ON THE REPRESENTATION, IN THE RING OF $p$-ADIC INTEGERS, OF A QUADRATIC FORM IN $n$ VARIABLES BY ONE IN $m$ VARIABLES\(^1\)

IRMA MOSES

**Introduction.** In this paper, we relate the existence of $p$-adically integral, linear transformations taking a quadratic form $f$ in $m$ variables into a quadratic form $g$ in $n$ variables with the representation of $g$ by $f$ rationally without essential denominator. Before stating our result, we introduce some terminology and recall some known theorems on the subject.

We denote by $R$, $R_\omega$, and $R_p$ respectively the rational field, the real field, and the $p$-adic field for $p$ an arbitrary, fixed prime. We also designate the ring of rational integers by $\mathbb{Z}$ and the ring of $p$-adic integers by $\mathbb{Z}_p$. We recall the definition that a form $f$, with matrix in $\mathbb{Z}$, represents a form $g$, with matrix in $\mathbb{Z}$, rationally without essential denominator, if, for every positive, rational integer $q$, $f$ may be taken into $g$ by a linear transformation whose elements are rational numbers with denominators relatively prime to $q$.

We assume throughout this paper that any considered transformation is linear and that the matrix of any considered quadratic form is nonsingular and has elements in $\mathbb{Z}$, unless otherwise specified. We shall feel free to phrase theorems and proofs either in terms of the matrix of a form or in terms of the form itself.

It was proved by Helmut Hasse [1, pp. 205–224]\(^2\) that if $f$ and $g$ are quadratic forms with the same number of variables, the existence of transformations in all $R_p$ and in $R_\omega$, each taking $f$ into $g$, implies the existence of such a transformation in $R$. He later [2, pp. 12–24] extended the theorem to the case where $f$ and $g$ do not necessarily contain the same number of variables.\(^3\) Then C. L. Siegel [5, pp. 678–680] proved that if $f$ and $g$ contain the same number of variables, the existence of transformations in all $J_p$ and in $R_\omega$, each taking $f$ into $g$, implies that $f$ represents $g$ rationally without essential denominator. We now wish to extend this theorem of Siegel to the case where $f$
and \( g \) do not necessarily contain the same number of variables. Siegel's proof must be modified to give the extension, as it uses, to a large degree, square matrices and their inverses, which do not exist in case \( f \) and \( g \) contain different numbers of variables. We now state the extension theorem formally. Its proof and a corollary will then occupy the remainder of the paper.

**Theorem.** Let \( S \) and \( T \) be symmetric, nonsingular matrices in \( J \), of orders \( m \) and \( n \), respectively. If there exists a transformation in each \( J_p \) and a transformation in \( R_w \), each taking \( S \) into \( T \), then \( S \) represents \( T \) rationally without essential denominator.

1. Canonical forms for quadratic forms with matrices in \( J_2 \). In the proof of the theorem, we use canonical forms for quadratic forms with matrices in \( J_2 \). B. W. Jones [3, pp. 726–727] and Gordon Pall [4, pp. 35–38] have established canonical forms, modulo an arbitrary, fixed power of 2, for quadratic forms with matrices in \( J \). By slight modifications of their respective theorems and proofs, we obtain the following results, designated as Lemmas 1, 2, and 3.

**Lemma 1.** Any quadratic form in \( s \) variables, with matrix in \( J_2 \), is equivalent in \( J_2 \) to a form,

\[
\phi = 2^{e_1}\theta_1 + \cdots + 2^{e_k}\theta_k,
\]

where \( \theta_1, \cdots, \theta_k \) are quadratic forms, each with matrix in \( J_2 \) having a 2-adic unit determinant, and each in variables different from those of the remaining forms; and where the \( e_i \) are in \( J \) \((0 \leq e_1 < e_2 < \cdots < e_k)\).

