QUADRATIC FORMS OVER FIELDS WITH A VALUATION

WILLIAM H. DURFEE

1. **Introduction.** The problem of the representation of a number by a quadratic form and of the equivalence of two such forms has been solved by Hasse [2, 3, 4, 5][1] for the case where the coefficient field is the field of $\mathfrak{p}$-adic numbers. In this paper we consider the problem more generally for forms over any field with a non-archimedean valuation subject to the restriction that the field is complete with respect to the valuation and that its residue-class field has characteristic not two. A complete solution is not obtained except under certain further restrictions described below, but the general problem is shown to be reducible to the case where the forms in question have unit coefficients, and to be equivalent to the corresponding problem previously studied by the author [1] for forms over valuation rings. It is also shown that a form with unit coefficients represents zero if and only if the image form over the residue-class field represents zero, and similarly for the equivalence of two such forms.

In the latter part of the paper we obtain a complete solution for forms over certain special fields. The Hilbert norm residue symbol is introduced and conditions are given under which the Hasse function $c(f)$ is invariant. With its aid the necessary and sufficient conditions of Hasse, expressed, however, in an improved form due to Pall [7], for the representation of zero and the equivalence of two forms over a $\mathfrak{p}$-adic field are shown to apply more generally to forms over any complete field with a valuation for which the residue-class field is finite and has characteristic not two; for example, the field of formal power series over a finite field of characteristic not two. We give a new proof of the invariance of $c(f)$ which is shorter than that given by Hasse.

2. **Definitions and notations.** Let $f=\sum_1^n a_{ij}x_ix_j$ be a quadratic form whose coefficients a_{ij} are in an integral domain D. Let D' be any integral domain containing D and m any element of D. f is said to *represent* m over D' if there exist α_i in D' $(i=1, 2, \cdots, n)$, not all zero, such that $\sum a_{ij}\alpha_i\alpha_j=m$. If $m=0$, f is called a *zero form* over D'. Let $g=\sum_1^n b_{ij}y_iy_j$ be another form over D. f is said to be *equivalent* to g over D', written $f\cong g$, if there is a linear transformation $x_i=\sum_{j=1}^n p_{ij}y_j$ $(i=1, 2, \cdots, n)$, p_{ij} in D', which carries f into g

Presented to the Society, April 26, 1947; received by the editors June 9, 1947.

[1] Numbers in brackets refer to the bibliography at the end of the paper.

and such that the inverse transformation exists and has all its coefficients in D'. When explicit mention of D' is omitted it will be understood to be the same as D. The order n of f will be denoted by $n(f)$.

It is easily shown [9, Theorem 15] that if D is a field the problem of the representation of a nonzero element by a form of order n is equivalent to the problem of the representation of zero by a form of order $n+1$. In view of this and since we shall be working for the most part with fields we shall consider only the latter problem.

We shall assume that all forms used are nonsingular. When we write $f+g$ for the sum of two forms it will always be understood that f and g have no variables in common.

In this paper we shall take D to be either a field K with a non-archimedean valuation V which is complete with respect to this valuation and such that the characteristic of the residue-class field $\overline{K}$ is not two, or its valuation ring R. Thus we can assume all forms symmetric, that is, $a_{ij}=a_{ji}$ for all i and j, and each equivalent to some diagonal form [1, Theorem 1]. (For an exposition of the general theory of valuations see [6, chap. 2] or [8, chap. 10].)

Use will often be made of Witt's cancellation theorem [9, Theorem 4] which says that if f, g and h are forms over a field of characteristic not two, then $f+g\cong f+h$ implies $g\cong h$. This was extended by the author [1, Theorem 5] to forms over the valuation ring R.

The form $(x_1^2-x_2^2)+(x_3^2-x_4^2)+\cdots+(x_{k-1}^2-x_k^2)$ will be denoted by H_k. Then $H_k\cong aH_k$ over the field K for any nonzero a in K [9, p. 34], and Witt showed that every zero form f could be expressed as $f\cong f^*+H_k$ where f^* is either vacuous or a nonzero form unique to within an equivalence [9, Theorem 5]. If $f\cong H$, we shall call f a *totally zero form*. We shall frequently omit the subscript on H when there is no ambiguity about its length.

3. **Forms over fields with a valuation.** We shall now suppose that the domain of coefficients of our forms and transformations is the field K. $\bar{a}$ will denote the homomorphic image in $\overline{K}$ of the element a of R.

DEFINITION. If k is an even integer, by $f\cong g+H_k$ we mean $f\cong g+H_k$ if $k>0$, $f\cong g$ if $k=0$, and $g\cong f+H_{-k}$ if $k<0$.

LEMMA 1. *$f-g\cong H_{n(f)+n(g)}$ if and only if $f\cong g+H_{n(f)-n(g)}$.*

PROOF. Suppose $n(f)\geqq n(g)$. If $f-g\cong H_{n(f)+n(g)}$, then

$$f-g+g\cong f+H_{2n(g)}\cong g+H_{n(f)+n(g)}.$$

Cancelling an $H_{2n(g)}$ from each side gives us the desired result. Con-

versely, if $f \cong g + H_{n(f)-n(g)}$, then

$$f - g \cong g + H_{n(f)-n(g)} - g \cong H_{n(f)-n(g)} + H_{2n(g)} = H_{n(f)+n(g)}.$$

A similar argument disposes of the case $n(f) < n(g)$.

