ACTA ARITHMETICA
LXII.4 (1992)

On the irreducibility of a class of polynomials, IV

by

K. GYŐRY (Debrecen)

To the memory of Z. Z. Papp

1. Introduction. In this paper, we continue our investigations (cf. [5], [6], [9]) concerning 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 K. We assume throughout this paper 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 we say that $g(x)$ is *of CM-type*. For example, cyclotomic polynomials and quadratic polynomials of negative discriminant are of CM-type. If $g(f(x))$ is reducible for some $f(x)$ then so are $g(f(x+a))$ for all $a \in \mathbb{Z}$. Polynomials $f(x)$ and $f(x+a)$ are called $\mathbb{Z}$-*equivalent* or simply *equivalent*. In part I of this paper (cf. [5]) we proved that for given $g(x)$, there are only finitely many pairwise inequivalent monic polynomials $f \in \mathbb{Z}[x]$ with distinct zeros in $\mathbb{Q}$ for which $g(f(x))$ is reducible. In parts II and III (cf. [6], [9]), 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 exceptions $f(x)$ for which $g(f(x))$ is reducible for a suitable $g(x)$ (cf. Lemma 2 in the present paper). However, the characterization of these exceptions led to a hard diophantine problem concerning certain arithmetic graphs.

Using some recent results on unit equations ([2], [4]), we solved in [10] (see also [11]) the diophantine problem in question. This enables us to give a precise description of the exceptional polynomials $f(x)$ mentioned above. Let K be a totally real algebraic number field, and $g \in \mathbb{Z}[x]$ a monic irreducible polynomial of CM-type. We shall prove that the exceptions $f(x)$

Research supported in part by Grant 1641 from the Hungarian National Foundation for Scientific Research.

have the following properties:

(1) $f \in \mathbb{Z}[x]$ is a monic quartic polynomial with distinct zeros in K such that $f = f_1 f_2$ with some monic polynomials f_1, f_2 for which $f_i(x) - f_i(0) \in \mathbb{Z}[x]$, $i = 1, 2$, $f_1(0)$ and $f_2(0)$ are rational integers or conjugate quadratic integers, $f_1(x) - f_2(x) = \gamma$ for some $\gamma \in K$ with $|N_{K/\mathbb{Q}}(\gamma)| \le (2g(0)^{1/n})^{[K:\mathbb{Q}]}$ $(n = \deg(g))$, and if β is a zero of $g(x)$ then

$$\beta = \delta(\delta - \gamma)$$

for some non-zero integer δ in $\mathbb{Q}(\beta, \gamma)$ with $f_2(0) + \delta \in \mathbb{Q}(\beta)$.

In this case we have

$$f(x) - \beta = (f_1(x) - \delta)(f_2(x) + \delta)$$

over $\mathbb{Q}(\beta)$ and hence, by Capelli's theorem (cf. Lemma 3), $g(f(x))$ is reducible over $\mathbb{Q}$.

It is easy to see that if K has a quadratic subfield then there are infinitely many pairwise inequivalent $f(x)$ satisfying (1) for a suitable $g(x)$ of CM-type. Indeed, if $\sqrt{d} \in K$ for some square-free positive integer d then there are infinitely many $a, b \in \mathbb{Z}$ with $a^2 - db^2 = 1$; in this case the polynomials $f(x) = (x^2 - 2ax + 1)(x^2 - 2ax)$ and the minimal polynomial $g(x)$ of $i(i-1)$ have the required properties. In this example, every polynomial $f(x)$ has a factorization $f = f_1 f_2$ having the property (1) with $f_1(0), f_2(0) \in \mathbb{Z}$. We now give another example where $f_1(0)$ and $f_2(0)$ are not rational. Let K be a totally real number field containing $\sqrt{3 \pm \sqrt{7}}$. There are infinitely many $a, b, c \in \mathbb{Z}$ with $a^2 - 2b^2 = 1$, $a > 0$, $b < 0$ and $c = 3 - 4b(a - 3b)$. It is easy to check that the polynomials

$$f(x) = (x^2 - (c + \sqrt{7}))(x^2 - (c - \sqrt{7})) \in \mathbb{Z}[x]$$

and the minimal polynomial $g(x)$ of $(1+i)((1+i)-2\sqrt{7})$ satisfy the properties listed in (1).

