On polynomials with integer coefficients and given discriminant, IV

By K. GYŐRY (Debrecen)

1. Introduction

Let us call the polynomials $f, f^* \in Z[x]$ *equivalent* if $f^*(x)=f(x+a)$ for some $a \in Z$. In [11] we proved that if $D \neq 0$ is a given integer then there are only finitely many pairwise non-equivalent monic polynomials $f \in Z[x]$ with discriminant $D(f)=D$ and such a system of polynomials can be effectively determined. In [12] we showed that for any monic polynomial $f \in Z[x]$ of degree $k \geqq 2$ with non-zero discriminant D $k=\deg(f) \leqq 2+2\,(\log 3)^{-1} \log |D|$ holds and there is a polynomial f^* equivalent to f such that the maximum $\|f^*\|$ of the absolute values of the coefficients of f^* satisfies

$$\|f^*\| < \exp\exp\{4(\log|D|)^{13}\}. \tag{1}$$

In [13] this last statement was proved, as a special case of a more general result, with the estimate

$$\|f^*\| < \exp\{c_1|D|^{\varkappa}\}, \tag{2}$$

where $\varkappa > 9(k-1)(k-2)/2$ and c_1 denotes an effectively computable positive constant depending only on k and $\varkappa$.

In our papers [10], [11], [12], [13] and [14] various applications of these results were given to reducibility of polynomials of the form $g(f(x))$, to polynomials of given discriminant, to algebraic numbers of given discriminant and to Diophantine equations.

In Section 2 of the present paper we generalize some theorems of [11], [12] and [13] to polynomials with algebraic integer coefficients and given discriminant. In Section 3 some applications of these results are presented to algebraic integers with given relative discriminant over a fixed algebraic number field.

p-adic generalizations and further applications are given in Part V [15] and in a joint paper of Z. Z. PAPP and the author [17].

2. Polynomials with algebraic integer coefficients and given discriminant

Throughout this paper L denotes an algebraic number field of degree $n \geqq 1$ with ring of integers Z_L. Let D_L be the absolute value of the discriminant of L. If $f \in Z_L[x]$ and $f^*(x)=f(x+a)$ for some $a \in Z_L$, then for their discriminants $D(f)=D(f^*)$ holds. Such polynomials $f, f^* \in Z_L[x]$ will be called Z_L-*equivalent*.

As usual, $|\overline{\alpha}|$ will denote the maximum absolute value of the conjugates of an algebraic number α and $|\overline{F}|$ will signify the maximum absolute value of the conjugates of the coefficients of a polynomial $F(x)$ with algebraic coefficients.

The following theorem contains Theorem 2 of [12], Corollary 1.6 of [13] and Corollary 1.3 of [14]. In the special case $L=Q$ (3) is obviously sharper than (2).

Theorem 1. *Let L be as above, and let δ be a non-zero integer in L with $|N_{L/Q}(\delta)|\leqq d$. If $f\in Z_L[x]$ is a monic polynomial of degree $k\geqq 3$ with discriminant δ, then it is Z_L-equivalent to a polynomial f^* for which*

$$|\overline{f^*}| < |\overline{\delta}|^{\frac{1}{k-1}} \exp\left\{(5nk^3)^{30nk^3}\left((dD_L^k)^{3/2}(\log dD_L)^{nk}\right)^{3(k-1)(k-2)}\right\} \tag{3}$$

holds.

Theorem 1 is still true for $k=2$ and, by Theorem 2, in this case we have

$$|\overline{f^*}| < \left(|\overline{\delta}|^{1/2}+(2D_L^{1/2})^{n^2}+1\right)^2 \tag{3'}$$

instead of (3). In what follows, all the consequences will be stated only for $k\geqq 3$, however in view of (3′) they remain valid even for $k=2$ with other estimates.

We note that in Theorem 1 and in its corollaries one may choose $d=|\overline{\delta}|^n$.

Corollary 1.1. *Let L be as in Theorem 1. Suppose that we are given a natural number $k\geqq 2$ and a non-zero $\delta\in Z_L$. Then there are only finitely many pairwise Z_L non-equivalent monic polynomials $f\in Z_L[x]$ with $\deg(f)=k$ and $D(f)=\delta$ and such a system of polynomials can be effectively determined.*

This corollary is a generalization of certain earlier results obtained in [11], [12] and [13].

Denote by $f^{(j)}(x)$ the j-th derivative of a polynomial $f(x)$. The next corollary generalizes Corollary 1.7 of [13].

Corollary 1.2. *Let L be as in Theorem 1. If $f\in Z_L[x]$ is a monic polynomial of degree $k\geqq 3$ with discriminant $D(f)=\delta\neq 0$ and $|N_{L/Q}(\delta)|=d$, then*

$$\begin{aligned}|\overline{D(f^{(j)})}| &< |\overline{\delta}|^{\frac{2(k-j-1)}{k-1}} \exp\left\{c_2\left((dD_L^k)^{3/2}(\log dD_L)^{nk}\right)^{3(k-1)(k-2)}\right\} < \\ &< \exp\left\{2c_2\left((|\overline{\delta}|^n D_L^k)^{3/2}(\log(|\overline{\delta}|^n D_L))^{nk}\right)^{3(k-1)(k-2)}\right\}\end{aligned} \tag{4}$$

for any $0\leqq j\leqq k-2$, where $c_2=2k(5nk^3)^{30nk^3}$.

