

# On definite quadratic forms, which are not the sum of two definite or semi-definite forms.

By

Paul Erdős and Chao Ko (Manchester).

Let

$$f_n = \sum_{i,j=1}^n a_{ij} x_i x_j \quad (a_{ij} = a_{ji})$$

be a positive definite quadratic form with determinant  $D_n$  and integer coefficients  $a_{ij}$ . Call it an even form if all  $a_{ij}$  are even, an odd form if at least one  $a_{ij}$  is odd. Then  $f_n$  is called non-decomposable, if it cannot be expressed as a sum of two non-negative quadratic forms with integer coefficients.

Mordell<sup>1)</sup> proved that  $f_2$  can always be decomposed into a sum of five squares of linear forms with integer coefficients. Ko<sup>2)</sup> proved that  $f_n$  can be expressed as a sum of  $n+3$  integral linear squares, when  $n=3, 4, 5$ .

When  $n=6$ , Mordell<sup>3)</sup> proved that the form

$$(1) \quad \sum_{i=1}^6 x_i^2 + \left( \sum_{i=1}^6 x_i \right)^2 - 2x_1 x_2 - 2x_2 x_3$$

of determinant 3 is non-decomposable; and Ko<sup>4)</sup> proved that (1) is the only non-decomposable form in six variables.

<sup>1)</sup> Mordell, Quart. J. of Math. (Oxford) 1 (1930), 276—88.

<sup>2)</sup> Ko, Quart. J. of Math. (Oxford), 8 (1937), 81—98.

<sup>3)</sup> Mordell, Annals of Math. 38 (1937), 751—757.

<sup>4)</sup> May appear in Acta Arithmetica.

When  $n = 7, 8$ , Mordell<sup>3)</sup> proved that the forms

$$\sum_{i=1}^n x_i^2 + \left( \sum_{i=1}^n x_i \right)^2 - 2x_1 x_2 - 2x_2 x_3 \quad (n = 7, 8)$$

with determinant  $D_7 = 2, D_8 = 1$  are non-decomposable.

In the present paper, we shall prove the following theorems:

**THEOREM 1.** *When  $D_n = 1$ , there exists an odd non-decomposable form, if  $n \geq 12$ , except possibly for 13, 16, 17, 19, 23; and an even non-decomposable form for all  $n \equiv 0 \pmod{8}$ .*

Hitherto the only method known for finding forms with  $D_n = 1$  for  $n > 8$  was that due to Minkowski<sup>4)</sup>.

**THEOREM 2.** *For every  $k > 0$  and  $n > 13k + 176$ , there exists a non-decomposable form in  $n$  variables with  $D_n = k$ .*

**THEOREM 3.** *There exist non-decomposable forms for every  $n > 5$ .*

From theorem 1, we can deduce that the class number  $h_n$  of positive definite quadratic forms with  $D_n = 1$  is greater than  $2^{1/n}$  for large  $n$ . But Magnus<sup>5)</sup> proved that the mass of the principal genus is greater than  $n^{n^2(1-\varepsilon)/4}$  for  $n > n_0$ , where  $\varepsilon = \varepsilon(n_0)$  is a small positive number, and so, as Dr. Mahler points out, it follows that  $h_n > n^{n^2(1-\varepsilon)/4}$  for  $n > n_0$ .

Any quadratic form can be reduced by a unimodular transformation, i. e. integer coefficients and determinant unity, to the form

$$\sum_{i=1}^n a_i x_i^2 + 2 \sum_{i=1}^{n-1} b_i x_i x_{i+1}.$$

This and its determinant may be denoted by

$$\begin{pmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ b_1 & b_2 & \dots & b_{n-1} & \end{pmatrix} \text{ and } \begin{vmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ b_1 & b_2 & \dots & b_{n-1} & \end{vmatrix}$$

respectively. If, however, say  $a_2 = a_3 = \dots = a_n = c$  and  $b_2 = b_3 = \dots = b_{n-1} = d$ , we may write  $\begin{pmatrix} a_1 & c_{(n-1)} \\ b_1 & d_{(n-2)} \end{pmatrix}$  with obviously similar extensions.

### 1. Some lemmas.

**LEMMA 1.** *The determinant of order  $n$*

<sup>3)</sup> Gesammelte Abhandlungen von H. Minkowski, 1, (1909), 77.

<sup>5)</sup> Magnus, Math. Annalen, 114 (1937), 465—475.

$$d_n = \left| \begin{matrix} 2_{(n)} \\ 1_{(n-1)} \end{matrix} \right| = n + 1.$$

It is evident that  $d_1 = 2$  and  $d_2 = 3$ . Suppose now  $d_m = m + 1$  for all  $m < n$ , then

$$d_n = 2d_{n-1} - d_{n-2} = 2n - (n - 1) = n + 1.$$

LEMMA 2. *The only squares which can be subtracted from the form*

$$f(x) = 2 \sum_{i=1}^n x_i + 2 \sum_{i=1}^{n-1} x_i x_{i+1} \quad (n > 3),$$

so that the remaining form is non-negative, are  $x_i^2$ ,  $(x_i + x_{i+1})^2$  ( $i = 1, \dots, n-1$ ), and  $x_n^2$ .