**Lemma 2.** Let \( \theta \) be a quadratic form in \( t \) variables, with matrix in \( J_2 \) having a 2-adic unit determinant. Then either \( \theta \) is equivalent in \( J_2 \) to a form of the type

\[
a_1x_1^2 + \cdots + a_tx_t^2,
\]

where the \( a_i \) are units in \( J_2 \); or \( \theta \) is equivalent in \( J_2 \) to a form of the type

\[
2(b_1x_1^2 + c_1x_1x_2 + d_1x_2^2) + \cdots + 2(b_rx_{t-1}^2 + c_rx_{t-1}x_t + d_rx_t^2),
\]

where the \( b_i \) and \( c_i \) are units in \( J_2 \), and the \( d_i \) are in \( J_2 \).

**Lemma 3.** Every form \( 2bx_1^2 + 2cx_1x_2 + 2dx_2^2 \), in which \( c \) is a unit in \( J_2 \), and \( b \) and \( d \) are in \( J_2 \), is equivalent in \( J_2 \) either to

\[
(1.1) \quad 2x_1x_2 \quad \text{or} \quad 2x_1^2 + 2x_1x_2 + 2x_2^2,
\]

according as \( bd \) is not a unit or is a unit.
We now combine Lemmas 1, 2, and 3 to see that for any quadratic form with matrix in $J_2$, there exists an equivalent form in $J_2$ of one of the following kinds: (1) a diagonal matrix; (2) a matrix with powers of 2 times the matrices of binary quadratic forms of type (1.1) on the principal diagonal and 0's elsewhere; and (3) a matrix which is a mixture of (1) and (2), containing matrices of both unary and binary quadratic forms on its principal diagonal and 0's elsewhere.

2. The main lemma for the proof of the theorem. In this section, we state and prove the main lemma used in the proof of the theorem. We shall use the results of §1, as well as the following two theorems from a paper of Siegel [6, pp. 536, 538], designated as Lemmas 4 and 5.

**Lemma 4.** Let $S$ and $T$ be symmetric matrices in $J$, of orders $m$ and $n$, respectively. Let $P$ designate any one of the fields $R$, $R\omega$, and $R_p$. Then if $C_0'SC_0 = T$ is a representation of $T$ by $S$ in $P$, then each other representation $C'SC = T$ in $P$, for which $(C_0'SC - T)^{-1}$ exists, can be written in the form,

$$C = C_0 + 2M(N - M'SM)^{-1}M'SC_0,$$

where $N$ is an $n$ by $n$ skew-symmetric matrix in $P$ and $M$ is an $m$ by $n$ matrix in $P$. If, conversely, $N$ is a skew-symmetric matrix in $P$ and $M$ is an arbitrary matrix in $P$, for which $(N - M'SM)^{-1}$ exists, then (2.1) furnishes a solution of $C'SC = T$.

**Lemma 5.** For every symmetric matrix in $J_p$, there exists an automorph in $J_p$ of determinant $-1$.

We wish now to prove the following lemma:

**Lemma 6.** Let a prime $p$ be given. Let $S$ in $J$ and $T$ in $J_p$ be non-singular, symmetric matrices, of orders $m$ and $n$, respectively. If $B$ in $R_p$ and $B_p$ in $J_p$ are transformations taking $S$ into $T$, then there is an automorph of $T$ in $J_p$, say $A_p$, such that $B_p = B_p A_p$ takes $S$ into $T$ and $|B'SB_p - T| \neq 0$.

We prove Lemma 6 by induction on $n$, finding it necessary to prove it first for $n = 1$ and $n = 2$.

**Case I.** $n = 1$. When $n = 1$, $T$ and $B'SB_p$ are scalars. If $B'SB_p \neq T$, we choose $B_p = B_p$; if $B'SB_p = T$, we choose $B_p = -B_p$. Since $T$ is nonsingular, we then surely have $|B'SB_p - T| \neq 0$.

