ACTA ARITHMETICA
LXVI.3 (1994)

Upper bounds for the degrees of decomposable forms of given discriminant

by

K. Győry (Debrecen)

1. Introduction. In our paper [5] a sharp upper bound was given for the degree of an arbitrary squarefree binary form $F \in \mathbb{Z}[X, Y]$ in terms of the absolute value of the discriminant of F. Further, all the binary forms were listed for which this bound cannot be improved. This upper estimate has been extended by Evertse and the author [3] to decomposable forms in $n \geq 2$ variables. The bound obtained in [3] depends also on n and is best possible only for $n = 2$. The purpose of the present paper is to establish an improvement of the bound of [3] which is already best possible for every $n \geq 2$. Moreover, all the squarefree decomposable forms in n variables over $\mathbb{Z}$ will be determined for which our bound cannot be further sharpened. In the proof we shall use some results and arguments of [5] and [3] and two theorems of Heller [6] on linear systems with integral valued solutions.

2. Results. Let $F(\boldsymbol{X}) = F(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$ be a decomposable form of degree r with splitting field K over $\mathbb{Q}$. Then F can be written as

$$F(\boldsymbol{X}) = l_1(\boldsymbol{X}) \ldots l_r(\boldsymbol{X}) \tag{1}$$

where $l_1, \ldots, l_r$ are linear forms with coefficients in K. Suppose that F is *squarefree*, i.e. that it is not divisible by the square of a linear form over K. Put

$$\operatorname{rank}(F) = \operatorname{rank}_K\{l_1, \ldots, l_r\}\,.$$

Assume that F has rank m. Obviously $m \leq n$. Let $\mathcal{I}(F)$ denote the collection of linearly independent subsets of $\{l_1, \ldots, l_r\}$ of cardinality m. Denote by O_K the ring of integers of K, and by (l_i) the (possibly fractional) O_K-ideal generated by the coefficients of l_i. For any subset $\mathcal{L} = \{l_{i_1}, \ldots, l_{i_m}\}$ in $\mathcal{I}(F)$,

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

denote by $l_{i_1} \wedge \ldots \wedge l_{i_m}$ the exterior product of the coefficient vectors of $l_{i_1}, \ldots, l_{i_m}$, and by $(l_{i_1} \wedge \ldots \wedge l_{i_m})$ the O_K-ideal generated by the coordinates of this exterior product. The O_K-ideal

$$\mathfrak{D}(\mathcal{L}) = \frac{(l_{i_1} \wedge \ldots \wedge l_{i_m})}{(l_{i_1}) \ldots (l_{i_m})}$$

is integral. As was proved in [3], there is a positive rational integer D_F, called the *discriminant* (1) of F, such that

$$(D_F) = \prod_{\mathcal{L} \in \mathcal{I}(F)} \mathfrak{D}(\mathcal{L})^2, \tag{2}$$

where (D_F) denotes the O_K-ideal generated by D_F. The integer D_F does not depend on the choice of $l_1, \ldots, l_r$ and $D_{\lambda F} = D_F$ for all non-zero $\lambda \in \mathbb{Q}$. If in particular F is a primitive squarefree binary form of degree ≥ 2 (i.e. the coefficients of F are relatively prime) then D_F is just the absolute value of the usual discriminant $D(F)$ of F (cf. [3]).

Two decomposable forms $F(X_1, \ldots, X_n)$ and $G(Y_1, \ldots, Y_m)$ with coefficients in $\mathbb{Z}$ are called *integrally equivalent* if each can be obtained from the other by a linear transformation of variables with rational integer coefficients. It is easy to see that integrally equivalent decomposable forms over $\mathbb{Z}$ have the same degree, same rank and same discriminant. For further properties of discriminants, we refer to [2] and [3].

