QUADRATIC FORMS OVER ARBITRARY FIELDS

B. BUZBY AND G. WHAPLES

Introduction. Witt [5] proved that two binary or ternary quadratic forms, over an arbitrary field (of characteristic not 2) are equivalent if and only if they have the same determinant and Hasse invariant. His proof is brief and elegant but uses a lot of the theory of simple algebras. The purpose of this note is to make this fundamental theorem more accessible by giving a short proof using only the general results of modern theory of cohomology of finite groups.

Professor Artin (Princeton lectures, 1956) gave such a proof for fields k over which local class field theory holds. For such fields, the group of values of the quadratic norm residue symbol is cyclic of order 2 while for arbitrary fields it may be any abelian group of exponent 2. So our proof is necessarily different from his; still it owes much to his methods.

Norm residue symbol. All fields mentioned here shall be assumed to have characteristic not 2. If K/k is normal then $H^2(K/k) = H^2(G(K/k), K^\cdot)$ shall denote the 2-cohomology group of the Galois group of K/k over $K^\cdot$. If K/k is cyclic then this group is isomorphic to the norm class group $k^\cdot/N_{K/k}K^\cdot$. This isomorphism is not canonical but depends on choice of a generator of the Galois group or of its character group. (For explicit descriptions see Chevalley [1] or Whaples [4].) But when K/k is of degree 2 there is only one such generator, hence a unique isomorphism.

For $\alpha, \beta \in k$ (and $\neq 0$) we define (α, β) to be the 2-cohomology class in $H^2(k(\alpha^{1/2})/k)$ corresponding to the element of the norm class group defined by β. However, we shall identify an element of $H^2(K/k)$ with an element of $H^2(L/k)$ whenever the lifts of these elements to $H^2(\Omega/k)$, for some $\Omega \supset K$ and $\Omega \supset L$, are equal. This is justified by the wellknown fact that for 2-cohomology groups over $K^\cdot$ the lift maps are isomorphisms into and form a transitive mapping system. (One may consider (α, β) as denoting an element of the group $H^2(G(k^{\text{clos}}/k), k^{\text{clos}})$, of the algebraic closure of k, this group being defined either as a direct limit or as a group of "continuous cocycles" of the Eilenberg-MacLane [2] type. But this notion can be avoided since all cohomology classes occurring in any discussion can be considered as elements of $H^2(\Omega/k)$ for some large but finite Ω/k.)

Thus $(\alpha_1, \alpha_2) = (\alpha_3, \alpha_4)$ means that these cocycles have the same lift to the field $k(\alpha_1^{1/2}, \alpha_3^{1/2})$. This can very well happen even when the

Received by the editors October 29, 1957.

fields $k(\alpha_i^{1/2})$ are four different fields; in this case $k(\alpha_1^{1/2})$ and $k(\alpha_3^{1/2})$ (and, because $(\alpha_i, \alpha_j) = (\alpha_j, \alpha_i)$, also $k(\alpha_2^{1/2})$ and $k(\alpha_4^{1/2})$) are each called a *field of definition* for (α_1, α_2).

Alternative descriptions: Witt [5] defined (α, β) to be a certain class of quaternion algebras; our (α, β) is the 2-cohomology class defining this algebra class. Under the original Eilenberg-MacLane [2] definitions, (α, β) is the cohomology class containing the function f with

$$f(\sigma, \tau) = \begin{cases} \beta \text{ if neither } \sigma \text{ nor } \tau \text{ is 1 on } k(\alpha^{1/2}), \\ 1 \text{ otherwise.} \end{cases}$$

By definition, $(\alpha, \beta) = 1$ if and only if β is a norm from $k(\alpha^{1/2})$. It satisfies the rules

(1) $(\alpha_1\alpha_2, \beta) = (\alpha_1, \beta)(\alpha_2, \beta)$; $(\alpha, \beta_1\beta_2) = (\alpha, \beta_1)(\alpha, \beta_2)$.

(2) $(\alpha, \beta) = (\beta, \alpha)$

(3) $(\alpha, \beta) = 1 \Longleftrightarrow \xi^2 - \alpha\eta^2 - \beta\zeta^2 = 0$ has a nontrivial solution in k.