Since we can write

$$f(x) = x_1^2 + \sum_{i=1}^{n-1} (x_i + x_{i+1})^2 + x_n^2,$$

the unimodular transformation

$$x_i = y_i, \quad x_i + x_{i+1} = (-1)^{i-1} y_{i+1}, \quad (i = 1, \dots, n-1)$$

carries  $f(x)$  into

$$f(y) = \sum_{i=1}^n y_i^2 + \left( \sum_{i=1}^n y_i \right)^2.$$

If 
$$F(y) = f(y) - (L(y))^2, \quad L(y) = \sum_{i=1}^n a_i y_i$$

is non-negative, then it is evident that  $a_i$  can be only  $\pm 1$  or 0 since

$$F(0, \dots, 0, 1, 0, \dots, 0) = 2 - a_i^2 \geq 0.$$

I. Suppose first that one of the  $a_i$ 's is zero, say  $a_n = 0$ . Without loss of generality, we can assume that  $a_1 = \pm 1$ . Then

$$F(a_1, a_2, \dots, a_{n-1}, -a_1) = 2 + \sum_{i=2}^{n-1} a_i^2 + \left( \sum_{i=2}^{n-1} a_i \right)^2 - \left( 1 + \sum_{i=2}^{n-1} a_i^2 \right)^2$$

$$\leq 1 - \sum_{i=2}^{n-1} a_i^2 < 0,$$

if at least two of the  $a_2, \dots, a_{n-1}$  are not zero. Hence we need only consider either  $a_2 = \dots = a_{n-1} = 0$ , and then  $L(y) = y_1$ , or only one of these  $a$ 's does not vanish, say  $a_2 \neq 0$ . But then  $F(y)$  is indefinite, since as  $n > 3$ ,

$$F(2a_2, 2a_2, -a_2, -a_2, 0, \dots, 0) = 2^2 + 2^2 + 1 + 1 + 2^2 - 4^2 < 0.$$

II. Suppose next that none of the  $a$ 's are zero. If two of them have different signs, say  $a_1 = -a_2$ , then

$$F(a_1, a_2, \dots, a_n) = n + \left( \sum_{i=3}^n a_i \right)^2 - n^2 \leq (n-2)^2 + n - n^2 < 0.$$

From I, and II, it follows that  $F(y)$  is non-negative, if and only if  $L(y) = y_i$  ( $i = 1, \dots, n$ ), or  $\sum_{i=1}^n y_i$ . This clearly proves the lemma.

LEMMA 3. *The form*

$$f(x) = \alpha x_1^2 + 2\beta x_1 x_2 + 2 \sum_{i=2}^n x_i^2 + 2 \sum_{i=2}^{n-1} x_i x_{i+1}$$

with determinant  $D_n < n$ , where  $\alpha > 0$ ,  $\beta \geq 0$  are integers satisfying the conditions:

$$\beta^2 > \alpha > (1 - 1/n)\beta^2, \quad 2\beta \leq n,$$

is positive definite and non-decomposable.

By lemma 1,  $f(x)$  is positive definite, since its determinant is

$$D_n = n\alpha - (n-1)\beta^2 > 0,$$

and clearly all its principal minors are positive.

First, we shall show that nondecomposition of  $f(x)$  involving a linear square exists. As in lemma 2, we can transform  $f(x)$  into

$$f(y) = \alpha y_1^2 + 2\beta y_1 y_2 + \sum_{i=2}^n y_i^2 + \left( \sum_{i=2}^n y_i \right)^2.$$

By lemma 2, it follows that the only squares which need be considered are

(1)  $(a_1 y_1)^2$ ,  $a_1 \neq 0$ , (2)  $(a_1 y_1 + y_2)^2$ , (3)  $(a_1 y_1 + y_l)^2$  ( $l = 3, \dots, n$ ) and

(4)  $(a_1 y_1 + \sum_{i=2}^n y_i)^2$ .

The case (1) is ruled out, since  $D_n - n a_1^2 < 0$ . For the cases (3) and (4), we need consider only the square  $(a_1 y_1 + y_n)^2$ , since  $f(y)$  is symmetrical in  $y_2, \dots, y_n$ , and the transformation

$$T: \quad y_2 \rightarrow -\sum_{i=2}^n y_i \quad y_j \rightarrow y_j \quad (j = 1, 2, 4, 5, \dots, n)$$

permutes  $y_2^2$  and  $(\sum_{i=2}^n y_i)^2$ .

