Multiplicative quadratic forms on algebraic varieties

By Akinari Hoshi

Department of Mathematical Sciences, Waseda University, 3-4-1, Ohkubo, Shinjuku-ku, Tokyo 169-8555

(Communicated by Heisuke Hironaka, M. J. A., April 14, 2003)

Abstract: In this note we extend Hurwitz-type multiplication of quadratic forms. For a regular quadratic space (K^n, q), we restrict the domain of q to an algebraic variety $V \subsetneq K^n$ and require a Hurwitz-type "bilinear condition" on V. This means the existence of a bilinear map $\varphi : K^n \times K^n \to K^n$ such that $\varphi(V \times V) \subset V$ and $q(\mathbf{X})q(\mathbf{Y}) = q(\varphi(\mathbf{X}, \mathbf{Y}))$ for any $\mathbf{X}, \mathbf{Y} \in V$. We show that the m-fold Pfister form is multiplicative on certain proper subvariety in K^{2^m} for any m. We also show the existence of multiplicative quadratic forms which are different from Pfister forms on certain algebraic varieties for $n = 4, 6$. Especially for $n = 4$ we give a certain family of them.

Key words: Multiplicative quadratic forms; Pfister forms; Dickson's system.

1. Introduction. Let K be a field whose characteristic is not 2. In 1898, Hurwitz showed that if there is an identity of the type

$$(X_1^2 + \cdots + X_n^2)(Y_1^2 + \cdots + Y_n^2) = Z_1^2 + \cdots + Z_n^2,$$

where the Z_k's are bilinear forms of the independent variables X_i and Y_j over K then $n = 1, 2, 4, 8$. In general, for a regular quadratic form $q(\mathbf{X}) := q(X_1, \ldots, X_n)$ over K, $q(\mathbf{X})$ is called multiplicative if there exists a formula

$$q(\mathbf{X})q(\mathbf{Y}) = q(\boldsymbol{Z}), \tag{1}$$

where the X_i and Y_j are independent variables and $Z_k \in K(\mathbf{X}, \mathbf{Y})$. $q(\mathbf{X})$ is called strictly multiplicative if there exists a formula (1) with Z_k linear in Y_j over $K(\mathbf{X})$. It is known that if $q(\mathbf{X})$ is isotropic then $q(\mathbf{X})$ is always multiplicative and in this case $q(\mathbf{X})$ is strictly multiplicative if and only if $q(\mathbf{X})$ is hyperbolic (see [4] or [7]). A quadratic form is called Pfister form if it is expressible as a tensor product of binary quadratic forms of the type $\langle 1, a\rangle$. We denote by $\langle\langle a_1, a_2, \ldots, a_m\rangle\rangle$ the m-fold Pfister form $\langle 1, a_1\rangle \otimes \langle 1, a_2\rangle \otimes \cdots \otimes \langle 1, a_m\rangle$. In 1965, A. Pfister showed the following theorem.

Theorem (Pfister [3]). *If q is a Pfister form, then q is strictly multiplicative. Conversely if q is an anisotropic multiplicative form over K, then q must be a Pfister form.*

Let $D_K(n)$ be the set of values in $K^\times$ represented by a sum of n squares in K, namely

$$D_K(n) = \{\alpha \in K^\times \mid \alpha = \alpha_1^2 + \cdots + \alpha_n^2,\ \alpha_j \in K\}.$$

The *Stufe* (or level) of a field K is defined as $s(K) := \mathrm{Inf}\{n \in \mathbf{N} : -1 \in D_K(n)\}$. From above theorem, we see that if n is a power of 2 then $D_K(n)$ is a multiplicative group. Using this fact, Pfister proved the following remarkable theorem (see [2] or [7]).

Theorem (Pfister). *For any field K, $s(K)$ is, if finite, always a power of 2. Conversely every power of 2 is the Stufe of some field K.*

2. Multiplicative quadratic forms on algebraic varieties. In this section, we extend the Hurwitz-type multiplicative quadratic forms in different way. For a regular quadratic space (K^n, q), we restrict the domain of q to an algebraic variety $V \subsetneq K^n$. Furthermore we require the Hurwitz-type "bilinear condition" for q on V. More precisely, we make the following.

