COMPOSITIO MATHEMATICA

C. T. C. WALL

On the classification of hermitian forms. I. Rings of algebraic integers

Compositio Mathematica, tome 22, nº 4 (1970), p. 425-451

<http://www.numdam.org/item?id=CM_1970__22_4_425_0>

COMPOSITIO MATHEMATICA, Vol. 22, Fasc. 4, 1970, pag. 425-451
Wolters-Noordhoff Publishing
Printed in the Netherlands

ON THE CLASSIFICATION OF HERMITIAN FORMS

I. RINGS OF ALGEBRAIC INTEGERS

by

C. T. C. Wall

In a recent paper [10], I gave an account of definitions of 'reflexive' and 'quadratic' forms in a fairly general situation, both generalising the classical notion of hermitian forms. In this paper I apply standard number theoretic techniques to classify nonsingular quadratic forms on projective, and especially on free modules, over rings R of algebraic integers, corresponding to some non-trivial involution α of R. If the quadratic field extension corresponding to α is at most tamely ramified, there is no distinction in this case between quadratic and hermitian forms. In the wildly ramified case, however, nonsingular hermitian forms are much harder to classify; since I am not interested in them for applications, we will not consider them further here.

To a large extent, this paper is a re-working of results of Shimura [9]. I feel that a new account is justified by the different emphasis: Shimura considered the general theory (in particular, he proved the strong approximation theory for SU while we merely quote it), and exemplified it by considering maximal lattices. Our concern is exclusively with modular lattices, which enables us to consider also fine details.

In a later paper I intend to apply the techniques of this one to study forms over arbitrary 'global rings' (orders in finite semisimple algebras over Q): the main result below for local structure will cover what is needed for this extension.

Statement of results

For nonsingular (α, u)-quadratic forms on R-modules M, with r the fixed subring of α, we have the following invariants:

1) The signatures at real places of r which ramify in R.

2) The discriminant with respect to a free base of M (if M is only projective, this can only be defined locally).

3) For dyadic ramified primes ρ of r, the Arf invariant of the induced form on $F_\rho = r/\rho$.

4) If M has a preferred base, and Q is a quotient of R with α trivial and $u = -1$ on Q, the determinant κ of a change from the given base over Q to a symplectic base.

We determine which values the invariants can take, and the relations between them. If the invariants 1), 2) and 3) are trivial (and the form of rank > 2, indefinite), we show that the form is hyperbolic; however, not necessarily on a free module. The structure of the Witt group of forms on projective, free, or free and based modules is determined, modulo the structure of the groups of units. We also establish cancellation and stability theorems.

Crucial for the local theory is a result which reduces the classification problem over the local rings R to a problem on the residue class fields. For the detailed local theory, there is an interesting distinction between 'bad' and 'good' primes, according as u is or is not equivalent in an appropriate sense to -1: this is important for the global theory.

Lifting forms to complete rings

For the benefit of readers unfamiliar with [10], we briefly recapitulate the main definitions. A is a ring (with unit), α an anti-automorphism of A and u a unit of A such that

$$\alpha(u) = u^{-1} \quad \text{and} \quad \alpha^2(x) = uxu^{-1} \quad \text{for all} \quad x \in A.$$

For M, N (right) A-modules, a map

$$\phi : M \times N \to A$$

is α-sesquilinear if

$$\phi(m, n_1 a_1 + n_2 a_2) \equiv \phi(m, n_1)a_1 + \phi(m, n_2)a_2$$
$$\phi(m_1 a_1 + m_2 a_2, n) = \alpha(a_1)\phi(m_1, n) + \alpha(a_2)\phi(m_2, n);$$

We write $S_\alpha(M)$ for the (additive) group of α-sesquilinear maps $M \times M \to A$. Define

$$T_u : S_\alpha(M) \to S_\alpha(M)$$

by

$$T_u(\phi)(m, n) = \alpha(\phi(n, m))u.$$

Then the (α, u)-reflexive maps are the elements of $R_{(\alpha,u)}(M) = \text{Ker}\,(T_u - 1)$, and the (α, u)-quadratic maps the elements of $Q_{(\alpha,u)}(M) = \text{Coker}\,(T_u - 1)$.

Multiplication by $T_u + 1$ induces a map (bilinearisation) $b : Q_{(\alpha,u)}(M) \to R_{(\alpha,u)}(M)$. Arguing as in the proof of [10, Theorem 1], we find that b is an isomorphism for all finitely generated projective M if it is so for A

itself. Making $\boldsymbol{Z}_2$ act on A by $T(x) = \alpha(x)u$, this is so if the $\boldsymbol{Z}_2$-module A is cohomologically trivial.

Let (B, β, v) satisfy the same conditions as (A, α, u). Let $f : A \to B$ be a ring homomorphism such that $f(u) = v$ and $\beta(f(a)) = f(\alpha(a))$ for $a \in A$. Then for any A-module M we define $N = M \otimes_A B$, regarding B as right A-module by f. For any $\phi \in S_\alpha(M)$, define $f_*(\phi) \in S_\beta(N)$ by

$$f_*(\phi)(m_1 \otimes b_1, m_2 \otimes b_2) = \beta(b_1)\phi(m_1, m_2)b_2 .$$

It is easy to check that this is compatible with the relations defining the tensor product, and that

$$T_v(f_*(\phi)) = f_*(T_u(\phi)).$$

Thus f_* induces a map

$$R_{(\alpha, u)}(M) \to R_{(\beta, v)}(N)$$

and similarly for Q.

LEMMA 1. *If $f : A \to B$ is surjective, and M is a projective A-module, then*

$$f_* : Q_{(\alpha, u)}(M) \to Q_{(\beta, v)}(N)$$

is surjective.

PROOF. Since $Q_{(\alpha, u)}(M)$ is a quotient of $S_\alpha(M)$, it is enough to show $S_\alpha(M) \to S_\beta(N)$ surjective. Choose M' with $M \oplus M'$ free. Since $S_\alpha(M \oplus M')$ splits naturally as a direct sum of 4 terms it is enough to show $S_\alpha(M \oplus M') \to S_\beta(N \oplus N')$ surjective; equivalently, we may suppose M free. Choose a basis $\{m_\alpha\}$. Taking ϕ to the matrix $\phi(m_\alpha, m_\beta)$ now gives a bijection of $S_\alpha(M)$ to a group of matrices over A. Now f_* acts on matrices by letting f act on each entry. Thus since f is surjective, so is f_*.

Note that already this result is false for hermitian forms.

We can never expect f_* to be injective too, but under suitable assumptions we can get as good a result. We will need conditions on both f and the forms.

A map $\phi \in S_\alpha(M)$ is called nonsingular if its adjoint $A\phi : M \to \mathrm{Hom}_A(M, A)$ defined by

$$A\phi(m_1)(m_2) = \phi(m_1, m_2)$$

is bijective. A quadratic form is nonsingular if its bilinearisation is. Evidently f_* preserves nonsingularity.

If A is a ring and I an ideal we have a quotient map $f : A \to A/I = B$. If $\alpha(I) = I$, α induces $\beta : B \to B$, and taking $v = u+I$ we satisfy the conditions for f to induce a map (even a surjective one) of quadratic forms. Note that here $N = M/MI$. For each $n \geqq 0$ we have the ideal I^n, and taking these as base of neighbourhoods of 0 defines the I-adic topology on A. We will suppose A complete in this topology, or equivalently, that the map

$$A \to \varprojlim A/I^n$$

is an isomorphism.

THEOREM 2. *Let A, I be as above; let M be a finitely generated projective A-module. Then $x \in Q_{(\alpha, u)}(M)$ is nonsingular if and only if $f_*(x)$ is. If x is nonsingular, and $f_*(x) = f_*(y)$, there is an automorphism λ of M with $\lambda^*(x) = y$ and $Im(\lambda - 1_M) \subset M \cdot I$.*

PROOF. That $f_*(x)$ nonsingular implies that x is follows from Nakayama's lemma. Indeed, it is standard (see e.g. Bourbaki [4]) that under our assumptions there is a bijection of isomorphism classes of finitely generated projectives over A and over A/I.

For the second part, suppose inductively that x and y agree modulo I^r, i.e. that there are representative $\xi, \eta \in S_\alpha(M)$ with

$$(\xi - \eta)(M \times M) \subset I^r.$$

Since x is nonsingular, so is its bilinearisation $\xi + T\xi$. Consider the composite

$$M \xrightarrow{A(\eta - \xi)} Hom_A(M, A) \xrightarrow{(A(\xi + T\xi))^{-1}} M,$$

which is an A-module map: call it f. Since $fM \subset M \cdot I^r$, $1_M + f$ is an isomorphism. We now compute $(1_M + f)^*(x)$. We have

$$\begin{aligned}(1_M+f)^*(\xi)(m_1, m_2) \\ &= \xi(m_1 + f(m_1), m_2 + f(m_2)) \\ &= \xi(m_1, m_2) + \xi(m_1, f(m_2)) + \xi(f(m_1), m_2) + \xi(f(m_1), f(m_2)).\end{aligned}$$

Now

$$\begin{aligned}\eta(m_1, m_2) - \xi(m_1, m_2) \\ &= A(\eta - \xi)(m_1)(m_2) \\ &= A(\xi + T\xi)(f(m_1))(m_2) \qquad \text{by definition of } f \\ &= \xi(f(m_1), m_2) + T\xi(f(m_1), m_2)\end{aligned}$$

so that

$$\begin{aligned}(1_M+f)^*(\xi)(m_1, m_2) \\ &= \eta(m_1, m_2) + \xi(m_1, f(m_2)) - T\xi(f(m_1), m_2) + \xi(f(m_1), f(m_2)).\end{aligned}$$

Here, the first term is η, as desired. The middle two terms define the zero quadratic form, since if we define $\chi \in S_\alpha(M)$ by

$$\chi(m_1, m_2) = \xi(m_1, f(m_2)),$$

then

$$\begin{aligned} T\chi(m_1, m_2) &= \alpha(\chi(m_2, m_1))u \\ &= \alpha(\xi(m_2, f(m_1)))u \\ &= T\xi(f(m_1), m_2). \end{aligned}$$

The last term belongs to I^{2r}. We have thus shown that if x and y agree modulo I^r, there is an automorphism $(1+f)$ of M such that $f(M) \subset M \cdot I^r$ and $(1+f)^*x$ agrees with y modulo I^{2r}.