LEMMA 2. *If* $f = \sum_1^n a_i x_i^2$, a_i *in* K, *is a zero form with* $\sum_1^n a_i \alpha_i^2 = 0$, *which has no zero subform, then* $Va_i\alpha_i^2 = Va_j\alpha_j^2$ *for all* i *and* j.

PROOF. None of the α_i can be zero since f has no zero subform. Rearrange the terms of f so that

$$Va_1\alpha_1^2 = Va_2\alpha_2^2 = \cdots = Va_r\alpha_r^2 < Va_{r+1}\alpha_{r+1}^2 \leqq \cdots \leqq Va_n\alpha_n^2.$$

Then

$$V(a_1\alpha_1^2 + a_2\alpha_2^2 + \cdots + a_r\alpha_r^2) = V(a_{r+1}\alpha_{r+1}^2 + \cdots + a_n\alpha_n^2) > Va_1\alpha_1^2.$$

Let $b = a_2\alpha_2^2 + \cdots + a_r\alpha_r^2$ (b exists since we must have $r \geqq 2$ for f to be a zero form). Hence $V(1 + ba_1^{-1}\alpha_1^{-2}) > 0$ and $V(ba_1^{-1}\alpha_1^{-2}) = 0$. This implies that the equation

$$x^2 + \overline{ba_1^{-1}\alpha_1^{-2}} = \bar{0}$$

over $\overline{K}$ has the solutions $\pm\bar{1}$ which are distinct since the characteristic of $\overline{K}$ is different from two. By the Hensel-Rychlik theorem the equation $x^2 + ba_1^{-1}\alpha_1^{-2} = 0$ has a solution β in K and therefore $a_1(\alpha_1\beta)^2 + a_2\alpha_2^2 + \cdots + a_r\alpha_r^2 = 0$. Since f has no zero subform we must have $r = n$.

DEFINITION. Let a and b be nonzero elements of K. Then a and b are *congruent*, written $a \equiv b$, if there is a unit u of R such that $a \cong bu$.

DEFINITION. A diagonal form $\sum_1^n a_i x_i^2$ will be called a *unit form* if $Va_i = 0$ for all i.

DEFINITION. A form of the type $\sum_{i=1}^r b_i f_i$, where $b_i \not\equiv b_j$ for $i \neq j$ and each f_i is a unit form, is called a *standard form*.

Every nonsingular diagonal form over K is equivalent to a standard form under transformations of the type $x_i = b_i y_i$ and a rearrangement of terms.

THEOREM 1. *A standard form* $f = \sum_{i=1}^r a_i f_i$ *over* K *is a zero form if and only if at least one of the* f_i *is a zero form.*

PROOF. Suppose f is a zero form. Let g be a zero subform of f which does not contain a proper zero subform. g may possibly be f itself. Write g as $g = \sum a_j g_j$, where the a_j are certain of the a_i and each g_j is a subform of some f_i, such an f_i contributing only the one subform g_j, if any. Let $g_j = \sum_k a_{jk} x_{jk}^2$, $Va_{jk} = 0$ for all j and k. Then

$\sum_j a_j(\sum_k a_{jk}\alpha_{jk}^2)=0$ for some α_{jk} in K. By Lemma 2, $V(a_j a_{j1}\alpha_{j1}^2) = V(a_m a_{m1}\alpha_{m1}^2)$ for each j and m. Therefore $a_j \equiv a_m$. But, since f is a standard form, this can happen only if $m=j$. Hence g must be a subform of some $a_i f_i$ and this f_i will be a zero form. The converse is obvious.

COROLLARY. *A standard form $f=\sum_{i=1}^r a_i f_i$ over K is a totally zero form if and only if each of the f_i is a totally zero form.*

PROOF. By the above theorem at least one of the f_i, say f_1, is a zero form and therefore $a_1 f_1 \cong a_1 f_1' + H_2$. Since $f \cong H_{n(f)}$ we have $a_1 f_1' + H_2 + \sum_2^r a_i f_i \cong H_{n(f)}$. Cancelling an H_2 from each side leaves us $a_1 f_1' + \sum_2^r a_i f_i \cong H_{n(f)-2}$. By repeating the argument we have eventually $f_i \cong H_{n(f_i)}$ for all i.

In certain important cases, such as p-adic fields, p an odd prime, K has the property that ax^2+by^2 represents 1 whenever $Va = Vb = 0$. When this is true we have the following simple criterion for the representation of zero by a given form f.

