$ divides an element of the following set

$$H := \{\pm i \pm \varepsilon, \pm i \pm (1 - \varepsilon)\},$$

in the ring of integers of the number field $L := \mathbb{Q}(i, \varepsilon)$. A simple calculation shows that all elements of H are units in L. Hence $u - w + i - \varepsilon$ should be a unit of this field, which after taking norm, turns out to be possible only if $w = u$ or $w = u - 1$. Hence we get that either $g_r(x + u) = x^2 - x + 1$, or $g_r(x + u) = x^2 + x + 1$ must hold.

Finally, let $g_r(x)$ be a polynomial with $H_1(\beta_r) = \pm 1$. Observe that then we also have $H_1(\overline{\beta_r}) = \pm 1$, which implies that $g_r(x)$ divides $H_1(x) \mp 1$ in $\mathbb{Z}[x]$. Then using our previous arguments, we get that $g_r(u + i) \in \{\pm 1, \pm i, \pm 1 \pm i\}$. Hence a simple calculation gives that $g_r(x + u)$ is one of

$$x^2 + 2, \quad x^2 + x + 1, \quad x^2 - x + 1, \quad x^2 + x + 2, \quad x^2 - x + 2.$$

Summarizing the above facts, we conclude that if $H_1(\beta_s) = \pm i$ is valid for some s, then there exists an integer u such $f(x+u)$ should have factors exclusively from the following set:

$$\{x-1, x, x+1, x^2+1, x^2-2x+2, x^2-x+1,$$
$$x^2+x+1, x^2+2, x^2+x+2, x^2-x+2\}.$$

Considering now all subsets of the above set and checking the irreducibility of the implied polynomials $P_{\pm}(x)$, we obtain that all the reducible cases are included in the statement. From each equivalence class we selected one representative. (For example, [1, 2, 9] is not mentioned, since it is equivalent to [2, 3, 10].)

Case II Suppose that $H_1(\beta_s) \in \{\pm\varepsilon, \pm(1-\varepsilon)\}$ for some s. As we have already seen in Case I, we may assume that $\beta_s = u + \varepsilon$ with some integer u. This yields $g_s(x+u) = x^2 - x + 1$.

As before, we look at all the possible other factors of $F(x)$ in turn. In view of Case I, without loss of generality we may clearly assume that there is no β_r with $H_1(\beta_r) = \pm i$.

Assume first that $F(x)$ has a linear factor $x - a_r$. Then using again $H_1(a_r) = \pm 1$, we get that $H_1(x) \mp 1 = (x - a_r)h_8(x)$ with some $h_8(x) \in \mathbb{Z}[x]$. Similarly as above, we can deduce that $\beta_s - a_r$ divides one of $\pm\varepsilon, \pm 1 \pm \varepsilon, \pm(2-\varepsilon)$ in $\mathbb{Z}[\varepsilon]$. Hence we obtain that one of $a_r = u-1, u, u+1, u+2$ must be valid. This clearly yields that

$$x + u - a_r \in \{x-2, x-1, x, x+1\}.$$

Assume next that for some β_r with $r \neq s$ we also have $H_1(\beta_r) \in \{\pm\varepsilon, \pm(1-\varepsilon)\}$. We already know that $\beta_r = w \pm \varepsilon$ must be valid with some $w \in \mathbb{Z}$. Without loss of generality we may assume that $w \geq u$. Further, we also have that

$$H_1(x) + v_0 = (x - \beta_r)h_9(x)$$

and

$$H_1(x) + \overline{v_0} = (x - \overline{\beta_r})h_{10}(x)$$

hold with some $v_0 \in \{\mp\varepsilon, \mp(1-\varepsilon)\}$ and $h_9(x), h_{10}(x) \in \mathbb{Z}[\varepsilon][x]$. Using (13) and (14) we get that

$$\beta_s - \beta_r | v_0 - u_0 \quad \text{and} \quad \beta_s - \overline{\beta_r} | \overline{v_0} - u_0 \quad \text{in } \mathbb{Z}[\varepsilon].$$

Checking all the possibilities one can easily verify that $w = u+1$ must be valid. Then we clearly have $g_r(x+u) = x^2 - 3x + 3$.

Finally, suppose that $H_1(\beta_r) = \pm 1$ holds for some r. Then we also have $H_1(\overline{\beta_r}) = \pm 1$, i.e. $g_r(x)$ divides $H_1(x) \mp 1$ in $\mathbb{Z}[x]$. Applying our previous argument, we get that $g_r(u+\varepsilon)$ divides one of $\pm\varepsilon, \pm 1 \pm \varepsilon, \pm(2-\varepsilon)$ in $\mathbb{Z}[\varepsilon]$. Hence a simple calculation

gives that $g_r(x+u)$ is one of

$$x^2+1,\quad x^2+2,\quad x^2-x+2,\quad x^2-2x+2,\quad x^2-2x+3.$$

Gathering all the above information, we get that in this case there is an integer u such that $f(x+u)$ can have factors exclusively from the following set:

$$\{x-2, x-1, x, x+1, x^2-x+1, x^2-3x+3,\\ x^2+1, x^2+2, x^2-x+2, x^2-2x+2, x^2-2x+3\}.$$

Now by a similar process as for Case I we get that also in Case II all the reducible polynomials of the form $P_{\pm}(x)$ are listed in the statement.

Case III Since $H_1(a_s) = \pm 1$ for all $s = 1, \ldots, m$ and since $H_1(x) \pm 1$ and $H_1(x)$ are of the same degree, we have $2\deg(H_1) = \deg(P_{\pm})$. Suppose that $H_1(\beta_s) = \pm 1$ for each index s. Then $g_s(x) \mid H_1(x) \mp 1$ for all $s = 1, \ldots, t$. We distinguish two subcases.

