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

By

Paul Erdös and Chao Ko (Manchester).

Let

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

be a positive definite quadratic form with determinant D_n and integer coefficients a_{ij}. Call it an even form if all a_{ii} are even, an odd form if at least one a_{ii} 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 [1]) proved that f_2 can always be decomposed into a sum of five squares of linear forms with integer coefficients. Ko [2]) 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 [3]) proved that the form

$$(1) \qquad \sum_{i=1}^{6} x_i^2 + \Big(\sum_{i=1}^{6} x_i\Big)^2 - 2x_1 x_2 - 2x_2 x_3$$

of determinant 3 is non-decomposable; and Ko [4]) proved that (1) is the only non-decomposable form in six variables.

[1]) Mordell, Quart. J. of Math. (Oxford) 1 (1930), 276—88.

[2]) Ko, Quart. J. of Math. (Oxford), 8 (1937), 81—98.

[3]) Mordell, Annals of Math. 38 (1937), 751—757.

[4]) May appear in Acta Arithmetica.

When $n = 7, 8$, Mordell [3]) proved that the forms

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

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 $n \geqslant 12$, 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 [5]).

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 $2^{\sqrt{n}}$ for large n But Magnus [6]) 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

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

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*

[5]) Gesammelte Abhandlungen von H. Minkowski, 1, (1909), 77.

[6]) Magnus, Math. Annalen, 114 (1937), 465—475.

$$d_n = \begin{vmatrix} 2_{(n)} & \\ & 1_{(n-1)} \end{vmatrix} = n + 1.$$

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*

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

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

$$x_1 = y_1,\ x_i + x_{i+1} = (-1)^{i-1} y_{i+1}, \qquad (i = 1, \ldots, n-1)$$

carries $f(x)$ into

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

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

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

$$F(0, \ldots, 0, 1, 0, \ldots, 0) = 2 - a_i^2 \geqslant 0.$$

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

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

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

if at least two of the $a_2, \ldots, a_{n-1}$ are not zero. Hence we need only consider either $a_2 = \ldots = a_{n-1} = 0$, 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 $n > 3$,

$$F(2a_1, 2a_2, -a_1, -a_2, 0, \ldots, 0) = 2^2 + 2^2 + 1 + 1 + 2^2 - 4^2 < 0.$$

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

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

From I, and II, it follows that $F(y)$ is non-negative, if and only if $L(y) = y_i$ $(i = 1, \ldots, n)$, 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:*

$$\beta^2 > \alpha > (1 - 1/n)\beta^2, \qquad 2\beta \leqslant n,$$

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

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

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) $(a_1 y_1 + y_i)^2$ $(i = 3, \dots, n)$ and (4) $(a_1 y_1 + \sum_{i=2}^{n} y_i)^2$.

The case (1) is ruled out, since $D_n - na_1^2 < 0$. For the cases (3) and (4), we need consider only the square $(a_1 y_1 + y_3)^2$, since $f(y)$ is symmetrical in $y_3, \dots, y_n$, and the transformation

$$T: \qquad y_3 \to -\sum_{i=2}^{n} y_i \quad y_j \to y_j \quad (j = 1,2,4,5, \dots, n)$$

permutes y_3^2 and $(\sum_{i=2}^{n} y_i)^2$.

Consider first the form

$$F_2 = f(y) - (a_1 y_1 + y_2)^2$$

$$= (\alpha - a_1^2)\, y_1^2 + 2\,(\beta - a_1) y_1 y_2 + \sum_{i=3}^{n} y_i^2 + (\sum_{i=2}^{n} y_i)^2.$$

The transformation

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

carries F_2 into

$$F_2' = (\alpha - a_1^2) y_1^2 - 2(\beta - a_1)\; y_1 (\sum_{i=2}^{n} y_i) + \sum_{i=2}^{n} y_i^2$$

$$= \sum_{i=2}^{n} (y_i - (\beta - a_1)\, y_1)^2 + (\alpha - a_1^2 - (n-1)(\beta - a_1)^2) y_1^2.$$