THEOREM 2. *If K has the property mentioned above, then the diagonal form f represents zero if and only if it contains a binary subform ax^2+by^2 with $-ab$ a square in K or a ternary subform $ax^2+by^2+cz^2$ with $a \equiv b \equiv c$.*

PROOF. By transformations of the type $x_i = d_i y_i$ and by a rearrangement of terms we can express f in a standard form $f \cong \sum_1^r b_i f_i$. If f is a zero form, then by the preceding theorem some f_i, say f_1, is a zero form. If f_1 is the binary $a'x^2+b'y^2$, we must have $-a'b'$ a square and hence if ax^2+by^2 is the corresponding binary subform of f, $-ab$ is also a square. If f_1 has order greater than two, it has a ternary subform $c_1x_1^2+c_2x_2^2+c_3x_3^2$ with $Vc_i = 0$ which by our assumption on K represents zero. Since the $b_1 c_i$ have equal values the corresponding coefficients of f are congruent to each other. Conversely, if $-ab$ is a square for some binary subform ax^2+by^2 of f, this binary, and hence f, will represent zero. If the ternary subform $g=ax^2+by^2+cz^2$ has $a \equiv b \equiv c$, then $b = au_1c_1^2$ and $c = au_2c_2^2$ for some units u_1 and u_2, and hence $g \cong a(x^2+u_1y^2+u_2z^2)$. Since the ternary in the brackets represents zero so does f.

THEOREM 3. *Let $f=\sum_1^r a_i f_i$ and $g=\sum_1^s b_j g_j$ be equivalent standard forms over K. If for a given a_i there is a b_j such that $a_i \equiv b_j$, then this b_j is unique and $f_i \cong u_j g_j + H$, where u_j is the unit defined by $b_j = a_i c_j^2 u_j$. If there is no such b_j, then $f_i \cong H$, and similarly if, for a given b_k, $b_k \not\equiv a_l$ for all l, then $g_k \cong H$.*

PROOF. If there is a b_j such that $a_i \equiv b_j$, it must be unique since the

relation of congruence is transitive. Rearrange the terms of f and g so that $a_i \equiv b_i$ $(i=1, 2, \cdots, t)$, $a_i \not\equiv b_j$ $(i, j>t)$. Then, using Lemma 1,

$$H \cong f - g \cong \sum_1^t a_i(f_i - c_i^2 u_i g_i) + \sum_{t+1}^r a_i f_i + \sum_{t+1}^s b_j g_j.$$

By the corollary to Theorem 1, $f_i - c_i^2 u_i g_i \cong H$ $(i=1, 2, \cdots, t)$, $f_i \cong H$ $(i=t+1, \cdots, r)$, $g_j \cong H$ $(j=t+1, \cdots, s)$. By Lemma 1 $f_i \cong c_i^2 u_i g_i + H \cong u_i g_i + H$ $(i=1, 2, \cdots, t)$.

As a converse of this theorem we have the following theorem.

THEOREM 4. *Let* $f = \sum_1^r a_i f_i$ *and* $g = \sum_1^s b_j g_j$ *be standard forms over* K. f *is equivalent to* g *if*

(i) $\sum_1^r n(f_i) = \sum_1^s n(g_j)$,

(ii) $a_i \equiv b_j$ *implies* $f_i \cong u_j g_j + H_{n(f_i)-n(g_j)}$, *where* u_j *is the unit defined by* $b_j = a_i c_j^2 u_j$,

(iii) *for a given* a_i, $a_i \not\equiv b_j$ *for all* j *implies* $f_i \cong H_{n(f_i)}$, *and for a given* b_k, $b_k \not\equiv a_l$ *for all* l *implies* $g_k \cong H_{n(g_k)}$.

PROOF. Rearrange the terms of f and g so that $a_i \equiv b_i$ $(i=1, 2, \cdots, t)$, $a_i \not\equiv b_j$ $(i, j>t)$. Then

$$f_i \cong u_i g_i + H_{n(f_i)-n(g_i)} \qquad (i = 1, 2, \cdots, t),$$

$$f_i \cong H_{n(f_i)} \quad \text{and} \quad g_j \cong H_{n(g_j)} \qquad (i, j > t).$$

$$\sum_1^r a_i f_i \cong \sum_1^t (a_i u_i g_i + a_i H_{n(f_i)-n(g_i)}) + \sum_{t+1}^r a_i H_{n(f_i)}$$

$$\cong \sum_1^t b_i g_i + \sum_1^r a_i H_{n(f_i)} + \sum_1^t a_i H_{-n(g_i)}$$

$$\cong \sum_1^t b_i g_i + \sum_1^s b_j H_{n(g_j)} + \sum_1^t b_j H_{-n(g_j)}$$

$$\cong \sum_1^t b_i g_i + \sum_{t+1}^s b_j H_{n(g_j)}$$

$$\cong \sum_1^t b_i g_i + \sum_{t+1}^s b_j g_j \cong \sum_1^s b_i g_j.$$

For fields K in which it is possible to tell whether or not any two given elements are congruent, Theorems 1, 3 and 4 reduce the problem of the representation of a given element in K by a given form and of the equivalence of two forms to the case of unit forms. In an earlier paper [1, Theorem 4] we performed a similar reduction for forms over valuation rings. We shall now show that the two prob-

lems are equivalent by proving (Theorem 5) that two unit forms are equivalent over the field K if and only if they are equivalent over the valuation ring R.

First we extend to forms over valuation rings some of the elementary properties of forms over general fields.

If f and g are forms over R, then $f \simeq g$ will mean that f is equivalent to g over R, while $f \cong g$ will stand for equivalence over K.

