AN EXTENSION OF A THEOREM OF WITT

BURTON W. JONES

1. **Introduction.** If $\mathfrak{u}_1, \cdots, \mathfrak{u}_n$ is a set of vectors such that $\mathfrak{u}_i\mathfrak{u}_j = \mathfrak{u}_j\mathfrak{u}_i$ are numbers of a field K for $i, j = 1, 2, \cdots, n$, all linear combinations of these vectors with coefficients in K constitute a *vector space*

$$\mathfrak{S} = \langle \mathfrak{u}_1, \cdots, \mathfrak{u}_n \rangle$$

over K and the symmetric matrix $\mathfrak{A} = (\mathfrak{u}_i\mathfrak{u}_j) = (a_{ij})$ is the *multiplication table* for the *basis* $\mathfrak{u}_1, \cdots, \mathfrak{u}_n$. The inner product of two vectors $\sum x_i\mathfrak{u}_i$ and $\sum y_i\mathfrak{u}_i$ is the bilinear form

$$\sum (\mathfrak{u}_i\mathfrak{u}_j)x_iy_j = \sum a_{ij}x_iy_j$$

and the *norm* of a vector is the inner product of a vector and itself; it can be expressed as a quadratic form.

If $\mathfrak{C}$ is a nonsingular transformation with coefficients in K and $(\mathfrak{u}_1, \cdots, \mathfrak{u}_n)\mathfrak{C} = (\mathfrak{v}_1, \cdots, \mathfrak{v}_n)$, the $\mathfrak{v}$'s will constitute a new basis of the same space $\mathfrak{S}$ and the multiplication table for the new matrix is $\mathfrak{C}'\mathfrak{A}\mathfrak{C}$. This has the same effect on the matrix of the quadratic form $\sum a_{ij}x_ix_j$ as the transformation $(x_1, \cdots, x_n)' = \mathfrak{C}(y_1, \cdots, y_n)'$. The quadratic forms f_1 and f_2 are *equivalent* (in K) if one may be taken into the other by a nonsingular transformation with coefficients in K. Then the corresponding vector spaces are said to be *equivalent* (in K). We write $f_1 \cong f_2$ and $\mathfrak{S}_1 \cong \mathfrak{S}_2$.

It should be noted, in passing, that two vector spaces may be equivalent without being identical. For example, if $n = 3$ and

$$\mathfrak{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

it is true that $\langle \mathfrak{u}_1, \mathfrak{u}_2 \rangle \cong \langle \mathfrak{u}_2, \mathfrak{u}_3 \rangle$. However, an isomorphism may be established between two sets of vectors having the same multiplication table.

Two vectors $\mathfrak{u}$ and $\mathfrak{v}$ are *orthogonal* if $\mathfrak{u}\mathfrak{v} = 0$. Two vector spaces are orthogonal if every vector of one is orthogonal to every vector of the other. Two subspaces, $\mathfrak{S}_1$ and $\mathfrak{S}_2$, of $\mathfrak{S}$ are *complementary* if every vector of $\mathfrak{S}$ is the sum of a vector of $\mathfrak{S}_1$ and a vector of $\mathfrak{S}_2$. If $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are complementary orthogonal subspaces of $\mathfrak{S}$ we write

Presented to the Society, September 5, 1941; received by the editors April 17, 1941.

$\mathfrak{S} = \mathfrak{S}_1 + \mathfrak{S}_2$. This is a direct sum if $\mathfrak{S}$ has no *radical*, that is, if its multiplication table is nonsingular.

Ernst Witt[1] proved a theorem which we shall state in two different ways. K is a field of characteristic not equal to 2 and the spaces have no radicals.

THEOREM A. *If $\mathfrak{S}_1$, $\mathfrak{S}_2$ and $\mathfrak{S}_3$ are vector spaces over K and $\mathfrak{S}_2$ and $\mathfrak{S}_3$ are orthogonal to $\mathfrak{S}_1$, then $\mathfrak{S}_1 + \mathfrak{S}_2 \cong \mathfrak{S}_1 + \mathfrak{S}_3$ implies $\mathfrak{S}_2 \cong \mathfrak{S}_3$.*

THEOREM B. *If f is a quadratic form in $x_1, \cdots, x_r$ and g and h are quadratic forms in $x_{r+1}, \cdots, x_n$ (with coefficients in K) then $f+g \cong f+h$ implies $g \cong h$.*

If the field K is replaced by a ring R we may make definitions analogous to those above. The vector space then becomes a vector lattice, $\mathfrak{L}$ (in the old-fashioned sense), and the transformations $\mathfrak{C}$ of the bases must, together with their inverses, have elements in the ring. Witt's restriction of convenience that the space shall have no radical is not necessary here except that *any result stated in terms of quadratic forms assumes that the forms are not equivalent to forms of fewer variables.*

This paper proves that Witt's result also holds for vector lattices over any ring of p-adic integers for which p is odd. We shall call such a ring an *odd p-adic integer ring* and denote it by R_p. The case $p=2$ presents difficulties all its own which we hope to resolve in a later paper. The completion of such a result would establish the theorem that if f is a quadratic form in $x_1, \cdots, x_r$ and g and h quadratic forms in $x_{r+1}, \cdots, x_n$, then $f+g$ and $f+h$ are of the same genus if and only if g and h are.