Note in particular that $(\alpha\xi^2, \beta) = (\alpha, \beta)$ and $(\alpha, -\alpha) = (\alpha, 1-\alpha) = 1$. (2) is a consequence of these rules and (1).

Hasse invariant. We use Witt's notion of metric spaces and a similar notation. Latin letters denote vectors, Greek letters field elements. $\mathfrak{U} \perp \mathfrak{V}$ denotes orthogonal sum of $\mathfrak{U}$ and $\mathfrak{V}$, each of which is called a *component* of $\mathfrak{U} \perp \mathfrak{V}$. $\langle x_1, \cdots, x_n \rangle$ denotes the metric space generated by $x_1 \cdots x_n$. The symbol $\cong$ denotes that two spaces are isometric; also, $\mathfrak{x} \cong (\alpha_{ij})$ means that $\mathfrak{x}$ has a basis $x_1, \cdots, x_n$ with $x_i x_j = \alpha_{ij}$. The *determinant* $d(\mathfrak{x})$ is the element of $k/k^{\cdot 2}$ containing $\det((\alpha_{ij}))$; it is clearly an invariant under isometry. (Sometimes we use $d(\mathfrak{x})$ to denote an element of k.) If $\mathfrak{x} = \langle x_1 \rangle \perp \langle x_2 \rangle \perp \cdots \perp \langle x_n \rangle$ with $x_i^2 = \alpha_i$ we write $\mathfrak{x} \cong \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$. We restrict ourselves to spaces with nonzero determinant. Witt showed that every such space can be put in form $\{\alpha_1, \cdots, \alpha_n\}$ and defined the *Hasse invariant* of such an expression by

$$(4) \quad S(\{\alpha_1, \cdots, \alpha_n\}) = \prod_{i \leq j} (\alpha_i, \alpha_j) = (\alpha_1 \cdots \alpha_n, -1) \prod_{i<j} (\alpha_i, \alpha_j).$$

(Of course, the symbols (α_i, α_j) here stand for cohomology, rather than algebra, classes.)

It is easy to show that

$$(5) \quad \begin{aligned} &S(\{\alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_m\}) \\ &\qquad = S(\{\alpha_1, \cdots, \alpha_m\}) \cdot S(\{\beta_1, \cdots, \beta_n\}) (\prod \alpha_\mu, \prod \beta_\nu). \end{aligned}$$

To show that S depends only on the space and not on choice of a representation $\{\alpha_1, \cdots, \alpha_n\}$, Witt showed that if $\{\alpha_1, \cdots, \alpha_n\} \cong \{\beta_1, \cdots, \beta_n\}$ then they can be connected by a chain of isometries each of which changes only the representation of a two dimensional component. By (5) this reduces the invariance proof to the two dimensional case. Witt's proof of this case uses algebras so we give another.

LEMMA 1. *$\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ are isometric if and only if their determinants and Hasse invariants are equal.*

PROOF. Suppose first that they are isometric. Then they have the same determinant. Since multiplying one of the α_i or β_i by a square does not change the Hasse invariant or the isometry class, we may assume that $\alpha_1\alpha_2 = \beta_1\beta_2$. Then our two forms can be rewritten as $\{\alpha, \beta\gamma\}$ and $\{\alpha\beta, \gamma\}$. ($\alpha = \alpha_1$, $\beta = \beta_1/\alpha_1$, $\gamma = \beta_2$.) The Hasse invariants are $(\alpha\beta\gamma, -1)(\alpha, \beta\gamma) = (\alpha\beta\gamma, -1)(\alpha, \gamma)(\alpha, \beta)$ and $(\alpha\beta\gamma, -1)(\alpha, \gamma) \cdot (\beta, \gamma)$. Hence they are equal if and only if $(\beta, \alpha\gamma) = 1$, which is true exactly when

$$\xi^2 - \eta^2\beta - \zeta^2\alpha\gamma = 0 \tag{6}$$

has a nontrivial solution in k. But (6) is equivalent to

$$\xi^2\alpha - \eta^2\alpha\beta - \omega^2\gamma = 0, \tag{7}$$

and if our spaces are isometric then (7) has a solution with $\xi = 1$ because $\{\alpha\beta, \gamma\}$ represents α.