To prove the theorem we apply this result inductively as follows. Start with representatives ξ, η of x and y which agree modulo I. Suppose we have found inductively endomorphisms f_i of M with $f_i(M) \subset M \cdot I^{2^{i-1}}$ and forms $\chi_i \in S_\alpha(M)$ taking values in $I^{2^{i-1}}$ for $1 \leqq i \leqq r$ with

$$\begin{aligned} \xi_r &= (1+f_r)(1+f_{r-1}) \cdots (1+f_1)^*\xi \\ &\equiv \eta + (1-T)(\chi_1 + \cdots + \chi_r) \qquad (\text{mod } I^{2r}). \end{aligned}$$

Applying the result we find f_{r+1} and χ_{r+1} to continue the induction. Now since A is I-adically complete, the product $\prod(1+f_i)$ converges to an automorphism λ of M, with

$$(\lambda - 1_M)(M) \subset M \cdot I,$$

and the sum $\sum \chi_i$ converges to a form $\chi \in S_\alpha(M)$, and taking the limit we have

$$\lambda^*\xi = \eta + (1-T)\chi,$$

hence $\lambda^*x = y$, as required.

The above result is far from being true for hermitian forms: in this sense it is the key result of this paper. Most of the applications below are as easily deduced from other considerations, but the wildly ramified case needs something like the argument above.

If A is a compact ring and J its radical, then A is complete in the J-adic topology, and A/J is the direct product of matrix rings over division rings. Now α leaves these invariant or interchanges them in pairs: the pairs contribute nothing, and the classification of nonsingular quadratic forms over A is thus reduced to matrix rings over division rings, and it is not hard to reduce further to forms over division rings.

Programme and notation

From now on, all our rings will be commutative. The assumptions above then simplify to:

α is an automorphism of A with $\alpha^2 =$ identity,
u is a unit of A with $\alpha(u) = u^{-1}$.

The involution α will always be fixed, and we denote it by a bar: $\alpha(x) = \bar{x}$. Write A^+ for the additive group of A, $A^\times$ for its multiplicative group. Thus we have $u \in A^\times, u\bar{u} = 1$. We regard both these as Z_2-modules, with Z_2 acting by α.

The rings to be considered are as follows. K is an algebraic number field, with involution 'bar'. The fixed field is k, so K is a quadratic extension of k. The rings of algebraic integers in K, k are denoted by R, r. For each prime ρ (= valuation) of k, k_ρ is the completion of k at ρ and $K_\rho = K \otimes_k k_\rho$. There are two possibilities: K_ρ may be a field which is a quadratic extension of k_ρ or a direct sum of two copies of k_ρ, interchanged by 'bar'. In the latter case we say that ρ is decomposed. If ρ is non-archimedean, r_ρ and R_ρ denote the corresponding completions of r and R. But we can always define $R_\rho = R \otimes_r r_\rho$. Then r_ρ is a local ring, and so (except in the decomposed case) is R_ρ; we write f_ρ and F_ρ for their residue class fields.

We have identified primes with valuations, but will in practice write $v_\rho : k^\times \to Z$; also $v_\rho : k_\rho^\times \to Z$ for the valuations, and ρ for the corresponding prime ideal $\{x : v_\rho(x) > 0\}$ of $r_\rho = \{x : v_\rho(x) \geqq 0\}$, or of r. We have $r_\rho^\times = \{x \in k_\rho^\times : v_\rho(x) = 0\}$. An element x of r_ρ with $v_\rho(x) = 1$ is called a prime. Similar terminology applies to R_ρ when it is a local ring.

Our objective is to classify nonsingular quadratic forms on finitely generated projective R-modules M. It is well known that such M are characterised by having $M \to M \otimes_R K$ injective and M finitely generated over R. Putting $V = M \otimes_R K$, it is thus natural to consider first forms on the vector space V and then $M \subset V$ as above: M is then called a *lattice* in V. The embedding determines the bilinearisation of the quadratic form but not in general the form itself: we will have to deal with this point later.

The completions come in since we can write $M_\rho = M \otimes_R R_\rho$, contained (as a lattice) in $V_\rho = V \otimes_K K_\rho$, and then $M = \cap M_\rho$, the intersection over all (non-archimedean) ρ. Two lattices $M, M' \subset V$ have $M_\rho = M'_\rho$ for almost all (i.e. all but a finite number) ρ; conversely, given lattices $M'_\rho = M_\rho$ for almost all ρ, $M' = \cap M'_\rho$ is a lattice in V.

In order to pass from the 'local theory' (classification over R_ρ) to the 'global theory' (classification over R), we need more than just the isomorphism classification of nonsingular quadratic forms over R_ρ; we must relate this to the classification over K_ρ; and given two lattices $M_\rho, M'_\rho \subset V_\rho$ we have to know not only when there exists an isomorphism $M_\rho \xrightarrow{A} M_\rho$, which (necessarily) induces an automorphism $A \otimes 1$ of V_ρ, but also when A can be chosen so that $A \otimes 1$ has determinant 1. In this case we call M_ρ and M'_ρ SU-equivalent.

Recall from [10, p. 2] that multiplying the values of a form ϕ by a unit v (scaling) converts u-quadratic to $uv/\bar{v}$-quadratic forms (we suppress mention of the involution, which remains fixed). We will use this technique to normalise the unit u as far as possible; naturally this is much easier in the local theory (and, of course, over fields one need only consider hermitian or skew-symmetric forms). Note that the equivalence classes of u just constitute the cohomology group $H^1(\mathbf{Z}_2; A^\times)$. It is possible (c.f. O'Meara [7]) to give an alternative formulation in terms of 'v-modular' (rather than unimodular) forms.

Finally note that for an (α, u)-reflexive form ϕ on a free module F over a commutative ring A, one can choose a basis $\{e_i\}$ of F and form the determinant $D = \det \phi(e_i, e_j)$. The form ϕ is nonsingular if and only if D is a unit: $D \in A^\times$. We have $\bar{D} = D$. If the basis is changed by a substitution with determinant δ (so $\delta \in A^\times$), D is multiplied by $\delta\bar{\delta}$. The multiplicative class of D modulo such elements is an important invariant of ϕ. For most purposes, however, it is convenient to modify it as follows. Suppose that F has rank $2k$. Then it admits also a form ψ which is a hyperbolic form on a free module of rank k. The quotient of the determinants D for ϕ and ψ is called the *discriminant* of ϕ. Since ψ has a matrix of blocks

$$\begin{pmatrix} 0 & 1 \\ u & 0 \end{pmatrix},$$

it has determinant $(-u)$, so the discriminant of ϕ is $(-u^{-1})^k D$. We usually denote it by Δ. When we refer to the discriminant of a form ϕ on a free module of rank $(2k+1)$, it does not matter whether we interpret it as D or $(-u^{-1})^k D$ (provided the interpretation is consistent). We define the discriminant of a quadratic form by first taking the bilinearisation.

Δ (or D) takes values in the quotient of the group of invariant units of $A(\Delta \in A^\times, \bar{\Delta} = \Delta)$ by the group of norms of units $(\delta\bar{\delta}, \delta \in A^\times)$. This is just the (Tate) cohomology group $H^0(\mathbf{Z}_2; A^\times)$. Note that the discriminant is unaltered by scaling: if the form has rank $2k$, D is multiplied by v^{2k} and $(-u^{-1})^k D$ by $(v\bar{v})^k$.

Local theory

DECOMPOSED CASE. The classification problem here is essentially trivial. Indeed, even in the non-abelian case, if $A = A_1 \oplus A_2$, with A_1 and A_2 interchanged by α.

REMARK. *There is a bijection between isomorphism classes of projective A_1-modules and of nonsingular (α, u)-quadratic (or reflexive) forms on projective A-modules.*

Let u have components (u_1, u_2): then $u_2 = \bar{u}_1^{-1}$. Taking $v = (u^{-1}, 1)$ we see that by scaling we can suppose $u = 1$. Again, one sees easily (the $\mathbf{Z}_2$-module A is induced (from A_1)) that bilinearisation is an isomorphism in this case. Finally an A-module M can be regarded as a pair (M_1, M_2) : M_1 an A_1-module, M_2 and A_2-module; and a quadratic or hermitian form amounts to a pairing between M_1 and M_2, nonsingular if and only if this pairing is.