The machinery which Witt set up for fields breaks down completely in at least two essential points when applied to R_p. Hence our Lemmas 3 and 4 have no analogues in Witt's theory.

It will be recalled that if a, b and c are integers in a p-adic field, $a \equiv b \pmod{c}$ means that $(a-b)/c$ is a p-adic integer; in other words, the highest power of p dividing c is a divisor of the highest power of p dividing $a-b$. Also it is true that if a and b are p-adic integers and if for q an arbitrary power of p there is a p-adic integer x such that $ax \equiv b \pmod{q}$ then there is a p-adic integer x such that $ax = b$. When we say that a set of vectors are *linearly independent* or *dependent* we mean independence or dependence (mod p).

It was surmised by a referee and has been established by the author that with only trivial and obvious modifications the lemmas and *final*

[1] *Theorie der quadratischen Formen in beliebigen Körpern*, Journal für die reine und angewandte Mathematik, vol. 176 (1937), pp. 31–48.

result of this paper hold equally well for vector lattices over any ring of $\mathfrak{P}$-adic integers when $\mathfrak{P}$ is any ideal prime to 2 in a field of algebraic numbers. The multiplication tables (that is, the matrices of the quadratic forms) as well as the transformations of bases and their inverses will have, of course, integers of the ring as elements.

2. **Lemmas.** We now prove the following lemmas:

LEMMA 1. *Let an n-dimensional lattice $\mathfrak{L}$ with coefficients in a p-adic integer ring be defined by the vectors $\mathfrak{u}_1, \cdots, \mathfrak{u}_n$, let $\mathfrak{v}_1, \cdots, \mathfrak{v}_r$ be r linearly independent* (mod p) *vectors of this lattice. Then there exist vectors $\mathfrak{v}_{r+1}, \cdots, \mathfrak{v}_n$ defining a complementary orthogonal lattice to $\langle \mathfrak{v}_1, \cdots, \mathfrak{v}_r\rangle$ in $\mathfrak{L}$ if and only if the highest power of p dividing the determinant of the first r columns of matrix $\mathfrak{A}$ (or $\mathfrak{B}$) below is a divisor of the* g.c.d. *of all determinants formed by replacing one of the first r columns by one of the last n.*

$$\mathfrak{A} = \begin{pmatrix} \mathfrak{v}_1^2 & \cdots & \mathfrak{v}_1\mathfrak{v}_r & \mathfrak{v}_1\mathfrak{u}_1 & \cdots & \mathfrak{v}_1\mathfrak{u}_n \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ \mathfrak{v}_r\mathfrak{v}_1 & \cdots & \mathfrak{v}_r^2 & \mathfrak{v}_r\mathfrak{u}_1 & \cdots & \mathfrak{v}_r\mathfrak{u}_n \end{pmatrix},$$

$$\mathfrak{B} = \begin{pmatrix} \mathfrak{v}_1^2 & \cdots & \mathfrak{v}_1\mathfrak{v}_r & \mathfrak{v}_1\overset{0}{\mathfrak{v}}_{r+1} & \cdots & \mathfrak{v}_1\overset{0}{\mathfrak{v}}_n \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ \mathfrak{v}_r\mathfrak{v}_1 & \cdots & \mathfrak{v}_r^2 & \mathfrak{v}_r\overset{0}{\mathfrak{v}}_{r+1} & \cdots & \mathfrak{v}_r\overset{0}{\mathfrak{v}}_n \end{pmatrix}$$

where $\mathfrak{v}_{r+1}^0, \cdots, \mathfrak{v}_n^0$ define a complementary (*not necessarily orthogonal*) *space to $\langle \mathfrak{v}_1, \cdots, \mathfrak{v}_r\rangle$ in $\mathfrak{L}$. For this lemma it is not necessary that p be odd.*

PROOF. First note that there is indeed a complementary lattice $\langle \mathfrak{v}_{r+1}^0, \cdots, \mathfrak{v}_n^0\rangle$. That one may use $\mathfrak{A}$ or $\mathfrak{B}$ follows from the fact that the last $n-r$ columns of the latter are linear combinations with coefficients in the ring of the last n columns of the former and the last n columns of the former are linear combinations of the n columns of the latter.

Set

$$\mathfrak{v}_k = \sum_{i=1}^{r} b_{ki}\mathfrak{v}_i + \overset{0}{\mathfrak{v}}_k, \qquad k = r+1, \cdots, n.$$

Then

$$\mathfrak{v}_k\mathfrak{v}_j = \sum_{i=1}^{r} b_{ki}\mathfrak{v}_i\mathfrak{v}_j + \mathfrak{v}_j\overset{0}{\mathfrak{v}}_k, \qquad j = 1, \cdots, r.$$

For any k we can choose r integers b_{ki} so that $\mathfrak{v}_k\mathfrak{v}_j=0$ for $j=1, \cdots, r$ if and only if the conditions of the theorem hold, using matrix $\mathfrak{B}$.

LEMMA 2. *Every n-dimensional lattice $\mathfrak{L}$ in a ring R_p of p-adic integers (p odd) has a basis* $\mathfrak{u}_1, \cdots, \mathfrak{u}_n$ *such that*

$$\mathfrak{L} = \langle \mathfrak{u}_1 \rangle + \cdots + \langle \mathfrak{u}_n \rangle.$$

This is a rather well known result.[2]

In the lemmas that follow, $\mathfrak{u}_1, \cdots, \mathfrak{u}_n$ is a canonical basis of a lattice $\mathfrak{L}$ over the p-adic integer ring, p odd, that is, $\mathfrak{L}=\langle \mathfrak{u}_1\rangle + \cdots + \langle \mathfrak{u}_n\rangle$. The c's are integers of the ring.