Consider first the form

$$\begin{aligned} F_2 &= f(y) - (a_1 y_1 + y_2)^2 \\ &= (a - a_1^2) y_1^2 + 2(\beta - a_1) y_1 y_2 + \sum_{i=3}^n y_i^2 + (\sum_{i=2}^n y_i)^2. \end{aligned}$$

The transformation

$$y_2 \rightarrow -\sum_{i=1}^n y_i \quad y_j \rightarrow y_j \quad (j = 1, 3, 4, \dots, n)$$

carries  $F_2$  into

$$\begin{aligned} F_2' &= (a - a_1^2) y_1^2 - 2(\beta - a_1) y_1 (\sum_{i=2}^n y_i) + \sum_{i=2}^n y_i^2 \\ &= \sum_{i=2}^n (y_i - (\beta - a_1) y_1)^2 + (a - a_1^2 - (n-1)(\beta - a_1)^2) y_1^2. \end{aligned}$$

The maximum of the coefficients of  $y_1^2$

$$A = a - a_1^2 - (n-1)(\beta - a_1)^2$$

for different  $a_1$  occurs when  $a_1 = (n-1)\beta/n$ . Since  $0 < \beta/n < 1$ , we have for  $a_1 = \beta$ ,  $\beta - 1$ , respectively,

$$A = \alpha - \beta^2 < 0 \quad \text{and} \quad A = \alpha - \beta^2 + 2\beta - n < 0,$$

so that  $F_2'$  is indefinite. This settles the case (2).

Consider next the form

$$\begin{aligned} F_3 &= f(y) - (a_1 y_1 + y_3)^2 \\ &= (\alpha - a_1^2) y_1^2 + 2\beta y_1 y_3 + y_3^2 + \sum_{i=2}^n y_i^2 + \left( \sum_{i=2}^n y_i \right)^2 - 2a_1 y_1 y_3. \end{aligned}$$

The transformation  $T$  carries  $F_3$  into

$$\begin{aligned} F_3' &= (\alpha - a_1^2) y_1^2 + 2\beta y_1 y_3 + 2a_1 y_1 \left( \sum_{i=2}^n y_i \right) + \sum_{i=2}^n y_i^2 \\ &= \sum_{i=3}^n (y_i + a_1 y_1)^2 + (y_3 + \beta + a_1) y_1^2 + (\alpha - a_1^2 - (\beta + a_1)^2 - (n-2)a_1^2) y_1^2. \end{aligned}$$

The maximum value of the coefficient of  $y_1^2$

$$A' = \alpha - a_1^2 - (\beta + a_1)^2 - (n-2)a_1^2$$

is reached when  $a_1 = -\beta/n$ . Since  $-1 < -\beta/n < 0$ , we have, for  $a_1 = 0, -1$ , respectively,

$$A' = \alpha - \beta^2 < 0 \quad \text{and} \quad A' = \alpha - \beta^2 + 2\beta - n < 0,$$

$F_3$  is indefinite and cases (3) and (4) are also settled.

Suppose now there is a decomposition

$$f(x) = f'(x) + f''(x).$$

No term  $x_i^2$  ( $i \geq 2$ ) can occur in either  $f'(x)$  or  $f''(x)$  for then a square can be taken out of  $f(x)$ . Hence we can assume  $f'(x)$ , say, has a term  $2x_n^2$ . Then  $f''(x)$  must also contain  $2x_{n-1}x_n$ , for otherwise  $f''(x)$  assumes negative values by choice of  $x_n$ . Then  $f'(x)$  contains also  $2x_{n-1}^2$ , for otherwise  $f'(x)$  will assume negative values by choice of  $x_{n-1}$ . Proceeding in this way,  $f'(x)$  will contain all the terms of  $f(x)$  involving  $x_n, x_{n-1}, \dots, x_2$ . Hence  $f''(x) = \alpha x_1^2$ , and so a square  $x_1^2$  can be taken out from  $f(x)$ , which contradicts what we have proved.

LEMMA 4. *If  $n \neq 2^a$ ,  $p^a$ ,  $2p^a$ , where  $p$  is an odd prime and  $a$  is a positive integer, then there exists an odd non-decomposable form in  $n$  variables with determinant unity.*

Consider the form

$$f_n = \begin{pmatrix} x & 2_{(n-1)} \\ y & 1_{(n-2)} \end{pmatrix}$$

in  $n$  variables. It is easy to calculate by using lemma 1 that its determinant has the value

$$D_n = nx - (n-1)y^2.$$

Putting  $D_n = 1$ , we have to solve the congruence

$$(2) \quad y^2 \equiv 1 \pmod{n}.$$

Since  $n \neq 2^a$ ,  $p^a$ ,  $2p^a$ , we can write

$$n = a \cdot b, \quad (a, b) = 1, \quad a > 2, \quad \text{and} \quad b > 2.$$

Suppose  $y_1, y_2$  are the solutions of the congruences:

$$y_1 \equiv -1 \pmod{a}, \quad y_1 \equiv 1 \pmod{b}, \quad 0 < y_1 < n;$$

$$y_2 \equiv 1 \pmod{a}, \quad y_2 \equiv -1 \pmod{b}, \quad 0 < y_2 < n.$$

Both  $y_1$  and  $y_2$  satisfy the congruence (2) and since

$$y_1 + y_2 \equiv 0 \pmod{n}, \quad 0 < y_1 < n, \quad 0 < y_2 < n,$$

we have

$$y_1 + y_2 = n.$$

Hence one of the  $y_1, y_2$  is less than  $\frac{1}{2}n$  and we take this value to be our  $y$ , which satisfies the inequality  $2y < n$ .

