Zeitschrift: Commentarii Mathematici Helvetici

Herausgeber: Schweizerische Mathematische Gesellschaft

Band: 33 (1959)

Artikel: An arithmetical property of quadratic forms.

Autor: Ledermann, Walter

DOI: https://doi.org/10.5169/seals-26005

An arithmetical property of quadratic forms

By WALTER LEDERMANN, Manchester

In their paper [1] F. HIRZEBRUCH and H. HOPF have encountered an interesting arithmetical property possessed by certain symmetric bilinear forms

$$f(x, y) = \sum_{i, j=1}^{n} a_{ij} x_i y_j \tag{1}$$

that arise in algebraic topology. In the forms which they consider, the coefficients a_{ij} and the variables are integers and $\det a_{ij} = \pm 1$; and it is known that there exists an integral vector w such that

$$f(x, x) \equiv f(x, w) \pmod 2 \tag{2}$$

for all x. If τ is the signature of f, then it is a corollary of their topological investigations that

$$\tau \equiv f(w, w) \pmod 4 . \tag{3}$$

It is desirable to give a purely algebraic proof of (3), and I am greatly indebted to Professor HOPF for having drawn my attention to this question, which will be discussed in this note.

In fact, it will be shown that (3) is a special case of a result concerning forms (1) in which the coefficients and variables are rational numbers with odd denominators. This subset, $\mathfrak{Q}$, of all rationals forms a ring, whose elements may be grouped into residue classes modulo any power of 2 by stipulating that

$$\frac{c_1}{d_1} \equiv \frac{c_2}{d_2} \pmod{2^\alpha}$$

whenever $c_1 d_2 - d_1 c_2 \equiv 0 \pmod{2^\alpha}$; since only odd denominators are allowed, this definition evidently does not depend on the representation of the fractions involved. In particular, a fraction is termed even or odd according as its numerator is even or odd; and we note that, if r is odd, $r^2 \equiv 1 \pmod 4$.

The set, V, of n-tuples or "row-vectors" $x = (x_1, x_2, \ldots, x_n)$ $(x_i \in \mathfrak{Q})$ is a $\mathfrak{Q}$-module. A change of basis of V amounts to replacing x by the n-tuple $\tilde{x} = xP$, where P is a fixed n-rowed matrix in $\mathfrak{Q}$ with odd determinant.

Let f be a symmetric bilinear form which relative to the original basis is expressed as xAy', where $A = (a_{ij})$. After the change of basis, f becomes $\tilde{x} B \tilde{y}'$, where

$$B = PAP' . \tag{4}$$

We write $\Delta = \Delta_f = \det A$, and throughout this paper we restrict ourselves to forms with odd determinants, a property which is clearly preserved by the transformation (4).

For a given form f we can in many ways determine a constant vector w such that (2) holds for all x in $\mathfrak{Q}$. Indeed, w may be taken as the solution of the vector equation

$$wA = (a_{11}, a_{22}, \ldots, a_{nn}) ,$$

this solution being in $\mathfrak{Q}$, because $\det A$ is odd. For since

$$f(x, x) \equiv \sum_i a_{ii} x_i^2 \equiv \sum_i a_{ii} x_i \pmod 2 ,$$

we have that

$$f(x, w) = wAx' = \Sigma a_{ii} x_i ,$$

and (2) is satisfied. If $\tilde{w}$ is another vector satisfying (2), then $f(x, \tilde{w} - w) \equiv 0 \pmod 2$ for all x, so that $(\tilde{w} - w)A \equiv 0 \pmod 2$. It follows that

$$\tilde{w} = w + 2z , \tag{5}$$

where z is a suitable vector in $\mathfrak{Q}$. Conversely, any vector of the form (5) satisfies (2). We have that

$$f(\tilde{w}, \tilde{w}) = f(w, w) + 4f(w, z) + 4f(z, z) .$$

Thus

$$f(\tilde{w}, \tilde{w}) \equiv f(w, w) \pmod{4} ,$$

that is, $f(w, w)$ (though not w itself) is an *invariant modulo* 4 of f.

Our aim is to prove the following

Theorem. *Let f be a quadratic form in n variables in $\mathfrak{Q}$ with odd determinant Δ and with signature τ. Then*[1])

$$f(w, w) - \tau \equiv \Delta - \operatorname{sgn}\Delta \pmod 4 , \tag{6}$$

where w is a solution of (2).

We remark that, whilst Δ is not an invariant of f, both $\operatorname{sgn}\Delta$ and Δ are invariants mod 4. For in a transformation of the type (4), Δ is multiplied by $(\det P)^2$, which is congruent with 1 mod 4, since $\det P$ is odd.

In particular, when f is unimodular, whether integral or not, we have that $\Delta = \operatorname{sgn}\Delta$, so that (6) reduces to (3).