LEMMA 3. *If* $f = \sum_1^n a_i x_i^2$, $Va_i = Va_j \geqq 0$ *(all* i, j*), represents zero over* K*, and* b *is any element of* R *for which* $Vb = Va_1$*, then* $f \simeq by_1^2 - by_2^2 + \phi(y_3, y_4, \cdots, y_n)$*, where* ϕ *is a quadratic form over* R*. Hence* f *represents* b *over* R.

PROOF. Let $\sum a_i \alpha_i^2 = 0$, α_i in K. We can assume that $V\alpha_i \geqq 0$ for all i and that some α_i, say α_1, has $V\alpha_1 = 0$. Since f is a zero form, some other α, say α_2, must also have $V\alpha_2 = 0$. The transformation over R

$$x_1 = \alpha_1 z_1, \qquad x_i = \alpha_i z_1 + z_i \quad (i = 2, 3, \cdots, n)$$

is unimodular and carries f into

$$2z_1 \sum_{i=2}^{n} a_i \alpha_i z_i + \sum_{i=2}^{n} a_i z_i^2. \tag{1}$$

Next apply the unimodular transformation

$$w_1 = z_1, \qquad w_2 = b^{-1} \sum_{j=2}^{n} a_j \alpha_j z_j, \qquad w_i = z_i \qquad (i = 3, 4, \cdots, n)$$

which takes (1) into

$$bw_2 \left(2w_1 + \frac{b}{a_2^2 \alpha_2^2} w_2 - \frac{2}{a_2 \alpha_2^2} \sum_{j=3}^{n} a_j \alpha_j w_j \right) + \phi(w_3, w_4, \cdots, w_n), \tag{2}$$

where ϕ is a form over R. The unimodular transformation

$$v_1 = 2w_1 + \frac{b}{a_2^2 \alpha_2^2} w_2 - \frac{2}{a_2 \alpha_2^2} \sum_{j=3}^{n} a_j \alpha_j w_j, \qquad v_i = w_i \qquad (i = 2, 3, \cdots, n)$$

carries (2) into

$$bv_1 v_2 + \phi(v_3, v_4, \cdots, v_n). \tag{3}$$

Finally the unimodular transformation

$$v_1 = y_1 + y_2, \qquad v_2 = y_1 - y_2, \qquad v_i = y_i \qquad (i = 3, 4, \cdots, n)$$

will take (3) into $by_1^2 - by_2^2 + \phi(y_3, y_4, \cdots, y_n)$.

LEMMA 4. *If* $f=\sum_1^n a_i x_i^2$, $Va_i = Va_j \geqq 0$ *(all* i, j*), represents over* K *any* b *for which* $Vb = Va_1$, *then* f *represents* b *over* R *and* $f \simeq by_1^2 + \psi(y_2, y_3, \cdots, y_n)$, *where* ψ *is a quadratic form over* R.

PROOF. Let $\sum a_i\alpha_i^2 = b$, α_i in K. Then $\sum a_i x_i^2 - bz^2$ is a zero form over K, and by Lemma 3

$$\sum_{i=1}^{n} a_i x_i^2 - bz^2 \simeq by_1^2 - bz^2 + \psi(y_2, y_3, \cdots, y_n).$$

By Witt's theorem for forms over a valuation ring we can cancel $-bz^2$ from each side giving us $f \simeq by_1^2 + \psi(y_2, y_3, \cdots, y_n)$.

THEOREM 5. *Two unit forms are equivalent over* K *if and only if they are equivalent over* R.

PROOF. The condition is obviously sufficient. Let the two forms be

$$f = \sum_{i=1}^{n} a_i x_i^2 \quad \text{and} \quad g = \sum_{i=1}^{n} b_i x_i^2, \qquad Va_i = Vb_i = 0 \text{ for all } i,$$

and assume $f \cong g$. We shall use induction on the order n of f. The theorem is true for unary forms. Suppose that it is true for forms of order $n-1$. Since f represents a_1 over R, g represents a_1 over K and by Lemma 4

$$g \simeq a_1 x_1^2 + \sum_{i=2}^{n} c_i x_i^2$$

for some c_i. Since the values of corresponding terms are invariant under a transformation over R [1, Lemma 2], $Vc_i = 0$ for all i. Applying Witt's cancellation theorem for forms over a field we have

$$\sum_{i=2}^{n} a_i x_i^2 \cong \sum_{i=2}^{n} c_i x_i^2$$

which with the induction hypothesis gives us

$$\sum_{i=2}^{n} a_i x_i^2 \simeq \sum_{i=2}^{n} c_i x_i^2.$$

From this it follows that $f \simeq g$.

We shall now show how the equivalence of two unit forms and the representation of zero by a unit form are connected with corresponding problems for related forms over the residue-class field.

If f is a form $\sum_1^n a_i x_i^2$ over R, then $\bar{f}$ will stand for the form $\sum_1^n \bar{a}_i x_i^2$ over the residue-class field $\overline{K}$.

THEOREM 6. *If f and g are unit forms, then $f \cong g$ over K if and only if $\bar{f} \cong \bar{g}$ over $\overline{K}$.*

A proof of this theorem is given in [1, Lemma 1 and Theorem 2].