(i) Assume first that there exists a β_s of the form $\beta_s = u + \alpha$ with $u \in \mathbb{Z}$ and

$$\alpha \in \{i, \varepsilon, i\sqrt{2}, (1+i\sqrt{7})/2\}. \tag{15}$$

In these cases we have that $g_s(x+u)$ is given by

$$x^2+1,\quad x^2-x+1,\quad x^2+2,\quad x^2-x+2,$$

respectively. Write $H_1(\beta_s) = u_0$ with $u_0 \in \{-1, 1\}$. Then by similar arguments as before, using that $H_1(x) - u_0 - (H_1(x) + u_0) = \pm 2$, we get that for the above values of α the only possible factors of $f(x+u)$ dividing $H_1(x+u) + u_0$ are given by

$$x-1,\quad x,\quad x+1,\quad x^2+2,\quad x^2+3,\quad x^2-x+1,\quad x^2+x+1,\\ x^2+x+2,\quad x^2-x+2\ (\alpha = i),$$
$$x-1,\quad x,\quad x^2-x+2,\quad x^2-x+3,\quad x^2+1,\quad x^2-2x+2,\quad x^2+x+1,\\ x^2-3x+3\ (\alpha = \varepsilon),$$
$$x,\quad x^2+1,\quad x^2+3,\quad x^2+4,\quad x^2-x+2,\quad x^2+x+2\ (\alpha = i\sqrt{2}),$$
$$x-1,\quad x,\quad x^2-x+1,\quad x^2-x+3,\quad x^2-x+4,\quad x^2+1,\quad x^2+2,\\ x^2-2x+2,\quad x^2-2x+3\ (\alpha = (1+i\sqrt{7})/2),$$

respectively. We handle these cases in turn. We only explain our method for $\alpha = i$, the other cases are similar. We take a subset of the possible factors of $H_1(x+u)+u_0$. For example, choose $\{x^2-x+1, x^2-x+2\}$. Then we have $(x^2-x+1)(x^2-x+2) \mid H_1(x+u) + u_0$. However, these factors immediately restrict the possible factors of $H_1(x+u) - u_0$. Namely, we get that the only possible factors of $f(x+u)$ dividing

$H_1(x+u)-u_0$ are

$$x-1, \quad x, \quad x^2+1, \quad x^2-x+3, \quad x^2-2x+2.$$

Hence we obtain a finite (in fact rather small) set, such that all possible factors of $f(x+u)$ belong to it. In other cases we have to produce similar lists and to compare them. Checking all possibilities, a computer calculation shows that all the cases with $P_{\pm}(x)$ reducible are given in the statement.

(ii) Finally, we are left with the case where there is no β_s of the form $u+\alpha$ with α satisfying (15). In this case a simple calculation shows that if $g_s(x) \mid H_1(x)-u_0$ then there is no linear polynomial dividing $H_1(x)+u_0$. Let now $g_r(x) \mid H_1(x)+u_0$ for some $r \neq s$. We recall the well-known fact (which can also be readily checked) that if 2 has a divisor different from $\pm 1, \pm 2$ in the ring of integers of an imaginary quadratic number field K then we have $K=\mathbb{Q}(\alpha)$ with α satisfying (15). Hence a simple calculation yields that now $g_r(\beta_s) \in \{-2,-1,1,2\}$ must be valid. However, since $g_s(\beta_s)=0$, this implies that $g_s(x)-g_r(x) \in \{-2,-1,1,2\}$. Hence using that $2\deg(H_1)=\deg(P_{\pm})$, fixing any $p(x):=g_s(x)$, all the possible factors of $F(x)$ can be listed, in terms of $p(x)$. Hence the statement follows by a simple calculation.

Case IV Finally, assume that $t=0$, i.e. $F(x)$ has only linear factors. This case has been completely treated by Flügel [16], however, for the sake of completeness we include this possibility as well. Let $x-a_s \mid g_1(x)-u_0$ with $u_0=\pm 1$. Then for any $r \neq s$ we have that $x-a_r \mid g_1(x)+u_0$, which implies $a_s-a_r \in \{-2,-1,1,2\}$. Hence the statement easily follows in this case, too. □

6 Polynomials of the form $h(x)f(x)+c$

In this section we use some lemmas from Sect. 3 to derive some new Schur-type results. These results depend on the minimal distance $\mathrm{Sep}(P)$ between the zeros of a polynomial $P(x) \in \mathbb{Z}[x]$.

Theorem 6.1 *Let m and n be integers with $1 \leq m \leq n$, $f(x)$ be given by (1), and $h(x) \in \mathbb{Z}[x]$ a polynomial of degree $n-m$. Let $h(x)f(x)$ have only simple zeros and write $\delta=\mathrm{Sep}(fg)$. Let k be an integer with $k<m$ and c an integer with*

$$0<|c|<\left(\frac{\delta}{2}\right)^k T_k. \tag{16}$$

Then the polynomial $P(x):=h(x)f(x)+c$ has no factor of degree k over $\mathbb{Z}$. Further, if all the zeros of $h(x)$ are real, then the statement remains valid with T_k replaced by $(k-1)!$.

Remark 6.1 Observe that the expression $(k-1)!$ is larger than T_k, so in the real case c can come from a larger interval.

We immediately obtain the following consequence of Theorem 6.1, since every factorization of $P(x)$ implies a factor of degree at most $n/2$ and a factor of degree at least $n/2$.

Corollary 6.1 *Under the assumptions and notation of Theorem 6.1, let* $2 \le n < 2m$. *If*

$$|c| < \min_{1 \le k \le n/2} \left\{ \left(\frac{\delta}{2}\right)^k T_k \right\}$$

then $P(x)$ *is irreducible over* $\mathbb{Z}$. *Further, if* $h(x)$ *has only real zeros, then in the above inequalities* T_k *can be replaced by* $(k-1)!$, *and the statement remains valid.*

To prove Theorem 6.1 we need some lemmas. The first one will be used in the real case.

Lemma 6.1 *Let* $\delta > 0$. *Let* $Q(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \in \mathbb{Z}[x]$ *have real zeros such that* $\alpha_{r+1} - \alpha_r \ge \delta$ *for* $r = 1, 2, \ldots, n-1$. *Let* c *be a real number satisfying* $|c| < (n-1)!|a|(\frac{\delta}{2})^n$. *Write* $P(x) := Q(x) + c = a(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n)$. *Then, for* $r = 1, 2, \ldots, n$, *the number* β_r *is real and, if* $\beta_1 \le \beta_2 \le \cdots \le \beta_n$, *then*

$$|\alpha_r - \beta_r| \le \frac{2^{n-1}|c|}{(n-1)!|a|\delta^{n-1}} < \frac{\delta}{2}. \tag{17}$$