Corollary 1.3. *Let $f(x)=x^k+a_1x^{k-1}+\ldots+a_k\in Z_L[x]$ be a polynomial of degree $k\geqq 3$ with discriminant $\delta\neq 0$ and let $|N_{L/Q}(\delta)|\leqq d$. If for some i, $1\leqq i\leqq k$, $|\overline{a_i}|\leqq A_i|\overline{f}|^\tau$ with $A_i\geqq 0$ and $0\leqq\tau<i/k$, then*

$$|\overline{a_j}| < \binom{k+1}{j}\left\{(kT)^{\min(i-k\tau,1)}+2^\tau A_i^{\min\left(\frac{1}{i-k\tau},1\right)}\right\}^{\max\left(\frac{j}{i-k\tau},j\right)} \tag{5}$$

for each j, $1\leqq j\leqq k$, where T denotes the expression occurring on the right side of inequality (3).

Corollary 1.3 generalizes some results of Parts II and III (see [12] and [13]) obtained in the special case $L=Q$.

By using the argument employed at the end of the proof of Theorem 1 of [13] we could easily extend Theorem 1 (and its corollaries) to polynomials with discriminant $\delta=0$ to get a generalization of Theorem 1 of [13]. We now generalize Theorem 1 of the present paper in another direction which also includes the case $\delta=0$.

Denote by $P_f(x)\in Z_L[x]$ the squarefree monic polynomial divisor of maximal degree[1]) of a monic polynomial $f\in Z_L[x]$. If $D(f)\neq 0$ we have obviously $P_f=f$. For linear P_f let $D(P_f)=1$.

Theorem 1 is an immediate consequence of the following result.

Theorem 2. *Let L be defined as in Theorem 1, and let δ be a non-zero integer in L with $|N_{L/Q}(\delta)|\leqq d$ $(d\geqq 2)$. If $f\in Z_L[x]$ is a monic polynomial of degree $k\geqq 2$ with $\deg(P_f)=l$ and $D(P_f)=\delta$, then f is Z_L-equivalent to a polynomial f^* satisfying*

$$|\overline{f^*}| < |\overline{\delta}|^{\frac{k}{l(l-1)}} \exp\left\{(5nl^3)^{30nl^3}\cdot(k/l)\left((dD_L^l)^{3/2}(\log dD_L)^{nl}\right)^{3(l-1)(l-2)}\right\} \tag{6}$$

for $l\geqq 3$ and

$$|\overline{f^*}| < (|\overline{\delta}|^{1/2}+(2D_L^{1/2})^{n^2}+1)^k \tag{6'}$$

for $l<3$.

It is clear that, by applying Theorem 2 in place of Theorem 1, Corollaries 1.1, 1.2 and 1.3 can be extended to polynomials with discriminant $\delta=0$ too.

3. Applications to algebraic integers with given relative discriminant

Suppose again that L is an algebraic number field of degree $n\geqq 1$ and let D_L denote the absolute value of its discriminant. As usual, denote by $D_{L(\alpha)/L}(\alpha)$ and $N_{L(\alpha)/L}(\alpha)$, or, more briefly, by $D(\alpha)$ and $N(\alpha)$ the discriminant and the norm of an algebraic number α relative to the extension $L(\alpha)/L$. If α is an algebraic integer with minimal polynomial f over L, then α and f have the same degree, say k, over L, $D(\alpha)=D(f)$, $N(\alpha)=(-1)^k f(0)$, $|\overline{f}|\leqq(2|\overline{\alpha}|)^k$ and $|\overline{\alpha}|\leqq k|\overline{f}|$.

We shall say that the algebraic integers α and α^* are Z_L-*equivalent* if $\alpha-\alpha^*\in Z_L$. In this case their minimal polynomials over L are also Z_L-equivalent.

Theorems 3A and 4 are immediate consequences of Theorem 1 and Corollary 1.3 respectively.

Theorem 3A. *Let L be as above. If α is an algebraic integer with degree $k\geqq 3$ and discriminant δ over L and $|N_{L/Q}(\delta)|\leqq d$, then there exists an α^* Z_L-equivalent to α such that*

$$|\overline{\alpha^*}| < |\overline{\delta}|^{\frac{1}{k(k-1)}} \exp\left\{(5nk^3)^{30nk^3}\left((dD_L^k)^{3/2}(\log dD_L)^{nk}\right)^{3(k-1)(k-2)}\right\}. \tag{7}$$

In fact Theorem 1 yields a slightly weaker estimate for $|\overline{\alpha^*}|$ in terms of $|\overline{\delta}|$. However, if we apply Theorem 2 to the minimal polynomial f of α over L, (25) implies (7).

---

[1]) In other words P_f is the monic polynomial divisor of maximal degree of f over Z_L such that $D(P_f)\neq 0$.

Theorem 3A generalizes and improves Theorem 3 of [13]*), obtained in the special case $L=Q$.

If we take into consideration even the discriminant of the number field generated by α over L, we get a sharper estimate for $|\overline{\alpha^*}|$ in terms of d.

