Thus, for $n \geqslant 2$, $r = 1$, $s = 1$, (50) is not satisfied and therefore $f(x, y)$ is not a polynomial in $x, y$. However

$$f(a+jp, y) = j\Big\{y - \sum_{b=0}^{p-1} bL_b(y)\Big\},$$

where $L_b(y)$ is defined by (46).

Remark. We note that Rédei and Szele [2] have made a detailed study of the polynomial representation of functions over rings and in particular over $Z_n$; the polynomials considered are in an enlarged ring.

### References

[1] L. E. Dickson, *Introduction to the theory of numbers*, Chicago 1929.

[2] L. Rédei und T. Szele, *Algebraisch-zahlentheoretische Betrachtungen über Ringe. I*, Acta Mathematica 79 (1947), pp. 291-320.

*Reçu par la Rédaction 19. 6. 1963*

---

ACTA ARITHMETICA
IX (1964)

# On the representation of rational functions as sums of squares

by

J. W. S. Cassels (Cambridge)

*To my teacher and friend Professor L. J. Mordell for his 75th birthday in gratitude*

Theorem 1. *Let $k$ be any field and denote by $k(x)$ and $k[x]$, respectively, the field of rational functions and the ring of polynomials in a single variable $x$ having coefficients in $k$. Then any $f \in k[x]$ which is the sum of squares of elements of $k(x)$ is the sum of the same number of squares of elements of $k[x]$.*

What is essentially new in this enunciation is that the same number of squares suffices. Without this condition the result stated has been proved by Artin [1], who adapted a proof by Landau [5] of the fact that every positive define function in $\boldsymbol{Q}[x]$ (where $\boldsymbol{Q}$ is the field of rationals) is the sum of eight squares of elements of $\boldsymbol{Q}[x]$ (cf. also Witt [6] for some related results).

As almost immediate consequences of Theorem 1 we have:

Theorem 2. *Let $d \in k$ and suppose that the characteristic of $k$ is not 2. A necessary and sufficient condition that $x^2 + d$ be the sum of $n > 1$ squares in $k(x)$ is that*

*either* $-1$ *is the sum of* $n-1$ *squares of* $k$
*or* $d$ *is the sum of* $n-1$ *squares of* $k$.

Theorem 3. *Let $\boldsymbol{R}$ denote the field of real numbers and let $x_1, \ldots, x_n$ be independent variables over $\boldsymbol{R}$. Then $x_1^2 + \ldots + x_n^2$ is not the sum of $n-1$ squares of elements of $\boldsymbol{R}(x_1, \ldots, x_n)$.*

Theorem 3 answers a problem of Professor N. J. Fine which reached me *via* Professor Mordell and Professor Davenport. The case $n \leqslant 4$ has already been proved by Davenport [4] in another way. I am grateful to him for showing me his manuscript before publication.

Proof of Theorem 1. The proof is essentially an adaption to the "power series case" of Davenport's proof [3] of my theorem [2] that if

a homogeneous quadratic form with rational integer coeffiicents has a non-trivial integral zero, then it has one whose coordinates are bounded in terms of the coefficients of the form. The proof given below is, however, quite self contained.

We denote the number of squares in Theorem 1 by $n$ and dispose first of some trivial cases.

First case. $n = 1$. This follows from the existence of unique factorization in $k[x]$.

Second case. *$k$ has characteristic* 2. Then any sum of squares is itself a square and the first case applies.

Third case. $-1$ *is the sum of* $n-1$ *squares of elements of* $k$. Let $-1 = a_2^2 + \ldots + a_n^2$. After the second case, we may suppose that $2 \neq 0$, and then

$$f = \left(\frac{f+1}{2}\right)^2 + \sum_{2 \leqslant j \leqslant n} \left\{\frac{a_j(f-1)}{2}\right\}^2. \tag{1}$$

From now on, we shall suppose that none of the first three cases applies. By hypothesis there is a solution $Z$, $Y_j$ $(1 \leqslant j \leqslant n)$ of the equation

$$fZ^2 = \sum_{1 \leqslant j \leqslant n} Y_j^2 \tag{2}$$

where $Z$, $Y_j \in k[x]$ and $Z \neq 0$. We have to show that there is a solution with $Z = 1$ and, by homogeneity, it is enough to show that there is a solution with $Z \in k$, $Z \neq 0$.

Since solutions of (2) exist with $Z \neq 0$, there is a solution $Y_j = y_j$, $Z = z$ with $z \neq 0$ for which the degree of $z$ is as small as possible. We shall show that $z \in k$ by proving that otherwise there exists a solution $Y_j = y_j'$, $Z = z'$ with $z' \neq 0$ for which $\deg z' < \deg z$. We suppose, then, that

$$\deg z > 0. \tag{3}$$

Let $\lambda_j$ $(1 \leqslant j \leqslant n)$ be the uniquely defined elements of $k[x]$ such that[1]

$$\deg \Lambda_j < 0 \qquad (1 \leqslant j \leqslant n), \tag{4}$$

where

$$\Lambda_j = \lambda_j - y_j/z. \tag{5}$$

[1] The degree of an element of $k(x)$ is defined in the obvious way.



We may suppose that

$$f \neq \sum \lambda_j^2, \tag{6}$$

since otherwise $z' = 1$, $y_j' = \lambda_j$ would be our required smaller solution.