THEOREM 7. *A unit form f is a zero form over K if and only if $\bar{f}$ is a zero form over $\overline{K}$.*

PROOF. Let $f = \sum_1^n a_i x_i^2$, $Va_i = 0$, for all i. If f is a zero form over K, then there are α_i in K $(i = 1, 2, \cdots, n)$, not all zero, such that $\sum a_i \alpha_i^2 = 0$. We can assume that $V\alpha_i \geqq 0$ for all i and that some α_i, say α_1, has $V\alpha_1 = 0$. Then $\sum \bar{a}_i \bar{\alpha}_i^2 = \bar{0}$ with $\bar{\alpha}_1 \neq \bar{0}$.

Conversely, suppose that $\bar{f}$ is a zero form over $\overline{K}$. Then there are $\bar{\alpha}_i$ in $\overline{K}$ $(i = 1, 2, \cdots, n)$, not all equal to $\bar{0}$, such that $\sum \bar{a}_i \bar{\alpha}_i^2 = \bar{0}$. Suppose that $V\alpha_i = 0$ $(i = 1, 2, \cdots, r)$ and $V\alpha_i > 0$ for $i > r$, where α_i is an antecedent in R of $\bar{\alpha}_i$. Since not all the $\bar{\alpha}_i$ are zero, $r \geqq 2$. Therefore $V(a_1\alpha_1^2 + a_2\alpha_2^2 + \cdots + a_r\alpha_r^2) > Va_1\alpha_1^2$, and as in the proof of Lemma 2 there is a nonzero β in K such that $a_1(\alpha_1\beta)^2 + a_2\alpha_2^2 + \cdots + a_r\alpha_r^2 = 0$. Thus f is a zero form over K.

COROLLARY. *If the unit form f represents over K any m in K for which $Vm > \min V\alpha_i^2$, where $\sum a_i \alpha_i^2 = m$, then f is a zero form over K.*

PROOF. Let $V\alpha_1 = \min V\alpha_i$. Then $\sum a_i(\alpha_1^{-1}\alpha_i)^2 = \alpha_1^{-2}m$. $V(\alpha_1^{-2}m) > 0$ and hence $\sum \bar{a}_i \bar{x}_i^2$ is a zero form over $\overline{K}$.

4. **The Hasse function.** The problem of determining when a form represents zero and when two forms are equivalent was solved for the $\mathfrak{p}$-adic case by Hasse. He made extensive use of the Hilbert norm residue symbol. We shall show that his results do not depend on having a $\mathfrak{p}$-adic field for a base but can be extended to any complete field with a discrete valuation whose residue-class field has characteristic not two, and having the property that the product of any two non-square units is a square and that $ax^2 + by^2 = 1$ has a solution whenever a and b are both units of R. An example of such a field is the one obtained by completing with respect to any one of its valuations the field of rational functions over a finite field of characteristic not two.

DEFINITION. If $ax^2 + by^2$ is a form over K with a and b not zero, we define the function (a, b) to have the value 1 or -1 according as the form does or does not represent 1 over K.

It is obvious that $(a, b) = (b, a)$, $(a, -a) = 1$ and that $(a, b) = 1$ if a or b is the square of an element in K.

LEMMA 5. *Let a and b be non-squares. Then*

(i) $a \not\equiv b$ *implies* $(a, b) = -1$,

(ii) $a \not\equiv 1$, $b \not\equiv 1$ *implies* $(a, b) = 1$ *if and only if* $-ab$ *is a square.*

PROOF. Let $f = ax^2 + by^2 - z^2$. If $a \not\equiv b$, the only possible standard forms of f are $(ax^2 - z^2) + b(y^2)$, $(by^2 - z^2) + a(x^2)$ or $a(x^2) + b(y^2) + (-z^2)$. By Theorem 1 if f is a zero form, at least one of the bracketed subforms must be a zero form. But this is impossible for each of the three possibilities. Hence $(a, b) = -1$.

If $a \not\equiv 1$, and $b \not\equiv 1$, the only possible standard forms of f are $a(x^2 + ba^{-1}y^2) + (-z^2)$ or $a(x^2) + b(y^2) + (-z^2)$. If $-ab$ is a square then f is a zero form. Conversely, if f is a zero form, then the first of the above possibilities for a standard form is the correct one and, by Theorem 1, $x^2 + ba^{-1}y^2$ must be a zero form, implying that $-ab$ is a square.

From now on we shall assume that the valuation of K is discrete with the integers as the value group. t will denote an element whose value is one.

LEMMA 6. *The product rule* $(a, b)(a, c) = (a, bc)$ *holds for all nonzero* a, b *and* c *in* K *if and only if the product of every two non-square units is a square and* $Va = Vb = 0$ *implies* $(a, b) = 1$.

PROOF. Suppose that, for all nonzero a, b and c, $(a, b)(a, c) = (a, bc)$. If a or b is a square, $(a, b) = 1$. Hence let a and b be two non-square units. Chose t such that $Vt = 1$. Since $Va = Vb = 0$, $t \not\equiv a$, $t \not\equiv b$, $ta \not\equiv b$ and, by Lemma 5, $(t, a) = (t, b) = (ta, b) = -1$. The product rule gives us $(t, b)(ta, b) = (a, b) = 1$. Also $(t, a)(t, b) = (t, ab) = 1$, and since $t \not\equiv ab$ we have by Lemma 5 that ab is a square.