Theorem 3B. *Let L be as in Theorem 3A, and let K be an extension of degree $k\geqq 3$ of L with discriminant $D_K=D_{K/Q}$. If α is an integer in K with $D_{K/L}(\alpha)=\delta\neq 0$ and $|N_{L/Q}(\delta)|\leqq d$, then there exists an $\alpha^*\in K$, Z_L-equivalent to α, for which*

$$(8)\quad |\overline{\alpha^*}| < |\overline{\delta}|^{\frac{1}{k(k-1)}} \exp\left\{(5c_3)^{30(c_3+2)}\left(|D_K|(\log|D_K|)^{nk}\right)^{3(k-1)(k-2)}(|D_K|^{3(k-1)(k-2)/2}+\log d)\right\}$$

holds, where $c_3=nk(k-1)(k-2)$.

Denoting by f the minimal polynomial of α over L, (8) immediately follows from (23). In particular if K/L is normal, it is easy to obtain

$$(8')\qquad |\overline{\alpha^*}| < |\overline{\delta}|^{\frac{1}{k(k-1)}} \exp\left\{(5nk)^{30(nk+2)}|D_K|(\log|D_K|)^{3nk-1}\cdot(|D_K|^{1/2}+\log d)\right\}$$

from the proof of Theorem 2.

An easy corollary of Theorem 3A and (3′) is the following

Corollary 3.1. *Let L be as in Theorem 3A. Suppose that we are given a natural number $k\geqq 2$ and a non-zero integer δ in L. Then there are only finitely many pairwise Z_L non-equivalent algebraic integers with degree k and discriminant δ over L and such a system of algebraic integers can be effectively determined.*

In the special case $L=Q$ this was earlier proved in [11] and, in an ineffective form, in [6].

We note that Corollary 3.1 can be deduced, in an ineffective form, from an ineffective theorem of B. J. Birch and J. R. Merriman [6] on binary forms with given degree and given discriminant, combining it with Siegel's theorem concerning the number of solutions of the generalized Thue equation in integers of an algebraic number field [25]. (For an effective version of Siegel's theorem see A. Baker [4] and A. Baker and J. Coates [5]).

Denote by $D_{K/L}$ the relative discriminant of K/L. As is well-known (see for example H. Hasse [18]), for every primitive integral element α of K/L the principal ideal generated by $D_{K/L}(\alpha)$ can be written as

$$(9)\qquad \left(D_{K/L}(\alpha)\right) = \mathfrak{I}^2(\alpha)D_{K/L}$$

with an integral ideal $\mathfrak{I}(\alpha)$ in L. $\mathfrak{I}(\alpha)$ is called the index of α with respect to K/L or the unessential divisor of the discriminant $D_{K/L}(\alpha)$. Evidently $\alpha\varepsilon$ has the same index for any unit ε of L.

The next corollary which contains Corollary 3.2 of [13] as a special case will be deduced from Theorem 3B.

Corollary 3.2. *Let L be as in Theorem 3A, $\mathfrak{I}$ a non-zero integral ideal in L with norm $\leqq M$ and K an extension of degree $k\geqq 3$ of L with discriminant $D_K=D_{K/Q}$.*

*) *Added in proof.* Very recently L.A. Trelina (Mat. Zametki **21** (1977), 289—296) has obtained a p-adic analogue of this theorem of [13].

Suppose that there is an integer α in K with index $\mathfrak{I}$. Then α is Z_L-equivalent to an algebraic integer of the form $\alpha^*\varepsilon$, where ε is a unit in L and

$$|\overline{\alpha^*}| < \exp\left\{(5nk^3)^{30nk^3}\left(|D_K|(\log|D_K|)^{nk}\right)^{3(k-1)(k-2)}(|D_K|^{3(k-1)(k-2)/2}+\log M)\right\}.$$

An important consequence of Corollary 3.2 is that up to the obvious multiplications by units of L there are only finitely many pairwise Z_L non-equivalent integers in K with a given index $\mathfrak{I}\neq 0$ and such a system of integers can be effectively determined.

By a theorem of E. ARTIN [2] the above relative extension K/L has a relative integral basis if and only if the index of a primitive integral element α of K with respect to K/L is principal. Consequently, if $D_{K/L}$ is principal and for example the class number of L/Q is odd, then K/L has a relative integral basis (for further results and references see e.g. W. NARKIEWICZ [19]). Moreover, as is well-known, numerous special relative extensions K/L have integral bases of the form $1, \alpha, \alpha^2, \ldots, \alpha^{k-1}$ with a suitable $\alpha\in Z_K$ when $Z_K=Z_L[\alpha]$. For earlier results the reader may consult [19]. Recently J. J. PAYAN [20], [21], M. N. GRAS [8], [9], G. ARCHINARD [1] and P. A. B. PLEASANTS [22] have obtained results connected with the existence of such an integral basis.*) The relative extensions having this property are generally called *monogenic*.

Corollary 3.2 yields the following general result on monogenic extensions.

Corollary 3.3. *Let L be an algebraic number field of degree $n\geqq 1$, and let K be an extension of degree $k\geqq 3$ of L with discriminant $D_K=D_{K/Q}$. Suppose that $Z_K=Z_L[\alpha]$ for some $\alpha\in Z_K$. Then α is Z_L-equivalent to an algebraic integer of the form $\alpha^*\varepsilon$, where ε is a unit in L and*

$$|\overline{\alpha^*}| < \exp\left\{(5nk^3)^{30nk^3}\left(|D_K|^{3/2}(\log|D_K|)^{nk}\right)^{3(k-1)(k-2)}\right\}.$$

This provides a general and effective algorithm for deciding whether a relative extension K/L is monogenic or not and for determining all $\alpha\in Z_K$ for which $Z_K=Z_L[\alpha]$.