Now suppose that our spaces have the same determinant (hence are again of form $\{\alpha\beta, \gamma\}$ and $\{\alpha, \beta\gamma\}$) and Hasse invariant. Then (6) has a nontrivial solution, so (7) has also. If $\{\alpha\beta, \gamma\}$ does not represent 0, then $\xi \neq 0$ in (7) so $\{\alpha\beta, \gamma\}$ represents α. Hence $\{\alpha\beta, \gamma\} \cong \{\alpha, \delta\}$ for some $\delta \in k$ and considering the determinant shows that δ can be taken to be $\beta\gamma$. So Lemma 1 is proved except for the case when one of the spaces represents 0. This case will be settled by Lemma 2.

LEMMA 2. *All binary forms which represent 0 are isometric. A binary form represents $0 \Leftrightarrow$ its determinant is negative of a square $\Rightarrow$ its Hasse invariant is $(-1, -1)$.*

PROOF. Equation $\xi^2\alpha + \eta^2\beta = 0$ has a nontrivial solution in k if and only if $\alpha\beta \in (-1)k^{\cdot 2}$. So a binary form which represents 0 can be put in the form $\langle x, y\rangle \cong \{\alpha, -\alpha\}$. Then

$$\langle (x - y)/2\alpha, x + y\rangle \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cong \{1, -1\}.$$

This proves the first sentence of the lemma and the first equivalence. Finally, $S(1, -1) = (1, -1)(-1, -1) = (-1, -1)$.

Ternary spaces. If $\mathfrak{S} \cong \{\alpha_1, \cdots, \alpha_n\}$ and $\alpha \in k$ we define (after O'Meara [3]) $\alpha \circ \mathfrak{S}$ to be the space $\{\alpha\alpha_1, \cdots, \alpha\alpha_n\}$. It is easy to see that $\alpha \circ \mathfrak{S}$ depends only on $\mathfrak{S}$ and not on the representation of it, and that

$$\begin{aligned} d(\alpha \circ \mathfrak{S}) &= \alpha^n d(\mathfrak{S}), \\ S(\alpha \circ \mathfrak{S}) &= \prod_{i \le j} (\alpha\alpha_i, \alpha\alpha_j) = \prod_{i \le j} ((\alpha_i, \alpha_j)(\alpha, \alpha_j)(\alpha, \alpha)(\alpha, \alpha_i)), \\ &= S(\mathfrak{S})(\alpha, d(\mathfrak{S}))^{n+1}(\alpha, -1)^{n(n+1)/2}. \end{aligned}$$

From this it follows that if $\mathfrak{S}$ and $\mathfrak{T}$ are spaces of the same dimension then they are isometric, have the same determinant, or have the same determinant and the same Hasse invariant if and only if the corresponding relation holds between $\alpha \circ \mathfrak{S}$ and $\alpha \circ \mathfrak{T}$.

THEOREM. *Two ternary forms are isometric if and only if they have the same determinant and Hasse invariant.*

PROOF. If $\mathfrak{S}$ and $\mathfrak{T}$ have determinant δ then $\delta \circ \mathfrak{S}$ and $\delta \circ \mathfrak{T}$ have determinants which are squares. So we may assume $\mathfrak{S}$ and $\mathfrak{T}$ have square determinants, hence that $\mathfrak{S} = \{\alpha, \beta, \alpha\beta\}$ and $\mathfrak{T} = \{\gamma, \delta, \gamma\delta\}$. Now

$$S(\{\alpha, \beta, \alpha\beta\}) = (\alpha, \beta)(\alpha, -\beta)(\beta, -\alpha) = (-1, -1)(-\alpha, -\beta), \tag{8}$$

and $S(\mathfrak{T}) = (-1, -1)(-\gamma, -\delta)$. So $(-\alpha, -\beta) = (-\gamma, -\delta)$. We shall now prove (Lemmas 3 and 4) that in this case $\mathfrak{S}$ represents γ. Our theorem follows if this is so because then $\mathfrak{T} = \{\gamma\} \perp \mathfrak{T}'$, $\mathfrak{S} = \{\gamma\} \perp \mathfrak{S}'$, where $\mathfrak{T}'$ and $\mathfrak{S}'$ are binary forms with the same determinant and Hasse invariant (by (5)), hence isometric.