From  $D_n = 1$ , we can obtain the inequalities  $y^2 > x > (1 - 1/n)y^2$ . Hence the form  $f_n$  satisfies all the conditions of lemma 3 and is non-decomposable.

$f_n$  is an odd form if  $x = ((n-1)y^2 + 1)/n$  is odd  $x$  is evidently odd if  $n$  is odd. If  $n$  is even, we write

$$x = y^2 - (y^2 - 1)/n.$$

Then  $y$  must be odd and from the congruences

$$y \equiv \pm 1 \pmod{a}, \quad y \equiv \mp 1 \pmod{b}, \quad (a, b) = 1, \quad ab = n,$$

it is clear that if  $a$  is even, then  $b$  is odd,  $y \pm 1$  is even and so  $(y^2 - 1)/n$  is even and so  $x$  is odd.





$$(-D_{4m-2}/D'_{4m-1}) = 1,$$

the symbol being that of quadratic residuacity. Since  $-D_{4m-2} \equiv 1 \pmod{4}$ , and  $D_{4m-2} \equiv -1 \pmod{8}$ , when  $t_{4m-1} > 0$ , we have

$$1 = (D'_{4m-1}/D_{4m-2}) = (D_{4m-1}/D_{4m-2}).$$

From the relation  $D_{4m-1} = a_{4m-1}D_{4m-2} - D_{4m-3}b_{4m-2}^2$  of (3),

$$\begin{aligned} 1 &= (-D_{4m-3}/D_{4m-2}) \\ &= (2^{4m-3}/D_{4m-2}) \cdot (-1)^{\frac{1}{2}(D'_{4m-3}+1)} (D_{4m-2}/D'_{4m-3}) \\ &= (2^{4m-3}/D_{4m-2}) \cdot (-1)^{\frac{1}{2}(D'_{4m-3}+1)} (-D_{4m-4}/D'_{4m-3}), \end{aligned}$$

since again from (3),  $D_{4m-2} = 4a_{4m-2}D_{4m-3} - D_{4m-4}b_{4m-3}^2$ . Hence

$$\begin{aligned} 1 &= (2^{4m-3}/D_{4m-2}) \cdot (-1)^{\frac{1}{2}(D'_{4m-3}+1)} + \frac{1}{2}(D'_{4m-3}-1) (D'_{4m-3}/D_{4m-4}) \\ &= -(2^{4m-3}/D_{4m-2}) (2^{4m-3}/D_{4m-4}) (D_{4m-3}/D_{4m-4}). \end{aligned}$$

From the relation  $4a_{4m-2}D_{4m-3} - D_{4m-4}b_{4m-3}^2 = D_{4m-2}$ , we have, when  $t_{4m-3} > 0$ , since  $b_{4m-3}$  is odd,  $D_{4m-2} + D_{4m-4} \equiv 0 \pmod{8}$ . Hence

$$\begin{aligned} (2/D_{4m-2}) &= (2/D_{4m-4}) \text{ and so} \\ (2^{4m-3}/D_{4m-2}) (2^{4m-3}/D_{4m-4}) &= 1. \end{aligned}$$

Hence

$$1 = -(D_{4m-3}/D_{4m-4}),$$

or

$$(D_{4m-3}/D_{4m-4}) = -1.$$

Continuing this process, we get

$$(D_{4m-8i-3}/D_{4m-8i-4}) = -1.$$

Hence

$$D_{4m-8i-4} \neq 1,$$

and so  $4m - 8i - 4 \neq 0$ , or  $n$  is divisible by 8.

LEMMA 7. *The positive definite forms:*

$$\begin{aligned} f_{8m-1} &= \begin{pmatrix} 8m & 2m & 2_{(8m-3)} \\ & 4m-1 & 1_{(8m-3)} \\ & & 2_{(8m-4)} \end{pmatrix}, \\ f_{8m-2} &= \begin{pmatrix} 8m & 2m & 2_{(8m-4)} \\ & 4m-1 & 1_{(8m-4)} \\ & & 1_{(8m-4)} \end{pmatrix}, \end{aligned}$$

In  $8m-1$  and  $8m-2$  variables with determinants 2 and 3, respectively, are non-decomposable.