The special case $L=Q$ is of particular interest. Corollary 3.3 generalizes and improves our earlier result obtained in the case $L=Q$ ([13], Corollary 3.3).

Corollary 1.3 implies the following

Theorem 4. *Let L be as in Theorem 3A, and let α be an algebraic integer of relative degree $k\geqq 3$ with norm μ and discriminant δ over L such that $|N_{L/Q}(\delta)|\leqq d$. Denote by $f(x)$ the minimal polynomial of α over L. Let $N\geqq 1$ and $0\leqq\tau<1$ be real numbers satisfying*

$$|\overline{\mu}| \leqq N|\overline{f}|^{\tau}.$$

Then

$$|\overline{\alpha}| \leqq k|\overline{f}| < k(k+1)\left\{(kT)^{\min((1-\tau)k,1)}+2^{\tau}N^{\min\left(\frac{1}{(1-\tau)k},1\right)}\right\}^{\max\left(\frac{1}{1-\tau},k\right)}, \tag{10}$$

where T denotes the expression occurring on the right side of (3).

Consequently, for any given algebraic number field L there are only finitely many algebraic integers with a given degree, a given norm and a given discriminant

*) *Added in proof.* Recently B. KNIGHT has obtained such a result in the case $L=Q$, $k=4$ (see W. M. SCHMIDT, Proc. Internat. Congress Math., Vancouver, 1974. Vol. I, pp. 177—185.)

over L and these integers can be effectively determined. In the special case $L=Q$ this was proved in [11] (see also [12] and [13]).

The next theorem provides an explicit upper bound for $|\overline{\alpha}|$ depending only on $|N_{L/Q}(\mu)|$ instead of $|\overline{\mu}|$.

Theorem 5. *Let L be as in Theorem 3A, and let α be an algebraic integer with degree $k\geqq 3$, with norm μ and discriminant δ over L. Suppose that $|N_{L/Q}(\delta)|\leqq d$ and $|N_{L/Q}(\mu)|\leqq N'$. Then we have*

$$|\overline{\alpha}| < \exp\Big\{(5nk^3)^{30nk^2(k+1)}\Big((dD_L^k)^{2/3}(\log dD_L)^{nk}\Big)^{3(k-1)}\Big[\log(|\overline{\delta}|N') + \\ + \Big((dD_L^k)^{3/2}(\log dD_L)^{nk}\Big)^{3(k-1)(k-2)}\Big]\Big\}. \tag{11}$$

Choosing $d=|\overline{\delta}|^n$ in Theorem 5, we immediately get the following

Corollary. *Let L be defined as in Theorem 3A. If ε is an algebraic unit with degree $k\geqq 3$ and discriminant $D(\varepsilon)$ over L, then*

$$|\overline{\varepsilon}| < \exp\Big\{c_4|\overline{D(\varepsilon)}|^{n(k-1)(9k/2-7)}\big(\log|\overline{D(\varepsilon)}|\big)^{3nk^3}\Big\}$$

and, provided that $|\overline{D(\varepsilon)}| > \exp\{9k\}$,

$$|\overline{D(\varepsilon)}| > c_5(\log|\overline{\varepsilon}|)^{(n(k-1)(5k-7))-1}$$

hold with effectively computable positive constants c_4, c_5 depending only on k, n and D_L.

By virtue of (11) it is easy to compute explicit values for c_4 and c_5.

We remark that in the special case $L=Q$ Theorem 4 gives a slightly sharper estimate for $|\overline{\varepsilon}|$. (10) implies

$$|\overline{\varepsilon}| < \exp\Big\{2k(5k^3)^{30k^3}\big(|D(\varepsilon)|^{3/2}(\log|D(\varepsilon)|)^k\big)^{3(k-1)(k-2)}\Big\}$$

for any algebraic unit ε of degree $k\geqq 3$ and discriminant $D(\varepsilon)$ over Q. This sharpens the estimates of Corollary 2.2 of [13] (see also the Corollary to Theorem 2 of [14]).

4. A preliminary result

Let M be an algebraic number field of degree m with s real and $2t$ complex conjugate fields. Write $r=s+t-1$. Let D_M denote the absolute value of the discriminant of M.

The proof of Theorem 2 depends on the following result which is proved in our paper [16].

Proposition. *Let M be as above, and let $\gamma_1, \gamma_2, \gamma_3$ be non-zero integers in M with $\max_i(|\overline{\gamma_i}|)\leqq G$. If Θ_1, Θ_2 and Θ_3 are non-zero integers of M satisfying*

$$\gamma_1\Theta_1+\gamma_2\Theta_2+\gamma_3\Theta_3=0 \quad \textit{and} \quad \max_i\{|N_{M/Q}(\Theta_i)|\}\leqq N,$$

then there exists a unit ε *in* M *such that*

$$\max_i (|\overline{\Theta_i \varepsilon}|) < \exp\{c_6 D_M (\log 2D_M)^{3m-1}(D_M^{1/2} + \log(GN))\},$$

where

$$c_6 = \frac{8^{2m}}{m^{m-3}} [16m(r+3)]^{15(r+2)}.$$

This proposition sharpens and generalizes Lemma 4 of [12] and Lemma 3 of [13]. Its proof is based on a recent explicit inequality of A. J. VAN DER POORTEN and J. H. LOXTON [23], [24] on linear forms in the logarithms of algebraic numbers.