Proof Let $\alpha_{r,r+1}$ denote the real number with $\alpha_{r+1} - \alpha_{r,r+1} = \alpha_{r,r+1} - \alpha_r$. We put $\alpha_{0,1} = \alpha_1 - \delta$ and $\alpha_{n,n+1} = \alpha_n + \delta$. Then, for $r = 0, \ldots, n$,

$$\begin{aligned} |Q(\alpha_{r,r+1})| &= |a| \prod_{s=1}^{n} |\alpha_{r,r+1} - \alpha_s| \\ &\ge |a| \cdot \frac{\delta}{2} \cdot \frac{\delta}{2} \cdot \frac{3\delta}{2} \cdot \frac{3\delta}{2} \cdot \frac{5\delta}{2} \cdots \ge |a|(n-1)! \left(\frac{\delta}{2}\right)^n > |c|. \end{aligned}$$

Observe that $P(\alpha_{0,1}), P(\alpha_{1,2}), \ldots, P(\alpha_{n,n+1})$ have alternating signs. By continuity it follows that for $r = 1, \ldots, n$ there is a zero β_r of $P(x)$ between $\alpha_{r-r,r}$ and $\alpha_{r,r+1}$. Hence the numbers β_r are all real. It further follows that, for $r = 1, 2, \ldots, n$, the number α_r is the zero of $Q(x)$ which is the nearest to the number β_r. We have, for such an r,

$$|\alpha_r - \beta_r| = \frac{|Q(\beta_r)|}{|a| \prod_{s \ne r} |\beta_r - \alpha_s|} \le \frac{|c|}{|a| \cdot \frac{\delta}{2} \cdot \delta \cdot \frac{3\delta}{2} \cdot 2\delta \cdots \frac{(n-1)\delta}{2}} \le \frac{2^{n-1}|c|}{(n-1)!|a|\delta^{n-1}}.$$

□

One of the basic tools in the proof of Theorem 6.1 in the complex case is the following lemma which is a straightforward consequence of Rouché's theorem.

Lemma 6.2 *Let* $Q(z)$ *be a nonzero polynomial with complex coefficients and* $c \in \mathbb{C}$. *Further, let* $\alpha_{r-1} \in \mathbb{C}$, $R \in \mathbb{R}$, $R > 0$, *and put*

$$C(\alpha_{r-1,r}, R) = \{z \in \mathbb{C} \,:\, |\alpha_{r,r+1} - z| < R\}.$$

If for every $z \in \mathbb{C}$ with $|\alpha - z| = R$ we have $|Q(z)| > |c|$ then the numbers of complex zeros of the polynomials $Q(z)$ and $Q(z) + c$ in $C(\alpha, r)$, counted according to multiplicities, coincide.

The following lemma is the complex variant of Lemma 6.1.

Lemma 6.3 *Let $\alpha_1, \ldots, \alpha_n$ be distinct complex numbers and let a be a nonzero complex number. Put $\delta = \min_{1 \le r < s \le n} |\alpha_r - \alpha_s|$ and*

$$Q(z) = a(z - \alpha_1) \cdots (z - \alpha_n).$$

Let $c \in \mathbb{C}$ with

$$|c| < |a| \cdot \left(\frac{\delta}{2}\right)^n \cdot T_n.$$

Then for each zero α_r of $Q(z)$ there exists a unique zero β_r of the polynomial $P(z) = Q(z) + c$ such that

$$|\beta_r - \alpha_r| \le \frac{|c|}{|a| T_n} \cdot \left(\frac{2}{\delta}\right)^{n-1} < \frac{\delta}{2}.$$

Further, if $\beta_{s_1}, \ldots, \beta_{s_t}$ are distinct zeros of $P(z)$ all different from β_r, then we have

$$\prod_{j=1}^{t} |\beta_{s_j} - \alpha_r| \ge \left(\frac{\delta}{2}\right)^t \cdot T_{t+1}. \tag{18}$$

Proof Let α_r be any zero of $Q(z)$, and let z be an arbitrary complex number with $|z - \alpha_r| = \delta/2$. Let $\gamma_1, \gamma_2, \ldots, \gamma_n$ be a rearrangement of the zeros $\alpha_1, \ldots, \alpha_n$ such that

$$|z - \gamma_1| \le |z - \gamma_2| \le \cdots \le |z - \gamma_n|$$

and let $d_r = |z - \gamma_r|$ for $r = 1, \ldots, n$. Then we have $d_1 = \delta/2$. Further, following the proof of Lemma 3.2 we obtain that, for $r > 1$,

$$d_r \ge \frac{\delta}{2} \quad \text{and} \quad \text{also} \quad d_r \ge \frac{\delta}{2}\left(\sqrt{r} - 1\right). \tag{19}$$

This yields

$$|Q(z)| = |a| \cdot \prod_{r=1}^{n} |z - \alpha_r| = |a| \cdot \prod_{r=1}^{n} |z - \gamma_r| = |a| \cdot \prod_{r=1}^{n} d_r \ge |a| \cdot \left(\frac{\delta}{2}\right)^n \cdot T_n.$$

Since

$$|c| < |a| \cdot \left(\frac{\delta}{2}\right)^n \cdot T_n$$

we get, by Lemma 6.2, that the polynomials $P(z)$ and $Q(z)$ have the same number of zeros in the open disc $C(\alpha_r, \delta/2)$ of radius $\delta/2$ with center α_r. As by the definition of δ the only zero of $Q(z)$ in this disc is α_r, there exists a unique zero β_r of $P(z)$ with $\beta_r \in C(\alpha_r, \delta/2)$. Then we have

$$|c| = |Q(\beta_r)| = |a| \cdot \prod_{s=1}^{n} |\beta_r - \alpha_s| \geq |a| \cdot |\beta_r - \alpha_r| \cdot \prod_{s=2}^{n} d_s,$$

whence, by (19),

$$|\beta_r - \alpha_r| \leq \frac{|c|}{|a|T_n} \cdot \left(\frac{2}{\delta}\right)^{n-1} < \frac{\delta}{2}.$$

Finally, using (19) again one can easily check that (18) is also valid, and the lemma follows. □