Let us first consider the form  $f_{8m-2}$ . From the argument used in the last part of the proof of lemma 5, it suffices to prove that no square can be subtracted from  $f_{8m-2}$ . Suppose  $f_{8m-2} - L^2$  is a non-negative quadratic form with integer coefficients, where  $L$  is a linear form in  $x_1, \dots, x_{8m-2}$  with integer coefficients having no common factor. By an unimodular transformation, we can write  $L = x_1$ , and then

$$f_{8m-2} \sim f'_{8m-2} = \sum_{i,j=1}^{8m-2} a_{ij} x_i x_j \quad (a_{ij} = a_{ji}),$$

where  $f'_{8m-2} - x_1^2$  is a non-negative form. Let the cofactor of  $a_{11}$  in the determinant of  $f'_{8m-2}$  be  $A_{21}$ ; then the determinant of  $f'_{8m-2} - x_1^2$  is  $3 - A_{11}$  and is not negative. Since the adjoint form of an even form in an even number of variables is even<sup>5</sup>),  $A_{21} = 2$ . Consider now the positive even definite form

$$f_{8m+4} = 8x_1^2 + 6x_1 x_2 + 2 \sum_{i=2}^6 x_i^2 + 2 \sum_{i=2}^6 x_i x_{i+1} + \sum_{i,j=1}^{8m-2} a_{ij} x_{i+6} x_{j+6}$$

in  $8m+4$  variables. On bearing in mind the method of lemma 1, the lower right corner, say 1. r. c.,  $(8m-1)$ -rowed minor of the determinant of  $f_{8m+4}$  has the value  $2 \cdot 3 - 2 = 4$ ; the 1. r. c.  $8m$ -rowed minor is  $2 \cdot 4 - 3 = 5$ , the 1 c. r.  $(8m+1)$ -rowed minor is  $2 \cdot 5 - 4 = 6$ , the 1 r. c.  $(8m+2)$ -rowed minor is  $2 \cdot 6 - 5 = 7$ , the 1. r. c.  $(8m+3)$ -rowed minor is  $2 \cdot 7 - 6 = 8$  and so the determinant of  $f_{8m+4}$  is  $8 \cdot 8 - 3^2 \cdot 7 = 1$ , which contradicts lemma 6.

Next we prove that no square can be taken out from  $f_{8m-1}$  and hence  $f_{8m-1}$  is non-decomposable. If  $f_{8m-1} - L^2$  is non-negative, then  $L$  cannot contain a term involving  $x_i$  ( $1 \leq i \leq 8m-2$ ), for otherwise, by putting  $x_{8m-1} = 0$ , we would get a decomposition of  $f_{8m-2}$ . Hence  $L = x_{8m-1}$ . But  $f_{8m-1} - x_{8m-1}^2$  is indefinite, since the determinant of  $f_{8m-1} - x_{8m-1}^2$  is  $2 - 3 < 0$ . This completes the proof.

LEMMA 8. Let the positive definite quadratic forms:

$$g_1 = f_m(x_1, \dots, x_m), \quad g_2 = f_{n-m-1}(x_{m+2}, \dots, x_n), \\ g_3 = bx_{m+1}^2 + 2x_{m+1}x_{m+2} + g_2$$

having determinants  $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$ , respectively, be non-decomposable. Denote

<sup>5</sup>) Bachmann, Zahlentheorie, vol. 4, part 1, 444.

by  $A$  the value of the upper left-hand corner principal  $(m-1)$ -rowed minor of  $\mathcal{D}_1$ . If there exists a positive definite quadratic form of determinant  $\mathcal{D} < \mathcal{D}_1 \mathcal{D}_2$ .

$$g = g_1 + ax_{m+1}^2 + 2x_m x_{m+1} + g_3,$$

where  $a$  is an integer and  $0 < a < A/\mathcal{D}_1$ , then  $g$  is non-decomposable.

Suppose  $g$  has a decomposition

$$(4) \quad g = h + h'.$$

If one of the  $h$ 's has a term involving  $x_i$  ( $i = 1, \dots, m$ ), it will contain all the terms of  $g_1$ , for otherwise we would get a decomposition of  $g_1$  by putting  $x_{m+1} = \dots = x_n = 0$ . Similarly, if one of the  $h$ 's, say  $h$ , has a term involving  $x_i$  ( $i = m+2, \dots, n$ ), it contains all the terms of  $g_2$ . Then  $h$  must contain the term  $2x_{m+1} x_{m+2}$ , for otherwise,  $h'$  will assume negative values by choice of  $x_{m+2}$ . Then  $h$  contains also a term  $b'x_{m+1}^2$  with  $b' > 0$ , for otherwise,  $h$  will assume negative values by choice of  $x_{m+1}$ . Next  $b' \geq b$ , for if  $b' < b$ , on putting  $x_1 = \dots = x_m = 0$ ,

$$h = g_2 + 2x_{m+1}x_{m+2} + b'x_{m+1}^2.$$

This is indefinite, since  $g_2$  is non-decomposable. Hence  $h$  contains  $g_2$ . Hence we may suppose that either  $h$  contains both  $g_1$  and  $g_2$ , or  $h$  contains  $g_1$  and  $h'$  contains  $g_2$ .

In the first case,  $h'$  can only contain the terms or part of the terms of  $g - (g_1 + g_2) = ax_{m+1}^2 + 2x_m x_{m+1}$ . Then  $h' = cx_{m+1}^2$  with  $0 < c \leq a$ , since if  $h'$  contains the  $2x_m x_{m+1}$ ,  $h'$  will assume negative values by choice of  $x_m$ . Hence

$$h = g - cx_{m+1}^2.$$

Since the cofactor of the coefficients of  $x_{m+1}^2$  in the determinant  $\mathcal{D}$  of  $g$  is  $\mathcal{D}_1 \mathcal{D}_2$ , the determinant of  $h$  is  $\mathcal{D} - c \mathcal{D}_1 \mathcal{D}_2$ . By hypothesis,  $\mathcal{D} - \mathcal{D}_1 \mathcal{D}_2 < 0$ ,  $h$  is indefinite.