One can regard this bijection as corresponding to the fact that a unitary group, as algebraic group over a field, is a k-form of the general linear group.

We thus see that the classification of forms both over K_ρ and over R_ρ, is trivial – a form being determined up to isomorphism by its rank. Likewise, the problem of SU-equivalence comes down to the problem of SL-equivalence of lattices over r_ρ (with no form on them). Here again it is worth beginning with a general observation.

REMARK. *Let M_ρ have a quadratic form ϕ_ρ; let G be the group of determinants of automorphisms of (M_ρ, ϕ_ρ). If M_ρ, M'_ρ are lattices in V_ρ, and A an isomorphism of M_ρ on M'_ρ, extending to an automorphism A of V_ρ, then M_ρ and M'_ρ are SU-equivalent if and only if det $A \in G$.*

Thus if H is the group of determinants of automorphisms of (V_ρ, ϕ_ρ), we have a bijection of SU-equivalence classes of lattices isomorphic to (M_ρ, ϕ_ρ) with H/G.

In the case at hand there is no ϕ_ρ but the principle is the same. Since r_ρ is a principal ideal domain (the only ideals are the powers of ρ), $M_{\rho 1}$ is a free r_ρ-module. Determinants of automorphisms must belong to $r_\rho^\times$: any element of $r_\rho^\times$ gives an automorphism of a free module of rank 1, and so does occur as a determinant. Similarly H can be identified as $k_\rho^\times$. Finally, v_ρ gives an isomorphism of $k_\rho^\times / r_\rho^\times$ with $\mathbf{Z}$. Thus we have a bijection of the set of SU-equivalence classes with $\mathbf{Z}$.

INERT CASE. Here, K_ρ is a field. We change notation, and write v_ρ : $K_\rho^\times \to \mathbf{Z}$ for its valuation. First we recall some facts about cohomology.

$H^1(\mathbf{Z}_2; K_\rho^\times) = 0$ as for any field

$H^0(\mathbf{Z}_2; K_\rho^\times) \cong \mathbf{Z}_2$ e.g. by local class field theory.

The exact cohomology sequence belonging to the coefficient sequence

$$1 \to R_\rho^\times \to K_\rho^\times \xrightarrow{v_\rho} \mathbf{Z} \to 0$$

now reduces to

$$0 \to H^0(\mathbf{Z}_2; R_\rho^\times) \to \mathbf{Z}_2 \xrightarrow{v_{\rho *}} \mathbf{Z}_2 \to H^1(\mathbf{Z}_2; R_\rho^\times) \to 0.$$

Clearly $v_{\rho *}$ is nonzero if and only if there exists $x \in k_\rho^\times$ with $v_\rho(x)$ odd:

in this case the extension is unramified, otherwise ramified.

In both cases there are two classes of forms over $K_\rho^\times$ of a given rank, which are distinguished by the discriminant. Other questions are all much more complicated in the ramified case, so we discuss the inert (non-ramified) case first.

Then α is non-trivial on F_ρ, and generates the Galois group of F_ρ/f_ρ, and v_ρ induces the valuation of k_ρ. Since the H^1 groups vanish, we can suppose by scaling that $u = 1$. The $\boldsymbol{Z}_2$-modules F_ρ^+, R_ρ^+, K_ρ^+ are cohomologically trivial, so there is no essential distinction between hermitian and quadratic forms. For forms over F_ρ, and hence (by Theorem 2) also over R_ρ there is just one isomorphism class of nonsingular forms of a given rank. Since an element x of $k_\rho^\times$ is a norm if and only if $v_\rho(x)$ is even, units are norms, so only the forms over K_ρ with $\Delta = 1$ contain unimodular (i.e. nonsingular) lattices. Certainly two lattices in the same V_ρ are equivalent: we claim that they are also SU-equivalent, which will complete our discussion of the inert case.

Any automorphism of V_ρ preserving the form must have determinant δ satisfying $\bar{\delta}\delta = 1$: it thus suffices to find an automorphism with determinant δ leaving M_ρ invariant. Now $v_\rho(\delta) = 0$, so $\delta \in R_\rho^\times$. Since a hermitian form over F_ρ is a direct sum, with one summand 1-dimensional, Theorem 2 implies that the same holds over R_ρ: let e generate such a summand. The required automorphism is now obtained by letting $e \to e\delta$, and leaving the orthogonal complement of e fixed.

Ramified case (non-Archimedean). This is the case when K_ρ is a field, but its valuation induces $2\times$ the valuation of k_ρ. In this case, α is trivial on $F_\rho = f_\rho$.

Again K_ρ^+ is cohomologically trivial (the extension K_ρ/k_ρ is separable, as the fields have characteristic 0). For R_ρ^+ and F_ρ^+ we have to distinguish the cases when F_ρ^+ has characteristic 2 or not. The ramification is described correspondingly as *wild* or *tame*. In the tame case, R_ρ^+ and F_ρ^+ are still cohomologically trivial; in the wild case they are not. We will not discuss reflexive forms over R_ρ and F_ρ in the wild case; only quadratic ones; in the other cases (and over K_ρ) it makes no difference.

Write U_ρ for the kernel of $R_\rho^\times \to F_\rho^\times$. In the tame case, U_ρ is cohomologically trivial and $H^*(R_\rho^\times) \cong H^*(F_\rho^\times)$. In the wild case, things are more complicated. However, it follows from the exact sequence mentioned earlier that (in either case) a representative of the non-trivial class in $H^1(\boldsymbol{Z}_2; R_\rho^\times)$ is $\bar{\pi}/\pi$, where $v_\rho(\pi) = 1$. Thus by scaling we can suppose that $u = 1$ or $u = \bar{\pi}/\pi$. It will be more convenient, however, to reduce to one of the cases

$$u = -\bar{\pi}/\pi \qquad u = -1$$

which we call respectively the *good* and *bad* cases. In the tame case, we can take $\bar{\pi}/\pi = -1$; in the wild case this may or may not be possible. But in the wild case the condition $\bar{u}u = 1$ implies anyway that u reduces to 1 in F_ρ.

There are thus three cases for forms over F_ρ:

GOOD TAME CASE (*characteristic odd*, $u = 1$).

We have a quadratic form over F_ρ. There are two isomorphism classes of these for each rank, classified by the discriminant. By Theorem 2, each lifts to a single isomorphism class over R_ρ: again distinguished by the discriminant. Thus each form over K_ρ contains a unimodular lattice, unique up to isomorphism. As in the inert case, we see that it is also unique up to SU-equivalence.

BAD TAME CASE (*characteristic odd*, $u = -1$).

We have a skew-symmetric form over F_ρ. For nonsingularity ,the rank must be even; in fact we can only have a hyperbolic space. By Theorem 2, the form over R_ρ must be hyperbolic too, hence also that over K_ρ. We defer the question of SU-equivalence.

WILDLY RAMIFIED CASE.

We have a quadratic form over the finite field F_ρ, of characteristic 2. For nonsingularity, the rank must be even. There are two isomorphism classes for each rank, and they are distinguished by the Arf invariant [1]: if $\{e_1, f_1, \cdots, e_r, f_r\}$ is a symplectic base for the bilinearisation of x, and q is the associated quadratic map of x,

$$c'(x) = \sum q(e_i)q(f_i)$$

is well defined modulo the additive group of elements $w+w^2$, $w \in F_\rho$. Let $S : F_\rho \to \mathbf{Z}_2$ be the map whose kernel consists of these elements; then $c(x) = Sc'(x)$ *is* well-defined. By Theorem 2, c is the only invariant needed for forms over R_ρ also. If $c = 0$, the form is hyperbolic, so the discriminant is 1. Otherwise, it is not clear a priori how the classifications over R_ρ and K_ρ compare.

THEOREM 3. *In the bad case, all nonsingular forms over R_ρ become hyperbolic over K_ρ.*

In the good case, nonsingular forms over R_ρ with different Arf invariants are not equivalent over K_ρ.

PROOF. Since each form over F_ρ splits as the direct sum of nonsingular 2-dimensional forms, by Theorem 2 the same holds over R_ρ. Thus it suffices to consider the two-dimensional case. A typical form has base $\{e, f\}$ and

$$\phi(e, e) = \phi(e, f) = 1 \qquad \phi(f, e) = 0 \qquad \phi(f, f) = b.$$

This has Arf invariant the class of b.

The above ϕ represents an x whose bilinearisation is $\phi + T\phi = \psi$. If $u = -1$, then $\psi(e, e) = 0$, so ψ is hyperbolic over K_ρ. This proves the first part of the Theorem.

In general,

$$\psi(e, e) = 1+u \qquad \psi(e, f) = 1$$
$$\psi(f, e) = u \qquad \psi(f, f) = b + u\bar{b}$$

so ψ has determinant $(1+u)(b+u\bar{b}) - u$ and discriminant the quotient of this by $-u$. Putting $u = -\bar{\pi}/\pi$, this is

$$\Delta = 1 + (\pi - \bar{\pi})(\pi b - \bar{\pi}\bar{b})/\pi\bar{\pi}.$$

We must show that this is not a norm.