Definition. Let $V \subsetneq K^n$ be an algebraic variety. We say a regular quadratic form $q(\mathbf{X})$ is multiplicative on V if there is a bilinear map $\varphi : K^n \times K^n \to K^n$ such that

$$\varphi(V \times V) \subset V \quad \text{and}$$
$$q(\mathbf{X})q(\mathbf{Y}) = q(\varphi(\mathbf{X}, \mathbf{Y})) \ \text{ for any } \ \mathbf{X}, \mathbf{Y} \in V.$$

Then the following natural problems arise.

Problem 1. Given a regular quadratic form $q(\mathbf{X})$, determine whether an algebraic variety $V \subsetneq K^n$ exists on which $q(\mathbf{X})$ is multiplicative.

Problem 2. Given an algebraic variety $V \subsetneq K^n$, determine whether a quadratic form $q(\mathbf{X})$ which is multiplicative on V exists.

2000 Mathematics Subject Classification. Primary 11E04, 11E25; Secondary 11T22.

Problem 3. If Problem 1 or 2 is affirmative, find a bilinear map φ explicitly.

Note that in the classical case $V = K^n$, an anisotropic quadratic form is multiplicative if and only if it is a Pfister form. Moreover, when we require the Hurwitz-type "bilinear condition" a multiplicative quadratic form exists only for dimension 1, 2, 4 and 8. In this note we assume that the quadratic form is diagonal in order to simplify an argument.

We first describe a simple example which is a slight generalization of Hurwitz's theorem (see [5]). Let A be a finite-dimensional K-algebra with involution τ. We define an algebraic variety $V_\tau := \{x \in A \mid x \cdot x^\tau \in K\}$ and a quadratic form $N_\tau(\alpha) := \alpha \cdot \alpha^\tau$, $\alpha \in V_\tau$. Then we see that

$$\begin{aligned} N_\tau(\alpha\beta) &= \alpha\beta(\alpha\beta)^\tau = \alpha\beta(\beta^\tau\alpha^\tau) = \alpha(\beta\beta^\tau)\alpha^\tau \\ &= N_\tau(\alpha)N_\tau(\beta), \quad \text{for any} \quad \alpha, \beta \in V_\tau. \end{aligned}$$

In particular we consider the following case, from which one can recover the Pfister form in natural way. Let $a_1, \ldots, a_m \in K^\times$ and suppose $L = K(\sqrt{-a_1}, \ldots, \sqrt{-a_m})$ is an extension field of degree 2^m over K. We put $S_m := \{1, 2, \ldots, m\}$ then $\{e_I := \prod_{i \in I} \sqrt{-a_i} \mid I \subseteq S_m\}$ is a basis for L/K. For $1 \le i \le m$, we define $\sigma_i \in \mathrm{Aut}(L/K)$ by

$$\sigma_i(\sqrt{-a_k}) = \begin{cases} -\sqrt{-a_k}, & \text{if} \quad k = i, \\ \sqrt{-a_k}, & \text{if} \quad k \ne i. \end{cases}$$

Hence $\mathrm{Gal}(L/K) \cong \langle \sigma_1, \ldots, \sigma_m \rangle$. We now consider $\tau \in \mathrm{Gal}(L/K)$ of order 2 and define $\mathrm{sgn}_\tau(i) \in \{\pm 1\}$ for $1 \le i \le m$ by the equation

$$\tau(\sqrt{-a_i}) = \mathrm{sgn}_\tau(i)\sqrt{-a_i}.$$

For $\alpha \in L$, we write

$$\alpha = \sum_{I \subseteq S_m} u_I e_I, \quad u_I \in K$$

and define

$$N_\tau(\alpha) := N_{L/L^{\langle\tau\rangle}}(\alpha) = \alpha \cdot \alpha^\tau \in L^{\langle\tau\rangle}.$$

Then there are 2^{m-1} quadratic forms $f_J(\mathbf{X}) := f_J(X_1, \ldots, X_{2^m})$, $(J \subseteq S_m,\ \tau(e_J) = e_J)$ such that

$$N_\tau(\alpha) = \sum_{\substack{J \subseteq S_m \\ \tau(e_J) = e_J}} f_J(u_J)e_J. \tag{2}$$

Note that $f_\emptyset(\mathbf{X})$ is the m-fold Pfister form $\langle\langle -\mathrm{sgn}_\tau(1)a_1, \ldots, -\mathrm{sgn}_\tau(m)a_m \rangle\rangle$. We see that

$$\{\alpha \in L^\times \mid N_\tau(\alpha) \in K\}$$

is a multiplicative group. Therefore we obtain the following fundamental proposition of the theory of multiplicative quadratic forms on algebraic varieties.