In the second case,  $h$  must contain the term  $2x_m x_{m+1}$ , for otherwise  $h'$  will assume negative values by choice of  $x_m$ . Then  $h$  contains also a term  $c'x_{m+1}^2$ ,  $c' > 0$ , for otherwise  $h$  will assume negative values by choice of  $x_{m+1}$ . Also

$$h = g_1 + 2x_m x_{m+1} + c'x_{m+1}^2, \quad h' = g_3 + dx_{m+1}^2,$$

since  $h'$  contains  $g_3$ . Hence  $a = c + d$  and so  $c \leq a$  for  $d$  cannot be negative, as  $g_3$  is indecomposable. It is easy to see that the determinant of  $h$  is  $c' \mathcal{D}_1 - A$ . By hypothesis,  $c' \mathcal{D}_1 \leq a \mathcal{D}_1 \leq A$ , and so  $h$  is indefinite. Hence (4) is impossible and the lemma is proved.



$$g_1 = \begin{pmatrix} a_1 & \cdots & a_{n_2-2} & a_{n_2-1} \\ b_1 & \cdots & b_{n_2-2} & \end{pmatrix}, \quad \mathcal{D}_1 = 2, \quad A = 3,$$

$$g_2 = \begin{pmatrix} 2(n_2-4) & 2 & x \\ 1(n_2-4) & y & \end{pmatrix}, \quad a = 1, \quad g_3 = \begin{pmatrix} 2(n_2-3) & 2 & x \\ 1(n_2-3) & y & \end{pmatrix},$$

$$\mathcal{D}_2 = \begin{vmatrix} 2(n_2-4) & 2 & x \\ 1(n_2-4) & y & \end{vmatrix}, \quad \mathcal{D}_3 = \begin{vmatrix} 2(n_2-3) & 2 & x \\ 1(n_2-3) & y & \end{vmatrix};$$

$f_n$  is non-decomposable if  $g_2, g_3$  are non-decomposable. From lemma 3, we need only show that

$$(8) \quad x < y^2,$$

$$(9) \quad 2y \leq n_2 - 2,$$

the determinant of order  $n_2 - 2$ ,

$$(10) \quad \mathcal{D}_2 < n_2 - 2,$$

and the determinant of order  $n_2 - 1$

$$(11) \quad \mathcal{D}_3 < n_2 - 1.$$

By lemma 1 and (7),

$$(12) \quad \begin{aligned} \mathcal{D}_2 &= (n_2 - 2)x - (n_2 - 3)y^2 = 1 - 2x + 2y^2, \\ \mathcal{D}_3 &= (n_2 - 1)x - (n_2 - 2)y^2 = 1 - x + y^2. \end{aligned}$$

We now solve (7). Since  $n_2 \neq 4, p^\alpha, 2p^\alpha$ ,

$$Y^2 \equiv 1 \pmod{n_2}$$

has a solution  $Y$  satisfying the inequalities

$$(13) \quad 1 < Y < \frac{1}{2}n_2.$$

Then taking  $y = Y$  in (7), we have a solution  $(x, y)$ . Then (8) evidently holds, as from (7) and (13),

$$x = y^2 + (1 - y^2)/n_2 < y^2.$$

If  $n_2$  is even, (9) follows from (13). If  $n_2$  is odd, say  $n_2 = 2n_3 + 1, y \neq n_3$ , since  $n_3^2 \equiv 1 \pmod{2n_3 + 1}$  for  $n_3 \neq 3$ . Hence from (13),  $y \leq n_3 - 1$  and (9) holds again. Since from (12),  $\mathcal{D}_2 - \mathcal{D}_3 = y^2 - x > 0$ , (11) holds if (10) holds. From (7) and (9), we get

$$y^2 - x = (y^2 - 1)/n_2 < n_3/4.$$

Thus (10) follows if  $n_2 \geq 6$ , since

$$\mathcal{D}_2 = 1 + 2y^2 - 2x < 1 + n_2/2 \leq n_2 - 2$$

is true for  $n_2 \geq 6$ . But  $n_2 \neq 4, p^\alpha, 2p^\alpha$ , and so  $n_2 \geq 8$ , hence  $f_n$  is non-decomposable.

Now from lemma 4, we need only prove that if  $n = 2^k$ ,  $p^k$ , or  $2p^k$ , where  $n \geq 12$ ,  $n \neq 13, 16, 17, 19, 23$ , the equation

$$n + 2 = n_1 + n_2$$

is solvable with the conditions  $n_1 = 8m$  or  $a^n - 1$ ,  $n_2 \neq 4$ ,  $p^\alpha$ ,  $2p^\alpha$  and  $n_1 > 0$ ,  $n_2 > 0$ .