My proof is fairly brutal. We may choose b with $S(b) = 1$ and $\bar{b} = b$. There are two cases, according as an element d of K_ρ with $\bar{d} = -d$ has $v_\rho(d)$ even or odd (we may suppose 0 or 1). If $v_\rho(d) = 1$, we can take d for π above. Then

$$\Delta = 1 + 2\pi \cdot 2\pi b / -\pi^2 = 1 - 4b.$$

If $L_\rho \subset K_\rho$ is the fixed field of α, then K_ρ is obtained from L_ρ by adjoining the square root of d^2. Thus Δ is a norm if and only if the Hilbert symbol $(\Delta, d^2)_v = +1$. But $\sqrt{\Delta}$ generates the non-ramified extension of L_ρ, and the prime element d^2 is not a norm from that, so in fact $(\Delta, d^2)_v = -1$. (The reason that $L_\rho[\sqrt{\Delta}]$ is non-ramified is that since $S(b) = 1$, b is not of the form $w + w^2$ mod ρ (in L_ρ): in the extension, we can take $w = \frac{1}{2}(1 + \sqrt{\Delta})$.)

If $v_\rho(d) = 0$, it is again convenient to work in L_ρ rather than K_ρ: if ω is a prime in L_ρ, then $K_\rho = L_\rho[\sqrt{a}]$ for some a of the form

$$a = 1 + u\omega^{2r+1} \qquad 0 \leqq r < e$$

for some unit u, where e is the absolute ramification index of L_ρ. Here we can take

$$\pi = \omega^{-r}(1 + \sqrt{a})$$

so that

$$\Delta = 1 + \frac{4ab}{1-a}.$$

Again, we must calculate $(a, \Delta)_v$. But by the last exercise in [8] (the conditions are easily verified: $a \in U^{2r+1}$, $\Delta \in U^{2e-2r-1}$),

$$\begin{aligned}(a, \Delta)_v &= (-1)^{(2r-1)S((a-1)(\Delta-1)/-4)}\\ &= (-1)^{(2r+1)S(ab)}\\ &= -1\end{aligned}$$

since a reduces to $1 \in F_\rho$, and $S(b) = 1$ by the choice of b.

It remains to consider SU-equivalence in the ramified case. As in the other cases, this amounts to finding which numbers δ with $\bar{\delta} = \delta^{-1}$ can arise as determinants of automorphisms of the given lattice.

THEOREM 4. *Suppose L has a hyperbolic summand H, and we are in the ramified case. In the bad case, the lattices isomorphic to L fall into two equivalence classes under SU. In the good case, they are all SU-equivalent.*

We discussed above the tamely ramified case with $u = 1$. In the other cases, the bilinearised form over F_ρ is skew (and hence even dimensional): the only forms excluded are non-hyperbolic and 2-dimensional.

PROOF. Let $\bar{\delta} = \delta^{-1}$. Then $\delta = \bar{\xi}/\xi$ for some ξ, and we can suppose $v_\rho(\xi) = 0$ or 1. If $v_\rho(\xi) = 0$, we can define an automorphism of L by fixing the orthogonal complement of H, and mapping H (with basis e, f) by

$$e \to e\xi^{-1} \qquad f \to f\bar{\xi}:$$

this has determinant δ. We have thus represented half the possible values of δ.

Next consider the automorphism

$$e \to fu \qquad f \to e:$$

this has determinant $-u$, and if $u = -\bar{\pi}/\pi$, this is $\bar{\pi}/\pi$, one of the values of δ missed before. Composing with the automorphisms above, we get all values of δ: thus for $u = -\bar{\pi}/\pi$ all isomorphic lattices are SU-equivalent.

To deal with the bad case, we need a lemma,

LEMMA. *Write $\mathfrak{A}$ for the ideal generated by all $x - \bar{x}$, $x \in R_\rho$. Let $\delta \in R_\rho$, $\delta\bar{\delta} = 1$. Then $\delta = \bar{\xi}/\xi$ with ξ a unit $\Leftrightarrow 1 - \delta \in \mathfrak{A}$.*

PROOF. If $\delta = \bar{\xi}/\xi$ with ξ a unit, then

$$1 - \delta = \xi^{-1}(\xi - \bar{\xi}) \in \xi^{-1}\mathfrak{A} = \mathfrak{A}.$$

If not, then $\delta = \bar{\pi}/\pi$ with π prime. Now any $x \in R_\rho$ can be written as $a + b\pi$ with a, b invariant under α (and in R_ρ), so $x - \bar{x} = b(\pi - \bar{\pi})$, and $\mathfrak{A}$ is the ideal generated by $\pi - \bar{\pi}$. Thus

$$1 - \delta = \pi^{-1}\{\pi - \bar{\pi}\}$$

does not belong to $\mathfrak{A}$.

Now $\mathfrak{A}$ is certainly an α-invariant ideal of R_ρ, so a form over R_ρ induces one over $R_\rho/\mathfrak{A} = Q_\rho$. By definition of $\mathfrak{A}$, α induces the identity on this quotient ring, so in the case $u = -1$ we have a nonsingular skew-symmetric form over it. Any automorphism of the form over R (with determinant δ) induces one of this quotient which, by a well known result (see e.g. [3, p. 85]) has determinant 1. Thus $\delta \equiv 1 \bmod \mathfrak{A}$, and by the lemma, this is equivalent to $\delta = \bar{\xi}/\xi$ with ξ a unit. This completes the proof of the theorem.

SUMMARY. There are essentially 4 cases: decomposed, inert or ramified with $u = -\bar{\xi}/\xi$ and $v_\rho(\xi)$ even (good) or odd (bad). We always get some nonsingular quadratic forms, though in the ramified case the rank must be even (except in the good, tamely ramified case). In tabular form, our conclusions are:

	Decomposed	Inert	Good	Bad
classes over R_ρ	1	1	2	2†
classes over K_ρ	1	2*	2	2*
SU-classes	$\boldsymbol{Z}$	1	1	$\boldsymbol{Z}_2$

Here 'classes over $R_\rho(K_\rho)$' denotes the number of isomorphism classes of nonsingular quadratic forms of a given rank; the * denotes that only one of the two contains nonsingular lattices (it is the one with determinant or discriminant 1). Also 'SU-classes' describes those in a given isomorphism class.

ARCHIMEDEAN CASE. This has to be discussed too for completeness. For completeness of notation, write $r_\rho = k_\rho$, $R_\rho = K_\rho$ here. If the archimedean prime of k decomposes then, as in the non-archimedean decomposed case, the classification is trivial – and there is here no question of SU-classification either.

If ρ ramifies, the extension is isomorphic to $\boldsymbol{C}$ over $\boldsymbol{R}$, and we have hermitian forms in the classical sense (as usual, we can reduce u to 1 by scaling). There are $(r+1)$ isomorphism classes of forms of rank $r \geqq 0$, represented by

$$\phi((x_1, \cdots x_r), (y_1, \cdots, y_r)) = \sum_1^p \bar{x}_i y_i - \sum_{p+1}^r \bar{x}_i y_i$$

for $0 \leqq p \leqq r$. The *signature* σ of the form is the number of positive minus the number of negative terms: $2p-r$ (this is chosen to be zero for hyperbolic forms. It satisfies the conditions $|\sigma| \leqq r$, and $\sigma \equiv r \pmod 2$.) We will usually deal with forms of even rank, and write $\sigma = 2\tau$.

† Only one in the tamely ramified case.

The determinant of the above form is $(-1)^{r-p}$ (modulo norms – i.e. positive real numbers). If $r = 2k$, since the hyperbolic form of that rank has determinant $(-1)^k$, the discriminant is $\Delta = (-1)^{k-p} = (-1)^{p-k} = (-1)^{\tau}$. Unlike the discriminant, τ can be changed by scaling. Scaling by v reproduces a hermitian form if $v \in \boldsymbol{R}^{\times}$: if v is positive, τ is unaltered, but if v is negative, it is replaced by $-\tau$. This is unimportant for our theory, but may necessitate a little care in using our results.

Global theory

We first recall the classification of hermitian forms over K (note that by scaling we can suppose $u = 1$ over fields). Nonsingular forms of a given rank are classified [6] by the discriminant, and the signatures at Archimedean ramified primes. Another mnemonic for this result is the 'Hasse principle for $H^1(SU)$' [5a]: for forms of fixed (nonzero) discriminant, the global classification is equivalent to classifications at the Archimedean ramified primes alone; it is easily seen that the discriminant can take any value already in the 1-dimensional case.

As we have already said, we will tackle forms over R by considering lattices in vector spaces V with forms over K. To economise notation, this will mean a lattice L in the usual sense (finitely generated R-module which spans V over K), together with a quadratic form (over R) on L inducing the given form on V. We inherit on the localised L_ρ quadratic forms over R_ρ. These are not determined by the form on V and the embedding of L in V (or locally) in general. But the bilinearised form *is* determined, and hence so is the quadratic form on L_ρ except when ρ is wildly ramified.

The key observation to circumvent this difficulty is that Q is an arithmetic functor in the following sense. Let F be a functor defined on pairs consisting of a ring A and an A-module M, perhaps with some extra structure (we will actually take $F = Q_{(\alpha, u)}(L)$ or $S_\alpha(L, M)$ with two modules involved); covariant in A and contravariant in M. We call F an *arithmetic functor* if the diagram

$$\begin{array}{ccc} F(R, L) & \rightarrow & \oplus_\rho F(R_\rho, L \otimes_R R_\rho) \\ \downarrow & & \downarrow \\ F(K, L \otimes_R K) & \rightarrow & \oplus_\rho F(K_\rho, L \otimes_K K_\rho) \end{array}$$

is a pullback, for the rings R etc. defined above, and L a projective R-module of finite type [1]. If F is additive in the variable L, then the diagram corresponding to $L \oplus M$ will be a pullback if and only if the

[1] For this to make sense in the decomposed case, the primes ρ must be interpreted as primes of r.

diagrams for L and for M both are. Thus it suffices to check the pullback property when L is free, or indeed just when $L = R$.

