WITT'S CANCELLATION THEOREM IN VALUATION RINGS

PAUL J. MCCARTHY

Let \( K \) be a field with an exponential valuation \( V \). The set of all \( a \in K \) such that \( V(a) \geq 0 \) forms a ring \( R \). The set of all \( a \in R \) such that \( V(a) > 0 \) forms a prime ideal in \( R \). This ideal consists of precisely the nonunits of \( R \). \( R \) is called the valuation ring of \( K \) with respect to \( V \).

If \( A \) and \( B \) are symmetric matrices over \( R \), we say that \( A \) and \( B \) are congruent, and write \( A \cong B \), if there is a unimodular matrix \( T \) over \( R \) such that \( TAT = B \). \( T \) is unimodular if it has an inverse over \( R \), i.e., if \( |T| \) is a unit in \( R \). If \( A_1 \) and \( A_2 \) are square matrices, we write \( A_1 + A_2 \) for the matrix

\[
\begin{bmatrix}
A_1 & 0 \\
0 & A_2
\end{bmatrix}.
\]

If \( a \) is an element of \( R \) and \( A \) is a square matrix, \( aA \) will have the obvious meaning.

In this paper we prove the following result.

**Theorem.** Assume that 2 is a unit in \( R \). If \( A \), \( B \), and \( C \) are non-singular symmetric matrices over \( R \), and if \( A + B \cong A + C \), then \( B \cong C \).

This theorem was first proved by E. Witt [5] for matrices over a field of characteristic not equal to 2. It was subsequently proved by B. W. Jones [2] for matrices over the ring of \( p \)-adic integers (\( p \) odd), by G. Pall [4] for Hermitian matrices over a skewfield of characteristic not equal to 2, and by W. H. Durfee [1] for matrices over a complete valuation ring with 2 a unit. Moreover, Durfee gave examples to show that the theorem is not true when 2 is a nonunit. We have not only eliminated the requirement that \( R \) be complete, but we give a proof which is considerably shorter than the proof of the corresponding theorem given by Durfee. The theorem is an immediate consequence of the following two lemmas.

**Lemma 1.** Assume that 2 is a unit in \( R \). If \( A \) is any \( n \times n \) symmetric matrix over \( R \), there are elements \( a_1, a_2, \ldots, a_n \) in \( R \) such that \( A \cong a_1 + a_2 + \cdots + a_n \).

**Lemma 2.** Assume that 2 is a unit in \( R \). If \( B \) and \( C \) are nonsingular
symmetric matrices over $R$, if $a$ is an element of $R$, and if $a+B \cong a+C$, then $B \cong C$.

The first of these lemmas is proved in precisely the same manner as the first part of Theorem 1 of [1].

The proof of the second lemma is similar to the proof of Theorem 8 of [3]. Let

$$T = \begin{bmatrix} t_0 & t_1 \\ t_2 & T_0 \end{bmatrix}$$

be a unimodular matrix such that $T^r(a+B)T = a+C$, where $t_0$ is an element of $R$ and $t_1$, $t_2$, and $T_0$ are of the appropriate dimensions. Then

$$t_0 a + t_2 B t_2 = a,$$

$$t_0 a t_1 + t_2 B T_0 = 0,$$

$$t_1 a t_1 + T_0^r B T_0 = C.$$

We can choose the correct sign in $t_0 \pm 1$ so that the resulting element, $u$, of $R$ is a unit. For, if $t_0 + 1$ and $t_0 - 1$ are both nonunits, then $(t_0 + 1) - (t_0 - 1) = 2$ is a nonunit.

If we now set $S = T_0 - t_2 u^{-1}$, we can use (1) to show that $S^r B S = C$. Since $T^r T = a C$, and $T^r$ is a unit, we have $V(B) = V(C)$. Hence $V(S^r) = 0$, so $S^r$ and therefore $S$ is a unit in $R$. Thus $S$ is unimodular, and this completes the proof of Lemma 2 and the theorem.

References


University of Notre Dame