Small values for  $n_1 - 2$  are

$$6, 13, 14, 22, 30, 38 \text{ and } 46.$$

Suppose first that  $n \equiv 0 \pmod{4}$ . Then we need only consider  $n = 2^k$ .

If  $2^k \equiv 2 \pmod{3}$ , then we can take  $n_2 = 2^k - 14$  or  $2^k - 38$ , if  $n > 38$ , unless

$$2^k - 14 = 2 \cdot 3^\beta, \quad 2^k - 38 = 2 \cdot 3^\gamma.$$

They give  $3^\beta - 3^\gamma = 12$ , which is impossible. But if  $n \leq 38$ , we get the exceptional case  $n = 32$ .

If  $2^k \equiv 1 \pmod{3}$ , then we can take  $n_2 = 2^k - 22$  or  $2^k - 46$ , if  $n > 46$ , unless

$$2^k - 22 = 2 \cdot 3^\beta, \quad 2^k - 46 = 2 \cdot 3^\gamma.$$

They give also the impossible equation  $3^\beta - 3^\gamma = 12$  and we get the exceptional value  $n = 16$ .

Suppose next  $n \equiv 2 \pmod{4}$ , we can take  $n_2 = n - 6$ , unless  $n_2 = 4$ , i. e.  $n = 10$ .

Suppose finally  $n$  is odd and so  $n = p^k$ . If  $n \equiv 0 \pmod{3}$ , we can take  $n_2 = n - 6$  or  $n - 30$ , if  $n > 30$ , unless

$$n - 6 = 3^\beta, \quad n - 30 = 3^\gamma.$$

They give the equation  $3^\beta - 3^\gamma = 24$ , which has only the solutions  $\beta = 3$  leading to  $n = 33 \neq p^k$ . The only exceptional value  $n = p^k \leq 30$  is 27.

If  $n \equiv 2 \pmod{3}$ , we can take  $n_2 = n - 14$ , or  $n - 38$ , if  $n > 38$ , unless

$$n - 14 = 3^\beta, \quad n - 38 = 3^\gamma.$$

They give the equation  $3^\beta - 3^\gamma = 24$ , which has the only solution  $\beta = 3$  and this corresponds  $n = 41$ . The other exceptional values  $\leq 38$  are 17, 23, 29.

If  $n \equiv 1 \pmod{3}$ , we can take  $n_2 = n - 22$  or  $n - 13$ , if  $n > 22$ , unless

$$n - 22 = 3^{\beta}, \quad n - 13 = 3^{\gamma}.$$

They give the impossible equation  $3^{\gamma} - 3^{\beta} = 9$ , and so the exceptional values in this case are only 13, 19.

Hence the exceptional values are

$$n = 13, 16, 17, 19, 23, 27, 29, 32 \text{ and } 41.$$

Since

$$27 - 6 = 21, \quad 29 - 14 = 15, \quad 41 - 6 = 35,$$

and 21, 15, 35  $\neq$  4,  $p^{\alpha}$ ,  $2p^{\alpha}$ , we can rule out the cases 27, 29 and 41. Hence the only exceptional values are

$$n = 13, 16, 17, 19, 23 \text{ and } 32.$$

But 32 can be excluded from the last. Write

$$f_{31} = \begin{pmatrix} 35 & & & & \\ & 6 & & & \\ & & 2(30) & & \\ & & & 1(29) & \\ & & & & 2 & 5 \end{pmatrix}, \quad f_{32} = \begin{pmatrix} 35 & & & & \\ & 6 & & & \\ & & 2(29) & & \\ & & & 1(29) & \\ & & & & 2 & 5 \end{pmatrix}.$$

Then  $f_{31}$  has determinant  $5 = 35 \cdot 31 - 6^2 \cdot 30$ ,  $f_{32}$  has determinant  $1 = 5 \cdot 5 - 2^2(35 \cdot 30 - 6^2 \cdot 29)$ . By lemma 3, the form  $f_{31}$  is non-decomposable. If there exists a decomposition for  $f_{32}$ , say

$$f_{32} = h_{32} + h_{32}'$$

and one of the  $h$ 's, say  $h_{32}$  must vanish identically if we put  $x_{32} = 0$ , for otherwise, there would exist a decomposition for  $f_{31}$ . Hence  $h_{32}'$  contains only  $cx_{32}^2$  with  $c \geq 1$ . This is impossible, since

$$\begin{vmatrix} 35 & & & & \\ & 6 & & & \\ & & 2(29) & & \\ & & & 1(29) & \\ & & & & 2 & 5 - c \end{vmatrix} = 1 - 5c < 0.$$

Hence  $f_{32}$  is non-decomposable and our lemma is proved.

It should be remarked that for  $n = 8^9)$ , 9, 10, 11,  $13^{10)}$ , it is known that there exist no odd non-decomposable forms with determinant unity. It still remains to be investigated whether there exist odd non-decomposable forms when  $n = 16, 17, 19$  and 23 with determinant unity.