The maximum of the coefficients of y_1^2

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

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

$$F_3 = f\,(y) - (a_1\, y_1 + y_3)^2$$

$$= (\alpha - a_1^2)\, y_1^2 + 2\beta y_1 y_2 + y_2^2 + \sum_{i=4}^{n} y_i^2 + (\sum_{i=2}^{n} y_i)^2 - 2a_1 y_1 y_3.$$

The transformation T carries F_3 into

$$F_3' = (\alpha - a_1^2)\, y_1^2 + 2\beta y_1\, y_2 + 2a_1 y_1\, (\sum_{i=2}^{n} y_i) + \sum_{i=2}^{n} y_1^2$$

$$= \sum_{i=3}^{n} (y_i + a_1 y_1)^2 + (y_2 + \beta + a_1)\, y_1)^2 + (\alpha - a_1^2 - (\beta + a_1)^2 - (n-2)a_1^2) y_1^2.$$

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 $(i \geqq 2)$ 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 $f''(x) = ax_1^2$, and so a square x_1^2 can be taken out from $f\,(x)$, which contradicts what we hawe proved.

LEMMA 4. *If $n \neq 2^\alpha$, p^α, $2p^\alpha$, where p is an odd prime and α 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

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

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

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

Suppose y_1, y_2 are the solutions of the congruences:

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

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

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

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

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

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

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.

LEMMA 5. *For any $n = 8m$, there exists an even non-decomposable form in n variables with determinant unity.*

Consider the form

$$f(x) = \begin{pmatrix} 8m & & 2m & & 2_{(8m-2)} \\ & 4m-1 & & 1_{(8m-2)} & \end{pmatrix}$$

in $8m$ variables. By lemma 1, the right lower corner $(8m-1)$-rowed minor or the determinant D_{8m} of $f(x)$ has the value

$$2m(8m-1) - (8m-2) = 16m^2 - 10m + 2 > 0,$$

and so

$$D_{8m} = 8m(16m^2 - 10m + 2) - (4m-1)^2(8m-1) = 1.$$

Hence it is clear that $f(x)$ is an even positive definite quadratic form with determinant unity.

To prove the non-decomposability of $f(x)$, we first show that no square can be taken out from $f(x)$.

Let Q be the matrix of $f(x)$, then the adjoint form of $f(x)$, say F, has matrix Q^{-1}. Since

$$QQ^{-1}Q = Q,$$

$F \sim f(x)$, and so F is also even. Hence all the $(8m-1)$-rowed minors of forms equivalent to $f(x)$ are even. Suppose now a square L^2 can be taken out from $f(x)$. A unimodular transformation carries $f(x)$ into

$$f'(x) = \sum_{i,j=1}^{8m} a_{ij} x_i x_j \qquad (a_{ij} = a_{ji})$$

and $L = x_1$. Then the determinant of $f(x) - x_1^2$ is

$$\begin{vmatrix} a_{11} - 1 & a_{12} \dots a_{1,8m} \\ a_{21} & a_{22} \dots a_{2,8m} \\ \dots & \dots\dots\dots \\ a_{8m,1} & a_{8m,2} \dots a_{8m,8m} \end{vmatrix} = 1 - A,$$

where A is the minor of the element a_{11} in the determinant of $f(x)$. Since A is even, $1 - A < 0$ and so $f'(x) - x_1^2$ is indefinite.

Suppose now $f(x)$ is decomposable, say

$$f(x) = f_1(x) + f_2(x).$$

By the same argument used in the last part of the proof of lemma 3, one of the $f_1(x), f_2(x)$, say $f_2(x)$, can at most contain the variables x_1 and x_2. Since all binary non-negative forms can be expressed as a sum of squares of linear forms, a square can be taken out from $f(x)$. This contradicts what we have just proved [7].

LEMMA 6. *If there exists an even positive form in n variables with determinant unity, then n is divisible by* 8.