5. Proofs

PROOF OF THEOREM *2*. Write

$$f(x) = (x-\alpha_1) \ldots (x-\alpha_k).$$

Suppose, for convenience, that the roots of P_f are $\alpha_1, \ldots, \alpha_l$. The case $l=1$ being trivial, we assume that $l \geqq 2$. Then we have

$$D(P_f) = \prod_{1 \leqq i < j \leqq l} (\alpha_j - \alpha_i)^2 = \delta. \tag{12}$$

First suppose that $l \geqq 3$. Choose any three from among $\alpha_1, \ldots, \alpha_l$. We may assume without loss of generality that these are $\alpha_1, \alpha_2, \alpha_3$. Putting $M = L(\alpha_1, \alpha_2, \alpha_3)$ and $m = [M: Q]$, from (12) we get

$$|N_{M/Q}(\alpha_j - \alpha_i)| \leqq |N_{M/Q}(\delta)|^{1/2} \leqq d^{m/2n} \tag{13}$$

for any $1 \leqq i < j \leqq 3$. Further we have

$$(\alpha_2 - \alpha_1) + (\alpha_3 - \alpha_2) + (\alpha_1 - \alpha_3) = 0. \tag{14}$$

Let D_M denote the absolute value of the discriminant of M and r the free rank of the group of units of M. Apply now the Proposition of Section 4 to (14) and (13). By this Proposition there is a unit ε and integers δ_{ji} in M such that

$$\alpha_j - \alpha_i = \varepsilon \delta_{ji} \tag{15}$$

for any $1 \leqq i < j \leqq 3$ and

$$\max_{1 \leqq i < j \leqq 3} (|\overline{\delta_{ji}}|) < \exp\{c_7 D_M (\log 2D_M)^{3m-1}(D_M^{1/2} + \log d)\} = T_1, \tag{16}$$

where $c_7 = \dfrac{8^{2m}}{2nm^{m-4}} [16m(r+3)]^{15(r+2)}$.

Let $M_i = L(\alpha_i)$ and $m_i = [M_i: Q]$ for $i = 1, \ldots, l$. Denote by D_{M_i} the absolute value of the discriminant of M_i. Put $D = \max_i D_{M_i}$ and let $D=2$ if $L(\alpha_1, \ldots, \alpha_l) = Q$. Then

$$D_M | D_{M_1}^{m/m_1} D_{M_2}^{m/m_2} D_{M_3}^{m/m_3} \leqq D^{3(l-1)(l-2)} \tag{17}$$

holds (see H. M. STARK [27]). (16) and (17) imply

$$T_1 < \exp\{c_8(D(\log D)^{nl})^{3(l-1)(l-2)}(D^{3(l-1)(l-2)/2}+\log d)\} = T_2,$$

where $c_8 = 2c_9^{4-c_9}(12(l-1)(l-2))^{3c_9-1}(4c_9)^{30(c_9+2)}$ and $c_9 = nl(l-1)(l-2)$.

We note that if P_f is irreducible over Z_L and the extensions M_i/L are normal then we may take $T_2=T_1$ replacing D_M in T_1 with D, $r+1$ with m and m with nl.

If $l>3$, we may repeat the above argument first for $\alpha_2-\alpha_1$, $\alpha_j-\alpha_2$, $\alpha_j-\alpha_1$ with $j=4, \ldots, l$, then for $\alpha_j-\alpha_i$, $\alpha_i-\alpha_1$, $\alpha_j-\alpha_1$ with $3\leqq i<j$. Then we get in the same way as in [11] and [12] that

$$\alpha_j-\alpha_i = \varepsilon\varrho_{ji}$$

for any $1\leqq i<j\leqq l$, where

$$\max_{j,i}(\overline{|\varrho_{ji}|}) < T_2^{2c_9+1} \quad \text{and} \quad \max_{j,i}(\overline{|\varrho_{ji}^{-1}|}) < T_2^{3c_9-1}.$$

Thus it follows from (12) that

$$\varepsilon^{l(l-1)} = \delta \prod_{1\leqq i<j\leqq l} \varrho_{ji}^{-2},$$

whence

$$\overline{|\varepsilon|} < \overline{|\delta|}^{\frac{1}{l(l-1)}} \cdot T_2^{3c_9-1}.$$

This implies

$$\overline{|\alpha_j-\alpha_i|} < \overline{|\delta|}^{\frac{1}{l(l-1)}} \cdot T_2^{5c_9} = T_3 \tag{18}$$

for any $1\leqq i<j\leqq l$.

If $l=2$, (18) immediately follows from (12) with $T_2=1$ instead of the above T_2.

Write now $\alpha_1+\ldots+\alpha_l=a_1$, where obviously $a_1\in Z_L$. By (18) we have [2])

$$l\alpha_i = a_1+\beta_i \tag{19}$$

for $i=1, \ldots, l$, β_i being integers such that

$$\max_i(\overline{|\beta_i|}) < (l-1)T_3. \tag{20}$$

There is an integral basis $1, \omega_2, \ldots, \omega_n$ for L with the property

$$\max_s(\overline{|\omega_s|}) < n2^{n(n-1)}D_L^{(n^2-1)/2}$$

(see [12]). Represent a_1 in such a basis. We can easily see that there is an $a_2\in Z_L$ congruent to $a_1 \pmod l$ for which

$$\overline{|a_2|} < ln^2 2^{n(n-1)}D_L^{(n^2-1)/2}. \tag{21}$$

---

[2]) The author is indebted to Z. Z. PAPP for his remark that in the proof of Theorem 2 of Part II (see [12], p. 139) one can use a deduction of the type (18)⇒(19) in place of employing an integral basis. This observation enables us to slightly simplify the above deduction (18)⇒(22), (23) too.