LEMMA 3. $\{\alpha, \beta, \alpha\beta\}$ *represents* $0 \Leftrightarrow$ *it is isometric to* $\{-1, -1, 1\}$ $\Leftrightarrow (-\alpha, -\beta) = 1 \Leftrightarrow$ *it represents every element of* k.

PROOF. If $\{\alpha, \beta, \alpha\beta\}$ represents 0 it contains a subspace isometric to $\{1, -1\}$; the other component must be $\{-1\}$ since determinant is a square. By (8), $(-\alpha, -\beta) = 1$ if $\{\alpha, \beta, \alpha\beta\} \cong \{1, -1, -1\}$.

Suppose $(-\alpha, -\beta) = 1$. Then $\xi^2 + \alpha\eta^2 + \beta\zeta^2$ represents 0 nontrivially; multiplying by $\alpha\beta$, we see that $\alpha\beta\xi^2 + \beta(\alpha\eta)^2 + \alpha(\beta\zeta)^2$ represents 0 nontrivially, q.e.d.

LEMMA 4. $\{\alpha, \beta, \alpha\beta\}$ *represents* $\gamma \in k$ *if and only if* $k((-\gamma)^{1/2})$ *is a field of definition for* $(-\alpha, -\beta)$.

PROOF. If the form represents γ then it is isometric to $\{\gamma, \delta, \gamma\delta\}$

for some $\delta \in k$ so $(-\alpha, -\beta) = (-\gamma, -\delta)$ by (8) and has $k((-\gamma)^{1/2})$ as field of definition.

To prove the other part let $K = k((-\gamma)^{1/2})$ and $\Omega = k((-\gamma)^{1/2}, (-\alpha)^{1/2}) = K((-\alpha)^{1/2})$ and let K be a field of definition for $(-\alpha, -\beta)$. Recall that the kernel of the restriction $H^2(\Omega/k) \to H^2(\Omega/K)$ is exactly the image of the lift $H^2(K/k) \to H^2(\Omega/k)$. So $(-\alpha, -\beta)$, considered as element of $H^2(\Omega/k)$, has K as field of definition if and only if its restriction to $H^2(\Omega/K)$ is 1. Denote this restriction by $(-\alpha, -\beta)^*$. Form the tensor product $\mathfrak{S} \times_k K$—i.e. the space $\{\alpha, \beta, \alpha\beta\}$ over K instead of over k. By Lemma 3, $(-\alpha, -\beta)^* = 1$ implies that there is a nonzero $U \in \mathfrak{S} \times_k K$ with $U^2 = 0$. We can write $U = u + v\Gamma$ with $u, v \in \mathfrak{S}$ and $\Gamma^2 = -\gamma$. Then

$$0 = U^2 = u^2 - \gamma v^2 + 2\Gamma u \cdot v. \tag{9}$$

Now if $\Gamma \in k$ then $(-\gamma, -\delta) = 1$ and our result follows by Lemma 3; likewise if $\mathfrak{S}$ represents 0. In the only remaining case, (9) implies that $u \cdot v = 0$, and since u and v are not 0 their squares are nonzero with $u^2 = \gamma v^2$. So $\mathfrak{S}$ contains the component $\langle u, v \rangle \cong \{\epsilon\gamma, \epsilon\}$. From the determinant we see that $\mathfrak{S} \cong \{\epsilon\gamma, \epsilon, \gamma\}$. q.e.d.

References

1. C. Chevalley, *Class field theory*, Nagoya, 1953.
2. S. Eilenberg and S. MacLane, *Cohomology theory in abstract groups* I, Ann. of Math. vol. 48 (1947) pp. 51–78.
3. O. T. O'Meara, *Integral equivalence of quadratic forms in ramified local fields*, Amer. J. Math. vol. 79 (1957) pp. 157–186.
4. G. Whaples, *Generalized local class field theory* I, Duke Math. J. vol. 19 (1952) pp. 505–517.
5. E. Witt, *Theorie der quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. vol. 176 (1937) pp. 31–44.

INDIANA UNIVERSITY