LEMMA 3. *If* $\mathfrak{v}=c_2\mathfrak{u}_2+\cdots+c_n\mathfrak{u}_n$ *and* $c_{i+1}\mathfrak{u}_{i+1}^2\equiv 0 \pmod{c_i\mathfrak{u}_i^2}$ *for* $i=2, 3, \cdots, n-1$, *there exists a* $\mathfrak{v}_0=c_{02}\mathfrak{u}_2+\cdots+c_{0n}\mathfrak{u}_n$ *such that* $\mathfrak{v}_0\mathfrak{v}=0$ *and* $\mathfrak{v}_0$ *has an orthogonal complementary space in* $\langle \mathfrak{u}_2, \cdots, \mathfrak{u}_n\rangle$ *unless for each k such that* $2\leqq k\leqq n-1$ *one of the following holds:*

1. $c_{k+1}\mathfrak{u}_{k+1}^2\equiv 0 \pmod{pc_k\mathfrak{u}_k^2}$ *and* $c_k\equiv 0 \pmod{pc_{k+1}}$. *This implies* $\mathfrak{u}_{k+1}^2\equiv 0 \pmod{p^2\mathfrak{u}_k^2}$.

2. $\mathfrak{u}_k^2/\mathfrak{u}_{k+1}^2$ *and* c_k/c_{k+1} *are units and*

$$1 + \frac{c_k^2\mathfrak{u}_k^2}{c_{k+1}^2\mathfrak{u}_{k+1}^2} \equiv 0 \pmod{p}.$$

Furthermore, such a $\mathfrak{v}_0$ *can be found if* 2 *holds for two successive values of k.*

PROOF. Throughout this proof it is understood that $2\leqq k\leqq n-1$. Choose $\mathfrak{v}_0=c\mathfrak{u}_k+\mathfrak{u}_{k+1}$. Using Lemma 1, we seek to determine c so that (1) $\mathfrak{v}_0\mathfrak{v}=cc_k\mathfrak{u}_k^2+c_{k+1}\mathfrak{u}_{k+1}^2=0$ and (2) $\mathfrak{v}_0\mathfrak{u}_{k+1}=\mathfrak{u}_{k+1}^2$ and $\mathfrak{v}_0\mathfrak{u}_k=c\mathfrak{u}_k^2$ are $\equiv 0 \pmod{\mathfrak{v}_0^2}$ where $\mathfrak{v}_0^2=\mathfrak{u}_{k+1}^2+c^2\mathfrak{u}_k^2$.

1. Suppose $c_{k+1}\mathfrak{u}_{k+1}^2\equiv 0 \pmod{pc_k\mathfrak{u}_k^2}$ and $c_{k+1}\equiv 0 \pmod{c_k}$. Choose c so that (1) holds and have

$$c^2\mathfrak{u}_k^2 = \frac{c_{k+1}}{c_k}\,\frac{c_{k+1}\mathfrak{u}_{k+1}^2}{c_k\mathfrak{u}_k^2}\,\mathfrak{u}_{k+1}^2 \equiv 0 \pmod{p\mathfrak{u}_{k+1}^2}$$

which implies $\mathfrak{v}_0^2\not\equiv 0 \pmod{p\mathfrak{u}_{k+1}^2}$. Also $c\mathfrak{u}_k^2=-c_{k+1}\mathfrak{u}_{k+1}^2/c_k\equiv 0 \pmod{\mathfrak{u}_{k+1}^2}$ and hence condition (2) holds.

2. Suppose $c_{k+1}\mathfrak{u}_{k+1}^2/(c_k\mathfrak{u}_k^2)$ is a unit. Choose c so that (1) holds and

---

[2] See, for example, Lemma 8 of C. L. Siegel's *Über die analytische Theorie der quadratischen Formen*, Annals of Mathematics, (2), vol. 36 (1935), pp. 527–606. In the statement of this lemma there is a misprint. R_p should be replaced by G_p. The corresponding theorem for $\mathfrak{P}$-adic integers is in the third paper of the same series, Annals of Mathematics, (2), vol. 38 (1937), p. 240.

see that c is a unit. If $\mathfrak{u}_k^2 \equiv 0 \pmod{p\mathfrak{u}_{k+1}^2}$ or $\mathfrak{u}_{k+1}^2 \equiv 0 \pmod{p\mathfrak{u}_k^2}$, (2) is seen to hold. We then have difficulty only if the first two parts of Condition 2 of the theorem hold and if in addition $\mathfrak{u}_{k+1}^2 + c^2\mathfrak{u}_k^2 \equiv 0 \pmod{p\mathfrak{u}_k^2}$. Then (1) implies

$$c^2\mathfrak{u}_k^2 = \frac{c_{k+1}^2\mathfrak{u}_{k+1}^4}{c_k^2\mathfrak{u}_k^2}$$

and thus

$$1 + \frac{c_{k+1}^2\mathfrak{u}_{k+1}^2}{c_k^2\mathfrak{u}_k^2} \equiv 0 \pmod{p}.$$

For the final remark notice that

$$1 + \frac{c_k^2\mathfrak{u}_k^2}{c_{k+1}^2\mathfrak{u}_{k+1}^2} \equiv 1 + \frac{c_{k+1}^2\mathfrak{u}_{k+1}^2}{c_{k+2}^2\mathfrak{u}_{k+2}^2} \equiv 0 \pmod{p}$$

implies

$$1 - \frac{c_k^2\mathfrak{u}_k^2}{c_{k+2}^2\mathfrak{u}_{k+2}^2} \equiv 0 \pmod{p},$$

and replace $\mathfrak{u}_{k+1}$ by $\mathfrak{u}_{k+2}$ to have the existence of $\mathfrak{v}_0$.