Proposition 1. *Let $f_J(\mathbf{X})$ be 2^{m-1} quadratic forms defined in* (2) *and let V be defined by the $2^{m-1} - 1$ equations $f_J(\mathbf{X}) = 0$, $(J \ne \emptyset)$. The m-fold Pfister form $f_\emptyset(\mathbf{X}) = \langle\langle -sgn_\tau(1)a_1, \ldots, -sgn_\tau(m)a_m \rangle\rangle$ is multiplicative on V.*

Let $V \subsetneq K^n$ be an algebraic variety and q be a quadratic form on V. Define $D_V(q)$ to be the set of values in $K^\times$ represented by q on V, namely

$$\begin{aligned} D_V(q) = \{\alpha \in K^\times \mid \alpha &= q(\alpha_1, \ldots, \alpha_n), \\ &\text{for} \ \ (\alpha_1, \ldots, \alpha_n) \in V\}. \end{aligned}$$

We see that if q is multiplicative on V and represents 1 then $D_V(q)$ is a multiplicative group. Note that we can also consider q over a commutative ring R requiring the Hurwitz-type "bilinear condition" over R. We shall give an application which is the case over the ring of integers $\mathbf{Z}$ in Section 3.

We now present an example of Proposition 1.

Example 2. The case $m = 2$. Suppose $L = K(\sqrt{-a_1}, \sqrt{-a_2})$ is an biquadratic extension field of K and let $\tau \in \mathrm{Gal}(L/K)$ of order 2 such that

$$\tau(\sqrt{-a_1}) = -\sqrt{-a_1}, \quad \tau(\sqrt{-a_2}) = -\sqrt{-a_2}.$$

For $\alpha, \beta \in L$, we write

$$\begin{aligned} \alpha &= X_1 + X_2\sqrt{-a_1} + X_3\sqrt{-a_2} + X_4\sqrt{-a_1}\sqrt{-a_2}, \\ \beta &= Y_1 + Y_2\sqrt{-a_1} + Y_3\sqrt{-a_2} + Y_4\sqrt{-a_1}\sqrt{-a_2}. \end{aligned}$$

We have

$$\begin{aligned} N_\tau(\alpha) = X_1^2 &+ a_1X_2^2 + a_2X_3^2 + a_1a_2X_4^2 \\ &+ 2(X_1X_4 - X_2X_3)\sqrt{-a_1}\sqrt{-a_2} \end{aligned}$$

and put

$$\begin{aligned} q(\mathbf{X}) &:= f_\emptyset(\mathbf{X}) = X_1^2 + a_1X_2^2 + a_2X_3^2 + a_1a_2X_4^2, \\ h(\mathbf{X}) &:= f_{1,2}(\mathbf{X}) = 2(X_1X_4 - X_2X_3). \end{aligned}$$

From Proposition 1, $q(\mathbf{X})$ is multiplicative on $V : h(\mathbf{X}) = 0$. Namely if $h(\mathbf{X}) = 0$ and $h(\mathbf{Y}) = 0$ then there is the bilinear map $\varphi : K^4 \times K^4 \to K^4$ such that $q(\mathbf{X})q(\mathbf{Y}) = q(\varphi(\mathbf{X}, \mathbf{Y}))$ and $h(\varphi(\mathbf{X}, \mathbf{Y})) = 0$. Since $N_\tau(\alpha)N_\tau(\beta) = N_\tau(\alpha\beta)$ and

$$\begin{aligned} \alpha\beta = (X_1Y_1 &- a_1X_2Y_2 - a_2X_3Y_3 + a_1a_2X_4Y_4) \\ &+ (X_2Y_1 + X_1Y_2 - a_2X_4Y_3 - a_2X_3Y_4)\sqrt{-a_1} \\ &+ (X_3Y_1 - a_1X_4Y_2 + X_1Y_3 - a_1X_2Y_4)\sqrt{-a_2} \\ &+ (X_4Y_1 + X_3Y_2 + X_2Y_3 + X_1Y_4)\sqrt{-a_1}\sqrt{-a_2}, \end{aligned}$$