THEOREM. *Let $g \in \mathbb{Z}[x]$ be a monic irreducible polynomial of CM-type. Apart from the possible exceptions $f(x)$ described in* (1), *there are only finitely many pairwise inequivalent monic polynomials $f \in \mathbb{Z}[x]$ with distinct zeros in K for which $g(f(x))$ is reducible over $\mathbb{Q}$.*

In the case when K is a quadratic number field, our Theorem implies an ineffective version of Theorem 1b of [6]. Further, our Theorem provides a more precise characterization of the exceptions $f(x)$ occurring in Theorem 1 of [9]. We should, however, remark that Theorem 1 of [9] has been established over an arbitrary totally real number field instead of $\mathbb{Q}$. Further, in contrast with the results of [6] and [9], our Theorem is ineffective, i.e., its proof does not make it possible to determine all $f(x)$ for which $g(f(x))$ is reducible over $\mathbb{Q}$ for a given $g(x)$. This is due to the fact that the proof of our Lemma 5 (cf. [10], [11]) depends on the above-mentioned finiteness theorems on unit equations [2], [4] which are ineffective.

COROLLARY 1. *Let $g \in \mathbb{Z}[x]$ be a monic irreducible polynomial of CM-type. There are only finitely many pairwise inequivalent monic polynomials $f \in \mathbb{Z}[x]$ of degree other than 4 and with distinct zeros in K such that $g(f(x))$ is reducible over $\mathbb{Q}$.*

This is an immediate consequence of our Theorem. The following corollary can also be easily deduced from the above Theorem.

COROLLARY 2. *Let $g \in \mathbb{Z}[x]$ be a monic irreducible polynomial of CM-type, and suppose that K has no quadratic subfield. Then there are only finitely many pairwise inequivalent monic polynomials $f \in \mathbb{Z}[x]$ with distinct zeros in K for which $g(f(x))$ is reducible over $\mathbb{Q}$.*

For $K = \mathbb{Q}$, this gives an ineffective version of Theorem 5 of [5].

As is shown by the following example, our results do not remain valid for any monic irreducible polynomial $g \in \mathbb{Z}[x]$ and for any number field K. Let K be an arbitrary (not necessarily totally real) algebraic number field having infinitely many units, $f \in \mathbb{Z}[x]$ a monic polynomial whose zeros are distinct units in K and $g(x) = x - f(0)$. Then the degree of f can be arbitrarily large and $g(f(x))$ is divisible by x over $\mathbb{Q}$.

2. Proof of the Theorem. To prove our Theorem we need several lemmas.

LEMMA 1. *Let $g \in \mathbb{Z}[x]$ be a monic irreducible polynomial of CM-type. There are only finitely many pairwise inequivalent monic polynomials $f(x) \in \mathbb{Z}[x]$ with degree ≤ 3 and with distinct real zeros for which $g(f(x))$ is reducible over $\mathbb{Q}$.*

Proof. This is a consequence of Theorem 2b of [6] which was proved in [6] in an effective way. ∎

For a polynomial $f \in \mathbb{Z}[x]$, we denote by $H(f)$ the height of f, i.e., the maximum absolute value of the coefficients of f. Further, for any algebraic number field M, O_M will denote the ring of integers of M, and O_M^* the unit group of O_M. Let K be a totally real algebraic number field of degree k. We may assume without loss of generality that K is a normal extension of $\mathbb{Q}$.

LEMMA 2. *Let $g(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial of CM-type with degree n, and let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree $m \geq 2$ with distinct zeros in K such that $g(f(x))$ is reducible over $\mathbb{Q}$. There is a number $C_1 = C_1(K, g)$ such that $m \leq C_1$. Further,*

(i) *$f(x)$ is equivalent to a polynomial $f^*(x)$ with $H(f^*) \le C_2(K,g,m)$, or*

(ii) *m is even, and f, g have the following properties*:

(2) *$f(x) = f_1(x)f_2(x)$ for some monic polynomials f_1, f_2 for which $f_1(x) - f_2(x) = \gamma$ with some non-zero integer γ in K with degree ≤ 2 over $\mathbb{Q}$ such that $|N_{K/\mathbb{Q}}(\gamma)| \le (2g(0)^{1/n})^k$, $f_i(x) - f_i(0) \in \mathbb{Z}[x]$ and $f_i(0) \in O_{\mathbb{Q}(\gamma)}$ for $i = 1, 2$, and each zero β of $g(x)$ satisfies $\beta = \delta(\delta - \gamma)$ with some non-zero $\delta \in O_{\mathbb{Q}(\beta,\gamma)}$ for which $\delta + f_2(0) \in O_{\mathbb{Q}(\beta)}$.*

Proof. This is an immediate consequence of Theorem 1 in [9]. We note that in [9], C_1 and C_2 are given explicitly. For some improvements of that C_1, see [3] and [10]. ■

We remark that for $m = 4$, the properties of f, g listed in (ii) coincide with those occurring in (1). In the remainder of the proof it suffices to restrict ourselves to polynomials $f(x)$ of bounded degree. Further, it is enough to prove that if f, g satisfy the assumptions listed in (ii) of Lemma 2 and if the degree of f is greater than 4, then $f(x)$ is equivalent to a polynomial of bounded height.

Lemma 3 (Capelli). *Let $f, g \in \mathbb{Z}[x]$ be monic polynomials, $g(x)$ irreducible over $\mathbb{Q}$ and β one of the zeros of $g(x)$. If*

$$f(x) - \beta = \prod_{i=1}^{s} (\pi_i(x))^{k_i}$$

is the irreducible factorization of $f(x) - \beta$ over $\mathbb{Q}(\beta)$ then

$$g(f(x)) = \prod_{i=1}^{s} (N(\pi_i(x)))^{k_i} \qquad (N \text{ denotes the norm } N_{\mathbb{Q}(\beta)(x)/\mathbb{Q}(x)})$$

is the irreducible factorization of $g(f(x))$ over $\mathbb{Q}$.

Proof. See [15] or [14]. We remark that Capelli proved this theorem in a less general form (cf. [15]).

Lemma 3 reduces the question of reducibility of polynomials $g(f(x))$ over $\mathbb{Q}$ to that of reducibility of polynomials of the form $f(x) - \beta$ over $\mathbb{Q}(\beta)$.

Let M be an arbitrary algebraic number field, and let $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ be a finite, non-empty subset of O_M. For given $N \ge 1$, we denote by $\mathcal{G} = \mathcal{G}_M(\mathcal{A}, N)$ the simple graph whose vertex set is $\mathcal{A}$ and whose edges are the unordered pairs $[\alpha_i, \alpha_j]$ having the property

$$|N_{M/\mathbb{Q}}(\alpha_i - \alpha_j)| > N\,.$$

Lemma 4. *Let M be a CM-field, $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ a finite set of real integers in M and β a non-real integer in M. If the graph $\mathcal{G}_M(\mathcal{A}, N_{M/\mathbb{Q}}(2\beta))$*

has a connected component of order $s \geq 2$ *then* $F(x) = (x - \alpha_1)\ldots \ldots(x - \alpha_m) - \beta$ *has no irreducible factor of degree less than* s *over* M. *If in particular* $s > \deg(F)/2$ *then* F *is irreducible over* M.

Proof. This is in fact Lemma 7 in [6]. As was pointed out in [5] and [6], it is not valid for arbitrary number fields M. Further, the estimate given for the degrees of the irreducible factors of F is in general best possible (cf. [6]). ∎

Let again M be an arbitrary algebraic number field, and let $\mathcal{N}$ be a finite, non-empty subset of non-zero integers of M. For each pair of distinct positive integers i, j we select an element of $\mathcal{N}$, denoted by $\delta_{i,j}$, such that $\delta_{i,j} = \delta_{j,i}$. 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 $[\alpha_i, \alpha_j]$ for which

$$\alpha_i - \alpha_j \notin \delta_{i,j} O_M^* .$$

Here $\mathcal{D}$ denotes the $\binom{m}{2}$-tuple $(\delta_{i,j})_{1 \leq i,j \leq m}$.