Remark. Condition 1 of the above lemma may be weakened but only by making the statement more complex and less manageable. That there is not always a $\mathfrak{v}_0$ orthogonal to $\mathfrak{v}$ and having a complementary orthogonal space is shown by the following example:

Let $\mathfrak{u}_2^2 = 1$, $\mathfrak{u}_3^2 = p^2$ and $\mathfrak{v} = p\mathfrak{u}_2 + \mathfrak{u}_3$. We show that no $\mathfrak{v}_0 = b_2\mathfrak{u}_2 + b_3\mathfrak{u}_3$ exists for which $\mathfrak{v}_0\mathfrak{v} = 0$ and which has an orthogonal complementary lattice in $\langle \mathfrak{u}_2, \mathfrak{u}_3 \rangle$. Now $\mathfrak{v}_0\mathfrak{v} = 0$ implies $b_2 = -pb_3$ and since $\mathfrak{v}_0$ can have a complementary orthogonal lattice only if b_3 is prime to p, we take $b_3 = 1$ and have $\mathfrak{v}_0 = -p\mathfrak{u}_2 + \mathfrak{u}_3$. Now $(g_1\mathfrak{u}_2 + g_2\mathfrak{u}_3)\mathfrak{v}_0 = -g_1p + g_2p^2 = 0$ implies $g_1 \equiv 0 \pmod{p}$. Hence

$$\begin{vmatrix} -p & 1 \\ g_1 & g_2 \end{vmatrix} \equiv 0 \pmod{p}$$

and $\mathfrak{v}_0$ has no complementary orthogonal lattice.

Lemma 4. *If $\langle \mathfrak{v}_1, \cdots, \mathfrak{v}_n \rangle \cong \langle \mathfrak{u}_1, \cdots, \mathfrak{u}_n \rangle$ are two canonical lattices with $\mathfrak{v}_1^2 = \mathfrak{u}_1^2$ and*

$$\mathfrak{v}_1 = c_1\mathfrak{u}_1 + c_2\mathfrak{u}_2 + \cdots + c_n\mathfrak{u}_n$$

while $\mathfrak{v}_1 - c_1\mathfrak{u}$, *has the property that, for each* k *for which* $2 \leqq k \leqq n-1$, *either* 1 *or* 2 *of Lemma* 3 *holds and if* 2 *does not hold for two successive values of* k, *then*

$$\langle \mathfrak{v}_2, \cdots, \mathfrak{v}_n \rangle \cong \langle \mathfrak{u}_2, \cdots, \mathfrak{u}_n \rangle.$$

PROOF. The lemma is obvious if $n=2$. Henceforth assume $n \geqq 3$. By renumbering $\mathfrak{u}_2, \cdots, \mathfrak{u}_n$, if necessary, we can have $c_{i+1}\mathfrak{u}_{i+1}^2 \equiv 0 \pmod{c_i\mathfrak{u}_i^2}$ for $i=2, \cdots, n-1$ as in Lemma 3.

We may write $\mathfrak{v}_i = \sum_{j=1}^n c_{ij}\mathfrak{u}_j$ where $c_{1j}=c_j$ and the determinant of the coefficients is prime to p. Write

$$A_i = \begin{vmatrix} c_{11} & \cdots & c_{1i} \\ \cdot & \cdots & \cdot \\ c_{i1} & \cdots & c_{ii} \end{vmatrix}.$$

We know $A_n \not\equiv 0 \pmod p$. Assume (what we shall soon prove) that $c_1 = c_{11} \not\equiv 0 \pmod p$. We now show that we may renumber $\mathfrak{v}_2, \cdots, \mathfrak{v}_n$, if necessary, to make $A_i \not\equiv 0 \pmod p$ for $2 \leqq i \leqq n$. Assume $A_{i-1} \not\equiv 0 \pmod p$; the Laplace expansion of A_n shows that the matrix $\mathfrak{M}_i$ composed of the first i columns of A_n is of rank i. The first $i-1$ rows of $\mathfrak{M}_i$ are linearly independent and not all the remaining $n-i+1$ rows of $\mathfrak{M}_i$ are linearly dependent on them.

Notice that $\mathfrak{v}_i\mathfrak{v}_j = c_{i1}c_{j1}\mathfrak{u}_1^2 + \cdots + c_{in}c_{jn}\mathfrak{u}_n^2$ and $\mathfrak{v}_i\mathfrak{v}_j = 0$ if $i \neq j$.

We next proceed to prove some preliminary results.

I. $c_2\mathfrak{u}_2^2 \equiv 0 \pmod{c_1\mathfrak{u}_1^2}$. Suppose the contrary were the case, that is, $c_1\mathfrak{u}_1^2 \equiv 0 \pmod{pc_2\mathfrak{u}_2^2}$. We have, by Lemma 3, two cases to consider.