PROPOSITION 5. *The functors* S_α, $R_{(\alpha, u)}$ *and* $Q_{(\alpha, u)}$ *are arithmetic.*

PROOF. $S_\alpha(L, M)$ is additive in L and in M, and $S_\alpha(R, R) \cong R$. Since the diagram

$$\begin{array}{ccc} R & \to & \oplus_\rho R_\rho \\ \downarrow & & \downarrow \\ K & \to & \oplus_\rho K_\rho \end{array}$$

is a pullback, the functor S_α is arithmetic. Now since $R_{(\alpha, u)}(L) = \operatorname{Ker}(1-T_u)$, arithmeticity of $R_{(\alpha, u)}$ follows by diagram chasing (essentially the snake lemma). For $Q_{(\alpha, u)}$ the result is not formal. But although Q is not additive, the (natural) splitting

$$Q_{(\alpha, u)}(L \oplus M) \cong Q_{(\alpha, u)}(L) \oplus S_\alpha(L, M) \oplus Q_{(\alpha, u)}(M)$$

shows, as in the additive case, that it is sufficient to consider the case $L = R$. Note that $Q_{(\alpha, u)}(R)$ is the quotient of R^+ by the additive subgroup of elements $x - u\bar{x}$ ($x \in R$); similarly for the other rings involved.

There are two things to check, which we will do in the next two paragraphs. The first amounts to this: let $z \in K$ be such that for all ρ there exists $x_\rho \in K_\rho$ with $z + x_\rho - u\bar{x}_\rho \in R_\rho$; then we must find $x \in K$ with $z + x - u\bar{x} \in R$. However, since $z \in R_\rho$ for almost all ρ (say $\rho \notin S$), it suffices to apply the strong approximation theorem (for K^+) to find $x \in K$ such that $x \in R_\rho$ for $\rho \notin S$ and $(x - x_\rho) \in R_\rho$ for $\rho \in S$. This x does what we need.

Secondly we must show that if $z \in R$ is of the form $x_\rho - u\bar{x}_\rho$ ($x_\rho \in R_\rho$) for all ρ, and of the form $x - u\bar{x}$ with $x \in K$, then we can choose $x \in R$. Let $\mathbf{Z}_2$ act on R^+ (and the other rings) by $x \mapsto u\bar{x}$. Since K^+ and K_ρ^+ are cohomologically trivial (we can divide by 2), what we have to show is that

$$H^1(\mathbf{Z}_2; R^+) \to \oplus_\rho H^1(\mathbf{Z}_2; R_\rho^+)$$

is an isomorphism. Now if ρ is non-dyadic, $H^1(\mathbf{Z}_2; R_\rho^+) = 0$. But $\oplus R_\rho$, extended over dyadic ρ, can be identified with the tensor product (over $\mathbf{Z}$) of R with the ring $\mathbf{Z}_{(2)}$ of 2-adic integers. It now remains only to observe that for any finitely generated $\mathbf{Z}_2$-module M, the natural map

$$H^1(\mathbf{Z}_2; M) \to H^1(\mathbf{Z}_2; M \otimes \mathbf{Z}_{(2)})$$

is an isomorphism.

It follows from the Proposition that the relation of L and the L_ρ is the classical one: assuming the local lattices L_ρ determine an R-module

L, there is one and only one quadratic form on L inducing the given forms on the L_ρ.

PROPOSITION 6. *Let V have a nonsingular u-quadratic form over K. Then V contains a nonsingular lattice if and only if $\Delta(V)$ is a norm at each inert and each bad ρ. Two such are in the same genus if and only if they have the same Arf invariant at each bad wild ρ.*

PROOF. Any lattice in V is nonsingular at almost all ρ: it follows at once from the description of lattices that V contains a nonsingular lattice if and only if each V_ρ does. The first result now follows by the local theory. So does the second, since except at bad wild ρ each form over K_ρ contains at most one class of lattices.

Now the extension K/k is quadratic, hence cyclic. By the Hasse norm theorem, an element of $k^\times$ is a norm if it is so everywhere locally (including Archimedean primes). Since this holds trivially at decomposed ρ, we see that the class of Δ modulo norms is determined (if Δ is as above) by its class at good (ramified) ρ and its class (i.e. sign) at Archimedean ramified ρ.

COROLLARY. *The class of Δ mod norms is determined by its classes at good ρ and signs at Archimedean ramified ρ. These are independent, except that an even number are non-trivial.*

The last statement follows at once from global class field theory. Note that Δ is a norm at inert ρ if and only if $v_\rho(\Delta)$ is even for such ρ.

Next we must describe when two lattices belong to the same SU-genus. It will be simpler first to describe the corresponding problem for SL. As we described in the discussion of decomposed primes above, we obtain integer obstructions: let us recapitulate. Let L, L' be lattices in V. For each prime ρ of K, L_ρ and L'_ρ are free R_ρ-modules, so there is an automorphism A_ρ of V_ρ with $A_\rho L_\rho = L'_\rho$. Then $v_\rho(\det A_\rho)$ does not depend on A_ρ, but only on the lattices L_ρ, L'_ρ: call it w_ρ. For almost all ρ, $L_\rho = L'_\rho$ so $w_\rho = 0$. Thus we can form an ideal

$$|L' : L| = \prod \rho^{w_\rho}.$$

We have shown that L and L' are in the same SL-genus if and only if $|L' : L| = R$.

Now we return to the case of SU. If L and L' are unimodular lattices, we see at once from the local theory that $w_\rho = 0$ for ρ inert or ramified. A decomposed prime ρ in r splits as the product of two primes $\rho'\rho''$ in R, interchanged by α, and the duality in the decomposed case shows that $w_{\rho'} = -w_{\rho''}$ is the obstruction we had before. Thus the obstruction in the decomposed case is detected by the ideal $\mathfrak{A} = |L' : L|$, and $\overline{\mathfrak{A}}\mathfrak{A} = 1$; conversely, any $\mathfrak{A}$ with $\overline{\mathfrak{A}}\mathfrak{A} = 1$ can so occur.

There remain the obstructions $\boldsymbol{Z}_2$ at the bad primes; these we can describe as follows. Choose an isomorphism A_ρ of L_ρ on L'_ρ, and write $\det A_\rho = \bar{\xi}_\rho/\xi_\rho$. Then the obstruction is $v_\rho(\xi_\rho)$ (mod 2); we denote it by $\theta_\rho(L, L')$.

SUMMARY. *Nonsingular lattices L and L' in the same genus are in the same SU-genus if and only if $|L' : L| = R$ and each $\theta_\rho(L, L') = 0$.*

More generally, the SU-genera of L' in the genus of L are classified by these invariants. which can vary independently.

The following basic result enables us to pass to a global classification.

THEOREM 7. *Lattices L and L' in an indefinite space V of rank $\geqq 2$ are isometric if and only if there exists an isometry A of V with AL and L' in the same SU-genus.*

PROOF. Necessity of the condition is clear. For sufficiency, we can replace L by AL, and so suppose L and L' locally SU-equivalent.

We have $L_\rho = L'_\rho$ for almost all ρ; for the others there exist isometries A_ρ with $A_\rho L_\rho = L'_\rho$. Any isometry close enough to A_ρ will also have this property. If ρ is wild, the condition $B_\rho L_\rho = L'_\rho$ does not imply that B_ρ is an isometry of quadratic forms, only of the bilinearisations; but there are only a finite number of forms with a given bilinearisation, and if B_ρ is close enough to A_ρ, it will given an isometry.

Since V is indefinite, we can apply the strong approximation theorem for SU [5b] [9] to find an SU-isometry B of V which preserves L_ρ when $L_\rho = L'_\rho$ and ρ is tame, and is close enough to A_ρ for other ρ to induce an isometry of L_ρ on L'_ρ. Then B gives an isometry of L_ρ on L'_ρ for all ρ and hence, since $Q_{(\alpha, u)}$ is arithmetic, of L on L'.

Note that the theorem does not assume the lattices unimodular. Also, the determinant of the isometry constructed equals that of the A given.

A similar argument with SL in place of SU shows that (ignoring forms) two lattices are isomorphic as R-modules if and only if there is an automorphism A of V with AL and L' in the same SL-genus, i.e. with $|L' : AL| = R$. Now $|AL : L|$ is the ideal $\langle \det A \rangle$ by definition, and $|L' : L| = |L' : AL||AL : L|$. Since any element of $K^\times$ is the determinant of an automorphism, L' is isomorphic to L if and only if $|L' : L|$ is principal; in general, we obtain a bijection of isomorphism classes (as modules) of lattices onto the ideal class group of R.