Suppose there exists an even form f_n with determinant $D_n = 1$. Then by a unimodular transformation, we can change f_n into

$$\left(\begin{array}{ccccccccc} 2a_1 & & 2a_2 & & 2a_3 & & \dots 2a_{n-1} & & 2a_n \\ & b_1 & & b_2 & & b_3 & \dots & b_{n-1} & \end{array}\right).$$

A simple determinant calculation shows that D_n is even if n is odd. Hence n is even. Let the left hand corner principal minors of D_n be $2D_1$ D_2, $2D_3$, $D_4, \dots, 2D_{n-1}$, and write $D_0 = 1$, then

$$\begin{aligned} 2D_1 &= 2a_1, D_2 = 4a_2 D_1 - D_0 b_1^2, \dots, D_{2i-1} = a_{2i-1} D_{2i-2} - D_{2i-3} b_{2i-2}^2, \\ D_{2i} &= 4a_{2i} D_{2i-1} - D_{2i-2} b_{2i-1}^2, \dots, D_n = 4a_n D_{n-1} - D_{n-2} b_{n-1}^2 = 1. \end{aligned} \tag{3}$$

From these relations, it is easy to see that $(D_i, D_{i+1}) \mid D_n = 1$ and so $(D_i, D_{i+1}) = 1$ for $i = 1, \dots, n-1$. Since

$$D_n \equiv \begin{vmatrix} 0 & & 0 & & 0 & \dots 0 & & 0 \\ & b_1 & & b_2 & & b_3 \dots & b_{n-1} & \end{vmatrix} \equiv b_1 b_3 \dots b_{n-1} \pmod 2,$$

all the b_{2i+1} are odd. By taking congruences modulus 4 in (3), we have

$$D_2 \equiv -b_1^2 \equiv -1, \qquad D_4 \equiv -D_2 b_3^2 \equiv 1 \pmod 4.$$

It follows, by induction, that in general

$$D_{4i+2} \equiv -1 \quad \text{and} \quad D_{4i} \equiv 1 \pmod 4.$$

Hence the D_{2i} are odd and $n \equiv 0 \pmod 4$, say $n = 4m$. Write $D_{2i+1} = 2^{t_{2i+1}} D'_{2i+1}$, where D'_{2i+1} is odd. It is evident from the last relation of (3), that the D'_{4m-1}, D_{4m-2} satisfy the relation

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

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),

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

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

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

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

$$(2/D_{4m-2}) = (2/D_{4m-4}) \text{ and so}$$

$$(2^{t_{4m-3}}/D_{4m-2})(2^{t_{4m-3}}/D_{4m-4}) = 1.$$

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:*

$$f_{8m-1} = \left(\begin{array}{ccccc} 8m & & 2m & & 2_{(8m-3)} \\ & 4m-1 & & 1_{(8m-3)} & \end{array}\right),$$

$$f_{8m-2} = \left(\begin{array}{ccccc} 8m & & 2m & & 2_{(8m-4)} \\ & 4m-1 & & 1_{(8m-4)} & \end{array}\right),$$

[7] This argument shows that the even positive definite form with determinant unity

$$h(x) = \sum_{i=1}^{8m} x_i^2 + \left(\sum_{i=1}^{8m} x_i\right)^2 - 2x_1 x_2 - 2x_2 x_{8m} + 2(m-1) x_{8m}^2$$

given by Korkine and Zolotareff in Mathematische Annalen, 6, 1873, p. 366—389 (brought to our notice by prof. L. J. Mordell) is non-decomposable. It is probable that $h(x)$ is equivalent to our $f(x)$ for the same m.