Write $a_1=la+a_2$. Then $a\in Z_L$. Since each $\alpha_j, j>l$, is equal to one of the α_i, $1\leqq i\leqq l$, by (19), (20), (21) and $D_L|D$ every α_i can be written in the form

$$\alpha_i = a+\gamma_i, \quad i = 1, \ldots, k, \tag{22}$$

where $\gamma_1, \ldots, \gamma_k$ are algebraic integers satisfying

(23)

$$\max_{1\leqq i\leqq k}(|\overline{\gamma_i}|) < |\overline{\delta}|^{\frac{1}{l(l-1)}} \exp\left\{(5c_9)^{30(c_9+2)}\left(D(\log D)^{nl}\right)^{3(l-1)(l-2)}\left(D^{3(l-1)(l-2)/2}+\log d\right)\right\}$$

if $l\geqq 3$ and

$$\max_{1\leqq i\leqq k}(|\overline{\gamma_i}|) < |\overline{\delta}|^{1/2}+(2D_L^{1/2})^{n^2} \tag{23'}$$

if $l=2$.

In the case $l=1$ we may choose $\gamma_i=0$ in (22) for any i.

We are going to derive an upper bound for $\max_i(|\overline{\gamma_i}|)$ not depending on D. Since D does not occur in (23′), it suffices to consider the case $l\geqq 3$. We recall that $D=D_{M_i}$ for some $M_i=L(\alpha_i)$, where $1\leqq i\leqq l$. The relative discriminant $D_{M_i/L}$ divides $D(P_f)$, consequently

$$D = D_{M_i} = N_{L/Q}(D_{M_i/L})D_L^{[M_i:L]} \leqq dD_L^l. \tag{24}$$

Finally, from (23) and (24) we get

$$\max_{1\leqq i\leqq k}(|\overline{\gamma_i}|) < |\overline{\delta}|^{\frac{1}{l(l-1)}} \exp\left\{(c_{10}/2l)\left((dD_L^l)^{3/2}(\log dD_L)^{nl}\right)^{3(l-1)(l-2)}\right\} \tag{25}$$

with $c_{10}=(5nl^3)^{30nl^3}$.

In view of (22) the polynomial

$$f^*(x) = (x-\gamma_1)\ldots(x-\gamma_k)\in Z_L[x]$$

is Z_L-equivalent to f and

$$|\overline{f^*}| \leqq (1+\max_{1\leqq i\leqq k}(|\overline{\gamma_i}|))^k.$$

This together with (25) and (23′) imply (6) and (6′).

Proof of Corollary 1.2. By Theorem 1 there is a polynomial f^*Z_L-equivalent to f such that

$$|\overline{f^*}| < T_4,$$

where, for brevity, T_4 denotes the upper bound given in Theorem 1 for $|\overline{f^*}|$. For $1\leqq j\leqq k-2$ this implies

$$|\overline{f^{*(j)}}| < k^j T_4,$$

whence

$$|\overline{D(f^{(j)})}| = |\overline{D(f^{*(j)})}| < (k^{2k}T_4)^{2(k-j-1)}$$

and (4) follows.

PROOF OF COROLLARY 1.3. By Theorem 1 there exists a polynomial $f^*(x)=x^k+b_1x^{k-1}+\ldots+b_k\in Z_L[x]$ such that $f(x)=f^*(x+a)$ for some $a\in Z_L$ and

$$|\overline{f^*}|<T_4, \tag{26}$$

where T_4, as above, denotes the expression occurring on the right side of (3). The case $a=0$ being trivial, we suppose that $a\neq 0$.

We have

$$|\overline{f}|\leqq|\overline{a}|^k+2^kT_4|\overline{a}|^{k-1}.$$

In case $|\overline{a}|<2^kT_4$ (33) immediately follows, hence we suppose $|\overline{a}|\geqq 2^kT_4$, when

$$|\overline{f}|\leqq 2|\overline{a}|^k. \tag{27}$$

On the other hand we have

$$a_i=\frac{f^{*(k-i)}(a)}{(k-i)!}=\binom{k}{k-i}a^i+\binom{k-1}{k-i}b_1a^{i-1}+\ldots+b_i. \tag{28}$$

Denote by $a^{(l)}$ such a conjugate of a over Q for which $|a^{(l)}|=|\overline{a}|$ holds. By taking the corresponding conjugates on both sides of (28) we get

$$a_i^{(l)}=\binom{k}{k-i}(a^{(l)})^i+\binom{k-1}{k-i}b_1^{(l)}(a^{(l)})^{i-1}+\ldots+b_i^{(l)}. \tag{29}$$

Since $|a^{(l)}|\geqq 1$, it follows from (26), (27) and (29) that

(30)

$$|\overline{a}|=\binom{k}{k-i}^{-1}\left|\binom{k-1}{k-i}b_1^{(l)}+\binom{k-2}{k-i}b_2^{(l)}(a^{(l)})^{-1}+\ldots+b_i^{(l)}(a^{(l)})^{-i+1}-a_i^{(l)}(a^{(l)})^{-i+1}\right|\leqq$$

$$\leqq\frac{i}{k-i+1}T_4+A_i|\overline{f}|^\tau/|\overline{a}|^{i-1}\leqq\frac{i}{k-i+1}T_4+2^\tau A_i|\overline{a}|^{k\tau-(i-1)}.$$