In [5] we proved that if $F \in \mathbb{Z}[X, Y]$ is a squarefree binary form of degree $r \geq 2$ then

$$r \leq 3 + \frac{2}{\log 3} \cdot \log |D(F)|. \tag{3}$$

Further, we showed that up to equivalence, the forms $XY(X-Y)$ and $XY(X-Y)(X^2+XY+Y^2)$ are the only binary forms for which equality occurs in (3). Recently Evertse and the author [3] proved that if $F \in \mathbb{Z}[X_1, \ldots, X_n]$ is a squarefree decomposable form of degree r and rank m then

$$r \leq 2^m - 1 + \frac{m}{\log 3} \cdot \log D_F. \tag{4}$$

For primitive and squarefree binary forms F with integer coefficients this implies (3).

We shall prove the following.

Theorem. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be a squarefree decomposable form of degree r and rank m. Then*

$$r \leq \binom{m+1}{2} + \frac{m}{\log 3} \cdot \log D_F. \tag{5}$$

(1) For polynomials in several variables there exists also another concept of discriminant; see e.g. [4].

Further, equality holds if and only if F is integrally equivalent to a multiple of one of the forms

$$G(Y_1,\ldots,Y_m)=Y_1\ldots Y_m\prod_{1\le i<j\le m}(Y_i-Y_j)$$

(*when* $D_F=1$) *and*

$$G(Y_1,Y_2)=Y_1Y_2(Y_1-Y_2)(Y_1^2+Y_1Y_2+Y_2^2)$$

(*when* $m=2$ *and* $D_F=3$).

For $n=2$, this gives the above-quoted result of the author [5]. Further, for $m>2$, (5) is an improvement of the estimate (4) of Evertse and the author [3].

3. Proof. To prove our Theorem, we need several lemmas. We shall keep the notation of Section 2.

LEMMA 1. *Let $F\in\mathbb{Z}[X_1,\ldots,X_n]$ be a squarefree decomposable form such that $F=F_1F_2$ where F_1 and F_2 have their coefficients in $\mathbb{Z}$. Then $D_{F_1}\cdot D_{F_2}$ divides D_F in $\mathbb{Z}$.*

Proof. This is an immediate consequence of Lemma 1 of [3]. ∎

In what follows, let $F\in\mathbb{Z}[X_1,\ldots,X_n]$ be a squarefree decomposable form of degree r and rank m, let K be the splitting field of F over $\mathbb{Q}$, and let

$$F=l_1\ldots l_r \tag{1}$$

be a factorization of F into linear factors over K. Let again $\mathcal{I}(F)$ denote the collection of linearly independent subsets of $\{l_1,\ldots,l_r\}$ of cardinality m.

LEMMA 2. *Let*

$$\mathcal{L}_1=\{l_{i_1},\ldots,l_{i_m}\}\,,\ \mathcal{L}_2=\{l_{j_1},\ldots,l_{j_m}\}\in\mathcal{I}(F)$$

and suppose that

$$l_{j_k}=\sum_{p=1}^m c_{kp}l_{i_p}\qquad \textit{for } k=1,\ldots,m\,.$$

Then

$$\frac{\mathfrak{D}(\mathcal{L}_2)}{\mathfrak{D}(\mathcal{L}_1)}=(\det(c_{kp}))\frac{(l_{i_1})\ldots(l_{i_m})}{(l_{j_1})\ldots(l_{j_m})}\,.$$

Proof. This is a special case of Lemma 3 of [3]. ∎

Following [6], a finite subset S of $\mathbb{Q}^n$ is said to be a *Dantzig set* if it has the following property: if a vector in S is a linear combination of a set of linearly independent vectors in S, then the coefficients in the combination are 1, -1 or 0. Each subset of S is then also a Dantzig set. By the dimension of S we mean the maximal number of linearly independent vectors in S. S is called maximal (for its dimension) if there is no Dantzig set of the same dimension properly containing S. Obviously a maximal Dantzig set must contain with each vector $\boldsymbol{a}$ also $-\boldsymbol{a}$. Further, it should contain the null vector.