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 $x_1, \ldots, x_{8m-2}$ with integer coefficients having no common factor. By an unimodular transformation, we can write $L=x_1$, and then

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

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 ist not negative. Since the adjoint form of an even form in an even number of variables is even [8]), $A_{11}=2$. Consider now the positive even definite form

$$f_{8m+4} = 8x_1^2+6x_1x_2+2\sum_{i=2}^{6} x_i^2+2\sum_{i=2}^{6} x_i x_{i+1}+\sum_{i,j=1}^{8m-2} a_{ij}\, x_{i+6}\, x_{j+6}$$

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 $2.3-2=4$; the 1. r. c. $8m$-rowed minor is $2.4-3=5$, the 1 c. r. $(8m+1)$-rowed minor is $2.5-4=6$, the 1 r. c. $(8m+2)$-rowed minor is $2.6-5=7$, the 1. r. c. $(8m+3)$-rowed minor is $2.7-6=8$ and so the determinant of f_{8m+4} is $8.8-3^2.7=1$, 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 $(1 \leqslant i \leqslant 8m-2)$, 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:*

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

having determinants $\mathfrak{D}_1, \mathfrak{D}_2, \mathfrak{D}_3$, *respectively, be non-decomposable. Denote by* A *the value of the upper left-hand corner principal* $(m-1)$*-rowed minor of* $\mathfrak{D}_1$. *If there exists a positive definite quadratic form of determinant* $\mathfrak{D}<\mathfrak{D}_1\mathfrak{D}_2$.

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

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

Suppose g has a decomposition

$$g=h+h'. \tag{4}$$

If one of the h's has a term involving x_i $(i=1,\ldots,m)$, it will contain all the terms of g_1, for otherwise we would get a decomposition of g_1 by putting $x_{m+1}=\ldots=x_n=0$. Similarly, if one of the h's, say h, has a term involving x_i $(i=m+2,\ldots,n)$, 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 $b' \geqq b$, for if $b'<b$, on putting $x_1=\ldots=x_m=0$,

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

This is indefinite, since g_3 is non-decomposable. Hence h contains g_3. Hence we may suppose that either h contains both g_1 and g_3, or h contains g_1 and h' contains g_3.

In the first case, h' can only contain the terms or part of the terms of $g-(g_1+g_3)=ax_{m+1}^2+2x_m x_{m+1}$. Then $h'=cx_{m+1}^2$ with $0<c\leqq a$, 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 $\mathfrak{D}$ of g, is $\mathfrak{D}_1\mathfrak{D}_2$, the determinant of h is $\mathfrak{D}-c\,\mathfrak{D}_1\mathfrak{D}_2$. By hypothesis, $\mathfrak{D}-\mathfrak{D}_1\mathfrak{D}_2<0$, 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 $c\leqq a$ for d cannot be negative, as g_3 is indecomposable. It is easy to see that the determinant of h is $c'\mathfrak{D}_1-A$. By hypothesis, $c'\mathfrak{D}_1\leqq a\mathfrak{D}_1\leqq A$, and so h is indefinite. Hence (4) is impossible and the lemma is proved.

[8]) Bachmann, Zahlentheorie, vol. 4, part 1, 444.

LEMMA 9. *For every $n \geqq 12$, except possibly for $n = 13, 16, 17, 19, 23$, there exists an odd non-decomposable quadratic form with determinant unity.*

Suppose $n+2$ can be expressed as the sum of two positive integers n_1, n_2, where $n_1 = 8m$ or a^2-1, and $n_2 \neq 4$, p^α, $2p^\alpha$, p being an odd prime and α an integer. Let the form

$$(5) \qquad \begin{pmatrix} a_1 & & a_2 & & a_3 & & \cdots a_{n_1-2} & & a_{n_1-1} \\ & b_1 & & b_2 & & b_3 & \cdots & b_{n_1-2} & \end{pmatrix}$$

in $n_1 - 1$ variables with determinant 2, containing a minor

$$(6) \qquad \begin{vmatrix} a_1 & & a_2 & & a_3 & & \cdots a_{n_1-3} & & a_{n_1-2} \\ & b_1 & & b_2 & & b_3 & \cdots & b_{n_1-3} & \end{vmatrix} = 3$$

be non-decomposable. Such forms always exist, for if $n_1 = 8m$, we can by lemma 7, take the form

$$\begin{pmatrix} 8m & & 2m & & 2_{(8m-3)} \\ & 4m-1 & & 1_{(8m-3)} & \end{pmatrix};$$

and if $n_1 = a^2-1$, by lemma 3, the form

$$\begin{pmatrix} a^2-1 & & 2_{(n_1-2)} & \\ & a & & 1_{(n_1-3)} \end{pmatrix}.$$

