ONE DIMENSIONAL WITT'S THEOREM OVER MODULAR LATTICES[1]

BY JOHN S. HSIA

Communicated by H. Bass, April 1, 1969

We first present the problem in a general setting. Let R be a commutative ring with unity. A *quadratic R-space*, in the sense of Bass [1], is a pair (P, q), where P is a finitely generated projective R-module and $q: P \to R$ is a nonsingular quadratic form. An element $x \in P$ is *unimodular* if its coefficient ideal $o_P(x) = \{f(x) \mid f \in \mathrm{Hom}_R(P, R)\} = R$. The orthogonal group $O(P)$ on (P, q) is the set of all R-automorphisms of P preserving the quadratic structure. The one-dimensional Witt's Theorem is concerned with finding the necessary and sufficient conditions under which $O(P)$ acts transitively on the unimodular elements of (P, q).

A. Roy [6] showed that with finiteness assumption on R and if 2 is unitary in R and, if further, the hyperbolic dimension on P is large enough, then $O(P)$ acts transitively on the nonsingular elements of P of a given norm. (A nonsingular element $x \in (P, q)$ is one which has norm $q(x)$ equaling to a unit.) In this paper, we do not assume the element 2 is a unit. However, we strongly restrict the nature of the ring R. Our ring R always denotes the ring of integers in a *local field* F. By a *local field* F, we shall mean here that F is either

(i) a finite extension of the p-adic number field Q_p, for any prime p, or in the characteristic two situation,

(ii) the field of formal power series in one uniformizing variable π over a finite field of constants having characteristic 2.

For such a ring R, a quadratic R-space is a free R-module by Nakayama, and we shall call the pair (P, q) then a *(uni-) modular quadratic R-lattice*. Given an unimodular (or *maximal*) element $z \in P$, the *characteristic set* $\mathfrak{M}_z$ of z in P is defined as

$$\mathfrak{M}_z = \{x \in P \mid B_q(z, x) = 1\},$$

where

$$\begin{aligned} q(x + y) - q(x) - q(y) &= 2B_q(x, y) \qquad \mathrm{Char}(R) \neq 2, \\ &= B_q(x, y) \qquad \mathrm{Char}(R) = 2. \end{aligned}$$

[1] This work has been supported in part by the National Science Foundation under contract GP8911.

The *norm group* $\mathfrak{g}(P)$ of P is defined by

$$\begin{aligned} \mathfrak{g}(P) &= q(P) + 2R \qquad \text{Char}(R) \neq 2, \\ &= q(P) + R \qquad \text{Char}(R) = 2. \end{aligned}$$

Two unimodular elements u and v in P are said to be *integrally equivalent* if and only if there exists an (integral) isometry $\alpha \in O(P)$ on P such that $\alpha(u) = v$.

We now state our main result, whose full proof together with the procedures for effective determination of the integral equivalence problems amongst unimodular elements will appear elsewhere.

MAIN THEOREM. *In an unimodular quadratic R-lattice P, where R is the ring of integers in a local field, two unimodular (maximal) elements u and v having the same norm $q(u) = q(v) = \delta$ are integrally equivalent if and only if their respective characteristic sets $\mathfrak{M}_u$ and $\mathfrak{M}_v$ represent the same elements in R; that is, $q(\mathfrak{M}_u) = q(\mathfrak{M}_v)$—here, q denotes the non-singular quadratic form associated with P.*

SKETCH PROOF. The proof is largely computational. We eliminate various special cases by proving a sequence of lemmas finally permitting us to assume the number δ takes on a particular form. Using this "reduction" result, we then show that for dim $P \geqq 5$, there is a vector $\bar{u} \in \mathfrak{M}_u$ such that $(Ru + R\bar{u})^{\perp}$ supports a hyperbolic component. Therefore, the case for dim $P = 5$ becomes a consequence of Theorem 4.4 [3]. Dim $P = 6$ case falls through by a "modified" 5-dimensional argument. The quaternary case is treated separately. (We remark here that the sequence of lemmas leading to the above mentioned "reduction" result is essentially an investigation of the quadratic defect behaviour for the number δ relative to the norm and weight (base) generators—see [5]—for both the norm groups $\mathfrak{g}(P)$ and $\mathfrak{g}(\langle u \rangle^{\perp})$.) Theorem 4.1 [3] finishes the remaining dimensions of P.

Computationally, the task of having to find all the numbers represented by a characteristic set is not always a very pleasant chore. Fortunately, for low dimensions (less or equal to three) the actual computations involved is not heavy. And for sufficiently high dimensions (greater or equal to five), we have the following theorem to remedy the situation.

THEOREM. *If there is a single pair of elements $\bar{u}$ from $\mathfrak{M}_u$ and $\bar{v}$ from $\mathfrak{M}_v$ such that $q(\bar{u}) = q(\bar{v})$, and if further, we have the norm groups for $\langle u \rangle^{\perp}$ and $\langle v \rangle^{\perp}$ being equal, then u is integrally equivalent to v whenever dim $P \geqq 5$.*

REMARKS. 1. The task of having to find only one such pair of elements is usually not difficult. The effective determination of norm groups is well known (see O'Meara [5]). Here the Jordan decompositions for a lattice like $\langle u\rangle^{\perp}$ are rather simple. The question of which pair of elements to seek is really not relevant, because if u and v were indeed integrally equivalent then the choice of any element $\bar{u}\in\mathfrak{M}_u$ should correspondingly imply the existence of a vector $\bar{v}\in\mathfrak{M}_v$ having the same norm. On the other hand, if one can concoct a pair $\bar{u}$ and $\bar{v}$ such that $q(\bar{u})$ is not congruent to $q(\bar{v})$ modulo $\mathfrak{G}$, where $\mathfrak{G}$ denotes the norm group for $\langle u\rangle^{\perp}$ (and hence also for $\langle v\rangle^{\perp}$), then it can be readily shown that u can not possibly be equivalent to v.

2. A well-known theorem in the integral classification of equivalent quadratic forms says that two modular (say unimodular) forms over the ring of integers in a local field are integrally equivalent if and only if they represent the same numbers in the ring. Observe the striking similarity between this statement and our main theorem mentioned above. Also, our theorem for dim $P\geqq 5$ compares closely with O'Meara's theorem about equivalence between modular forms, (respectively, for dim $P\geqq 6$ to Sah's theorem, see [7], in the characteristic 2 case). Indeed, for dim $P\geqq 7$ (respectively dim $P\geqq 8$) the analogy becomes even more striking.

REFERENCES

1. H. Bass, *Topics in algebraic K-theory*, Mathematical Lecture Notes, Tata Institute of Fundamental Research, Bombay, 1967.

2. J. S. Hsia, *Integral equivalence for vectors over depleted modular lattices on dyadic local fields*, Amer. J. Math. 90 (1968), 285–294.

3. ———, *Integral equivalence of vectors over local modular lattices*, Pacific J. Math. 23 (1967), 527–542.

4. ———, *A note on the integral equivalence of vectors in characteristic* 2, Math. Ann. 179 (1968), 63–69.

5. O. T. O'Meara, *Introduction to quadratic forms*, Grundlehren der Mathematischen Wissenschaften, Springer-Verlag, Berlin, 1963.

6. A. Roy, *Cancellation of quadratic forms over commutative rings*, J. Algebra (3) 10 (1968), 286–298.

7. C. H. Sah, *Quadratic forms over fields of characteristic* 2, Amer. J. Math., 82 (1960), 812–830.

THE OHIO STATE UNIVERSITY, COLUMBUS, OHIO 43210