In applying the above theorem, note that A only appears via $\delta = \det A$ in determining the SU-genus of AL, and that the possible δ are precisely those elements of $K^\times$ satisfying $\delta\bar{\delta} = 1$, or equivalently, those of the form $\bar{\xi}/\xi$ with $\xi \in K^\times$. Recalling from the local theory the description of SU-genera in a genus, we have

COROLLARY. *Locally equivalent nonsingular lattices L and L′ in an indefinite space V of dimension* $\geqq 3$ *are isometric if and only if there exists* $\xi \in K^\times$ *with*

(i) $|L' : L| = \langle \bar{\xi}/\xi \rangle$
(ii) $\theta_\rho(L, L') = v_\rho(\xi)$ (mod 2) *for bad* ρ.

We have already observed that $|L' : L|$ and the $\theta_\rho(L, L')$ can vary independently.

Next we want to concentrate on free lattices: we must compare the above theory with the classification of modules. Also, we acquire a new invariant: the discriminant with respect to a free basis of the lattice.

Call a free R-module *based* if we are given an equivalence class of bases, two such being equivalent if and only if the determinant of the transformation relating them is 1. (You can think of this as a basis for the top exterior power, or as a sort of orientation.) For a based lattice L, $\Delta(L) \in K^\times$ is the discriminant of the form with respect to any preferred basis. If L and L' are two based lattices in V, and A is an automorphism of V, carrying a preferred base of L to one of L' and with determinant δ, then

$$\Delta(L') = \delta\bar{\delta}\Delta(L). \tag{1}$$

For a lattice L which need not be free (or nonsingular) we know at least that the L_ρ are free, and the numbers

$$\alpha_\rho = v_\rho(\Delta(L_\rho))$$

do not depend on choice of basis (e.g. by (1) since $\delta \in R_\rho^\times$ for an automorphism). We define the ideal (of r)

$$\Delta^0(L) = \prod \rho^{\alpha_\rho}.$$

If L is free, this is the ideal generated by $\Delta(L)$. Applying (1) locally we find that for lattices L, L' in general

$$\Delta^0(L') = |L' : L|\alpha(|L' : L|)\Delta^0(L). \tag{2}$$

PROPOSITION 8. *The space V contains a free lattice L′ in the genus of a given lattice L if and only if there is an* $x \in \Delta(V)$ *which generates* $\Delta^0(L)$; *moreover, we can then choose L′ based with* $\Delta(L') = x$.
(Note that here we do not assume L nonsingular.)

PROOF. Certainly if L' exists then $x = \Delta(L')$ belongs to $\Delta(V)$ and generates $\Delta^0(L') = \Delta^0(L)$. Conversely, suppose x given. Choose a free (based) lattice L''. Since $\Delta(L'') \in \Delta(V)$, there exists $b \in K$ such that

$$\Delta(L'') = b\bar{b}x.$$

Now by (2),

$$\langle b\bar{b}x\rangle = \Delta^0(L'') = |L'' : L|\alpha(|L'' : L|)\Delta^0(L).$$

Since $\Delta^0(L) = \langle x\rangle$, the ideal $\mathfrak{A} = \langle b^{-1}\rangle|L'' : L|$ satisfies

$$\bar{\mathfrak{A}}\mathfrak{A} = R.$$

We now choose L' so that $|L' : L| = \mathfrak{A}$. In fact, we can take $L'_\rho = L_\rho$ if ρ is inert (or ramified), and at decomposed primes we can subject the dual vector spaces to (dual) automorphisms with prescribed determinant, and so define $L'_\rho = A_\rho L_\rho$.

Now $|L'' : L'| = |L'' : L|/|L' : L| = \langle b\rangle$ is principal, so L' is free. This proves the main part of the Proposition. Let A be an automorphism of V (as vector space) with $\det A = b$ and $AL' = L''$. Give L' the base corresponding by A to the base of L''. Then

$$\Delta(L') = \Delta(L'')/b\bar{b} = x,$$

which concludes the proof.

COROLLARY. *V contains a free nonsingular lattice if and only if there exists $x \in R^\times$ such that $x \in \Delta(V)$, and for each bad ρ, x is a norm from $K_\rho^\times$.*

By Proposition 6 (or by the local theory) if V contains a nonsingular lattice, $\Delta(V)$ is a norm from $K_\rho^\times$ for bad ρ. Now if L is nonsingular, $\Delta^0(L) = R$, so $R^\times$ is the set of its generators. The assertion thus follows from Propositions 6 and 8.

The classification of based lattices is now given, assuming V indefinite, of dimension $\geqq 2$ (but the result is trivial when $\dim V = 1$) by

PROPOSITION 9. (i) *Let L, L' be based lattices in V with the same (non-zero) discriminant. Then there is an isometry A of V with $|L' : AL| = R$.*

(ii) *If also $|L' : L| = R$, and L is unimodular, then L and L' are isometric (preserving the base) if and only if $\theta_\rho(L, L') = 0$ for all bad ρ.*

PROOF. (i) Let $B : L \to L'$ be an isomorphism induced by the given bases, extending to an automorphism B of V. Since the discriminants are the same, $b = \det B$ satisfies $b\bar{b} = 1$. Choose A to be an isometry of V with determinant b. (ii) An isometry preserving the base of L has determinant 1, so belongs to SU. The question is thus whether L and L' are SU-equivalent; by Theorem 7, this amounts to local SU-equivalence, and the result follows from our description of this condition.

This gives the isometry classification of based free lattices. If we change the basis of L by an automorphism with determinant ε, we must have $\varepsilon \in R^\times$, and all elements of $R^\times$ so arise. If the discriminant is to be unchanged, $\varepsilon\bar{\varepsilon} = 1$. Write $\varepsilon = \bar{\xi}/\xi$: then $\theta_\rho(L, L')$ will be changed by $v_\rho(\xi)$.

Thus free lattices in a given genus and with a given discriminant are classified by an obstruction in the cokernel $\mathscr{G}_u$ of the map

$$\{\varepsilon \in R^\times : \varepsilon\bar{\varepsilon} = 1\} \to \bigoplus_{\rho \text{ bad}} \boldsymbol{Z}_2$$

just described.

We can describe this group somewhat differently by writing I^+ for the group of α-invariant ideals $\Pi\rho^{m_\rho}$, and $I^{+,u}$ for the subgroup with m_ρ even for ρ bad, so that

$$I^+/I^{+,u} \cong \bigoplus_{\rho \text{ bad}} \boldsymbol{Z}_2 .$$

The above map is given by taking the image of the ideal $\langle\xi\rangle$. Now $\bar{\xi}/\xi \in R^\times$ if and only if $\langle\xi\rangle \in I^+$, so we must factor out the principal ideals in I^+ to obtain

$$\mathscr{G}_u = I^+/(P \cap I^+)\cdot I^{+,u}.$$

Cancellation and stability theorems

We prove two theorems analogous to ones well known for projective modules. Both are easy consequences of the preceding.

THEOREM 10. *Let L, L', M be projective R-modules of finite type with nonsingular (α, u)-quadratic forms, such that $L \oplus M \cong L' \oplus M$. If L is indefinite, of rank $\geqq 3$, then $L \cong L'$.*

PROOF. Let q be the form on M. Then $(M, q) \oplus (M, -q) \cong H(M)$. Let N be such that $M \oplus N$ is free of finite type. Adding $(M, -q)$ and $H(N)$, we see that it is sufficient to prove the theorem when M is hyperbolic on a free module. By induction, it suffices to consider the case $M = H(R)$.

Since the cancellation theorem holds for fields, we can suppose L, L' lattices in the same space V with form over K. Since it holds locally, L and L' are in the same genus. Let A be the extension to $V \oplus H(K)$ of the given isometry of $L \oplus H(R)$ on $L' \oplus H(R)$; let $\det A = \delta = \bar{\xi}/\xi$. Then

$$|L' : L| = |L' \oplus H(R) : L \oplus H(R)| = \langle\delta\rangle$$

and

$$\theta_\rho(L, L') = \theta_\rho(L' \oplus H(R), L \oplus H(R)) = v_\rho(\xi) \pmod 2 \text{ for } \rho \text{ bad}.$$

By Theorem 7, Corollary, L and L' are isometric.

Note that this does not follow from the results of Bak [2], who had to assume that L possessed a hyperbolic summand. Note that also the assumption of rank $\geqq 3$ can be abandoned if we can prove Theorem 4 for non-hyperbolic planes.

THEOREM 11. *Let L be a projective R-module of finite type with rank $\geqq 3$ and nonsingular (α, u)-quadratic form which is indefinite at each archimedean ramified place. Then there exist a form on a module M and an isometry $L \cong M \oplus H(R)$.*

PROOF. The hypothesis about archimedean places enables us to use the classification over K and write

$$L \otimes_R K = V \oplus H(K)$$

(the isomorphism preserving the form). For any lattice in V, the isomorphism will hold locally at most ρ; in fact, since we have arranged things over K, V has a nonsingular lattice M' and the isomorphism holds at all but bad wild ρ. Adjusting M' at these ρ to get M'', we can suppose $M'' \oplus H(R)$ in the genus of L. As usual, we can find a lattice M''' so that

$$|M''' : M''| = |L : M'' \oplus H(R)|,$$

and thus $|L : M''' \oplus H(R)| = R$. Now further change M''' at the bad primes so that $\theta_\rho(M, M''') = \theta_\rho(L, M''' \oplus H(R))$ and it follows from Theorem 7 Corollary that $L \cong M \oplus H(R)$. (Note that if L has rank 3, there are no bad primes.)