Case 1. If $c_i\mathfrak{u}_i^2 \equiv 0 \pmod{pc_2\mathfrak{u}_2^2}$ and $c_2 \equiv 0 \pmod{pc_i}$ for all $i>2$, then $\mathfrak{v}_1\mathfrak{v}_i = 0$ implies $c_{i2}c_2\mathfrak{u}_2^2 \equiv 0 \pmod{pc_2\mathfrak{u}_2^2}$ and hence $c_{i2} \equiv 0 \pmod p$ for $i>1$. Since if $n \geqq 3$, $c_2 \equiv 0 \pmod p$; and hence $A_n \equiv 0 \pmod p$, which is false.

Case 2. If $c_i\mathfrak{u}_i^2 \equiv 0 \pmod{pc_2\mathfrak{u}_2^2}$ and $c_2 \equiv 0 \pmod{pc_i}$ for $i>3$ while Condition 2 of Lemma 3 holds for $k=2$, then $\mathfrak{v}_1\mathfrak{v}_i = 0$ implies $c_{i2}c_2\mathfrak{u}_2^2 + c_{i3}c_3\mathfrak{u}_3^2 \equiv 0 \pmod{pc_2\mathfrak{u}_2^2}$ (for $i=1$, Condition 2 of Lemma 3 implies the congruence). Hence $A_n \equiv 0 \pmod p$, contrary to fact.

II. $c_1 = c_{11} \not\equiv 0 \pmod p$. (This shows $A_i \not\equiv 0 \pmod p$, $i=1, \cdots, n$.) We know $\mathfrak{v}_1^2 - c_1^2\mathfrak{u}_1^2 \equiv 0 \pmod{c_2\mathfrak{u}_2^2}$. Hence $\mathfrak{v}_1^2 - c_1^2\mathfrak{u}_1^2 = \mathfrak{u}_1^2 - c_1^2\mathfrak{u}_1^2 \equiv 0 \pmod{c_1\mathfrak{u}_1^2}$ and $\mathfrak{u}_1^2 \equiv 0 \pmod{c_1\mathfrak{u}_1^2}$.

III. For $k>r \geqq 1$ it is true that

$$c_{k1}\mathfrak{u}_1^2 \equiv \cdots \equiv c_{kr}\mathfrak{u}_r^2 \equiv 0 \pmod{\mathfrak{u}_{r+1}^2}.$$

If $r \geqq 2$ we know that in all cases of the previous lemma $\mathfrak{u}_{r+1}^2 \equiv 0 \pmod{\mathfrak{u}_r^2}$. Hence for $r \geqq 1$ we have for each $k>r$,

$$\mathfrak{v}_k\mathfrak{v}_j \equiv c_{k1}c_{j1}\mathfrak{u}_1^2 + \cdots + c_{kr}c_{jr}\mathfrak{u}_r^2 \equiv 0 \pmod{\mathfrak{u}_{r+1}^2} \qquad \text{for } j = 1, \cdots, r,$$

and since $A_r \not\equiv 0 \pmod{p}$ we have the desired result.

IV. If $\mathfrak{u}_{r+1}^2 \equiv 0 \pmod{p\mathfrak{u}_r^2}$ then $\mathfrak{u}_{r+1}^2 \equiv 0 \pmod{p\mathfrak{u}_i^2}$ for $2 \leqq i \leqq r$ and III implies

$$c_{k2} \equiv \cdots \equiv c_{kr} \equiv 0 \pmod{p} \qquad \text{for each } k > r.$$

V. $c_{k1} \equiv 0 \pmod{p}$ for all $k > 2$ or > 3 according as $\mathfrak{u}_3^2 \equiv 0 \pmod{p\mathfrak{u}_2^2}$ or not. A glance at Lemma 3 shows

$$\mathfrak{v}_k\mathfrak{v}_1 \equiv c_{k1}c_1\mathfrak{u}_1^2 + c_{k2}c_2\mathfrak{u}_2^2 + c_{k3}c_3\mathfrak{u}_3^2 \equiv 0 \pmod{pc_2\mathfrak{u}_2^2}.$$

If $\mathfrak{u}_3^2 \equiv 0 \pmod{p\mathfrak{u}_2^2}$ then $c_3\mathfrak{u}_3^2 \equiv 0 \pmod{pc_2\mathfrak{u}_2^2}$ and IV shows c_{k2}, and hence by I, c_{k1} are congruent to 0 (mod p) for $k > 2$. Otherwise $\mathfrak{u}_4^2 \equiv 0 \pmod{p\mathfrak{u}_3^2}$ while $\mathfrak{u}_3^2/\mathfrak{u}_2^2$ and c_3/c_2 are units; then IV implies c_{k2} and c_{k3} and hence c_{k1} are congruent to 0 (mod p) for $k > 3$. This also holds for all $k \geqq 2$, if perchance $c_2\mathfrak{u}_2^2 \equiv 0 \pmod{p\mathfrak{u}_1^2}$.

We now have two cases to consider corresponding to the two cases of Lemma 3. In what follows i is some fixed one of $2, 3, \cdots, n$. In the first place we assume that either $i = 2$ and Case 1 holds for $k = 2$, or $i > 2$ and Case 1 holds for $k = i$ and $k = i - 1$; we then show that $\langle \mathfrak{v}_i \rangle \cong \langle \mathfrak{u}_i \rangle$. In the second place we assume that Case 2 holds for $k = i$; then, with one exception which is dealt with separately, we show that $\langle \mathfrak{v}_i, \mathfrak{v}_{i+1} \rangle \cong \langle \mathfrak{u}_i, \mathfrak{u}_{i+1} \rangle$.