The theorem is proved by an induction with respect to n which is based on the following simple matrix formula. Consider a partitioning of A, say

$$A = \begin{pmatrix} K & L' \\ L & M \end{pmatrix} ,$$

[1]) As usual, we define sgn Δ to be $+1$ or -1 according as $\Delta > 0$ or $\Delta < 0$.

where K is non-singular and of dimension less than n. Put

$$P = \begin{pmatrix} I & O \\ -LK^{-1} & I \end{pmatrix}$$

where the identity matrices on the diagonal are of dimensions (in general distinct) equal to those of K and M respectively. Then

$$PAP' = \begin{pmatrix} K & O \\ O & M - LK^{-1}L' \end{pmatrix} . \tag{7}$$

When $\det K$ is odd, this transformation is admissible, since P then lies in $\mathfrak{Q}$. Now if not all diagonal elements of A are even, we may, without loss of generality, assume that a_{11} is odd and then put $K = (a_{11})$. If, on the other hand, all diagonal elements are even, then each row of A must contain at least one odd element, or else $\det A$ could not be odd. We may then assume that a_{12} is odd and that K is the leading 2-rowed submatrix; for in that case $\det K = a_{11}a_{22} - a_{12}^2 \equiv -1 \pmod 4$, which is certainly odd. Thus, when $n > 2$, we can always apply a transformation of the type (7), in which the dimension of K is either 1 or 2.

When V is referred to the new basis, f splits and we write

$$f(x, x) = g(x^{(1)}, x^{(1)}) + h(x^{(2)}, x^{(2)}) ,$$

where $x = (x^{(1)}, x^{(2)})$ and the dimensions of the vectors $x^{(1)}$ and $x^{(2)}$ are those of K and M respectively[2]). Evidently

$$\Delta_f = \Delta_g \Delta_h , \; \tau_f = \tau_g + \tau_h ,$$

where suffixes are used to distinguish quantities corresponding to different forms. Also, if $w^{(1)}$ and $w^{(2)}$ are such that

$$g(x^{(1)}, x^{(1)}) \equiv g(x^{(1)}, w^{(1)}) \pmod 2$$

for all $x^{(1)}$ and

$$h(x^{(2)}, x^{(2)}) \equiv h(x^{(2)}, w^{(2)}) \pmod 2$$

for all $x^{(2)}$, then $w = (w^{(1)}, w^{(2)})$ satisfies (2).

Leaving aside for the present the cases in which $n = 1$ or $n = 2$, we may assume, by induction, that the theorem holds for the forms g and h. Then, since

$$f(w, w) - \tau_f = (g(w^{(1)}, w^{(1)}) - \tau_g) + (h(w^{(2)}, w^{(2)}) - \tau_h) ,$$

we have that

$$f(w, w) - \tau_f \equiv \Delta_g - \operatorname{sgn}\Delta_g + \Delta_h - \operatorname{sgn}\Delta_h , \tag{8}$$

---

[2]) A somewhat similar method of reduction, but in a different context, has been employed by MINKOWSKI ([2], 16–20).

with the convention that henceforth all congruences are mod 4. Now, if r and s are odd, $(1-r)(1-s)$ is divisible by 4, so that

$$r+s\equiv 1+rs\,.$$

Hence, in particular,

$$\varDelta_g+\varDelta_h\equiv 1+\varDelta_g\varDelta_h=1+\varDelta_f$$

and

$$\operatorname{sgn}\varDelta_g+\operatorname{sgn}\varDelta_h\equiv 1+\operatorname{sgn}(\varDelta_g\varDelta_h)=1+\operatorname{sgn}\varDelta_f\,.$$

Substituting in (8) we immediately obtain (6).

It only remains to verify the theorem for the two lowest dimensions. When $n=1$, $f=a_{11}x_1^2$, where a_{11} is odd. We may then put $w_1=1$ to satisfy (2). Thus $f(w,w)=a_{11}=\varDelta$. Since $\tau=\operatorname{sgn}a_{11}=\operatorname{sgn}\varDelta$, the relation (6) is certainly true. When $n=2$, that is when $f=a_{11}x_1^2+a_{22}x_2^2+2a_{12}x_1x_2$, we have to distinguish two cases.

(i) Assume that a_{11} and a_{22} are not both even, so that we may assume that a_{11} is odd. The transformation (7) can then be applied with $K=(a_{11})$, and f splits into two unary forms. The induction argument is therefore available as before.

(ii) If a_{11} and a_{22} are both even, a_{12} is necessarily odd and $\varDelta=a_{11}a_{22}-a_{12}^2\equiv-1$. Evidently, $f(x,x)$ is even for all x, so that the vector $w=0$ satisfies (2). We have therefore to show that

$$-\tau\equiv-1-\operatorname{sgn}\varDelta\,. \tag{9}$$

When $\operatorname{sgn}\varDelta=-1$, the form is indefinite, that is $\tau=0$, and (9) is true. On the other hand, when $\operatorname{sgn}\varDelta=1$, then $\tau=2$ or $\tau=-2$ according as $a_{11}>0$ or $a_{11}<0$. But $2\equiv-2$, and again (9) holds in each case.

REFERENCE

[1] F. Hirzebruch and H. Hopf, *Felder von Flächenelementen in 4-dimensionalen Mannigfaltigkeiten*. Math. Annalen 136 (1958).

[2] H. Minkowski, *Gesammelte Abhandlungen I* (Leipzig 1911).

(Received April 14, 1958)