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 $\alpha_i' = \varepsilon\alpha_i + \beta$ for some $\varepsilon \in O_M^*$ and $\beta \in O_M$, $i = 1, \ldots, m$. It is obvious that the graphs $\mathcal{H}(\mathcal{A})$ and $\mathcal{H}(\mathcal{A}')$ are then isomorphic.

The following lemma is the crucial new element in the proof of our Theorem.

Lemma 5. *Let* $m \geq 3$ *be an integer different from* 4. *Then for all but at most finitely many* O_M^**-equivalence classes of ordered subsets* $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ *of* O_M, *the graph* $\mathcal{H}(\mathcal{A})$ *has a connected component of order at least* $m - 1$.

Proof. This is an immediate consequence of Theorem 1 of [10]. In fact, Theorem 1 of [10] gives a more precise description of the graphs $\mathcal{H}(\mathcal{A})$ under consideration. The proof of Theorem 1 in [10] depends among other things on a finiteness result of Evertse and Győry [2] on unit equations in several unknowns. We note that Lemma 5 can also be proved by using the finiteness of the number of solutions of unit equations in two unknowns and the sharp upper bound derived in [4] for the number of solutions of such equations. Further, we remark that using an explicit bound of Schlickewei [12] for the number of solutions of unit equations, we obtained in [11] a refined and quantitative version of our Lemma 5. Together with quantitative versions of our other lemmas, this would enable one to establish a quantitative version of our Theorem. We shall not work this out here. ∎

Lemma 6. *There are only finitely many pairwise inequivalent monic polynomials in* $\mathbb{Z}[x]$ *with a given non-zero discriminant.*

P r o o f. This was proved in [7] in an effective way. For an explicit version, see also [8]. In [1], an explicit upper bound was given for the number of equivalence classes consisting of such polynomials which have all their zeros in a given number field. ∎

P r o o f o f t h e T h e o r e m. Let again K be a totally real algebraic number field with degree k, and suppose that $K/\mathbb{Q}$ is normal. Let $g(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial of CM-type with degree n, let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree m with distinct zeros in K, and suppose that $g(f(x))$ is reducible over $\mathbb{Q}$. As was mentioned above, in view of Lemmas 1 and 2 it suffices to deal with the case when m is even and greater than 4, $m \le C_1$ (with the bound C_1 occurring in Lemma 2) and f, g have the properties specified in (2).

Let β be a fixed zero of $g(x)$. Then, by Lemma 3, $f(x) - \beta$ is reducible over the number field $M := K(\beta)$. The field M is also of CM-type. Denote by $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ the set of zeros of $f(x)$. It follows from Lemma 4 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

$$(3) \qquad (N_{M/\mathbb{Q}}(2\beta))^{1/[M:K]} = (N_{\mathbb{Q}(\beta)/\mathbb{Q}}(2\beta))^{[M:\mathbb{Q}(\beta)]/[M:K]} = 2^k g(0)^{k/n}.$$

Denote by $\mathcal{N}$ a maximal set of pairwise non-associate elements in O_K whose norms in absolute value do not exceed $2^k g(0)^{k/n}$. Then $|\mathcal{N}|$, the cardinality of $\mathcal{N}$, can be explicitly estimated from above in terms of K and g (see [13] and [9]). For each pair of distinct positive integers i, j with $1 \le i, j \le m$, we select an element of $\mathcal{N}$, denoted by $\delta_{i,j}$, for which $\delta_{i,j} = \delta_{j,i}$. In this way, we get a set, say $\mathcal{C}$, of $\binom{m}{2}$-tuples $(\delta_{i,j})_{1 \le i,j \le m}$ whose cardinality is $|\mathcal{N}|^{\binom{m}{2}}$. For a fixed $\binom{m}{2}$-tuple $\mathcal{D} = (\delta_{i,j})_{1 \le i,j \le m}$ and for a subset $\mathcal{B} = \{\beta_1, \ldots, \beta_m\}$ of O_K, consider the graph $\mathcal{H}(\mathcal{B}) = \mathcal{H}_K(\mathcal{B}, \mathcal{D})$ defined above. We recall that $\mathcal{B}$ denotes the vertex set of $\mathcal{H}(\mathcal{B})$, and its edge set consists of those unordered pairs $[\beta_i, \beta_j]$ for which