LEMMA 3. *A Dantzig set of dimension m in $\mathbb{Q}^n$ has at most $m(m+1)$ elements* (*not counting the null vector*).

Proof. This is a consequence of Theorem (4.2) of Heller [6]. ∎

Remark 1. Lemma 3 implies that if a Dantzig set S of dimension m in $\mathbb{Q}^n$ consists of non-zero, pairwise non-proportional vectors, then its cardinality is at most $\binom{m+1}{2}$. We shall need this consequence of Lemma 3.

LEMMA 4. *If a Dantzig set S of dimension m in $\mathbb{Q}^n$ contains $m(m+1)$ vectors* (*not counting the null vector*), *then there exist linearly independent vectors $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ in S such that $S = \{\boldsymbol{a}_i - \boldsymbol{a}_j; i \neq j,\ i, j = 0, 1, \ldots, m\}$ where $\boldsymbol{a}_0 = \mathbf{0}$.*

In other words, S is the set of edges (that is, one-dimensional faces, taken in both orientations and interpreted as vectors) of an m-simplex.

Proof. Lemma 4 is a special case of Theorem (4.6) of Heller [6]. ∎

LEMMA 5. *The set of edges of a simplex is a Dantzig set.*

Proof. See the statement (2.3) of [6]. ∎

For a positive integer a, denote by (a) the ideal generated by a in $\mathbb{Z}$, and by $\Omega(a)$ the total number of prime factors of a. For a $\mathbb{Z}$-ideal $\mathfrak{a} = (a)$ put $\Omega(\mathfrak{a}) = \Omega(a)$.

LEMMA 6. *Let $F \in \mathbb{Z}[X_1, \ldots, X_n]$ be as above*, *and assume that F has splitting field $\mathbb{Q}$. Then*

$$r \le \binom{m+1}{2} + \frac{1}{2}\Omega(D_F)\,. \tag{6}$$

Remark 2. Lemma 6 seems to be interesting in itself. This should be compared with Theorem 4 of [3] on decomposable forms over number fields. Our Lemma 6 is an improvement of Theorem 4 of [3] in the special case when the ground ring is $\mathbb{Z}$ and the splitting field is $\mathbb{Q}$.

Proof of Lemma 6. We shall need Lemmas 2 and 3 and some arguments from the proof of Theorem 4 of [3].

We may assume without loss of generality that in the factorization (1) of F, each linear factor l_i has relatively prime rational integer coefficients. Then $(l_i) = (1)$ for $i = 1, \ldots, r$.

First assume that $\mathfrak{D}(\mathcal{L})$ is properly contained in (1) for each $\mathcal{L} \in \mathcal{I}(F)$. We show that the cardinality of $\mathcal{I}(F)$ is at least $r-m+1$. Indeed, suppose that

$$\mathcal{L}_0 = \{l_1, \ldots, l_m\} \in \mathcal{I}(F)\,.$$

Then we have

$$l_i = \sum_{j=1}^{m} c_{ij} l_j\,, \qquad i = m+1, \ldots, r$$

for some $c_{ij} \in \mathbb{Q}$, at least one of which, say $c_{i,j(i)}$, is different from zero. Putting $\mathcal{L}_i = (\mathcal{L}_0 \cup \{l_i\}) \setminus \{l_{j(i)}\}$ for $i = m+1, \ldots, r$, the sets $\mathcal{L}_0, \mathcal{L}_{m+1}, \ldots, \mathcal{L}_r$ are contained in $\mathcal{I}(F)$. Hence, by (2), we get

$$r - m + 1 \le \Omega(\mathfrak{D}(\mathcal{L}_0)) + \Omega(\mathfrak{D}(\mathcal{L}_{m+1})) + \ldots + \Omega(\mathfrak{D}(\mathcal{L}_r)) \le \frac{1}{2}\Omega(D_F)\,,$$

which implies (6).