Case 1. Suppose $c_{i+j}\mathfrak{u}_{i+j}^2 \equiv 0 \pmod{pc_i\mathfrak{u}_i^2}$, $c_i \equiv 0 \pmod{pc_{i+j}}$ and $\mathfrak{u}_{i+j}^2 \equiv 0 \pmod{p\mathfrak{u}_i^2}$ for all j for which $1 \leqq j \leqq n - i$, while $c_i\mathfrak{u}_i^2 \equiv 0 \pmod{pc_{i-j}\mathfrak{u}_{i-j}^2}$, $c_{i-j} \equiv 0 \pmod{pc_i}$ and $\mathfrak{u}_i^2 \equiv 0 \pmod{p\mathfrak{u}_{i-j}^2}$ for all j for which $i - 2 \geqq j \geqq 1$. If $i > 2$ take $r = i - 1$ and $k = i$, in IV above and have $c_{i2} \equiv \cdots \equiv c_{ii-1} \equiv 0 \pmod{p}$ and V shows that $c_{i1} \equiv 0 \pmod{p}$. Hence $A_i \not\equiv 0 \pmod{p}$ implies $c_{ii} \not\equiv 0 \pmod{p}$. If $i = 2$, $n \geqq 3$ implies $c_2 \equiv 0 \pmod{p}$ and $A_2 \not\equiv 0 \pmod{p}$ implies $c_{22} \not\equiv 0 \pmod{p}$. Hence in both cases $c_{ii} \not\equiv 0 \pmod{p}$.

In III above put $r = i - 1$, $k = i$ and have

$$c_{i1}\mathfrak{u}_1^2 \equiv \cdots \equiv c_{ii-1}\mathfrak{u}_{i-1}^2 \equiv 0 \pmod{\mathfrak{u}_i^2}.$$

But $\mathfrak{v}_i^2 \equiv c_{i1}(c_{i1}\mathfrak{u}_1^2) + \cdots + c_{ii}(c_{ii}\mathfrak{u}_i^2) \pmod{p\mathfrak{u}_i^2}$ and hence we have shown $\mathfrak{v}_i^2 \equiv 0 \pmod{\mathfrak{u}_i^2}$. If $i > 2$ we have shown above that $c_{i1} \equiv \cdots \equiv c_{ii-1} \equiv 0 \pmod{p}$ and hence $\mathfrak{v}_i^2 \equiv c_{ii}^2\mathfrak{u}_i^2 \pmod{p\mathfrak{u}_i^2}$. If $i = 2$, $\mathfrak{v}_1\mathfrak{v}_2 \equiv c_1c_{21}\mathfrak{u}_1^2 + c_2c_{22}\mathfrak{u}_2^2 \equiv 0 \pmod{pc_2\mathfrak{u}_2^2}$ and $c_1 \not\equiv 0 \pmod{p}$ implies $c_{21} \equiv -c_2c_{22}\mathfrak{u}_2^2/(c_1\mathfrak{u}_1^2) \pmod{pc_2\mathfrak{u}_2^2/\mathfrak{u}_1^2}$. Hence

$$c_{21}^2\mathfrak{u}_1^2 \equiv c_2\frac{c_2\mathfrak{u}_2^2}{c_1^2\mathfrak{u}_1^2}c_{22}^2\mathfrak{u}_2^2 \pmod{pc_2\mathfrak{u}_2^2}$$

and $c_2 \equiv 0 \pmod{p}$ shows $c_{21}^2 \mathfrak{u}_1^2 \equiv 0 \pmod{p\mathfrak{u}_2^2}$. In both cases, then, we have $\mathfrak{v}_i^2 \equiv c_{ii}^2 \mathfrak{u}_i^2 \pmod{p\mathfrak{u}_i^2}$ which implies $\mathfrak{v}_i^2 \equiv c_{ii}^2 \mathfrak{u}_i^2 \pmod{q}$ is solvable for q, an arbitrary power of p. Hence there exists a unit b in R_p such that $\mathfrak{v}_i^2 = b^2 \mathfrak{u}_i^2$.

Case 2. Suppose $3 \leqq i+1 \leqq n$, $\mathfrak{u}_i^2/\mathfrak{u}_{i+1}^2$ and c_i/c_{i+1} are units, $1 + c_i^2 \mathfrak{u}_i^2/(c_{i+1}^2 \mathfrak{u}_{i+1}^2) \equiv 0 \pmod{p}$, $c_{i+j}\mathfrak{u}_{i+j}^2 \equiv 0 \pmod{pc_i \mathfrak{u}_i^2}$, $c_i \equiv 0 \pmod{pc_{i+j}}$, $\mathfrak{u}_{i+j}^2 \equiv 0 \pmod{p\mathfrak{u}_i^2}$ for all j for which $n - i \geqq j \geqq 2$. Also $c_i \mathfrak{u}_i^2 \equiv 0 \pmod{pc_{i-j}\mathfrak{u}_{i-j}^2}$; $\mathfrak{u}_i^2 \equiv 0 \pmod{p\mathfrak{u}_{i-j}^2}$ for all j such that $1 \leqq j < i-1$. Recall I and II above.