Consider now the odd form:

$$f_n = \begin{pmatrix} a_1 & & a_2 & & a_3 & & \cdots a_{n_1-2} & & a_{n_1-1} & & 3 & & 2_{(n_2-3)} & & x \\ & b_1 & & b_2 & & b_3 & \cdots & b_{n_1-2} & & 1 & & 1_{(n_2-3)} & & y & \end{pmatrix},$$

in n variables with x, y satisfying the relation

$$(7) \qquad n_2 x - (n_2-1)y^2 = 1.$$

From (5) and (6),

$$\begin{vmatrix} a_1 & & a_2 & & a_3 & & \cdots a_{n_1-2} & & a_{n_1-1} & & 3 \\ & b_1 & & b_2 & & b_3 & \cdots & b_{n_1-2} & & 1 & \end{vmatrix} = 3.2-3 = 3,$$

and so as in lemma 1,

$$\begin{vmatrix} a_1 & & \cdots a_{n_1-2} & & a_{n_1-1} & & 3 & & 2(n_2-4) \\ & b_1 & \cdots & b_{n_1-2} & & 1 & & 1(n_2-4) & \end{vmatrix} = n_2 - 1,$$

$$\begin{vmatrix} a_1 & & \cdots a_{n_1-2} & & a_{n_1-1} & & 3 & & 2(n_2-3) \\ & b_1 & \cdots & b_{n_1-2} & & 1 & & 1(n_2-3) & \end{vmatrix} = n_2,$$

and the determinant of f_n is $n_2 x - (n_2-1)y^2 = 1$. From lemma 8, on taking

$$g_1 = \begin{pmatrix} a_1 & & \cdots a_{n_1-2} & & a_{n_1-1} \\ & b_1 & \cdots & b_{n_1-2} & \end{pmatrix}, \quad \mathcal{D}_1 = 2, \ A = 3,$$

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

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

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

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

$$(9) \qquad 2y \leqslant n_2 - 2,$$

the determinant of order $n_2 - 2$,

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

and the determinant of order $n_2 - 1$

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

By lemma 1 and (7),

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

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

$$(13) \qquad 1 < Y < \tfrac{1}{2} n_2.$$

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 $n_3^2 \not\equiv 1 \pmod{2n_3+1}$ for $n_2 \neq 3$. Hence from (13), $y \leqslant n_3 - 1$ 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

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

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

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

is true for $n_2 \geqq 6$. But $n_2 \neq 4$, p^α, $2p^\alpha$, and so $n_2 \geqq 8$, 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 $n \geqq 12$, $n \neq 13, 16, 17, 19, 23$, the equation

$$n+2=n_1+n_2$$

is solvable with the conditions $n_1 = 8m$ or a^2-1, $n_2 \neq 4$, p^α, $2p^\alpha$ 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

$$2^k - 14 = 2.3^\beta, \qquad 2^k - 38 = 2.3^\gamma.$$

They give $3^\beta - 3^\gamma = 12$, which is impossible. But if $n \leqslant 38$, 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

$$2^k - 22 = 2.3^\beta, \qquad 2^k - 46 = 2.3^\gamma.$$

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

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

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 $n=p^k \leqslant 30$ is 27.

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

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

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 $\leqslant 38$ 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

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

and 21, 15, $35 \neq 4$, p^α, $2p^\alpha$, 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

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

Then f_{31} has determinant $5=35\,.\,31-6^2\,.\,30$, f_{32} has determinant $1=5\,.\,5-2^2(35\,.\,30-6^2\,.\,29)$. 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 $c \geqq 1$. This is impossible, since

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

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*

[9] Mordell, J. de Mathématiques, 17 (1938), 41—46. Also see Ko, Quart. J. of Math. (Oxford), 8 (1937) 85.