**LEMMA 10.** *For every odd integer  $n > 176$ , a non-decomposable form in  $n$  variables with determinant 2 exists such that the upper left-hand*

<sup>9)</sup> Mordell, *J. de Mathématiques*, 17 (1938), 41—46. Also see Ko, *Quart. J. of Math. (Oxford)*, 8 (1937) 85.

<sup>10)</sup> Ko, "On the positive definite quadratic forms with determinant unity", which may appear in *Acta Arithmetica*.

$(n-1)$ -rowed principal minor of its determinant is odd and greater than unity.

We prove first the existence of two such forms in  $16k+1$ ,  $22h+1$  variables respectively.

Consider first the form in  $16k+1$  variables:

$$(14) f_{16k+1} = \begin{pmatrix} 2^{(15)} & 2 & 34 & 10 & 2^{(14)} & 34 & 10 & 2^{(14)} \dots 34 & 10 & 2^{(14)} & 34 \\ 1^{(15)} & 6 & 1 & 1^{(14)} & 6 & 1 & 1^{(14)} \dots 6 & 1 & 1^{(14)} & 6 \end{pmatrix},$$

where the part  $\begin{pmatrix} 34 & 10 & 2^{(14)} \\ 1 & 1^{(14)} & 6 \end{pmatrix}$  occurs  $k-1$  times. Denote the upper left-hand  $i$ -rowed minor of its determinant by  $A_i$ . Then  $A_{16k+1}$  is the determinant of  $f_{16k+1}$ .

For  $k=1$ , the form in 17 variables

$$f_{17} = \begin{pmatrix} 2^{(15)} & 2 & 34 \\ 1^{(15)} & 6 & 6 \end{pmatrix}$$

is non-decomposable by lemma 3. By lemma 1,  $A_{15} = 16$ ,  $A_{16} = 17$ , and  $A_{17} = 34 \cdot 17 - 6^2 \cdot 16 = 2$ .

Suppose now that for  $k=m$ , in (14) the form  $f_{16m+1}$  is non-decomposable and  $A_{16m} = 17$ ,  $A_{16m+1} = 2$ . Take  $k=m+1$ , Then  $A_{16m+2} = 10 \cdot 2 - 17 = 3$ ,  $A_{16m+3} = 2 \cdot 3 - 2 = 4$ , and so step by step,  $A_{16m+16} = 17$ ,  $A_{16m+17} = 34 \cdot 17 - 6^2 \cdot 16 = 2$ .

From lemma 8, on taking

$$g_1 = f_{16m+1}, \quad \mathcal{D}_1 = 2, \quad A = 17,$$

$$g_2 = \begin{pmatrix} 2^{(13)} & 2 & 34 \\ 1^{(13)} & 6 & 6 \end{pmatrix}, \quad \mathcal{D}_2 = 34 \cdot 15 - 6^2 \cdot 14 = 6,$$

$$g_3 = \begin{pmatrix} 2^{(14)} & 2 & 34 \\ 1^{(14)} & 6 & 6 \end{pmatrix}, \quad \mathcal{D}_3 = 34 \cdot 16 - 6^2 \cdot 15 = 4,$$

and  $a=8$ , then  $g = f_{16m+17}$  is non-decomposable, since from lemma 3,  $g_2, g_3$  are non-decomposable. Hence  $f_{16k+1}$  is non-decomposable for any  $k > 0$ .

Consider next the form in  $22h+1$  variables

$$(15) f'_{22h+1} = \begin{pmatrix} 2^{(21)} & 2 & 24 & 13 & 2^{(20)} & 24 & 13 & 2^{(20)} \dots 24 & 13 & 2^{(20)} & 24 \\ 1^{(21)} & 5 & 1 & 1^{(20)} & 5 & 1 & 1^{(20)} \dots 5 & 1 & 1^{(20)} & 5 \end{pmatrix}$$

the part  $\begin{pmatrix} 24 & 13 & 2^{(20)} \\ 1 & 1^{(20)} & 5 \end{pmatrix}$  occurring  $h-1$  times. Denote the minors corresponding to the  $A_i$ 's above by  $A'_i$ .







Since  $6 \equiv -2$ ,  $7 \equiv -1$ ,  $23 \equiv -1 \pmod{8}$ , by lemma 7, we have a non-decomposable form for  $n = 6, 7^{11}$ , and 23. For  $n = 9, 10, 11, 13, 17, 19$ , we have that by lemma 3 the forms

$$\begin{pmatrix} 15 & 2_{(i)} \\ 4 & 1_{(i)} \end{pmatrix} \quad (i+1 = 9, 10, 11, 13);$$

$$\begin{pmatrix} 24 & 2_{(i)} \\ 5 & 1_{(i)} \end{pmatrix} \quad (i+1 = 17, 19)$$

are non-decomposable.

In closing, we should like to thank Prof. Mordell for suggesting shorter proofs of lemmas 2, 3 and for his kind help with the manuscript.

(Received 28 March, 1938.)

<sup>11)</sup> These are the same forms given by Prof. Mordell. See footnote 3).