Proof of Theorem 6.1 Assume first that all the zeros of $h(x)$ are real. Write $\alpha_1, \ldots, \alpha_m$ and $\alpha_{m+1}, \ldots, \alpha_n$ for the zeros of $f(x)$ and $h(x)$, respectively. According to Lemma 6.1, for every r with $1 \leq r \leq n$ there exists a zero β_r of $P(x)$ such that (17) holds. Let $\beta_1, \ldots, \beta_n$ be the zeros of $P(x)$, indexed according to this property. Suppose $P(x) = P_1(x)P_2(x)$ with $P_1(x), P_2(x) \in \mathbb{Z}[x]$ and $\deg(P_1) = k$. Write $P_1(x) = a_1(x - \beta_{r_1}) \cdots (x - \beta_{r_k})$, $P_2(x) = a_2(x - \beta_{r_{k+1}}) \cdots (x - \beta_{r_n})$. Since $k < m$, there exists an r_0 with $k + 1 \leq r_0 \leq n$ such that $P_2(\beta_{r_0}) = 0$. Then for the corresponding zero α_{r_0} of $f(x)$ we have

$$|c| = |P(\alpha_{r_0})| = |P_1(\alpha_{r_0})| \cdot |P_2(\alpha_{r_0})| = |P_2(\alpha_{r_0})| \cdot |a_1| \cdot \prod_{s=1}^{k} |\alpha_{r_0} - \beta_{r_s}|.$$

Since $|P_2(\alpha_{r_0})| \geq 1$, $|a_1| \geq 1$ and

$$\left| \prod_{s=1}^{k} (\alpha_{r_0} - \beta_{r_s}) \right| \geq \frac{\delta}{2} \cdot \frac{\delta}{2} \cdot \frac{3\delta}{2} \cdot \frac{3\delta}{2} \cdot \frac{5\delta}{2} \cdots \geq (k-1)! \left(\frac{\delta}{2}\right)^k,$$

we obtain $|c| \geq (k-1)!(\frac{\delta}{2})^k$. Thus, if (16) holds with T_k replaced by $(k-1)!$, then $P(x)$ cannot have a factor of degree k.

Suppose now that $h(x)$ has nonreal zeros, too. Assume that $P(x)$ has a factor of degree k. Following the proof in the real case, but using Lemma 6.3 in place of of

Lemma 6.1, we obtain

$$|c| \geq \left(\frac{\delta}{2}\right)^k T_k$$

This contradiction with (16) proves the statement. □

7 Polynomials of the form $g(f(x))$ with $g(x)$ of degree 2 and 3

Let $f(x)$ be given by (1). Brauer et al. [7] proved that if $K = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{-d})$, with squarefree $d \in \mathbb{Z}_{>0}$, and $g(x) \in O_K[x]$ is irreducible of degree at most 3, then $g(f(x))$ is reducible over K for only finitely many equivalence classes of polynomials f. Here O_K denotes the ring of integers of K, and $f_1, f_2 \in O_K[x]$ are said to be equivalent if $f_2(x) = f_1(x + a)$ for some $a \in O_K$.

Dorwart and Ore [12] showed that if $g(x) = ax^2 + bx + 1 \in \mathbb{Z}[x]$ is irreducible, then $g(f(x))$ is also irreducible when $m \geq 5$. Moreover, they were able to classify all cases in which $g(f(x))$ is reducible when $m < 5$. In particular, $P(x) = a(f(x))^2 + 1$ is irreducible if $a \neq -b^2$ and $P(x)$ is not equivalent to

$$-8(x-1)^2x^2(x+1)^2 + 1 = (2x^2-1)(-4x^4+6x^2-1).$$

The following result on general polynomials $g(x) = ax^2 + bx + c$ follows immediately from Theorem 4.1.

Theorem 7.1 *Let c and m be nonzero integers with $m > 2\tau(c)(2 + \lfloor \log_2 |c| \rfloor)$. Let $f(x)$ be given by (1), and $g(x)$ be an irreducible polynomial of degree at most 2 with integral coefficients such that $g(0) = c$. Then $g(f(x))$ is irreducible over $\mathbb{Q}$.*

Proof Assume that $g(f(x))$ is reducible over $\mathbb{Q}$. The result follows immediately from Theorem 4.1 if g is linear. Let $g(x) = ax^2 + bx + c$ with a, b integers and $a \neq 0$. By Corollary 4.1 we have

$$af(x) + b = h_1(x)h_2(x)f(x) + c_2h_1(x) + c_1h_2(x)$$

with $c_1c_2 = c$. Hence h_1 and h_2 are integers with $h_1h_2 = a$ and $c_2h_1 + c_1h_2 = b$. It follows that $g(x) = ax^2 + bx + c = (h_1x + c_1)(h_2x + c_2)$ is reducible. □

The next result deals with the case that the degree of $g(x)$ is 3. We say that $\{a_1, \ldots, a_{2r}\}$ is a Prouhet–Tarry–Escott set if it splits into two subsets of equal cardinality, $A := \{a_1, \ldots, a_r\}$ and $B := \{a_{r+1}, \ldots, a_{2r}\}$ say, such that $(x - a_1) \cdots (x - a_r) - (x - a_{r+1}) \cdots (x - a_{2r})$ is a constant. We call (A, B) a PTE pair. For information on PTE pairs see [3,4,25]. PTE pairs in the context of this paper occur already in [10,32].

Theorem 7.2 *Let the conditions of Theorem 7.1 be satisfied, but with $g(x) = ax^3 + bx^2 + vx + c$ an irreducible polynomial of degree 3 with integral coefficients. If $g(f(x))$ is reducible over $\mathbb{Q}$, then*

$-ac$ and v^2-4bc are positive squares with $4ac|(v^2-4bc)$,
m is even, $m \le 2+\log_2 \frac{v^2-4bc}{ac}$,
$b=0$ or $m \le 2\tau(b)(\lfloor \log_2 b \rfloor + 2)$,
$(a_1,\ldots,a_m)$ is a Prouhet–Tarry–Escott set, and
$cg(f(x))$ factorizes into two polynomials of degree $3m/2$ each, viz.

$$f(x)\left(\frac{1}{2}v \pm \frac{1}{2}\sqrt{v^2-4bc-4acf(x)}\right)+c.$$

Proof By Corollary 4.1 we have

$$a(f(x))^2+bf(x)+v = h_1(x)h_2(x)f(x)+c_2h_1(x)+c_1h_2(x)$$

with $h_1(x), h_2(x) \in \mathbb{Z}[x]$. Hence $\deg(h_1)+\deg(h_2) = \deg(f)$ and $c_2h_1(x)+c_1h_2(x) = v+lf(x)$ for some $l \in \mathbb{Z}$. It follows that either h_1 is a constant or h_2 is a constant or $l=0$.

Suppose h_1 is constant. Then $h_2(x) = \frac{l}{c_1}f(x)+\frac{v-c_2h_1}{c_1} \in \mathbb{Z}[x]$ and $ax^3+bx^2+vx+c = (h_1x+c_1)(xh_2(x)+c_2)$ is reducible. Thus $g(x)$ is reducible over $\mathbb{Z}$. The case h_2 is constant is similar.