**Case II.** $n = 2$. If $|B'SB_p - T| \neq 0$, we set $B_p = B_p$. If $|B'SB_p - T| = 0$, we may take $B_p = -B_p$, providing that $-B'SB_p - T| \neq 0$. If both $|B'SB_p - T| = 0$ and $|-B'SB_p - T| = 0$, we may add the ex-
pansions of the determinants to get \( |B'SB_p| = -|T| \). In this case, we use Lemma 5 to find an automorph of \( T \) in \( J_p \), say \( L_p \), with \( |L_p| = -1 \). Then, since \( |T| \neq 0 \),

\[
|B'SB_pL_p| = -|B'SB_p| \neq -|T|.
\]

Thus, at least one of \( |B'SB_pL_p - T| \) and \( |-B'SB_pL_p - T| \) is different from zero, and we can define \( \tilde{B}_p \) accordingly.

**Case III.** \( n \geq 3 \). If \( p \) is odd, we assume the lemma true for \( n - 1 \) and proceed to show it holds for \( n \). By a well known theorem, since \( p \) is odd, there exists a unimodular transformation, say \( C_p \), in \( J_p \), taking \( T \) into a form,

\[
Q_a = \begin{pmatrix} Q_{a0} & 0 \\ 0 & q_a \end{pmatrix},
\]

where \( Q_{a0} \) is an \( n-1 \) by \( n-1 \) matrix in \( J_p \) and \( q_a \) is a scalar in \( J_p \).

If \( p \) is even, we use the results of §1 to obtain a canonical form in \( J_2 \) for \( T \) in \( J_2 \). The first possibility mentioned there, (1), gives us the same kind of form \( Q_a \) that we have just indicated for an odd \( p \), and we handle (1) exactly as the case for \( p \) odd. To treat (2), we proceed with an induction proof, assuming the theorem for \( n - 2 \) and proving it for \( n \). We rely here upon the fact that the lemma has been proved for both \( n = 1 \) and \( n = 2 \). For the third possibility, we may surely make an induction proof, for which, at each stage of the induction, either the treatment for (1) or that for (2) will be suitable.

We consider now the proof for (2), wherein the theorem is assumed true for \( n - 2 \) and is to be proved for \( n \). From the previous discussion we know there exists a unimodular transformation, \( C_2 \), in \( J_2 \), taking \( T \) into a form \( Q_6 \) which is schematically either

\[
\begin{align*}
\text{(i)} & \quad 2^k \begin{pmatrix} Q_{60}/2^k & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix} \\
\text{(ii)} & \quad 2^k \begin{pmatrix} Q_{60}/2^k & 0 \\ 0 & 2 & 5 \\ 0 & 5 & 12 \end{pmatrix},
\end{align*}
\]

where \( Q_{60} \) is an \( n-2 \) by \( n-2 \) matrix in \( J_2 \) and \( k \) is a non-negative, rational integer. Form (ii) follows directly from (1.1), since the unimodular matrix

\[
\begin{pmatrix} 3 & -2 \\ -1 & 1 \end{pmatrix}
\]

For a proof of this theorem, see, for example, C. L. Siegel [6, p. 535]. In the statement of Siegel’s lemma, \( R_p \) should be replaced by \( G_p \).
We proceed now, regardless of the parity of \( p \). Let \( Q \) designate appropriately \( Q_a \) or \( Q_b \), \( Q_0 \) either \( Q_{a0} \) or \( Q_{b0} \), and \( q \) the appropriate one of \( q_a \), \( 2^k \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \), and \( 2^k \begin{pmatrix} 2 & 5 \\ 5 & 12 \end{pmatrix} \).

We now define \( V = BC_p \) and \( V_p = B_p C_p \), noting that \( V'SV = V'_p S V_p = Q \). If we partition \( V \) and \( V_p \) into \( V = (U, u) \) and \( V_p = (W, w) \), where \( u \) and \( w \) each designate a unicolumnar matrix in case \( q \) is a scalar and each a duocolumnar matrix in case \( q \) is a 2 by 2 matrix, we see readily that \( U'SU = W'SW = Q_0 \), that \( U'Su = W'Sw = 0 \) and that \( u'Su = w'Sw = q \).