Next assume that there are $\mathcal{L} \in \mathcal{I}(F)$ with $\mathfrak{D}(\mathcal{L}) = (1)$. Let $\mathcal{S}$ be a maximal subset of $\{l_1, \ldots, l_r\}$ with the following property: for each subset $\mathcal{L}'$ of $\mathcal{S}$ of cardinality m which is contained in $\mathcal{I}(F)$, we have $\mathfrak{D}(\mathcal{L}') = (1)$. We may assume without loss of generality that $\mathcal{S} = \{l_1, \ldots, l_s\}$ where $m \le s \le r$. Then for each l_i with $s+1 \le i \le r$ there is an $\mathcal{L}_i \in \mathcal{I}(F)$ with $\mathfrak{D}(\mathcal{L}_i) \ne (1)$ which contains l_i and $m-1$ linear forms from $\mathcal{S}$. This implies that

$$r - s \le \Omega(\mathfrak{D}(\mathcal{L}_{s+1})) + \ldots + \Omega(\mathfrak{D}(\mathcal{L}_r)) \le \frac{1}{2}\Omega(D_F)\,. \tag{7}$$

Let now $\mathcal{L}$ be an arbitrary subset of $\mathcal{S}$ with $\mathcal{L} \in \mathcal{I}(F)$. Assume for instance that $\mathcal{L} = \{l_1, \ldots, l_m\}$. Then $\mathfrak{D}(\mathcal{L}) = (1)$. Each l_i with $m+1 \le i \le s$ can be expressed uniquely in the form

$$l_i = \sum_{j=1}^{m} c_{ij} l_j \qquad \text{with } c_{ij} \in \mathbb{Q}\,.$$

For $m+1 \le i \le s$, $1 \le j \le m$, put $\mathcal{L}_{ij} = (\mathcal{L} \cup \{l_i\}) \setminus \{l_j\}$. By Lemma 2 we have

$$\mathfrak{D}(\mathcal{L}_{ij}) = \frac{\mathfrak{D}(\mathcal{L}_{ij})}{\mathfrak{D}(\mathcal{L})} = (c_{ij})\,,$$

whence $c_{ij} = 0$, 1 or -1. Hence S, the set of the coefficient vectors of the linear forms in $\mathcal{S}$, is a Dantzig set of dimension m in $\mathbb{Q}^n$. Further, the vectors in S are pairwise non-proportional and the null vector is not contained in S. Thus, by Lemma 3 and Remark 1, we have

$$s \le \binom{m+1}{2}.$$

Together with (7) this implies (6). ■

P r o o f o f t h e T h e o r e m. In our proof we shall use Lemmas 1, 4, 5 and 6 as well as some arguments from the proof of Theorem 1 of [3]. Let $F(\boldsymbol{X}) \in \mathbb{Z}[X_1, \ldots, X_n]$ be a squarefree decomposable form of rank m and degree r. Then

$$F(\boldsymbol{X}) = \prod_{k=1}^{r} (\alpha_{k1} X_1 + \ldots + \alpha_{kn} X_n)$$

with some algebraic numbers $\alpha_{k1}, \ldots, \alpha_{kn}$, $k = 1, \ldots, r$. As is known (see e.g. [1]), the $\mathbb{Z}$-module generated by the vectors $(\alpha_{1j}, \ldots, \alpha_{rj})^T$, $j = 1, \ldots, n$, in $\overline{\mathbb{Q}}^r$ has a basis. Further, it is easy to show that its rank is just m. Consequently, F is integrally equivalent to a form in m variables. Hence we may assume without loss of generality that in F we have $m = n$. Further, one may assume that $F(1, 0, \ldots, 0) \neq 0$ (see e.g. [1]) and that the coefficients of F are relatively prime.