Calculation of Witt groups

We have completed the main theoretical work of classification of forms; it still remains, however, to formulate our results more conveniently for applications – in particular, to replace the language of lattices by that of modules.

Consider the set of isometry classes of nonsingular (α, u)-quadratic forms on finitely generated projective R-modules M. Orthogonal direct sum gives a composition law on this set which makes it an abelian monoid. One problem is to describe the universal group of this monoid: in view of the cancellation theorem, this is equivalent to the classification in ranks $\geqq 4$. Examples of forms are given by the hyperbolic spaces on finitely generated projective R-modules: factoring out the subgroup these generate gives a quotient which we denote by $W_P(R; \alpha, u)$, and will compute below.

We can also restrict to free modules, and indeed to ones with preferred classes of bases. The discussion is as above; this time we only factor out the hyperbolic spaces on free based R-modules, to define the Witt group $W_B(R; \alpha, u)$. We wish to describe this group; also the subgroup $W_{SB}(R; \alpha, u)$ corresponding to forms with discriminant 1, and the quotient group $W_F(R; \alpha, u)$ obtained by forgetting the preferred basis. We restrict ourselves for a while to forms of even rank.

Since our invariants c and τ are additive, and Δ is multiplicative, for orthogonal direct sums, and all are trivial on hyperbolic spaces, they define homomorphisms of the Witt groups. We shall determine the kernels and cokernels of these homomorphisms. The main tool for computing W_P is the following.

THEOREM 12. *A form on a projective R-module M is hyperbolic if and only if it becomes so over each* R_ρ.

PROOF. Clearly the condition is necessary. If it is satisfied, the form is hyperbolic over each K_ρ, so the signature is zero and the discriminant is locally, hence globally a norm, so the form also become hyperbolic over K. Thus we can regard M as a lattice in a hyperbolic space V over K.

Let L be a hyperbolic lattice in V, on a free R-module: $L = H(R^k)$. By hypothesis, M is in the genus of L. Then $|L : M| \in I^-$. Choose an ideal $\mathfrak{A}_1$, with only decomposed primes as factors, such that $\overline{\mathfrak{A}}_1 \mathfrak{A}_1^{-1} = |L : M|$. Define $\mathfrak{A}_2$ as the product over bad primes

$$\mathfrak{A}_2 = \Pi\, \rho^{\theta_\rho(L, M)}.$$

I claim that $N = H(\mathfrak{A}_1 \mathfrak{A}_2 + R^{k-1})$ is the SU-genus of M, and hence isometric to it, which will conclude the proof.

First

$$\begin{aligned} |N : L| &= |H(\mathfrak{A}_1 \mathfrak{A}_2 + R^{k-1}) : H(R^k)| \\ &= |\mathfrak{A}_1 \mathfrak{A}_2 : R||\overline{\mathfrak{A}}_1^{-1} \overline{\mathfrak{A}}_2^{-1} : R| \\ &= \mathfrak{A}_1 \mathfrak{A}_2 \overline{\mathfrak{A}}_1^{-1} \overline{\mathfrak{A}}_2^{-1} = |L : M|^{-1}, \end{aligned}$$

so $|M : N| = 1$. Next, for bad ρ, choose π a prime of R_ρ and write m for $\theta_\rho(L, M)$; then an automorphism of $H(K_\rho)$ sending $H(R_\rho)$ to $H((\mathfrak{A}_1 \mathfrak{A}_2)_\rho) = H(\rho^m R_\rho)$ is

$$e \to e\pi^m \qquad f \to f \bar{\pi}^{-m},$$

with determinant $(\pi/\bar{\pi})^m$. Thus $\theta_\rho(H(R), H(\mathfrak{A}_1 \mathfrak{A}_2)) = m = \theta_\rho(L, M)$, and so $\theta_\rho(L, N) = \theta_\rho(L, M)$ and hence $\theta_\rho(M, N) = 0$. Thus M and N are in the same SU-genus, as required.

It follows from this result that the class of a form in W_P is determined by its local invariants. We have already determined all the relations between these. Indeed, the invariants are:

$\tau_\rho \in \mathbf{Z}$	for Archimedean ramified ρ
$c_\rho \in \mathbf{Z}_2$	for bad, wildly ramified ρ
$\Delta_\rho \in \mathbf{Z}_2$	for good ramified ρ.

In fact, Δ_ρ is a class modulo norms but the group of such classes only has two elements. We can exclude the Archimedean case here since Δ_ρ would only be the mod 2 reduction of τ_ρ. The only relation between the invariants is the one from global class field theory:

$$\sum_\rho \Delta_\rho = 0$$

where ρ runs over all ramified ρ, including Archimedean: we can express this in the notation above as

$$\sum_\rho \tau_\rho + \sum_\rho \Delta_\rho = 0 \pmod 2.$$

We can also recall that for good wildly ramified ρ we also had an Arf invariant c_ρ, and in the present notation, $c_\rho = \Delta_\rho$. For good tame ρ we can regard Δ_ρ as a class mod squares in $F_\rho^\times$.

For W_B we can again list the available invariants: they are

$$\tau_\rho \in \boldsymbol{Z} \qquad \text{for Archimedean ramified } \rho$$

$$c_\rho \in \boldsymbol{Z}_2 \qquad \text{for bad, wildly ramified } \rho$$

and $\Delta \in r^\times$.

The relations between these are:

$(-1)^{\tau_\rho}\Delta$ is positive at ρ (Archimedean ramified),

Δ is a norm from $K_\rho^\times$ for ρ bad.

Given two forms with the same invariants, we can add hyperbolic spaces till both are indefinite, of the same rank $\geqq 4$. As in the proof of Theorem 12, they become equivalent over K, so we may regard them as lattices in the same spaces. By Proposition 9, we may suppose $|L : L'| = R$; the forms are then (base-preserving) isometric if and only if $\theta_\rho(L, L') = 0$ for each bad ρ, and the θ_ρ can take any value. Since θ_ρ is unaltered by adding a common hyperbolic summand to L and L', it appears in W_B. More precisely, we have shown

PROPOSITION 13. *There is an exact sequence*

$$0 \to \bigoplus_{\rho \text{ bad}} \boldsymbol{Z}_2 \xrightarrow{(\theta)} W_B(R, \alpha, u) \xrightarrow{(\tau, c, \Delta)} \bigoplus_{\substack{\rho \text{ Arch} \\ \text{ram}}} \boldsymbol{Z} \oplus \bigoplus_{\substack{\rho \text{ bad} \\ \text{wild}}} \boldsymbol{Z}_2 \oplus r^\times \xrightarrow{(\Delta)} \bigoplus_{\substack{\rho \text{ Arch} \\ \text{ram}}} \boldsymbol{Z}_2 \oplus \bigoplus_{\rho \text{ bad}} \boldsymbol{Z}_2,$$

where the maps are as described above.

To determine this extension, we define a new invariant of based forms, using the proof of Theorem 4. Note that a based (α, u)-quadratic form over R determines in turn forms over R_ρ and over $Q_\rho = R_\rho/\mathfrak{A}$. The corresponding reflexive form over Q_ρ is (in the bad case) strictly skew-symmetric. Then (see e.g. Bourbaki [4, p. 79] – or indeed our own treatment of the local case) this is, ignoring bases, hyperbolic. Let

$\kappa_\rho \in Q_\rho^\times$ be the determinant of a change of base from the given base to a symplectic base. Since any automorphism of the form has determinant 1, κ_ρ is well-defined. The discriminant of the form with respect to the given base is then κ_ρ^2.

However, we can be more precise. The proof of Theorem 4 shows that the bilinearised skew-hermitian form is in fact hyperbolic over R_ρ. Thus we can find a change of base from the given base to a symplectic base over R_ρ: if this has determinant x, the form has discriminant $\Delta = \bar{x}x$. Clearly κ_ρ is the reduction of x mod $\mathfrak{A}$, so (as just noted) $\kappa^2 = \bar{\kappa}_\rho\kappa_\rho$ is the reduction of Δ mod $\mathfrak{A}$. In fact, though, κ_ρ determines Δ mod $\mathfrak{A}^2$, for if $x, x' \in R^\times$ with $x-x' \in \mathfrak{A}$, the quotient $x'/x \in 1+\mathfrak{A}$ has the form

$$1+a(\bar{\pi}-\pi) \qquad a = R_\rho,$$

thus

$$\begin{aligned}\bar{x}'x'/\bar{x}x &= \{1+a(\bar{\pi}-\pi)\}\{1-\bar{a}(\bar{\pi}-\pi)\}\\ &= 1+(a-\bar{a})(\bar{\pi}-\pi)-a\bar{a}(\bar{\pi}-\pi)^2 \in 1+\mathfrak{A}^2,\end{aligned}$$

so

$$\bar{x}'x' \equiv \bar{x}x \mod \mathfrak{A}^2.$$

We shall write

$$\bar{\kappa}_\rho\kappa_\rho = \Delta \pmod{\mathfrak{A}^2}$$

to denote that for some (hence all) $x \in R_\rho$ reducing mod $\mathfrak{A}$ to κ_ρ we have

$$\bar{x}x \equiv \Delta \pmod{\mathfrak{A}^2}.$$

We shall now show that this is the only further relation obtained when κ_ρ is added to our list of invariants. For this it suffices (by our earlier discussion) to show that Δ determines κ_ρ up to multiplication by $\bar{\pi}/\pi$ (mod $\mathfrak{A}$). Since the relation is multiplicative, this amounts to showing that

$$\bar{\kappa}\kappa = 1 \pmod{\mathfrak{A}^2}$$

implies that κ is 1 or $\bar{\pi}/\pi$. Using the lemma from the proof of theorem 4, this now follows from