we obtain the bilinear map φ explicitly as follows:

$$\begin{aligned}\varphi(\mathbf{X},\mathbf{Y}) = (&X_1Y_1 - a_1X_2Y_2 - a_2X_3Y_3 + a_1a_2X_4Y_4,\\ &X_2Y_1 + X_1Y_2 - a_2X_4Y_3 - a_2X_3Y_4,\\ &X_3Y_1 - a_1X_4Y_2 + X_1Y_3 - a_1X_2Y_4,\\ &X_4Y_1 + X_3Y_2 + X_2Y_3 + X_1Y_4).\end{aligned}$$

Moreover using above bilinear map φ, we have the following equations.

Corollary 3. *Let $q(\mathbf{X})$, $h(\mathbf{X})$, $\varphi(\mathbf{X},\mathbf{Y})$ be as above in Example 2. Then*

$$\begin{aligned}q(\mathbf{X})q(\mathbf{Y}) &= q(\varphi(\mathbf{X},\mathbf{Y})) - a_1a_2h(\mathbf{X})h(\mathbf{Y}),\\ h(\varphi(\mathbf{X},\mathbf{Y})) &= q(\mathbf{X})h(\mathbf{Y}) + h(\mathbf{X})q(\mathbf{Y}),\end{aligned}$$

where the X_i and Y_j are independent variables.

Remark. From Corollary 3, the 2-fold Pfister form $q(\mathbf{X}) = X_1^2 + a_1X_2^2 + a_2X_3^2 + a_1a_2X_4^2$, $a_1, a_2 \in K^\times$ is multiplicative on $V : h(\mathbf{X}) = 0$ without the supposition that $K(\sqrt{-a_1}, \sqrt{-a_2})$ is a field of degree 4 over K as in Example 2.

The following problem arises as the next natural question after Proposition 1.

Problem 4. Does there exist a quadratic form $q(\mathbf{X})$ which is different from a Pfister form and multiplicative on an algebraic variety $V \subsetneq K^n$.

As in the case which is over vector space K^n, one might expect that a multiplicative quadratic form on algebraic variety is always a Pfister form. However we give the following result for 4-dimensional quadratic forms.

Theorem 4. *For $a, b, c \in K^\times$ with $b^2 + 4ac \neq 0$, let $V_{(a,b,c)}$ be a hypersurface on $\mathbf{A}^4$ defined by $X_1X_2 + aX_3^2 + bX_3X_4 - cX_4^2 = 0$. For any $\lambda \in K^\times$, $q(\mathbf{X}) = X_1^2 + (b^2+4ac)ac\lambda^2X_2^2 + (b^2+4ac)a\lambda X_3^2 + (b^2+4ac)c\lambda X_4^2$ is multiplicative on $V_{(a,b,c)}$. Moreover the bilinear map φ is given explicitly as follows*:

$$\begin{aligned}\varphi(\mathbf{X},\mathbf{Y}) = \\ (&X_1Y_1 + (b^2+4ac)ac\lambda^2X_2Y_2\\ &\quad + (b^2+4ac)a\lambda X_3Y_3 + (b^2+4ac)c\lambda X_4Y_4,\\ &X_2Y_1 + X_1Y_2 + 2aX_3Y_3\\ &\quad + bX_4Y_3 + bX_3Y_4 - 2cX_4Y_4,\\ &X_3Y_1 + 2ac\lambda X_3Y_2 + bc\lambda X_4Y_2\\ &\quad - X_1Y_3 - 2ac\lambda X_2Y_3 - bc\lambda X_2Y_4,\\ &X_4Y_1 + ab\lambda X_3Y_2 - 2ac\lambda X_4Y_2\\ &\quad - ab\lambda X_2Y_3 - X_1Y_4 + 2ac\lambda X_2Y_4).\end{aligned}$$

Proof. Put $f(\mathbf{X}) := X_1X_2 + aX_3^2 + bX_3X_4 - cX_4^2$. Using φ, we can show the following relations by direct calculation.