[10] 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:

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

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

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

is non-decomposable by lemma 3. By lemma 1, $A_{15}=16$, $A_{16}=17$, and $A_{17}=34.17-6^2.16=2.$

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 $A_{16m+2}=10.2-17=3$, $A_{16m+3}=2.3-2=4$, and so step by step, $A_{16m+16}=17$, $A_{16m+17}=34.17-6^2.16=2$.

From lemma 8, on taking

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

$$g_2=\begin{pmatrix} 2(13) & & 2 & 34 \\ & 1(13) & 6 & \end{pmatrix},\quad \mathfrak{D}_2=34.15-6^2.14=6,$$

$$g_3=\begin{pmatrix} 2(14) & & 2 & 34 \\ & 1(14) & 6 & \end{pmatrix},\quad \mathfrak{D}_3=34.16-6^2.15=4,$$

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

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

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's above by A_i'.

For $h=1$, the form in 23 variables

$$f'_{23}=\begin{pmatrix} 2(21) & & 2 & 24 \\ & 1(21) & 5 & \end{pmatrix}$$

is non-decomposable by lemma 3. By lemma 1, $A_{22}'=23$, and $A_{23}'=24.23-5^2.22=2$. Suppose now for $h=m$, in (15) the form f'_{22m+1} is non decomposable and that $A'_{22m+1}=23$, $A'_{22m+1}=2$. Take $h=m+1$. Then $A'_{22m+2}=13.2-23=3$, $A'_{22m+3}=2.3-2=4$, and so step by step, $A'_{22m+22}=23$, $A'_{22m+23}=24.23-5^2.22=2$.

From lemma 8, on taking

$$g_1=f'22m+1,\ \mathfrak{D}_1=2,\ A=23,$$

$$g_2=\begin{pmatrix} 2(19) & & 2 & 24 \\ & 1(19) & 5 & \end{pmatrix},\ \mathfrak{D}_2=24.21-5^2.20=4,$$

$$g_3=\begin{pmatrix} 2(20) & & 2 & 24 \\ & 1(20) & 5 & \end{pmatrix},\ \mathfrak{D}_2=24.22-5^2.21=3,$$

and $a=11$, then $g=f'_{22m+23}$ is non-decomposable, since by lemma 3, g_2, g_3 are non-decomposable. Hence f'_{22h+1} is non-decomposable for any $h>0$.

Finally, we consider the form in $16k+22h+1$ variables $f''_{16k+22h+1}=$

$$\begin{pmatrix} 2(15) & 2\ 34\ 10 & 2(14)\ldots 34\ 10 & 2(14) & 34\ 10 & 2(20)\ 24\ 13 & 2(20)\ldots 24\ 13 & 2(20)\ 24 \\ 1(15)\ 6\ 1 & 1(14)\ldots\ 6 & 1\ 1(14) & 6 & 1\ 1(20)\ 5 & 1\ 1(20)\ \ldots 5 & 1\ 1(20) & 5 \end{pmatrix}$$

with $k>0$, $h>0$. Denote the corresponding minors now by A_i''. Then

$$A''16k+1=A16k+1=2,\ A''16k+2=A16k+2=10.2-17=3,$$
$$A''16k+3=A_3'=4,\ \text{etc.},\ A''16k+22h=A'22h=23,\ A''16k+22h+1=A'22h+1=2.$$

From lemma 8, on taking

$$g_1=f16k+1,\quad \mathfrak{D}_1=2,\ A=17,$$

$$g_2=\begin{pmatrix} 2(19) & & 2 & 24 \\ & 1(19) & 5 & \end{pmatrix},\quad \mathfrak{D}_2=4,$$

$$g_3=\begin{pmatrix} 2(20) & & 2 & 24 \\ & 1(20) & & \end{pmatrix},\quad \mathfrak{D}_3=3,\ a=8,$$

the form $g=f''16k+22h+1$ is non-decomposable. Then as in the proof of the non-decomposability of $f'22h+1$, we can show that $f''16k+22h+1$ is non-decomposable for any $k>0$, $h>0$.