$$\beta_i - \beta_j \notin \delta_{i,j} O_K^* .$$

If $[\alpha_i, \alpha_j]$ is an edge of the complement of $\mathcal{G}_M(\mathcal{A}, N_{M/\mathbb{Q}}(2\beta))$ then, by (3), $|N_{K/\mathbb{Q}}(\alpha_i - \alpha_j)| \le 2^k g(0)^{k/n}$. Hence $\alpha_i - \alpha_j$ 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 $\mathcal{D} = (\delta_{i,j})_{1 \le i,j \le m}$ of $\mathcal{C}$, the connected components of the graph $\mathcal{H}(\mathcal{A})$ have orders at most $m/2$. It follows now from Lemma 5 that there is a finite subset $\mathcal{M}$ of m-tuples in O_K, which depends only on K and g, such that $\mathcal{A}$ is O_K^*-equivalent to one of the elements of $\mathcal{M}$, say to $\mathcal{A}' = \{\alpha_1', \ldots, \alpha_m'\}$. In other words, we have

$$\alpha_i = \varepsilon \alpha_i' + \varrho , \qquad i = 1, \ldots, m ,$$

for some $\varepsilon \in O_K^*$ and $\varrho \in O_K$. Thus we have

$$|D(f)|^k = |N_{K/\mathbb{Q}}(D(f))| = \prod_{1\le i<j\le m} |N_{K/\mathbb{Q}}(\alpha_i' - \alpha_j')|^2 \neq 0\,.$$

This implies that $D(f)$ can assume only finitely many values. Consequently, it follows from Lemma 6 that up to $\mathbb{Z}$-equivalence, there are only finitely many possibilities for $f(x)$. This completes the proof of our Theorem. ∎

References

[1] J. H. Evertse and K. Győry, *On the number of polynomials and integral elements of given discriminant*, Acta Math. Hungar. 51 (1988), 341–362.

[2] —, —, *On the numbers of solutions of weighted unit equations*, Compositio Math. 66 (1988), 329–354.

[3] J. H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, *S-unit equations and their applications*, in: New Advances in Transcendence Theory, A. Baker (ed.), Cambridge University Press, 1988, 110–174.

[4] —, —, —, —, *On S-unit equations in two unknowns*, Invent. Math. 92 (1988), 461–477.

[5] K. Győry, *Sur l'irréductibilité d'une classe des polynômes I*, Publ. Math. Debrecen 18 (1971), 289–307.

[6] —, *Sur l'irréductibilité d'une classe des polynômes II*, ibid. 19 (1972), 293–326.

[7] —, *Sur les polynômes à coefficients entiers et de discriminant donné*, Acta Arith. 23 (1973), 419–426.

[8] —, *Sur les polynômes à coefficients entiers et de discriminant donné II*, Publ. Math. Debrecen 21 (1974), 125–144.

[9] —, *On the irreducibility of a class of polynomials III*, J. Number Theory 15 (1982), 164–181.

[10] —, *On arithmetic graphs associated with integral domains*, in: A Tribute to Paul Erdős (A. Baker, B. Bollobás and A. Hajnal, eds.), Cambridge University Press, 1990, 207–222.

[11] —, *On arithmetic graphs associated with integral domains II*, in: Sets, Graphs and Numbers, Budapest 1991, Colloq. Math. Soc. J. Bolyai 59, North-Holland, to appear.

[12] H. P. Schlickewei, *S-unit equations over number fields*, Invent. Math. 102 (1990), 95–107.

[13] J. S. Sunley, *Class numbers of totally imaginary quadratic extensions of totally real fields*, Trans. Amer. Math. Soc. 175 (1973), 209–232.

[14] L. Rédei, *Algebra*, Akadémiai Kiadó, Budapest 1967.

[15] N. Tschebotaröw und H. Schwerdtfeger, *Grundzüge der Galois'schen Theorie*, Noordhoff, Groningen/Djakarta 1950.

MATHEMATICAL INSTITUTE
KOSSUTH LAJOS UNIVERSITY
H-4010 DEBRECEN, HUNGARY

Received on 25.2.1992 (2232)