Taking $r = i-1$ in IV and using V we have

$$c_{k1} \equiv \cdots \equiv c_{ki-1} \equiv 0 \pmod{p} \qquad \text{for } k = i,\ i+1 \text{ and } i > 2.$$

This with $A_{i+1} \not\equiv 0 \pmod{p}$ implies

$$B_i = \begin{vmatrix} c_{ii} & c_{ii+1} \\ c_{i+1i} & c_{i+1i+1} \end{vmatrix} \not\equiv 0 \pmod{p}.$$

The last holds even if $i = 2$ unless $n = 3$ and $c_2 \not\equiv 0 \pmod{p}$ since $n > 3$ implies $c_2 \equiv c_3 \equiv 0 \pmod{p}$. We postpone this exceptional case.

Take $r = i-1$ in III above and have

$$c_{k1}\mathfrak{u}_1^2 \equiv \cdots \equiv c_{ki-1}\mathfrak{u}_{i-1}^2 \equiv 0 \pmod{\mathfrak{u}_i^2} \qquad \text{for } k = i,\ i+1.$$

Now

$$\mathfrak{v}_k^2 \equiv c_{k1}(c_{k1}\mathfrak{u}_1^2) + \cdots + c_{ki+1}(c_{ki+1}\mathfrak{u}_{i+1}^2) \pmod{p\mathfrak{u}_i^2},$$

and

$$c_{k1} \equiv \cdots \equiv c_{ki-1} \equiv 0 \pmod{p} \qquad \text{for } k = i,\ i+1 \text{ and } i > 2$$

implies

$$\mathfrak{v}_i^2 \equiv c_{ii}(c_{ii}\mathfrak{u}_i^2) + c_{ii+1}(c_{ii+1}\mathfrak{u}_{i+1}^2) \pmod{p\mathfrak{u}_{i+1}^2},$$

$$\mathfrak{v}_{i+1}^2 \equiv c_{i+1i}(c_{i+1i}\mathfrak{u}_i^2) + c_{i+1\,i+1}(c_{i+1\,i+1}\mathfrak{u}_{i+1}^2) \pmod{p\mathfrak{u}_{i+1}^2},$$

$$\mathfrak{v}_i\mathfrak{v}_{i+1} \equiv c_{i+1i}(c_{ii}\mathfrak{u}_i^2) + c_{i+1\,i+1}(c_{i\,i+1}\mathfrak{u}_{i+1}^2) \equiv 0 \pmod{p\mathfrak{u}_{i+1}^2}.$$

The argument in Case 1 for $i = 2$ may be used here to show that the three congruences above hold even when $i = 2$ except in the case postponed above. In fact, if $\mathfrak{u}_2^2 \equiv 0 \pmod{p\mathfrak{u}_1^2}$, III implies $c_{21} \equiv c_{31} \equiv 0 \pmod{p}$, $B_2 \not\equiv 0 \pmod{p}$ and the argument used in Case 1 carries through to show that the three congruences hold. We thus postpone the case in which $n = 3$, $c_2 c_3 \not\equiv 0 \pmod{p}$ and $\mathfrak{u}_2^2/\mathfrak{u}_1^2$ is a unit.

Divide the three congruences by $\mathfrak{u}_i^2$; let $d = \mathfrak{u}_{i+1}^2/\mathfrak{u}_i^2$. The resulting situation is covered by the next lemma which shows that there are p-adic integers a, b, c, e such that $ae-bc$ is prime to p and

$$\mathfrak{v}_i^2 = (a\mathfrak{u}_i + b\mathfrak{u}_{i+1})^2, \qquad \mathfrak{v}_{i+1}^2 = (c\mathfrak{u}_i + e\mathfrak{u}_{i+1})^2,$$
$$(a\mathfrak{u}_i + b\mathfrak{u}_{i+1})(c\mathfrak{u}_i + e\mathfrak{u}_{i+1}) = 0.$$

Hence $\langle \mathfrak{v}_i, \mathfrak{v}_{i+1}\rangle \cong \langle \mathfrak{u}_i, \mathfrak{u}_{i+1}\rangle$.

It remains to consider the postponed case $n=3$, $c_2c_3 \not\equiv 0 \pmod p$ and $\mathfrak{u}_2^2/\mathfrak{u}_1^2$ is a unit. Then $c_2^2\mathfrak{u}_2^2 + c_3^2\mathfrak{u}_3^2 \equiv 0 \pmod{p\mathfrak{u}_1^2}$ implies that $\mathfrak{v}_1^2 \equiv c_1^2\mathfrak{u}_1^2 = 0 \pmod{p\mathfrak{u}_1^2}$ and hence $c_1 \equiv 0 \pmod p$, contrary to fact.

LEMMA 5. *If the congruences*

$$x^2 + dy^2 \equiv g_1 \pmod p, \quad z^2 + dt^2 \equiv g_2 \pmod p, \quad xz + dyt \equiv g_3 \pmod p,$$

with $d \not\equiv 0 \pmod p$, *have solutions* x_0, y_0, z_0, t_0 *with* $x_0t_0 - z_0y_0 \not\equiv 0 \pmod p$, *then there are p-adic integers* x, y, z, t *such that* $x^2+dy^2=g_1$, $z^2+dt^2=g_2$, $xz+dyt=g_3$ *and* $xt-zy\not\equiv 0 \pmod p$.