First suppose that $k\tau-(i-1)\geqq 0$, that is $\frac{1}{i-k\tau}\geqq 1$. Applying Lemma 5 of [13] to the linear polynomial $x-\frac{i}{k-i+1}T_4$, we get

$$|\overline{a}|\leqq\left[\left(\frac{i}{k-i+1}T_4\right)^{i-k\tau}+2^\tau A_i\right]^{\frac{1}{i-k\tau}}. \tag{31}$$

Let now $k\tau-(i-1)<0$, that is $\frac{1}{i-k\tau}<1$. Since $|\overline{a}|\leqq A_i^{\frac{1}{i-k\tau}}$ immediately implies (32), hence we assume that $|\overline{a}|>A_i^{\frac{1}{i-k\tau}}$. This yields

$$A_i|\overline{a}|^{k\tau-(i-1)}<A_i^{\frac{1}{i-k\tau}},$$

whence, by (30),

$$\overline{|a|} \leqq \left[\frac{i}{k-i+1} T_4 + 2^{\tau} A_i^{\frac{1}{i-k\tau}}\right]. \tag{32}$$

From (31) and (32) we get

$$\overline{|a|} \leqq \left[(kT_4)^{\min(i-k\tau,1)} + 2^{\tau} A_i^{\min\left(\frac{1}{i-k\tau},1\right)}\right]^{\max\left(\frac{1}{i-k\tau},1\right)} = T_5. \tag{33}$$

Finally we obtain

$$\overline{|a_j|} = \overline{\left|\frac{f^{*(k-j)}(a)}{(k-j)!}\right|} \leqq \binom{k+1}{j} T_5^j$$

which was to be proved.

Proof of Corollary 3.2. By (9) the discriminant $D_{K/L}(\alpha)$ satisfies

$$(D_{K/L}(\alpha)) = \mathfrak{J}^2 D_{K/L},$$

whence

$$\left|N_{L/Q}(D_{K/L}(\alpha))\right| = N_{L/Q}(\mathfrak{J}^2) N_{L/Q}(D_{K/L}) \leqq M^2 |D_K|. \tag{34}$$

Let r denote the free rank of the group of units of L. If $r>0$, by a theorem of C. L. Siegel [26] there exist independent units $\eta_1, \ldots, \eta_r$ in L such that

$$\left|\log \overline{|\eta_l|}\right| < 3n \left(\frac{5 \log D_L}{2n-2}\right)^{n-1} D_L^{1/2} = T_6$$

for $l=1, \ldots, r$. Let U denote the multiplicative group generated by $\eta_1, \ldots, \eta_r$. A well-known argument shows (see e.g. Z. I. Borevich and I. R. Shafarevich [7] or A. Baker [3]) that there is a unit $\eta \in U$ such that

$$\overline{|D_{K/L}(\alpha) \cdot \eta|} < [M^2 |D_K|]^{1/n} \exp\{n^2 T_6\}. \tag{35}$$

Further η can be written in the form $\eta = \eta' \varepsilon^{-k(k-1)}$ with $\eta', \varepsilon \in U$ for which

$$\overline{|\eta'|} < \exp\{rk(k-1) T_6\}.$$

Writing $\delta = D_{K/L}(\varepsilon^{-1}\alpha)$, we obtain from (35)

$$\overline{|\delta|} < [M^2 |D_K|]^{1/n} \exp\{n^2 k(k-1) T_6\}.$$

In view of (34) this is still true for $r=0$ with $\varepsilon=1$ and $T_6=0$. Applying now Theorem 3B to $\varepsilon^{-1}\alpha$, we get an α^* Z_L-equivalent to $\varepsilon^{-1}\alpha$ for which

$$\overline{|\alpha^*|} < \exp\left\{(5nk^3)^{30nk^3} \left(|D_K| (\log |D_K|)^{nk}\right)^{3(k-1)(k-2)} \left(|D_K|^{3(k-1)(k-2)/2} + \log M\right)\right\}.$$

This proves Corollary 3.2.

Proof of Theorem 5. By Theorem 3A α can be written in the form $\alpha = \alpha^* + a$, where $a \in Z_L$ and for $\overline{|\alpha^*|}$ (7) holds. For brevity, denote by T_7 the upper bound given in Theorem 3A for $\overline{|\alpha^*|}$.

By taking the norm of α over L we get

$$(\alpha_1^*+a)\dots(\alpha_k^*+a)=\mu,$$

where $\alpha_1^*,\dots,\alpha_k^*$ denote the conjugates of α^* over L. Suppose, for convenience, that $\alpha^*=\alpha_1^*$. Writing $\alpha_i^*+a=\mu_i$ for $i=1,2$, we obtain

$$\mu_1-\mu_2=\alpha_1^*-\alpha_2^*. \tag{36}$$

Put $M=L(\alpha_1^*,\alpha_2^*)$ and $m=[M:Q]$. Let D_M be the absolute value of the discriminant of M. Then $m\leqq nk(k-1)$ and we obtain $D_M\leqq(dD_L^k)^{2(k-1)}$ by the same reasoning as in (17) and (24). Further $|N_{M/Q}(\mu_i)|\leqq N'^{k(k-1)}$. Apply now the Proposition of Section 4 to (36) with $\gamma_1=\gamma_2=\Theta_3=1$ and $\gamma_3=\alpha_2^*-\alpha_1^*$. By virtue of this Proposition there is a unit ε in M such that