Lemma 14. *Let $x \in R_\rho^\times$, $\bar{x}x \in 1+\mathfrak{A}^2$. Then there exists $y \in 1+\mathfrak{A}$ such that $z = xy$ satisfies $\bar{z}z = 1$.*

Proof. We prove the result by successive approximation. Write

$$\bar{x}x = 1+a(\bar{\pi}-\pi)^2 \qquad a \in r_\rho.$$

Choose

$$y_1 = 1+a\pi(\bar{\pi}-\pi).$$

Then

$$\begin{aligned}\bar{y}_1y_1 &= \{1+a\pi(\bar{\pi}-\pi)\}\{1-a\bar{\pi}(\bar{\pi}-\pi)\}\\ &= 1-a(\bar{\pi}-\pi)^2-a^2\pi\bar{\pi}(\bar{\pi}-\pi)^2,\end{aligned}$$

so

$$\bar{x}x\bar{y}_1y_1 = 1-a^2(\bar{\pi}-\pi)^4-a^2\pi\bar{\pi}(\bar{\pi}-\pi)^2x\bar{x}.$$

Thus replacing x by xy_1 has the effect of replacing a by

$$a_1 = -a^2(\bar{\pi}-\pi)^2-a^2\pi\bar{\pi}x\bar{x}$$

which is clearly of a higher value. If we iterate the process, with

$$\overline{(xy_1\cdots y_{n-1})}(xy_1\cdots y_{n-1}) = 1+a_n(\bar{\pi}-\pi)^2$$

then $v(a_n)\to\infty$, so as $y_n = 1+a_n\pi(\bar{\pi}-\pi)$, the product $\prod y_n$ converges to y, say and the result follows.

COROLLARY. *A complete determination of W_B is obtained by adding $\{\kappa_\rho : \rho \text{ bad}\}$ to the list of invariants, and*

$$\bar{\kappa}_\rho\kappa_\rho \equiv \Delta \pmod{\mathfrak{A}_\rho^2}$$

to the list of relations.

For calculations it is worth noting that if ρ is tame then $\mathfrak{A}_\rho = \rho$, so $Q_\rho = F_\rho$, $\kappa_\rho \in F_\rho^\times$, and the relation states merely that the image of Δ in $F_\rho^\times$ is κ_ρ^2.

This shows that the extension in Proposition 13 need not split, though of course the 'part' involving signature and Arf invariant – i.e. Ker Δ – does. Thus we have

$$(\kappa,\tau,c) : W_{SB} \cong \bigoplus_{\rho\text{ bad}} Z_2 \oplus \bigoplus_{\rho\text{ Arch ram}} 2Z \oplus \bigoplus_{\rho\text{ bad wild}} Z_2.$$

An example is as follows.

EXAMPLE. $K = \boldsymbol{Q}[\sqrt{5}]$, $k = \boldsymbol{Q}$, $r = \boldsymbol{Z}$, $R = \boldsymbol{Z}[\tau]$ with $2\tau = \sqrt{5}-1$. Then 5 is the only ramified prime. If $u = -1$, 5 is bad. The only invariants are

$$\Delta \in r^\times = \{\pm 1\}$$
$$\kappa \in F_\rho^\times$$

and the only non-trivial relation that $\Delta = \kappa^2 \pmod 5$. Thus $\kappa : W_B \cong F_\rho^\times$, which is cyclic of order 4.

It is not so easy to determine W_F explicitly as to give W_B. Clearly we have an exact sequence

$$R^\times \xrightarrow{\delta} W_B \to W_F \to 0,$$

where $\delta(x)$ represents a change of base with determinant x, and is given in terms of our invariants by

$$\tau(\delta(x)) = 0 \qquad c(\delta(x)) = 0$$
$$\Delta(\delta(x)) = \bar{x}x \qquad \kappa_\rho(\delta(x)) = x \pmod{\mathfrak{A}_\rho}.$$

Provided $r^{\times}$, $R^{\times}$ can be effectively determined, this gives an effective computation of W_F. In the example above, since $2+\sqrt{5}$ is a unit whose image generates $F_{\rho}^{\times}$, $W_F = 0$. Our earlier theory amounted to the less effective sequence

$$0 \to \mathscr{G}_u \to W_F \xrightarrow{(\tau, c, \Delta)} \bigoplus_{\substack{\rho \text{ Arch} \\ \text{ram}}} \boldsymbol{Z} \oplus \bigoplus_{\substack{\rho \text{ bad} \\ \text{wild}}} \boldsymbol{Z}_2 \oplus r^{\times}/NR^{\times} \to \bigoplus_{\substack{\rho \text{ Arch} \\ \text{ram}}} \boldsymbol{Z}_2 \oplus \bigoplus_{\rho \text{ bad}} \boldsymbol{Z}_2 .$$

The example which motivated our study was the case where K is a cyclotomic field, α takes each root of unity to its inverse, and $u = \pm 1$. Since always $-1 \in K$, write $2N$ for the order of the group of roots of unity in K; R etc. as usual. The determination of the Witt groups is given in general above: all that remains is to classify the ramified primes and to compute G_u.

The degree of K over $\boldsymbol{Q}$ is $\phi(2N)$ (the Euler ϕ-function); all Archimedean primes ramify in K/k, thus there are $\frac{1}{2}\phi(2N)$ of them. If N has more than one prime divisor, no other primes ramify. If N is a power of p, just one non-Archimedean prime ρ in k ramifies in K: the residue class field has order p. If p is odd, ρ is good if $u = 1$, bad if $u = -1$. If p is even, since K is generated over k by $\omega - \omega^{-1}$ ($\omega = \exp 2\pi i/2N$) with square in k: one easily computes $v_{\rho}(\omega - \omega^{-1}) = 2$, so if π is a prime, $v = (\omega - \omega^{-1})/\pi\bar{\pi}$ is a unit with $\bar{v}/v = -1$. Thus both the cases $u = \pm 1$ are bad. Now the extension for W_B splits, for since the only root of unity in k, -1, is not positive at ramified Archimedean primes, the image of the invariant map is free abelian. As to W_F, we note that $G_u = 1$: indeed, $\omega = \xi/\bar{\xi}$ with $\xi = 1+\omega$ and $v_{\rho}(1+\omega) = 1$ (compute its norm). The only other remark to add to the general discussion is that $r^{\times}$ is (by the Dirichlet theorem) the direct product of $\{\pm 1\}$ and a free abelian group of rank $\frac{1}{2}\phi(2N) - 1$: if (as happens sometimes but not always) the signs of these units are independent, then the class of a unit in $r^{\times}/NR^{\times}$ is determined by its signs, so the invariant Δ can be dropped.

Finally, we mention the case when (α, u) are such that there exist nonsingular forms of odd rank: by the local theory and Proposition 6, this is the case when all non-Archimedean ramified primes are tame and good. Since there are no bad primes, the isomorphism class of a free lattice is determined by its determinant and the signatures (provided the form is indefinite, of rank $\geqq 2$). All that needs doing now is to describe the relations. Rather than τ it is more convenient to use as invariant the index – i.e. the number q of negative terms. Then D has the sign of $(-1)^q$, and the invariants q are independent otherwise (except that $0 \leqq q \leqq r$, where r is the rank of the form); these and the rank r give all we need.

REFERENCES

C. Arf
[1] Untersuchungen über quadratische Formen in Körpern der Charakteristik 2. Crelle's Journal 183 (1941), 148–167.

A. Bak
[2] On modules with quadratic forms. In 'Algebraic K-theory and its Geometrical Applications'. Springer Lecture Notes, vol. 108 (1969), 55–66.

N. Bourbaki
[3] Algèbre Ch. 9: Formes sesquilinéaires et formes quadratiques. Hermann, Paris 1959.

N. Bourbaki
[4] Algèbre Commutative Ch. 3: Graduations, filtrations et topologies. Hermann, Paris, 1961.

M. Kneser
[5] (a) Hasse principle for H^1 of simply connected groups, pp. 159–163. (b) Strong approximation. pp. 187–196, in Proceedings of Symp. in Pure Math. IX: Algebraic groups and discontinuous subgroups. Amer. Math. Soc. 1966.

W. Landherr
[6] Aquivalenz Hermitscher Formen über einem beliebigen algebraischen Zahlkörper. Abh. Math. Sem. Hamburg 11 (1936), 245–248.

O. T. O'Meara
[7] Introduction to quadratic forms. Springer-Verlag.

J.-P. Serre
[8] Corps Locaux. Hermann, 1962.

G. Shimura
[9] Arithmetic of unitary groups. Ann. of Math. 79 (1964), 369–409.

C. T. C. Wall
[10] On the axiomatic foundations of the theory of Hermitian forms. Proc. Camb. Phil. Soc. 67 (1970), 243–250.

(Oblatum 9–II–1970)

Prof. C. T. C. Wall,
Department of Pure Mathematics,
The University of Liverpool,
Liverpool-3,
Great-Britain.