Conversely, suppose that the product of two non-square units is a square and that $Va = Vb = 0$ implies $(a, b) = 1$. If $(x_1, y_1, 1)$ is a solution of $ax^2 + by^2 - z^2 = 0$ and $(x_2, y_2, 1)$ a solution of $ax^2 + cy^2 - z^2 = 0$, then $(x_1 - x_2, y_1y_2, 1 - ax_1x_2)$ is a solution of $ax^2 + bcy^2 - z^2 = 0$. It is well known [9, p. 39] that if a form represents zero with some zero terms in the solution, then there is a solution in which none of the terms is zero. Thus $(a, b) = (a, c) = 1$ implies $(a, bc) = 1$. Suppose that $(a, b) = 1$ and $(a, c) = -1$. If $(a, bc) = 1$, then by the case just discussed, $(a, bc)(a, b) = (a, c) = 1$, a contradiction. Hence $(a, bc) = -1$. Similarly $(a, b) = -1$ and $(a, c) = 1$ imply $(a, bc) = -1$. Suppose finally that $(a, b) = (a, c) = -1$. Then a, b and c are non-squares. In view of our assumption that $Va = Vb = 0$ implies $(a, b) = 1$ we need consider only the following cases:

Case 1. $Va = 0$, $Vb = Vc = 1$.

Let $b = tv$, $c = tw$, where $Vt = 1$. Then $Vv = Vw = 0$ and $(a, bc) = (a, vw) = 1$.

Case 2. $Va=1$, $Vb=Vc=0$.

bc is a square and $(a, bc)=1$.

Case 3. $Va=Vb=1$, $Vc=0$.

Let $a=tu$, $b=tv$. Then $Vu=Vv=0$. $(a, b)=-1$ implies by Lemma 5 that $-ab$ and hence $-uv$ is a non-square. Therefore $-uvc$ and $-abc$ are squares and by Lemma 5 again $(a, bc)=1$.

The case $Va=1$, $Vb=0$, $Vc=1$ is treated similarly.

Case 4. $Va=Vb=Vc=1$.

Let $a=tu$, $b=tv$, $c=tw$. Then $Vu=Vv=Vw=0$. As in the preceding case $(a, b)=(a, c)=-1$ implies that $-uv$ and $-uw$ are non-squares. Hence vw and bc are squares, and $(a, bc)=1$.

This establishes the product rule.

THEOREM 8. *If $\overline{K}$ is a finite field with p^m elements, p an odd prime, then the product rule $(a, b)(a, c)=(a, bc)$ holds in K for all nonzero a, b and c.*

PROOF. The nonzero elements of $\overline{K}$ form under multiplication a cyclic group of order p^m-1. If $\bar{\eta}$ is a generator of this group, the p^m elements of $\overline{K}$ can be listed as 0, $\bar{\eta}$, $\bar{\eta}^2$, $\cdots$, $\bar{\eta}^{p^m-1}=1$. If an odd power of $\bar{\eta}$ were a square, then $\bar{\eta}^{1/2}$ would exist in $\overline{K}$ and we should have $\bar{\eta}^{1/2}=\bar{\eta}^h$ for some h, $1\leqq h\leqq p^m-1$. This implies that $\bar{\eta}=\bar{\eta}^{2h}$ and hence that $2h\equiv 1 \pmod{p^m-1}$, an impossibility, since p^m-1 is even. Thus $\overline{K}$ has exactly $1+(p^m-1)/2$ squares and the product of two non-squares of $\overline{K}$ is a square. Using Theorem 7 we see that the product of two non-square units of K will be a square. Suppose now that $Va=Vb=0$, and consider $\bar{a}x^2+\bar{b}y^2=\bar{1}$. x^2, and hence $\bar{a}x^2-\bar{1}$, takes on $1+(p^m-1)/2$ different values as x runs through all values of $\overline{K}$. Similarly so does $-\bar{b}y^2$. Two of these must be equal if we are not to have p^m+1 different elements in $\overline{K}$. Therefore $\bar{a}x^2+\bar{b}y^2=\bar{1}$ has a solution in $\overline{K}$ which obviously is not $(\bar{0}, \bar{0})$. Hence by Theorem 7 $ax^2+by^2=1$ has a solution in K. From Lemma 6 it follows that the product rule is valid in K.

We shall now assume that not only is the valuation of K discrete but also that the product rule holds in K. Under these two assumptions it is possible to obtain a complete set of criteria for the representation of zero by a given form and for the equivalence of two forms in terms of the Hasse invariants. The conditions are the same as those for forms over the p-adic numbers as given first by Hasse [**2** and **3**, Theorem 2] and recently in a more convenient form by Pall [**7**].