Then by the hypothesis of our induction, with \( B \) replaced by \( U \), \( B_p \) by \( W \), and \( T \) by \( Q_0 \), we see that there exists an automorph, say \( H \), in \( J_p \) of \( Q_0 \), such that for \( \tilde{W} = WH \), it is true that

\[
| U'S\tilde{W} - Q_0 | \neq 0. \tag{2.2}
\]

We take \( \tilde{w} = wL \), where \( L \) is an automorph of \( q \) in \( J \) to be chosen later, and \( \tilde{V}_p = (\tilde{W}, \tilde{w}) \). Then \( \tilde{W}'Sw = 0 \) implies \( H'\tilde{W}'SwL = 0 \); that is, \( \tilde{W}'S\tilde{w} = 0 \). Thus, since surely \( \tilde{W}'S\tilde{W} = H'Q_0H = Q_0 \) and \( \tilde{w}'\tilde{w} = q \), we have \( \tilde{V}_p'S\tilde{V}_p = Q_0 \). Now, schematically,

\[
| \tilde{V}'S\tilde{V}_p - Q | = \left| \begin{pmatrix} U' \\ w' \end{pmatrix} S(\tilde{W}, \tilde{w}) - Q \right|
\]

\[
= \begin{vmatrix} U'S\tilde{W} - Q_0 & U'S\tilde{w} \\ w'S\tilde{W} & w'S\tilde{w} - q \end{vmatrix}.
\tag{2.3}
\]

If \( q \) is of form \( q_a \), we take \( L \) successively equal to +1 and -1. Thus we first assume \( \tilde{w} = w \), whence expansion of the above determinant, (2.3), by the last column will give us

\[
(u'Sw - q) | U'S\tilde{W} - Q_0 | + K,
\]

where \( K \) is a linear combination of the elements of \( w \). If, on the other hand, we assume that \( \tilde{w} = -w \), we see that the above determinant becomes

\[
(- u'Sw - q) | U'S\tilde{W} - Q_0 | - K.
\]

The sum of these two determinants is \( -2q | U'S\tilde{W} - Q_0 | \), which is
nonzero, since the nonsingularity of $T$ implies $q \neq 0$ and (2.2) tells us that $|U'S\tilde{W} - Q_0| \neq 0$. Thus, at least one of the two determinants is different from zero.

If $q$ is of form (i), namely,

$$2^k \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix},$$

we take $L$ successively equal to

(a) \[ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \]

(b) \[ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \]

(c) \[ \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \]

and

(d) \[ \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}. \]

If $q$ is of form (ii), namely,

$$2^k \begin{pmatrix} 2 & 5 \\ 5 & 12 \end{pmatrix},$$

we take $L$ successively equal to

(a') \[ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \]

(b') \[ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \]

(c') \[ \begin{pmatrix} 1 & 5 \\ 0 & -1 \end{pmatrix}, \]

and

(d') \[ \begin{pmatrix} -1 & -5 \\ 0 & 1 \end{pmatrix}. \]

That the $L$'s are indeed automorphs of the respective $q$'s may be verified directly.

If we add the determinants, obtained from (2.3), for the values of $L$ given by (a), (b), (c), and (d), we find their sum is $3 \cdot 2^{3k+2} |U'S\tilde{W} - Q_0|$. If we add the determinants, obtained from (2.3), for the values of $L$ given by (a'), (b'), (c'), and (d'), we find their sum is $-2^{3k+2} |U'S\tilde{W} - Q_0|$. From (2.2), $|U'S\tilde{W} - Q_0| \neq 0$, so that at least one of the determinants in the first sum and one of the determinants in the second sum are different from zero.

We have thus shown that in case $q$ is of the form

$$q_a, \quad 2^k \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \quad \text{or} \quad 2^k \begin{pmatrix} 2 & 5 \\ 5 & 12 \end{pmatrix},$$

we may choose $\tilde{w}$ appropriately so that

(2.4) \[ |V'S\tilde{\nu}_p - Q| \neq 0. \]
Now

\[ \tilde{V}_p = (W, w) \begin{pmatrix} H & 0 \\ 0 & L \end{pmatrix}, \]

or denoting

\[
\begin{pmatrix} H & 0 \\ 0 & L \end{pmatrix}
\]

by \( D \), we have \( \tilde{V}_p = V_p D \), where \( D \) is an obvious automorph of \( Q \) in \( J_p \).