The form F can be factored as

$$F = F_0 F_1 \ldots F_t\,,$$

where F_0 is the product of linear forms with relatively prime coefficients in $\mathbb{Z}$, and F_i is an irreducible norm form in $\mathbb{Z}[X_1, \ldots, X_m]$ of degree ≥ 2, i.e.

$$F_i(\boldsymbol{X}) = \lambda_i N_{K_i/\mathbb{Q}}(X_1 + \beta_{2i} X_2 + \ldots + \beta_{mi} X_m)$$

where $K_i = \mathbb{Q}(\beta_{2i}, \ldots, \beta_{mi})$ is an extension of $\mathbb{Q}$ of degree $\deg F_i$ and $\lambda_i \in \mathbb{Z} \setminus \{0\}$ for $i = 1, \ldots, t$. Let

$$r_i = \deg F_i\,, \qquad m_i = \operatorname{rank} F_i\,, \qquad D_i = D_{F_i} \qquad \text{for } i = 0, 1, \ldots, t\,.$$

We have

$$\Omega(a) \leq \frac{\log |a|}{\log 2} \qquad \text{for every } a \in \mathbb{Z} \text{ with } a \neq 0\,. \tag{8}$$

By Lemma 6 and (8) we have

$$r_0 \leq \binom{m_0 + 1}{2} + \frac{m_0}{2 \log 2} \cdot \log D_0 \leq \binom{m_0 + 1}{2} + \frac{m_0}{\log 3} \cdot \log D_0\,. \tag{9}$$

Hence, by $m_0 \leq m$ and (9), we have

$$r_0 \leq \binom{m + 1}{2} + \frac{m}{\log 3} \cdot \log D_0 \tag{10}$$

where equality can occur only for $D_0 = 1$. Further, as was proved in the proof of Theorem 1 of [3],

$$r_i \leq \frac{m_i}{\log 3} \cdot \log D_i \qquad \text{for } i = 1, \ldots, t\,, \tag{11}$$

whence, by $m_i \leq m$, we get

$$r_1 + \ldots + r_t \leq \frac{m}{\log 3} \cdot \log D_1 \ldots D_t\,. \tag{12}$$

Finally, from Lemma 1 it follows that $D_0 D_1 \ldots D_t$ divides D_F in $\mathbb{Z}$ and so, (10) and (12) give

$$r \le \binom{m+1}{2} + \frac{m}{\log 3} \cdot \log D_F \,. \tag{5}$$

Consider now the case when equality occurs in (5). Then equality must also occur in (9)–(12). Therefore $D_0 = 1$, $m_i = m$ for $i = 0, \ldots, t$ and $r_0 = \binom{m+1}{2}$. This means that in this case F must have linear factors with rational coefficients.

First suppose that each linear factor of F has coefficients in $\mathbb{Q}$, i.e. that $F = F_0$. Denote by S the set of the coefficient vectors of the linear factors of F. Then it follows from $D_F = 1$ and (2) that every determinant of order m composed of the coordinates of vectors of S is equal to 1, -1 or 0. This implies that S is a Dantzig set in $\mathbb{Q}^m$ of dimension m. Denote by $\pm S$ the set consisting of all vectors $\pm\boldsymbol{a}$ for which $\boldsymbol{a} \in S$. Then $\pm S$ is also a Dantzig set in $\mathbb{Q}^m$ with dimension m and cardinality $m(m+1)$. Hence, by Lemma 4, there are m linear forms among $l_1, \ldots, l_r$, say $l_1, \ldots, l_m$, such that $\det(l_1, \ldots, l_m) = \pm 1$ and that

$$F(\boldsymbol{X}) = \pm l_1(\boldsymbol{X}) \ldots l_m(\boldsymbol{X}) \prod_{1 \le i < j \le m} (l_i(\boldsymbol{X}) - l_j(\boldsymbol{X})) \,.$$

But then F is integrally equivalent to a multiple of the form

$$G(\boldsymbol{Y}) = Y_1 \ldots Y_m \prod_{1 \le i < j \le m} (Y_i - Y_j) \,.$$

On the other hand, it follows from Lemma 5 that if S' denotes the set of the coefficient vectors of the linear factors of G then $\pm S'$ has the Dantzig property. Thus it is easy to show that $D_G = 1$, i.e. that in (5) equality occurs.