For any nonsingular diagonal form $f=\sum_1^n a_i x_i^2$ we define the function, with the values ± 1,

$$c(f) = \prod_{i=1}^{n} (-d_{i-1}, d_i),$$

where $d_i = a_1 a_2 \cdots a_i$ if $i \geqq 1$ and $d_0 = 1$. This function was introduced by Hasse, his definition, though different, being equivalent to ours. It is easily shown that if f and g are diagonal forms with no variables in common that

$$c(f+g) = c(f)c(g)(|f|, |g|), \tag{4}$$

where $|f|$ is the determinant of f, and for any nonzero m

$$c(mf) = (m, (-1)^{n(n+1)/2} |f|^{n+1}) c(f). \tag{5}$$

THEOREM 9. *If f and g are equivalent diagonal forms, then $c(f) = c(g)$.*

PROOF. Replacing any coefficient a in f by ac^2 for any nonzero c obviously does not change $c(f)$. If we interchange two adjacent terms of f, say the jth and $(j+1)$th, the only change in the expression for $c(f)$ will be to replace $(-d_{j-1}, d_j)(-d_j, d_{j+1})$ by $(-d_{j-1}, D_j) \cdot (-D_j, d_{j+1})$, where $D_j = a_1 a_2 \cdots a_{j-1} a_{j+1}$. If we use the relation $D_j = d_j a_{j+1} a_j^{-1}$, it is easy to show that these two products are equal and hence that $c(f)$ is unchanged. By transformations of these two simple types we can express f and g in their standard forms: $f \cong f_1 + tf_2$, $g \cong g_1 + tg_2$, where $V(t) = 1$ and the forms f_i and g_i have unit coefficients, and have $c(f) = c(f_1 + tf_2)$, $c(g) = c(g_1 + tg_2)$. If f_1, f_2, g_1, g_2 all exist, then $c(f_i) = c(g_i) = 1$ $(i = 1, 2)$ and by (4) and (5)

$$\begin{aligned} c(f) = c(f_1 + tf_2) &= c(tf_2)(|f_1|, |tf_2|) \\ &= (t, (-1)^{r(r+1)/2} |f_2|^{r+1})(|f_1|, t^r |f_2|) \\ &= (t, (-1)^{r(r+1)/2} |f_2|^{r+1})(|f_1|, t^r), \\ c(g) = c(g_1 + tg_2) &= (t, (-1)^{s(s+1)/2} |g_2|^{s+1})(|g_1|, t^s), \end{aligned}$$

where r and s are the respective orders of f_2 and g_2. By Theorem 3, assuming without loss in generality that $r \leqq s$, we have $f_1 \cong g_1 + H_{s-r}$, $g_2 \cong f_2 + H_{s-r}$ (since the valuation is discrete we can take $u_j = 1$ in Theorem 3). Let $h = |H_{s-r}| = (-1)^{(s-r)/2}$. Then $|g_1| \cong |f_1| h$, $|g_2| \cong |f_2| h$ and

$$c(g) = (t, (-1)^{s(s+1)/2} |f_2|^{s+1} h^{s+1})(|f_1| h, t^r),$$

since $s - r$ is even. If $r = s$, this will still be correct, though H does not exist, provided we take $h = 1$. $c(f)c(g) = (t, (-1)^{\nu})(h, t^r)$ where

$$\nu = [r(r+1) + s(s+1) + (s-r)(s+1)]/2 \equiv r(r-s)/2 \pmod 2.$$

If r, and hence s, is even, then so is ν and $c(f)c(g)=1$. If r is odd,

$$c(f)c(g) = (t, (-1)^{\nu+(s-r)/2})$$

which is unity since $\nu+(s-r)/2$ is even. If any of f_1, f_2, g_1 or g_2 are non-existent, a similar argument can be used to show that in these cases too $c(f)=c(g)$.

THEOREM 10. *A form of f order n is a zero form if and only if for*

$$\begin{aligned} n &= 2, && -|f| \text{ is a square,} \\ n &= 3, && c(f) = 1, \\ n &= 4, && c(f) = 1 \text{ or } |f| \text{ is not a square,} \\ n &\geqq 5, && \text{always.} \end{aligned}$$

PROOF. $n=2$: Let $f=a_1x_1^2+a_2x_2^2$. If f is a zero form, then $(x_1x_2^{-1})^2 = -a_1^{-1}a_2$ and $-|f|$ is a square. Conversely, if $-|f|$ is a square, then $x_1=(-a_1a_2)^{1/2}$, $x_2=a_1$ is a zero of f.

$n=3$: Let $f=a_1x_1^2+a_2x_2^2+a_3x_3^2$. A short computation shows that $c(f)=(-a_1a_2, -a_1a_3)$. If f is a zero form, let ξ, η, ζ be a solution of $f=0$. We can assume $\xi\neq 0$. Then $x=\eta(a_1\xi)^{-1}$, $y=\zeta(a_1\xi)^{-1}$ is a solution of

$$-a_1a_2x^2 - a_1a_3y^2 = 1. \tag{6}$$

Conversely, if $c(f)=1$, then (6) has a solution and hence so has $a_2x_2^2+a_3x_3^2=-a_1x_1^2$.