Now every integer $n=2m+1>176$ is of the form $16k+22h+1$, since $m=8k+11h$ has a solution with $h\geqq 0$, $k\geqq 0$ for $m>87$. Our lemma is proved.

LEMMA 11. *There exist even and odd non-decomposable forms in less than* $13k$ *variables with determinant* $k+2$.

Let r be an integer such that

$$(16) \qquad 10k > r^2 > 2k+4 \qquad (k>0).$$

Such integers always exist, for if we write

$$r^2 > 2k+4 \geqq (r-1)^2,$$

$$r^2 \leqslant (\sqrt{2k+4}+1)^2 = 2k+5+2\sqrt{2k+4}.$$

Then (16) holds, if

$$10k > 2k+5+2\sqrt{2k+4}$$

or

$$8(8k-11)k+9>0,$$

which is true for all $k>1$. If $k=1$, $r=3$ suffices.

Consider the form in r^2-k-2 variables

$$f_{r^2-k-2}=\begin{pmatrix}2_{(r^2-k-4)} & & 2 & r^2-1\\ & 1_{(r^2-k-4)} & r & \end{pmatrix}.$$

By lemma 1, its determinant is $(r^2-1)(r^2-k-2)-r^2(r^2-k-3)=k+2$. It is non-decomposable; for by lemma 3, it tuffices to show that

$$r^2-k-2>k+2, \qquad 2r\leqslant r^2-k-2.$$

The first inequality follows from (16). The second is true for $k=1$. For $k=2$, we can take $r=4$. For $k>2$, we have $r\geqq 4$. Suppose then the second ineqaulity is not true, i. e. $2r>r^2-k-2$, and so

$$(r-1)^2\leqslant k+2.$$

Then from $r^2\geqq 2k+5$, we get

$$2(r-1)^2<r^2,$$

which is false for $r\geqq 4$. Hence f_{r^2-k-2} is non-decomposable.

Consider next the form in $(r+1)^2-k-2$ variables with determinant $k+2$

$$f_{(r+1)^2-k-2}=\begin{pmatrix}2_{((r+1)^2-k-4)} & & 2 & (r+1)^2-1\\ & 1_{((r+1)^2-k-4)} & r+1 & \end{pmatrix}.$$

It is non-decomposable; for by lemma 3, it suffices to show that

$$(r+1)^2-k-2>k+2, \qquad 2(r+1)\leqslant(r+1)^2-k-2.$$

Both of the inequalities follow from $r^2>2k+4$.

Since $(r+1)^2-k-2<13k$ and the number of variables of one of the forms f_{r^2-k-2}, $f_{(r+1)^2-k-2}$ is even and of the other is odd, the lemma is proved.

2. *Proofs of the theorems* 1, 2 *and* 3.

Theorem 1 evidently follows from lemma 5 and 9.

To prove theorem 2, we put $n=m+1+s$, where $s>176$ is an odd integer and with the r of (16), $m=r^2-k-2$ or $(r+1)^2-k-2$, the choice being determined by $m\equiv n \pmod 2$. Let the form in s variables obtained in lemma 12 be f_s. Then the upper left-hand minor A_{s-1} is odd and >1. Let

$$u=\tfrac{1}{2}(A_{s-1}+3).$$

Then u is an integer and $0<u-2<\frac{1}{2}A_{s-1}$. Suppose first $m=r^2-k-2$. Consider the form

$$f_n=f_s+2x_sx_{s+1}+ux_{s+1}^2+2x_{s+1}x_{s+2}+f_{r^2-k-2}(x_{s+2},\ldots,x_{s+r^2-k-1}),$$

where f_{r^2-k-2} is the form obtained from lemma 11. Denote the upper left-hand i-rowed principal minor of f_n by A_i. Then

$$A_s=2, A_{s+1}=2u-A_{s-1}=3, \quad A_{s+2}=2.3-2=4, \text{ etc.},$$

$$A_{s+r^2-k-3}=r^2-k-1, \; A_{s+r^2-k-2}=r^2-k;$$

and so the determinant of f_n is $(r^2-1)(r^2-k)-r^2(r^2-k-1)=k$.