We then have

(2.5) \[ V'S\tilde{V}_p - Q = V'SV_pD - Q = C_p'B'SB_pC_pD - Q. \]

Multiplying (2.5) on the left by \((C_p')^{-1}\) and on the right by \( C_p^{-1} \), and using (2.4), we have

\[ |B'SB_p(C_pDC_p^{-1}) - T| \not= 0. \]

Noting that \( C_pDC_p^{-1} \) is an automorph of \( T \) in \( J_p \), we define \( B_p = B_p(C_pDC_p^{-1}) \), and this completes the basis for our induction.

3. Proof of the theorem. To prove the theorem, we shall use Lemmas 4 and 6, as well as the theorem of Hasse, referred to in the introduction. We proceed with the proof.

Since the hypotheses of the theorem satisfy the conditions of Hasse's theorem, there exists a rational transformation, say \( B \), taking \( S \) into \( T \). Since \( T \) in \( J \) is in each \( J_p \), Lemma 6 is applicable, so that there is a \( S_p \) in each \( J_p \), such that \( B_pS_p = T \) and

(3.1) \[ |B'SB_p - T| \not= 0. \]

Now let \( q \) be any given, positive, rational integer and \( p \) a prime factor of \( q \). Then using Lemma 4, by virtue of (3.1), we see that for each \( p \), there exists a skew-symmetric matrix \( N_p \) in \( R_p \) and a matrix \( M_p \) in \( R_p \) such that

(3.2) \[ B_p = B + 2M_p(N_p - M_p'SM_p)^{-1}M_p'SB. \]

If \( \beta \) is an arbitrarily large rational integer, by the Chinese Remainder Theorem, we can find a matrix \( M \) in \( R \), satisfying the congruence \( M \equiv M_p \) (mod \( p^\beta \)), for all prime factors \( p \) of \( q \), and a skew-symmetric matrix \( N \) in \( R \), satisfying the congruence \( N \equiv N_p \) (mod \( p^\beta \)).

Now Lemma 4 implies the existence of \((N_p - M_p'SM_p)^{-1}\) for each \( p \); hence, \(|N_p - M_p'SM_p| \not= 0\). We then have, for \( \beta \) sufficiently large,
\[ |N - M'SM| = |N_p - M'_pSM_p| \not\equiv 0 \pmod{p^q} \]

for any \( p \). Thus, \( |N - M'SM| \not\equiv 0 \).

Now we define a matrix \( \tilde{B} \) in \( R \),

\[(3.3) \quad \tilde{B} = B + 2M(N - M'SM)^{-1}M'SB.\]

Since \( \tilde{B}_p \) has \( p \)-adic integers as elements, then, by virtue of (3.2) and (3.3), for \( \beta \) sufficiently large, \( \tilde{B} \) is \( p \)-adically integral for all prime factors \( p \) of \( q \). This means that the denominators of the elements of \( \tilde{B} \) are relatively prime to \( q \). Finally, if we use (3.3) in Lemma 4, we see that \( \tilde{B} \) takes \( S \) into \( T \).

4. An application of the theorem. We now prove an immediate corollary of the theorem.

**Corollary.** If \( S \) and \( T \) are symmetric, nonsingular matrices in \( J \), of orders \( m \) and \( n \), respectively, and if there exist transformations in all \( J_p \) and in \( R_n \), taking \( S \) into \( T \), then there exists a rational integer \( q \), prime to any given rational integer \( r \), such that there is a transformation in \( J \) taking \( S \) into \( q^2T \).

Let \( r \) be given. Then, according to the theorem, \( S \) may be taken into \( T \) by a transformation, \( B \), in \( R \), the denominators of the elements of which are relatively prime to \( r \). If we denote the least common multiple of the denominators of the elements of \( B \) by \( q \), then \( (q, r) = 1 \), and

\[ B'SB = T, \quad qB'SqB = q^2T. \]

Surely \( qB \) is in \( J \).

**References**


Temple University