There remains the case when F has linear factors both with rational and with non-rational coefficients. We recall that $D_0 = 1$, $r_0 = \binom{m+1}{2}$, $m_i = m$ for $i = 0, \ldots, t$ and

$$r_i = \frac{m_i}{\log 3} \cdot \log D_i \quad \text{for } i = 1, \ldots, t \,. \tag{13}$$

By Lemma 2 of [3], $D_i^{m_i}$ is divisible by $D_{K_i/\mathbb{Q}}^2$ in $\mathbb{Z}$ where $D_{K_i/\mathbb{Q}}$ denotes the discriminant of $K_i/\mathbb{Q}$ for $i = 1, \ldots, t$. This gives

$$2 \log |D_{K_i/\mathbb{Q}}| \le m_i \log D_i \quad \text{for } i = 1, \ldots, t \,. \tag{14}$$

On the other hand, for $r_i \ge 3$ we have (cf. [5], p. 130)

$$r_i = [K_i : \mathbb{Q}] \le \log |D_{K_i/\mathbb{Q}}| \tag{15}$$

and hence, by (14) and (15),

$$2r_i \le m_i \log D_i \,.$$

But this contradicts (13). Thus we have $r_i = 2$ for $i = 1, \ldots, t$. This implies that $m_i = 2$ for $i = 1, \ldots, t$ and so $m = 2$. In other words, F is a binary form with relatively prime coefficients in $\mathbb{Z}$. By the result of [5], quoted in Section 2, F is integrally equivalent to the binary form

$$G(Y_1, Y_2) = Y_1 Y_2 (Y_1 - Y_2)(Y_1^2 + Y_1 Y_2 + Y_2^2).$$

It is easy to see that G has discriminant $D_G = 3$ and, for G, equality occurs in (5). This completes the proof of the Theorem. ∎

Acknowledgements. I would like to thank Professors V. T. Sós and P. Hajnal for their useful remarks and Professor L. Lovász for calling my attention to the paper [6] of Heller.

Added in proof (April 1994). Some results of Heller [6] were earlier obtained by A. Korkine and G. Zolotarev (Math. Ann. 11 (1877), 242–292).

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1967.

[2] J. H. Evertse and K. Győry, *Effective finiteness theorems for decomposable forms of given discriminant*, Acta Arith. 60 (1992), 233–277.

[3] —, —, *Discriminants of decomposable forms*, in: Analytic and Probabilistic Methods in Number Theory, F. Schweiger and E. Manstavičius (eds.), VSP Int. Science Publ., Zeist, 1992, 39–56.

[4] I. M. Gelfand, A. V. Zelevinsky and M. M. Karpanov, *On discriminants of polynomials of several variables*, Funktsional. Anal. i Prilozhen. 24 (1990), 1–4 (in Russian).

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

[6] I. Heller, *On linear systems with integral valued solutions*, Pacific J. Math. 7 (1957), 1351–1364.

Corrections to [3]

P. 53, line 7: for "$\Omega(\mathcal{L}_0)$", "$\Omega(\mathcal{L}_{m+1})$", "$\Omega(\mathcal{L}_r)$" read "$\Omega(\mathfrak{D}(\mathcal{L}_0))$", "$\Omega(\mathfrak{D}(\mathcal{L}_{m+1}))$"; "$\Omega(\mathfrak{D}(\mathcal{L}_r))$", respectively.
lines 7 and 9: for "$\Omega(\mathfrak{D})$" read "$\frac{1}{2}\Omega(\mathfrak{D})$";
line 10: for "Theorem 2" read "Theorem 4".

INSTITUTE OF MATHEMATICS
LAJOS KOSSUTH UNIVERSITY
H-4010 DEBRECEN, HUNGARY

Received on 30.8.1993 (2476)