Suppose $l=0$. Then $af(x)+b = h_1(x)h_2(x)$ and $c_2h_1(x)+c_1h_2(x) = v$. Hence $\deg(h_1) = \deg(h_2) = m/2$ which is possible only if m is even. The factorization of $af(x)+b$ is possible only if $b=0$ or $m \le 2\tau(b)(2+\lfloor \log_2 b \rfloor)$, by Theorem 4.1. Let $x^2-vx+bc = (x-\alpha_1)(x-\alpha_2)$. Since $ch_1(a_r)h_2(a_r) = bc$ and $c_2h_1(a_r)+c_1h_2(a_r) = v$ for $r=1,\ldots,m$, we have $(c_2h_1(a_r), c_1h_2(a_r)) \in \{(\alpha_1,\alpha_2),(\alpha_2,\alpha_1)\}$. Since a non-constant polynomial of degree $m/2$ cannot attain the same value more than $m/2$ times, the set $\{a_1,\ldots,a_m\}$ splits into two subsets A and B of cardinality $m/2$ each such that $c_2h_1(a_r) = \alpha_1$ for $r \in A$ and $c_2h_1(a_r) = \alpha_2$ for $r \in B$. Hence

$$c_2h_1(x)-\alpha_1 = c_3\prod_{a_r\in A}(x-a_r),\ c_2h_1(x)-\alpha_2 = c_3\prod_{a_r\in B}(x-a_r),$$
$$c_1h_2(x)-\alpha_2 = -c_3\prod_{a_r\in A}(x-a_r),\ c_1h_2(x)-\alpha_1 = -c_3\prod_{a_r\in B}(x-a_r)$$

for some integer c_3 with $-c_3^2 = ac_1c_2 = ac$. Thus $-4ac$ is the square of an integer. Furthermore, if $b \in B$, then $c_3\prod_{a_r\in A}(b-a_r) = \alpha_2-\alpha_1$. Hence, $-4ac(\prod_{a_r\in A}(b-a_r))^2 = v^2-4bc$. Thus $4ac$ divides v^2-4bc, v^2-4bc is the square of an integer and, since the product contains at least $m-4$ factors with absolute value >1, $v^2-4bc \ge |ac|2^{m-2}$. This yields the latter inequality for m. From $ch_1(x)h_2(x) = acf(x)+bc$ and $c_2h_1(x)+c_1h_(x) = v$ we obtain

$$c_2h_1(x), c_1h_2(x) = \frac{-v \pm \sqrt{v^2-4bc-4acf(x)}}{2}.$$

Hence $\sqrt{v^2-4bc-4acf(x)} \in \mathbb{Z}[x]$. □

Remark 7.1 It is remarkable that even for $m = 24$ there exist irreducible polynomials $g(x) \in \mathbb{Z}[x]$ of degree 3 and monic polynomials $f(x)$ of the form (1) such that $g(f(x))$ is reducible. Thus the conditions on m in Theorem 7.2 are insufficient to conclude that $g(f(x))$ is reducible. To show this, suppose $A = \{a_1, \ldots, a_r\}$ and $B = \{a_{r+1}, \ldots, a_{2r}\}$ are PTE pairs with

$$\prod_{s=1}^{r}(x - a_s) - \prod_{s=r+1}^{2r}(x - a_s) = v \neq 2.$$

Put $f(x) = \prod_{s=1}^{2r}(x - a_s)$, $g(x) = x^3 + vx - 1$, that is we choose $a = 1, b = 0, c = -1$. Then $g(x)$ is irreducible and $g(f(x))$ factorizes into

$$\left(f(x)\prod_{s=1}^{r}(x - a_s) - 1\right)\left(f(x)\prod_{s=r+1}^{2r}(x - a_s) + 1\right),$$

as can easily be checked. PTE pairs are known for $r = m/2 \leq 10$ and for $r = m/2 = 12$. For $m = 1, 2, 3, 4, 5, 6, 7, 8, 10$ even infinitely many essentially different PTE pairs are known. One of the two known cases for $r = 12$ is given by

$$A = \{\pm 22, \pm 61, \pm 86, \pm 127, \pm 140, \pm 151\},$$
$$B = \{\pm 35, \pm 47, \pm 94, \pm 121, \pm 146, \pm 148\},$$

due to Chen Shuwen et al. [9].

8 Polynomials of the form $g(f(x))$ with $g(x)$ of CM-type

In this section we deal with the reducibility of polynomials of the form $g(f(x))$ over $\mathbb{Q}$, where $g(x)$ is a monic irreducible polynomial in $\mathbb{Z}[x]$ and $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$ with distinct zeros in $\mathbb{Q}$ or, more generally, in a given algebraic number field. We assume throughout that the splitting field of $g(x)$ over $\mathbb{Q}$ is a CM-field, i.e., a totally imaginary quadratic extension of a totally real algebraic number field. In this case $g(x)$ is called of *CM-type*. For example, cyclotomic polynomials and quadratic polynomials with negative discriminant are of CM-type.

It was proved in [17] that for given $g(x)$, there are only finitely many pairwise inequivalent monic polynomials $f(x) \in \mathbb{Z}[x]$ with distinct zeros in $\mathbb{Q}$ for which $g(f(x))$ is reducible. In [18–20] this result was extended to polynomials $f(x)$ having all their zeros in a given totally real algebraic number field K. It turned out that in this more general situation there can exist infinitely many pairwise inequivalent quartic exceptions $f(x)$ for which $g(f(x))$ is reducible for a suitable $g(x)$. These exceptions have been completely described in [20].

In [15,17–20] some effective and quantitative versions were also established. For example, it was shown in [15] that under the above assumptions concerning f and g there is an effectively computable positive constant c_1 which depends only on the

degree, class number and discriminant of K such that if

$$\deg(f) > c_1 |g(0)|^{2/\deg(g)} \tag{20}$$

then $g(f(x))$ is irreducible over $\mathbb{Q}$. We now prove the following.

Theorem 8.1 *Let $g(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial of CM-type, and K a totally real algebraic number field of degree d. Further, let $m \geq 3$ be an integer with $m \neq 4$. Then there are at most*

$$\left(c_2 |g(0)|^{1/\deg(g)}\right)^{d\binom{m}{2}} \tag{21}$$

equivalence classes of monic polynomials $f(x) \in \mathbb{Z}[x]$ of degree m with distinct zeros in K for which $g(f(x))$ is reducible over $\mathbb{Q}$. Here c_2 denotes an effectively computable positive constant depending only on d and the discriminant of K.