$$\max(|\overline{\mu_1\varepsilon}|,|\overline{\mu_2\varepsilon}|,|\overline{\varepsilon}|)<\exp\{c_{11}D_M(\log 2D_M)^{3m-1}\big(D_M^{1/2}+\log(2T_7N'^{k(k-1)})\big)\}=T_8$$

with $c_{11}=\dfrac{8^{2m}}{m^{m-3}}(4m)^{30(m+2)}$. Since $|\overline{\varepsilon^{-1}}|<T_8^{m-1}$, hence we have

$$|\overline{\alpha}|=|\overline{\mu_1}|<T_8^m<\exp\Big\{(5nk^3)^{30nk^2(k+1)}\big((dD_L^k)^{2/3}(\log dD_L)^{nk}\big)^{3(k-1)}\big[\log(|\overline{\delta}|N')+$$
$$+\big((dD_L^k)^{3/2}(\log dD_L)^{nk}\big)^{3(k-1)(k-2)}\big]\Big\}.$$

References

[1] G. Archinard, Extensions cubiques cycliques de Q dont l'anneau des entiers est monogène, *Enseignement Math.* **20** (1974), 179—203.

[2] E. Artin, Questions de la base minimale dans la théorie des nombres algébriques, *Colloques Internat. du Centre National Recherche Scientifique*, No. **24**, CNRS, Paris, 1950, pp. 19—20; Collected papers of Emil Artin, *Reading, (Mass.)*, 1965, 229—231.

[3] A. Baker, Contributions to the theory of Diophantine equations, *Philos. Trans. Roy. Soc. London, Ser. A*, **263** (1968), 173—208.

[4] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Camb. Phil. Soc.* **65** (1969), 439—444.

[5] A. Baker and J. Coates, Integer points on curves of genus 1, *Proc. Camb. Phil. Soc.* **67** (1970), 595—602.

[6] B. J. Birch and J. R. Merriman, Finiteness theorems for binary forms with given discriminant, *Proc. London Math. Soc.* **25** (1972), 385—394.

[7] Z. I. Borevich and I. R. Shafarevich, Number theory, Academic Press, *New York* and *London*, 2nd ed., 1967 *(Translated from the Russian* (1964) *ed.)*

[8] M.-N. Gras, Sur les corps cubiques cycliques dont l'anneau des entiers est monogène, *Annales scientifiques de l'Université de Besançon*, 3e série, fasc. **6** (1973), (26 pages).

[9] M.-N. Gras, Lien entre le groupe des unités et la monogenéité des corps cubiques cycliques *Publ. Math. Univ. Besançon*, fasc. **1** (1975—76), (19 pages)

[10] K. Győry, Sur l'irréductibilité d'une classe des polynômes, II., *Publ. Math. (Debrecen)* **19** (1972), 293—326.

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

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

[13] K. Győry, Sur les polynômes à coefficients entiers et de discriminant donné, III., *Publ. Math. (Debrecen)* **23** (1976), 141—165.

[14] K. Győry, Polynomials with given discriminant, *Coll. Math. Soc. János Bolyai* **13**, *Debrecen*, 1974. Topics in number theory (edited by P. Turán), pp. 65—78. *Amsterdam—Oxford—New York*, 1976.

[15] K. GYŐRY, On polynomials with integer coefficients and given discriminant, V. p-adic generalizations, to appear.
[16] K. GYŐRY, On the solutions of linear diophantine equations in algebraic integers of bounded norm, to appear.
[17] K. GYŐRY and Z. Z. PAPP, On discriminant form and index form equations, to appear.
[18] H. HASSE, Zahlentheorie, Zweite Auflage, *Berlin*, 1963.
[19] W. NARKIEWICZ, Elementary and analytic theory of algebraic numbers, *Warszawa*, 1974.
[20] J. J. PAYAN, Ordres monogènes des corps cycliques de degré premier, *Sém. Théorie Nombres Univ. Grenoble*, 1971—72.
[21] J. J. PAYAN, Sur les classes ambiges et les ordres monogènes d'une extension cyclique de degré premier impair sur Q ou sur un corps quadratique imaginaire, *Arkiv för Mat.* **11** (1973), 239—244.
[22] P. A. B. PLEASANTS, The number of generators of the integers of a number field, *Mathematika*, **21** (1974), 160—167.
[23] A. J. VAN DER POORTEN and J. H. LOXTON, Computing the effectively computable bound in Baker's inequality for linear forms in logarithms, *Bull. Austral. Math. Soc.* **15** (1976), 33—57.
[24] A. J. VAN DER POORTEN and J. H. LOXTON, Multiplicative relations in number fields, *Bull. Austral. Math. Soc.* **16** (1977), 83—98. Corregindum and addendum, ibid. **17** (1977), 151—156.
[25] C. L. SIEGEL, Approximation algebraischer Zahlen, *Math. Z.* **10** (1921), 173—213.
[26] C. L. SIEGEL, Abschätzung von Einheiten, *Nachr. Akad. Wiss. Göttingen, math.—phys. Kl.* 1969, 71—86.
[27] H. M. STARK, Some effective cases of the Brauer—Siegel theorem, *Inv. Math.* **23** (1974), 135—152.

(Received January 28, 1975; in revised form February 17, 1977)