From lemma 8, on taking

$$g_1=f_s, \mathcal{D}_1=2, A=A_{s-1}\geqq 3, g_2=f_{r^2-k-2}, \mathcal{D}_2=k+2,$$

$$g_3=\begin{pmatrix}2_{(r^2-k-3)} & & 2 & r^2-1\\ & 1_{(r^2-k-3)} & r & \end{pmatrix}, \quad \mathcal{D}_3=k+1, a=u-2,$$

$g=f_n$ is non-decomposable, if g_3 is non-decomposable. By lemma 3, g_3 is non-decomposable, if $\mathcal{D}_3<r^2-k-1$, or $2k+2<r^2$ and this follows from the choice of r in lemma 11.

Similarly, f_n is non-decomposable if $m=(r+1)^2-k-2$.

Hence theorem 2 is proved.

To prove theorem 3, by theorem 1, we need only supply special results for $n=6, 7, 9, 10, 11, 13, 17, 19, 23$.

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.)

[11]) These are the same forms given by Prof. Mordell. See footnote [3]).

Zur Verallgemeinerung des Galoisschen Kriteriums der algebraischen Auflösbarkeit.

Von
S. Lubelski (Warszawa).

Das berühmte Galoissche Kriterium [1]) der algebraischen Auflösbarkeit eines Polynoms kann gruppentheoretisch folgendermassen formuliert werden: „Eine Permutationsgruppe $\mathfrak{G}$ vom Primzahlgrad p kann dann und nur dann auflösbar sein, wenn $\mathfrak{G} = \mathfrak{A}\,\mathfrak{P}$ ist, wo $\mathfrak{A}$ und $\mathfrak{P}$ zyklisch sind, dabei ist $\mathfrak{P}$ bzw. $\mathfrak{A}$ von der Ordnung p. bzw. d, $d/p-1$". Wir wollen in dieser Arbeit vor allem zeigen, dass dieses Kriterium eigentlich die Folgerung eines allgemeinen Permutationssatzes ist:

Ist p prim, so ist der Normalisator einer p-Sylowgruppe $\mathfrak{P}$ der symmetrischen Gruppe $\mathfrak{S}$ von p Elementen, Produkt zweier zyklischer Gruppen $\mathfrak{A}$ und $\mathfrak{P}$, wo $\mathfrak{A}$ die Ordnung $p-1$ und $\mathfrak{P}$ die Ordnung p hat (s. Satz 1).

Das Hauptziel dieser Arbeit ist aber den Galoisschen Satz auch auf solche Polynome, deren Grad nicht prim ist, zu erweitern und zu verallgemeinern. Zu diesem Behufe betrachten wir zunächst verallgemeinerte auflösbare Permutationsgruppen vom Grade p^n, die einen Abelschen Normalteiler von demselben Grade p^n haben. Für derartige Gruppen beweisen wir den nachstehenden Satz.

Voraussetzung: *p ist prim und t eine natürliche Zahl, $\mathfrak{G}$ ist eine Permutationsgruppe vom Grade p^t, die einen transitiven Abelschen Normalteiler $\mathfrak{A}$ enthält*".

Behauptung: *$\mathfrak{G}$ enthält nur solche Permutationen, die höchstens eine Ziffer unverändert lassen, oder es finden sich solche Permutationen $S \neq E$ in $\mathfrak{G}$,*

[1]) E. Galois. Oeuvres, S. 48. (herausgegeben von Liouville im 11. Bande des Journal de mathem. pures et appl. 1846, S. 381 — 444).