$n=4$: Let $f=a_1x_1^2+a_2x_2^2+a_3x_3^2+a_4x_4^2$. We can assume $Va_i=0$ or 1. Suppose f is a zero form. If $Va_i=0$ for all i, then $c(f)=1$. If, for some i, $Va_i\neq 0$, then by Theorem 1 either some binary or ternary subform with coefficients of like value must represent zero. In the former case let $f=f_1+f_2$. If both the binary subforms f_1 and f_2 represent zero, then $f\cong H_4$ and $c(f)=1$. If f_1 is the only binary representing zero, then $-|f_1|$ is a square while $-|f_2|$ is not a square. Hence $|f|$ is not a square. Returning to the other possibility let g be the ternary subform representing zero. By the preceding case for $n=3$, $c(g)=1$. If $f=ax^2+g$, then, by (4), $c(f)=(a, |f|)c(g)=(a, |f|)$. If $c(f)\neq 1$, then $|f|$ cannot be a square. Conversely, suppose $c(f)=1$ or $|f|$ is not a square. We can assume that f has a standard form $f\cong f_1+tf_2$, where $f_1=b_1x_1^2+b_2x_2^2$ and $f_2=b_3x_3^2+b_4x_4^2$, $Vb_i=0$ for all i, since any other possible standard form for f would imply that f had a ternary subform with coefficients of like value which would by Theorem 2 represent zero. Using (4) we have $c(f)=(t, -b_3b_4)$. If $c(f)=1$, then, by Lemma 5, $-b_3b_4$ is a square, and so f_2 and hence f is a zero form.

$|f| \cong (-b_1b_2)(-b_3b_4)$. If $|f|$ is not a square, then either $-b_1b_2$ or $-b_3b_4$ must be a square implying again that f is a zero form.

$n \geqq 5$: Since f must contain a ternary subform with coefficients of like value, it is a zero form by Theorem 2.

THEOREM 11. *Two nonsingular forms f and g of order n are equivalent if and only if $|f| \cong |g|$ and $c(f) = c(g)$.*

PROOF. We have already shown the necessity of these conditions. Suppose now that $|f| \cong |g|$ and $c(f) = c(g)$. We use induction on n. The theorem is true for $n = 1$. Suppose it true for forms of order $n-1$. Write f as $f = ax^2 + f'$, where a is the leading coefficient of f and f' is a form of order $n-1$. Using (4) we have

$$c(f - ax^2) = (-a, -|f|)c(f) = c(g - ax^2).$$

Since $f - ax^2$ represents zero, we have by Theorem 10 that so does $g - ax^2$ for any n. g then represents a and can be written $g \cong ax^2 + g'$, where g' is a form of order $n-1$. By (4)

$$c(f) = (-1, a)c(f')(a, |f'|), \qquad c(g) = (-1, a)c(g')(a, |g'|).$$

Therefore $c(f') = c(g')$ since $|f'| \cong |g'|$. By the induction hypothesis $f' \cong g'$ and hence $f \cong g$.

Since the product of two non-square units is a square, every unit of K is equivalent either to 1 or to some arbitrary but fixed non-square unit ν. Also $\nu x^2 + \nu y^2$, since it represents 1, is equivalent by Lemma 4 to $x^2 + y^2$. Thus every form f of order n is equivalent to

$$(7) \quad x_1^2 + x_2^2 + \cdots + x_{r-1}^2 + ax_r^2 + tx_{r+1}^2 + tx_{r+2}^2 + \cdots + tx_{n-1}^2 + tbx_n^2,$$

where a and b are 1 or ν.

THEOREM 12. *Expression (7) is a canonical form for f.*

PROOF. We need to show only that two different expressions of form (7) are inequivalent. Let

$$y_1^2 + y_2^2 + \cdots + y_{r-1}^2 + a'y_r^2 + ty_{r+1}^2 + ty_{r+2}^2 + \cdots + ty_{n-1}^2 + tb'y_n^2$$

be another form of this type. If they were equivalent, we could cancel like terms and get

$$ax_r^2 + tbx_n^2 \cong a'y_r^2 + tb'y_n^2.$$

Theorem 3 now implies that $a = a'$ and $b = b'$.

BIBLIOGRAPHY

1. W. H. Durfee, *Congruence of quadratic forms over valuation rings*, Duke Math. J. vol. 11 (1944) pp. 687–697.

2. H. Hasse, *Über die darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen*, J. Reine Angew. Math. vol. 152 (1923) pp. 129–148.

3. ———, *Über die Äquivalenz quadratischer Formen in Körper der rationalen Zahlen*, J. Reine Angew. Math. vol. 152 (1923) pp. 205–224.

4. ———, *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper*, J. Reine Angew. Math. vol. 153 (1924) pp. 113–130.

5. ——, *Äquivalenz quadratischer Formen in einem beliebigen algebraischen Zahlkörper*, J. Reine Angew, Math. vol. 153 (1924) pp. 158–162.

6. S. MacLane, *Algebraic functions*, Ann Arbor, Michigan, 1940.

7. G. Pall, *The arithmetical theory of quadratic forms*, Toronto, Canada, not yet published.

8. B. L. van der Waerden, *Moderne Algebra*, vol. 1, 2d ed., Berlin, 1937.

9. E. Witt, *Theorie der quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. vol. 176 (1937) pp. 31–44.

DARTMOUTH COLLEGE