It may readily be verified that

$$\begin{aligned} y_j' &= y_j\left\{\sum_u \lambda_u^2 - f\right\} - 2\lambda_j\left\{\sum_u \lambda_u y_u - fz\right\}, \\ z' &= z\left\{\sum_u \lambda_u^2 - f\right\} - 2\left\{\sum_u \lambda_u y_u - fz\right\} \end{aligned} \tag{7}$$

is another solution[2] of (2). Clearly, $y_j' \in k[x]$, $z' \in k[x]$.

On substituting (5) in (7) we have

$$z' = z\sum_u \Lambda_u^2.$$

Hence

$$\deg z' < \deg z$$

by (4). On the other hand, (6) implies that not all the $\Lambda_j$ are 0, and hence $\sum_u \Lambda_u^2 \neq 0$ on considering the terms of highest degree in $x$ and remembering that the *third case* (above) does not apply. Hence $z' \neq 0$. We have now reached a contradiction to our assumption that $\deg z$ is as small as possible and satisfies (3). This completes the proof of Theorem 1.

Proof of Theorem 2. If $d$ is the sum of $n-1$ squares in $k$ then trivially $x^2 + d$ is the sum of $n$ squares in $k[x]$. If $-1$ is the sum of $n-1$ squares in $k$, then (1) with $f = x^2 + d$ gives a representation of $x^2 + d$ as the sum of $n$ squares. Hence all that is required to complete the proof is to show that if $-1$ is not the sum of $n-1$ squares in $k$ and $x^2 + d$ is the sum of $n$ squares in $k(x)$, then $d$ is the sum of $n-1$ squares in $k$.

By Theorem 1, we then have

$$x^2 + d = \sum_{1 \leqslant j \leqslant n} Y_j^2, \qquad Y_j \in k[x]. \tag{8}$$

On applying the condition about $-1$ to the terms of highest degree in $x$ on both sides we see that the $Y_j$ are linear in $x$ (or constants), say

$$Y_j = a_j x + b_j, \qquad a_j, b_j \in k. \tag{9}$$

Then for at least one choice of sign we can find $c \in k$ such that

$$c = \pm(a_n c + b_n).$$

[2] It is the second point of intersection of the quadric (2) with the line joining $(y_j, z)$ to $(\lambda_j, 1)$ in $n$-dimensional projective space over the field $k(x)$.

On putting $x = c$ in (8) we then have

$$d = \sum_{1 \leqslant j \leqslant n-1} (a_j c + b_j)^2,$$

as required.

Proof of Theorem 3. This follows from Theorem 2 on putting

$$x = x_n, \qquad k = \boldsymbol{R}(x_1, \ldots, x_{n-1})$$

and using induction on $n$.

Added in proof. Dr A. Pfister has made some interesting applications of these theorems which will be published in the Journal of the London Mathematical Society.

### References

[1] E. Artin, *Über die Zerlegung definiter Funktionen in Quadrate*. Abh. Math. Sem. Hamburg 5 (1927), pp. 100-115.

[2] J. W. S. Cassels, *Bounds for the least solutions of homogeneous quadratic equations*, Proc. Cambridge Phil. Soc. 51(1955), pp. 262-264.

[3] H. Davenport, *Note on a theorem of Cassels*, Proc. Cambridge Phil. Soc. 53(1957), pp. 539-540.

[4] — *A problematic identity*, Mathematika 10(1963), pp. 10-12.

[5] E. Landau, *Über die Darstellung definiter Funktionen durch Quadrate*, Math. Ann. 62 (1906), pp. 272-285.

[6] E. Witt, *Zerlegung reeller algebraischer Funktionen in Quadrate, Schiefkörper über reellem Funktionenkörper*, J. reine angew. Math. 171 (1934), pp. 4-11.

TRINITY COLLEGE, CAMBRIDGE

*Reçu par la Rédaction le 18. 6. 1963*

ACTA ARITHMETICA
IX (1964)

# Symplectic modulary groups

by

M. NEWMAN and J. R. SMART (Washington)

*Dedicated to Professor L. J. Mordell on the occasion on his 75th birthday*

**1. Introduction.** In this article we extend our investigation of modulary groups of matrices initiated in [2] for the $t \times t$ modular group to the $2t \times 2t$ symplectic modular group. The principal difficulty that had to be overcome was the proof of Theorem 1 below, which itself is a result of much interest, and suggests the following general question: Suppose that $f$ is a mapping of the ring of $p \times p$ rational integral matrices into the ring of $q \times q$ rational integral matrices. Suppose further that $n$ is a positive integer and that the congruence $f(A) \equiv 0 (\mathrm{mod}\, n)$ has a solution $A$, where $A$ is a $p \times p$ rational integral matrix. For what mappings $f$ is it possible to deduce the existence of a matrix $B$ such that $B \equiv A (\mathrm{mod}\, n)$ and $f(B) = 0$? Examples of such mappings are $f(A) = 1 - \det(A)$, $f(A) = A - A'$ (Lemma 1 below) and $f(A) = AJA' - J$ (Theorem 1 below), where $J$ is the $2t \times 2t$ matrix

$$\begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}.$$

Here $I$ is the $t \times t$ identity matrix, and will stand in what follows for the identity matrix of arbitrary size.

In the discussion that follows *all* matrices will have rational integral entries. $\Gamma$ will denote the $2t \times 2t$ symplectic modular group. Then $\Gamma$ is the group of automorphs of $J$ and consists of all $2t \times 2t$ matrices

$$M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

such that $MJM' = J$. Such a matrix will be referred to as *symplectic*. It is easy to verify that $M$ is symplectic if and only if

$$AD' - BC' = I, \qquad AB' = BA', \qquad CD' = DC'.$$

It is also true that if $M$ is symplectic then so is $M'$.