Together with (20), this gives a quantitative version of the main result (the Theorem) of [20]. An important feature of our bound (21) is that apart from the constant term $g(0)$, it does not depend on the coefficients of $g(x)$.

As was pointed out in [20], if K has a quadratic subfield then, for a suitable $g(x) \in \mathbb{Z}[x]$, there exist infinitely many pairwise inequivalent monic quartic polynomials $f(x) \in \mathbb{Z}[x]$ with distinct zeros in K for which $g(f(x))$ is reducible over $\mathbb{Q}$. Following our proof, it is easy to see that Theorem 8.1 is true for $m = 4$ as well, provided that K has no quadratic subfield. Finally, we note that Theorem 8.1 does not remain valid if we drop the restriction that g is of CM-type or that the zeros of f belong to a fixed number field.

For the proof of Theorem 8.1 we shall use some arguments from the proof of the Theorem in [20].

Let M be an arbitrary algebraic number field, and let $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ be a finite subset of O_M, the ring of integers of M. For given $N \geq 1$, let $\mathcal{G}_M(\mathcal{A}, N)$ denote the simple graph whose vertex set is $\mathcal{A}$ and whose edges are the unordered pairs $[\alpha_r, \alpha_s]$ having the property

$$|N_{M/\mathbb{Q}}(\alpha_r - \alpha_s)| > N.$$

Lemma 8.1 *Let M be a CM-field, $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ a finite set of real integers in M and β a nonreal integer in M. If the graph $\mathcal{G}_M(\mathcal{A}, N_{M/\mathbb{Q}}(2\beta))$ has a connected component of order $k \geq 2$ then $F(x) = (x - \alpha_1) \cdots (x - \alpha_m) - \beta$ has no irreducible factor of degree less than k over M. In particular, if $k > \deg(F)/2$ then F is irreducible over M.*

Proof See Lemma 7 in [18] and Lemma 4 in [20]. □

In general the bound given for the degrees of the irreducible factors of F is best possible. As is pointed out in [17,18], Lemma 8.1 is not true for arbitrary number fields M.

Let now again M be arbitrary, and $\mathcal{N}$ a finite, nonempty subset of O_M. For each pair of distinct positive integers r, s we select an element of $\mathcal{N}$, denoted by $\delta_{r,s}$, such that $\delta_{r,s} = \delta_{s,r}$. For any finite ordered subset $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ of O_M with $m \geq 3$, we denote by $\mathcal{H}_M(\mathcal{A}, \mathcal{D})$ or simply by $\mathcal{H}(\mathcal{A})$ the simple graph with vertex set $\mathcal{A}$ whose edges are the unordered pairs $[\alpha_r, \alpha_s]$ for which

$$\alpha_r - \alpha_s \notin \delta_{r,s} O_M^*.$$

Here O_M^* is the unit group of O_M, and $\mathcal{D}$ denotes the $\binom{m}{2}$-tuple $(\delta_{r,s})_{1 \leq r,s \leq m}$.

The ordered subsets $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ and $\mathcal{A}' = \{\alpha_1', \ldots, \alpha_m'\}$ of O_M are called *O_M-equivalent*, if

$$\alpha_r' = \varepsilon \alpha_r + \gamma, \quad r = 1, \ldots, m$$

for some $\varepsilon \in O_M^*$ and $\gamma \in O_M$. It is clear that the graphs $\mathcal{H}(\mathcal{A})$ and $\mathcal{H}(\mathcal{A}')$ are then isomorphic. In the sequel by sets $\mathcal{A}, \mathcal{A}', \mathcal{B}$ we shall mean ordered sets where the ordering is fixed by the indices.

The following lemma is the crucial new element in the proof of Theorem 8.1. Let ϱ denote the unit rank of O_M.

Lemma 8.2 *Let $m \geq 3$ be an integer with $m \neq 4$. Then for all but at most*

$$\left((m+1)10^{78(\varrho+1)}\right)^{4(m-2)} \tag{22}$$

O_M-equivalence classes of ordered subsets $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ of O_M, the graph $\mathcal{H}_M(\mathcal{A}, \mathcal{D})$ has a connected component of order at least $m - 1$.

This is a quantitative version of Lemma 5 of [20]. It is an important feature of our bound in (22) that it depends only on m and ϱ. For more general but much weaker quantitative versions, see Theorem 2 of [21] and Theorem 2.1 of [23].

Proof of Lemma 8.2 The assertion has been proved in [21, Theorem 1], with (22) replaced by

$$\prod_{r=3}^{m} \binom{r+1}{4} \left(6^2 C(3, O_M^*)\right)^{m-2}. \tag{23}$$

Here $C(3, O_M^*)$ denotes an upper bound for the number of solutions of the unit equation

$$a_1 u_1 + a_2 u_2 + a_3 u_3 = 1 \quad \text{in } u_1, u_2, u_3 \in O_M^*$$

with $\sum_{r \in I} a_r u_r \neq 0$ for each nonempty $I \subseteq \{1, 2, 3\}$, where a_1, a_2, a_3 are nonzero elements of M. The existence of such a bound $C(3, O_M^*)$ which is independent of a_1, a_2, a_3 was first proved in [14]. In view of Remark 5 of [22]

$$6^{2(m-2)} \prod_{r=3}^{m} \binom{r+1}{4} \leq (m+1)^{4(m-2)}. \tag{24}$$

Further, it follows from Theorem 3 of [13] that

$$C(3, O_M^*) \le \left(2^{35} \cdot 3^2\right)^{3^3(\varrho+1)}. \tag{25}$$

Now (22) is an immediate consequence of (23), (24) and (25). □

Proof of Theorem 8.1 Let $g(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial of CM-type of degree n, and let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree $m \ge 3$ with $m \ne 4$ and with distinct zeros in K. Suppose that $g(f(x))$ is reducible over $\mathbb{Q}$. Let β be a fixed zero of $g(x)$ in $\mathbb{C}$. Then by Capelli's theorem (cf. [31] or Lemma 3 in [20]), the polynomial $f(x) - \beta$ is reducible over the number field $M := K(\beta)$. By assumption K is totally real, hence M is of CM-type. Let $\alpha_1, \dots, \alpha_m$ be the zeros of $f(x)$ in K, and put $\mathcal{A} = \{\alpha_1, \dots, \alpha_m\}$. Then it follows from Lemma 8.1 that the graph $\mathcal{G}_M(\mathcal{A}, N_{M/\mathbb{Q}}(2\beta))$ has no connected component of order greater than $m/2$. We note that

$$\left(N_{M/\mathbb{Q}}(2\beta)\right)^{1/[M:K]} = \left(N_{\mathbb{Q}(\beta)/\mathbb{Q}}(2\beta)\right)^{[M:\mathbb{Q}(\beta)]/[M:K]} = 2^d g(0)^{d/n}, \tag{26}$$

where d denotes the degree of K over $\mathbb{Q}$.