PROOF. To prove the lemma, assume that x_0, y_0, z_0, t_0 is a solution of the congruences with p replaced by q. We seek an x, y, z, t so that

$$\begin{aligned} (x_0 + qx)^2 + d(y_0 + qy)^2 &\equiv g_1 \pmod{pq}, \\ (z_0 + qz)^2 + d(t_0 + qt)^2 &\equiv g_2 \pmod{pq}, \\ (x_0 + qx)(z_0 + qz) + d(y_0 + qy)(t_0 + qt) &\equiv g_3 \pmod{pq}. \end{aligned}$$

That is,

$$\begin{aligned} x_0x + dy_0y &\equiv h_1 \pmod p, \\ z_0z + dt_0t &\equiv h_2 \pmod p, \\ x_0z + z_0x + d(y_0t + t_0y) &\equiv h_3 \pmod p, \end{aligned}$$

for some integers h_1, h_2 and h_3. The matrix of the coefficients on the left is

$$\begin{pmatrix} x_0 & dy_0 & 0 & 0 \\ 0 & 0 & z_0 & dt_0 \\ z_0 & dt_0 & x_0 & dy_0 \end{pmatrix}$$

which is of rank 3 (mod p).

3. **Final results.** We have the following theorems.

THEOREM 1. *If* $\langle \mathfrak{v}_1, \cdots, \mathfrak{v}_n\rangle$ *and* $\langle \mathfrak{u}_1, \cdots, \mathfrak{u}_n\rangle$ *are two equivalent lattices in a ring* R_p *of p-adic integers* (p *odd*) *and if* $\mathfrak{v}_1^2 = \mathfrak{u}_1^2 \neq 0$ *and* $\mathfrak{v}_1\mathfrak{v}_i = \mathfrak{u}_1\mathfrak{u}_i = 0$, $i \neq 1$, *then*

$$\langle \mathfrak{v}_2, \cdots, \mathfrak{v}_n \rangle \cong \langle \mathfrak{u}_2, \cdots, \mathfrak{u}_n \rangle.$$

PROOF. Assume the theorem true for all lesser values of n. Also, $\langle \mathfrak{v}_2, \cdots, \mathfrak{v}_n \rangle$ and $\langle \mathfrak{u}_2, \cdots, \mathfrak{u}_n \rangle$ may be considered to be in canonical form. Lemma 4 establishes the theorem unless Lemma 3 applies. We then have the existence of a vector $\mathfrak{v}_0$ such that $\mathfrak{v}_0\mathfrak{v}_1 = \mathfrak{v}_0\mathfrak{u}_1 = 0$ and $\mathfrak{v}_0$ has an orthogonal complementary space in $\langle \mathfrak{u}_2, \cdots, \mathfrak{u}_n \rangle$ and hence such a space, $\langle \mathfrak{v}_0 \rangle^*$, in $\mathfrak{L} = \langle \mathfrak{u}_1, \cdots, \mathfrak{u}_n \rangle$, that is, $\mathfrak{L} = \langle \mathfrak{v}_0 \rangle + \langle \mathfrak{v}_0 \rangle^*$. Then $\langle \mathfrak{v}_0 \rangle^* \cong \langle \mathfrak{v}_1 \rangle + \mathfrak{V} \cong \langle \mathfrak{u}_1 \rangle + \mathfrak{U}$ where[3] $\mathfrak{V}$ and $\mathfrak{U}$ are the complementary orthogonal spaces of $\langle \mathfrak{v}_1 \rangle$ and $\langle \mathfrak{u}_1 \rangle$, respectively, in $\langle \mathfrak{v}_0 \rangle^*$. By the hypothesis of the induction $\mathfrak{V} \cong \mathfrak{U}$ and $\mathfrak{L} \cong \langle \mathfrak{v}_0 \rangle + \langle \mathfrak{v}_1 \rangle + \mathfrak{V} \cong \langle \mathfrak{v}_0 \rangle + \langle \mathfrak{u}_1 \rangle + \mathfrak{U}$ implies

$$\langle \mathfrak{v}_2, \cdots, \mathfrak{v}_n \rangle = \langle \mathfrak{v}_0 \rangle + \mathfrak{V} \cong \langle \mathfrak{v}_0 \rangle + \mathfrak{U} = \langle \mathfrak{u}_2, \cdots, \mathfrak{u}_n \rangle.$$

THEOREM 2. *If lattices $\mathfrak{L}_1$ and $\mathfrak{L}_2$ over a ring R_p of p-adic integers (p odd) have no radical, then*

$$\mathfrak{L}_3 + \mathfrak{L}_4 = \mathfrak{L}_1 \cong \mathfrak{L}_2 = \mathfrak{L}_3 + \mathfrak{L}_5$$

implies

$$\mathfrak{L}_4 \cong \mathfrak{L}_5.$$

This theorem is easily established by induction using Lemma 2 and Theorem 1. It may also be stated in terms of quadratic forms in a manner analogous to Theorem B.

CORNELL UNIVERSITY

[3] The existence of $\mathfrak{V}$ (and similarly of $\mathfrak{U}$) follows from Lemma 1 since $\mathfrak{v}_1^2$ is a divisor of the product of $\mathfrak{v}_1$ by any vector of $\mathfrak{L}$ and hence of $\langle \mathfrak{v}_0 \rangle^*$.