Let O_K and O_K^* denote the ring of integers and the unit group, respectively, of K. Denote by $\mathcal{N}$ a maximal set of pairwise nonassociate elements of O_K whose norms in absolute value do not exceed $2^d g(0)^{d/n}$. As is known, the cardinality $|\mathcal{N}|$ of $\mathcal{N}$ is at most $c_3 g(0)^{d/n}$ where c_3 and c_4, c_5 below are effectively computable positive numbers which depend only on d and the discriminant of K; for an explicit value of c_3 we refer to [41]. For each pair of distinct positive integers r, s with $1 \le r, s \le m$, we select an element of $\mathcal{N}$, denoted by $\delta_{r,s}$, for which $\delta_{r,s} = \delta_{s,r}$. In this way we get a set, say $\mathcal{C}$, of $\binom{m}{2}$-tuples $(\delta_{r,s})_{1\le r,s\le m}$ whose cardinality is $|\mathcal{N}|^{\binom{m}{2}}$. For a fixed $\binom{m}{2}$-tuple $\mathcal{D} = (\delta_{r,s})_{1\le r,s\le m}$ and for a subset $\mathcal{B} = \{\beta_1, \dots, \beta_m\}$ of O_K, consider the graph $\mathcal{H}(\mathcal{B}) = \mathcal{H}_K(\mathcal{B}, \mathcal{D})$ defined above, but with K in place of M. We recall that $\mathcal{B}$ denotes the vertex set of $\mathcal{H}(\mathcal{B})$, and its edge set consists of those unordered pairs $[\beta_r, \beta_s]$ for which $\beta_r - \beta_s \notin \delta_{r,s} O_K^*$.

If $[\alpha_r, \alpha_s]$ is an edge of the complement of the graph $\mathcal{G}_M(\mathcal{A}, N_{M/\mathbb{Q}}(2\beta))$ then, by (26),

$$|N_{K/\mathbb{Q}}(\alpha_r - \alpha_s)| \le 2^d g(0)^{d/n}.$$

Hence $\alpha_r - \alpha_s$ is an associate of one of the elements of $\mathcal{N}$. Together with the fact that $\mathcal{G}_M(\mathcal{A}, N_{M/\mathbb{Q}}(2\beta))$ has no connected component of order $> m/2$, this implies that for at least one suitable $\binom{m}{2}$-tuple $\mathcal{D} = (\delta_{r,s})_{1\le r,s\le m}$ of $\mathcal{C}$, the connected components of the graph $\mathcal{H}_K(\mathcal{A}, \mathcal{D})$ have orders at most $m/2$. But the number of $\binom{m}{2}$-tuples $\mathcal{D}$ in question is at most $\left(c_4 g(0)^{1/n}\right)^{d\binom{m}{2}}$. Together with Lemma 8.2 (applied with K in place of M) and $\operatorname{rank}(O_K^*) + 1 \le d$, this gives that there are at most $\left(c_5 g(0)^{1/n}\right)^{d\binom{m}{2}}$ m-tuples $\mathcal{A}'$ in O_K such that $\mathcal{H}_K(\mathcal{A}', \mathcal{D})$ has no connected component of order $> m/2$ for some $\mathcal{D}$ and that $\mathcal{A}$ is O_K-equivalent to one of these $\mathcal{A}'$, say to $\mathcal{A}' = \{\alpha_1', \dots, \alpha_m'\}$.

In other words,

$$\alpha_r = \varepsilon\alpha'_r + \eta, \quad r = 1, \ldots, m \tag{27}$$

with some $\eta \in O_K$ and $\varepsilon \in O_K^*$. From among these O_K-equivalence classes consider now only those ones which contain a representative $\mathcal{A}' = \{\alpha'_1, \ldots, \alpha'_m\}$ for which $f_1(x) := (x - \alpha'_1) \ldots (x - \alpha'_m) \in \mathbb{Z}[x]$. If such a class has another representative, say $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ with $f_2(x) := (x - \alpha_1) \ldots (x - \alpha_m) \in \mathbb{Z}[x]$ then taking the discriminant of f_1 and f_2 and using (27) we infer that $\varepsilon^{m(m-1)} \in O_K^* \cap \mathbb{Q}$ whence $\varepsilon = \pm 1$ follows. Further, summing up the relations (27) from $r = 1$ to m, we deduce that $\eta \in O_K \cap \mathbb{Q} = \mathbb{Z}$. Consequently, each O_K-equivalence class under consideration contains at most two $\mathbb{Z}$-equivalence classes of m-tuples $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ from O_K for which $f(x) := (x - \alpha_1) \ldots (x - \alpha_m)$ has its coefficients in $\mathbb{Z}$. Here two tuples $\{\alpha_1, \ldots, \alpha_m\}$ and $\{\alpha'_1, \ldots, \alpha'_m\}$ are considered to be $\mathbb{Z}$-equivalent if there is an $a \in \mathbb{Z}$ such that $\alpha_r - \alpha'_r = a$ for some $r = 1, \ldots, m$. □

Remark 8.1 In the proof of the Theorem of [20] the author arrived also at the relations (27). However, there he followed another argument which cannot be made quantitative.

Acknowledgments The authors are grateful to the referee for the useful suggestions.

References

1. Ankeny, N.C., Brauer, R., Chowla, S.: A note on the class numbers of algebraic number fields. Am. J. Math. **78**, 51–61 (1956)
2. Bilu, Yu.F., Luca, F.: Divisibility of class numbers: enumerative approach. J. Reine Angew. Math. **578**, 79–91 (2005)
3. Borwein, P.: Computational Excursions in Analysis and Number Theory CMS Books in Mathematcs, Ch 11. Springer, New York (2002)
4. Borwein, P., Lisoněk, P., Percival, C.: Computational investigations of the Prouhet–Tarry–Escott problem. Math. Comput. **72**, 2063–2070 (2002)
5. Brauer, A.: Bemerkungen zu einem Satz von Herrn G. Pólya. Jahresber. Deutschen Math. Ver. **43**, 124–129 (1933)
6. Brauer, A., Brauer, R.: Über Irreduzibilitätskriterien von I. Schur und G. Pólya. Math. Z. **40**, 242–265 (1936)
7. Brauer, A., Brauer, R., Hopf, H.: Über die Irreduzibilität einiger spezieller Klasse von Polynomen. Jahresber. Deutschen Math. Ver. **35**, 99–112 (1926)
8. Brauer, A., Ehrlich, G.: On the irreducibility of certain polynomials. Bull. Am. Math. Soc. **52**, 844–856 (1946)
9. Chen, S.: The Prouhet-Tarry-Escott problem. http://member.netease.com/~chin/eslp/-TarryPrb.htm
10. Dorwart, H.L.: Concerning certain reducible polynomials. Duke Math. J. **1**, 70–73 (1935)
11. Dorwart, H.L.: Irreducibility of polynomials. Am. Math. Mon. **42**, 369–381 (1935)
12. Dorwart, H.L., Ore, O.: Criteria for the irreducibility of polynomials. Ann. Math. **34**, 81–94 (1933)
13. Evertse, J.H.: The number of solutions of decomposable form equations. Invent. Math. **122**, 559–601 (1995)
14. Evertse, J.H., Győry, K.: On the number of solutions of weighted unit equations. Compos. Math. **66**, 329–354 (1988)

15. Evertse, J.H., Győry, K., Stewart, C.L., Tijdeman, R.: S-unit equations and their applications. In: Baker, A. (ed.) New Advances in Transcendence Theory, pp. 110–174. Cambridge University Press, Cambridge (1988)
16. Flügel, W.: Solution to problem 226. Archiv. der Math. Und Physik **15**, 271 (1909)
17. Győry, K.: Sur l'irreducibilité d'une classe des polynômes I. Publ. Math. Debrecen **18**, 289–307 (1971)
18. Győry, K.: Sur l'irreducibilité d'une classe des polynômes II. Publ. Math. Debrecen **19**, 293–326 (1972)
19. Győry, K.: On the irreducibility of a class of polynomials III. J. Number Theory **15**, 164–181 (1982)
20. Győry, K.: On the irreducibility of a class of polynomials IV. Acta Arith. **62**, 399–405 (1992)
21. Győry, K.: On arithmetic graphs associated with integral domains II. In: Sets, Graphs and Numbers 365–374. North-Holland Publ. Comp., Amsterdam (1992)
22. Győry, K.: On the number of pairs of polynomials with given resultant or given semi-resultant. Acta Sci. Math. **57**, 515–529 (1993)
23. Győry, K.: On certain arithmetic graphs and their applications to diophantine problems. Functiones et Approximation **39**, 289–314 (2008)
24. Győry, K., Rimán, J.: On irreducibility criteria of Schur type (in Hungarian, English summary). Matematikai Lapok **24** (1973), 225–253 (1977)
25. Hua, L.K.: Introduction to Number Theory. Springer, Berlin (1982)
26. Ille, H.: Einige Bemerkungen zu einem von G. Pólya herrüherenden Irreduzibilitätskriterium. Jahresber. Deutschen Math. Ver. **35**, 204–208 (1926)
27. Levit, R.J.: Irreducibility of polynomials with low absolute values. Trans. Am. Math. Soc. **132**, 297–305 (1968)
28. Ore, O.: Einige Bemerkungen über Irreduzibilität. Jahresber. Deutsche Math. Ver. **44**, 147–151 (1934)
29. Pirgov, D.: An extension of I. Seres's theorem on the irreducibility of integral polynomials (Bulgarian), Godišnik Visš. Tehn. Učebn. Zaved. Mat. **8**, 31–34 (1972)
30. Pólya, G.: Verschiedene Bemerkungen zur Zahlentheorie. Jber. Deutsch. Math.-Verein. **28**, 31–40 (1919)
31. Rédei, L.: Algebra. Akadémiai Kiadó, Budapest (1967)
32. Schulz, W.: Über Reduzibilität bei gewissen Polynomen und das Tarry-Escottsche Problem. Math. Z. **63**, 133–144 (1955/1956)
33. Schur, I.: Problem 226. Arch. Math. Physik **13**(3), 367 (1908)
34. Schur, I.: Problem 275. Arch. Math. Physik **15**(3), 259 (1909)
35. Seres, I.: Über eine Aufgabe von Schur. Publ. Math. Debrecen **3**, 138–139 (1953)
36. Seres, I.: Lösung und Verallgemeinerung eines Schurschen Irreduzibilitätsproblems für Polynome. Acta Math. Acad. Sci. Hungar. **7**, 151–157 (1956)
37. Seres, I.: Über die Irreduzibilität gewisser Polynome. Acta Arith. **8**, 321–341 (1963)
38. Seres, I.: Irreducibility of polynomials. J. Algebra **2**, 283–286 (1965)
39. Seres, I.: On the irreducibility of certain polynomials (Hungarian). Mat. Lapok **16**, 1–7 (1965)
40. Sprindžuk, V.G.: Classical Diophantine Equations. Springer, Berlin (1993)
41. Sunley, J.S.: Class numbers of totally imaginary quadratic extensions of totally real fields. Trans. Am. Math. Soc. **175**, 209–232 (1973)
42. Tatuzawa, T.: Über die Irreduzibilität gewisser ganzzahliger Polynome. Proc. Jpn. Acad. **15**, 253–254 (1939)
43. Tverberg, H.: A study in irreducibility of polynomials, Doctoral thesis, University of Bergen (1968)
44. Tverberg, H.: On the irreducibility of polynomials taking small values. Math. Scand. **32**, 5–21 (1973)
45. Wegner, U.: Über die Irreduzibilität einer Klasse von ganzen rationalen Funktionen. Jahresber. Deutschen Math. Ver. **40**, 239–241 (1931)
46. Weisner, L.: Irreducibility of polynomials of degree n which assume the same value n times. Bull. Am. Math. Soc. **41**, 248–252 (1935)
47. Westlund, J.: On the irreducibility of certain polynomials. Am. Math. Mon. **16**, 66–67 (1909)