$$\begin{aligned}q(\mathbf{X})q(\mathbf{Y}) &= q(\varphi(\mathbf{X},\mathbf{Y}))\\ &\qquad - 4(b^2+4ac)ac\lambda^2f(\mathbf{X})f(\mathbf{Y}),\\ f(\varphi(\mathbf{X},\mathbf{Y})) &= q(\mathbf{X})f(\mathbf{Y}) + f(\mathbf{X})q(\mathbf{Y}).\end{aligned}$$

□

Corollary 5. *Let a, b, c, $V_{(a,b,c)}$ be as above in Theorem 4. Suppose $b^2+4ac \notin K^{\times 2}$. Then there are infinitely many 4-dimensional diagonal multiplicative quadratic forms on $V_{(a,b,c)}$ which are different from Pfister forms.*

Remark. For Theorem 4, if we consider $q(\mathbf{X})$ over the field $K(\sqrt{b^2+4ac})$ then we see that Theorem 4 is a consequence of Proposition 1. In fact if we use the non-singular linear transformation of variables as follows:

$$\begin{aligned}&X_1 \to \widetilde{X}_1, \quad X_2 \to \widetilde{X}_4,\\ &X_3 \to \frac{1}{2a}\left(\widetilde{X}_2 - a\widetilde{X}_3 - \frac{b(\widetilde{X}_2 + a\widetilde{X}_3)}{\sqrt{b^2+4ac}}\right),\\ &X_4 \to \frac{\widetilde{X}_2 + a\widetilde{X}_3}{\sqrt{b^2+4ac}},\end{aligned}$$

then we can show that $q(\mathbf{X})$ and $f(\mathbf{X})$ in Theorem 4 are transformed to

$$\begin{aligned}q(\widetilde{\mathbf{X}}) &= \widetilde{X}_1^2 + m_1\widetilde{X}_2^2 + m_2\widetilde{X}_3^2 + m_3\widetilde{X}_4^2,\\ f(\widetilde{\mathbf{X}}) &= \widetilde{X}_1\widetilde{X}_4 - \widetilde{X}_2\widetilde{X}_3,\end{aligned}$$

where

$$\begin{aligned}m_1 &= \frac{\lambda}{2a}\left(b^2 + 4ac - b\sqrt{b^2+4ac}\right),\\ m_2 &= \frac{a\lambda}{2}\left(b^2 + 4ac + b\sqrt{b^2+4ac}\right),\\ m_3 &= m_1m_2 = (b^2+4ac)ac\lambda^2.\end{aligned}$$

The following theorem shows that, in contrast to the classical case, a multiplicative quadratic form $q(\mathbf{X})$ exists in the *non* 2-power dimensional case for some algebraic varieties V.

Theorem 6. *Let $q(\mathbf{X}) = X_1^2 + 21X_2^2 + 21X_3^2 + 21X_4^2 + 14X_5^2 + 42X_6^2$ and V:*

$$\begin{cases} 3X_2^2 + 6X_2X_3 - 6X_2X_4 + 12X_3X_4\\ -3X_4^2 + 3X_5^2 + 4X_1X_6 + 2X_5X_6 - 9X_6^2 = 0,\\ 12X_2X_3 + 3X_3^2 + 6X_2X_4 + 6X_3X_4 - 3X_4^2\\ +2X_1X_5 + X_5^2 + 2X_1X_6 + 10X_5X_6 - 3X_6^2 = 0.\end{cases}$$

Then $q(\mathbf{X})$ is multiplicative on V. Moreover the bilinear map φ is given explicitly as follows:

$$\begin{aligned}
&\varphi(\mathbf{X},\mathbf{Y}) = \\
&\big(-X_1Y_1 - 21X_2Y_2 \\
&\quad - 21X_3Y_3 - 21X_4Y_4 - 14X_5Y_5 - 42X_6Y_6, \\
&\quad X_2Y_1 - X_1Y_2 + X_5Y_2 - 3X_6Y_2 \\
&\quad - 3X_5Y_3 - 3X_6Y_3 - 3X_5Y_4 + 3X_6Y_4 - X_2Y_5 \\
&\quad + 3X_3Y_5 + 3X_4Y_5 + 3X_2Y_6 + 3X_3Y_6 - 3X_4Y_6, \\
&\quad X_3Y_1 - 3X_5Y_2 - 3X_6Y_2 - X_1Y_3 - 2X_5Y_3 \\
&\quad - 6X_6Y_4 + 3X_2Y_5 + 2X_3Y_5 + 3X_2Y_6 + 6X_4Y_6, \\
&\quad X_4Y_1 - 3X_5Y_2 + 3X_6Y_2 \\
&\quad - 6X_6Y_3 - X_1Y_4 + X_5Y_4 + 3X_6Y_4 \\
&\quad + 3X_2Y_5 - X_4Y_5 - 3X_2Y_6 + 6X_3Y_6 - 3X_4Y_6, \\
&(-2X_5Y_1 + 3X_2Y_2 - 9X_3Y_2 \\
&\quad -9X_4Y_2 - 9X_2Y_3 - 6X_3Y_3 - 9X_2Y_4 \\
&\quad +3X_4Y_4 - 2X_1Y_5 + X_5Y_5 - 9X_6Y_5 - 9X_5Y_6)/2, \\
&(-2X_6Y_1 - 3X_2Y_2 - 3X_3Y_2 + 3X_4Y_2 - 3X_2Y_3 \\
&\quad -3X_6Y_6 - 6X_4Y_3 + 3X_2Y_4 - 6X_3Y_4 + 3X_4Y_4 \\
&\quad -3X_5Y_5 - X_6Y_5 - 2X_1Y_6 - X_5Y_6 + 9X_6Y_6)/2\big).
\end{aligned}$$

Proof. We put

$$\begin{aligned}
f_1(\mathbf{X}) :&= 3X_2^2 + 6X_2X_3 - 6X_2X_4 + 12X_3X_4 - 3X_4^2 \\
&\quad + 3X_5^2 + 4X_1X_6 + 2X_5X_6 - 9X_6^2, \\
f_2(\mathbf{X}) :&= 12X_2X_3 + 3X_3^2 + 6X_2X_4 + 6X_3X_4 - 3X_4^2 \\
&\quad + 2X_1X_5 + X_5^2 + 2X_1X_6 + 10X_5X_6 - 3X_6^2.
\end{aligned}$$

Using φ, we find the following relations which can be checked by direct calculation.

$$\begin{aligned}
q(\mathbf{X})q(\mathbf{Y}) &= q(\varphi(\mathbf{X},\mathbf{Y})) - 14f_1(\mathbf{X})f_1(\mathbf{Y}) \\
&\quad + 7f_1(\mathbf{X})f_2(\mathbf{Y}) + 7f_2(\mathbf{X})f_1(\mathbf{Y}) \\
&\quad - 14f_2(\mathbf{X})f_2(\mathbf{Y}), \\
f_1(\varphi(\mathbf{X},\mathbf{Y})) &= q(\mathbf{X})f_1(\mathbf{Y}) + f_1(\mathbf{X})q(\mathbf{Y}) \\
&\quad - 2f_1(\mathbf{X})f_1(\mathbf{Y}) - f_1(\mathbf{X})f_2(\mathbf{Y}) \\
&\quad - f_2(\mathbf{X})f_1(\mathbf{Y}) + 3f_2(\mathbf{X})f_2(\mathbf{Y}), \\
f_2(\varphi(\mathbf{X},\mathbf{Y})) &= q(\mathbf{X})f_2(\mathbf{Y}) + f_2(\mathbf{X})q(\mathbf{Y}) \\
&\quad - 3f_1(\mathbf{X})f_1(\mathbf{Y}) + 2f_1(\mathbf{X})f_2(\mathbf{Y}) \\
&\quad + 2f_2(\mathbf{X})f_1(\mathbf{Y}) + f_2(\mathbf{X})f_2(\mathbf{Y}).
\end{aligned}$$

□

3. Applications. We give one example of applications which use the multiplicative quadratic forms on algebraic varieties over the ring of integers $\mathbf{Z}$.

Let p be a prime $\equiv 1 \pmod 5$. It is well known that the following system of diophantine equations has exactly four integer solutions.

$$16p = x^2 + 125w^2 + 50v^2 + 50u^2, \tag{3}$$

$$xw = v^2 - 4uv - u^2, \tag{4}$$

$$x \equiv -1 \pmod 5. \tag{5}$$

This system is often called "Dickson's system" since above result was discovered by Dickson [1] in 1935. If (x,w,v,u) is one integer solution then the remaining three are $(x,-w,-u,v)$, $(x,w,-v,-u)$, $(x,-w,u,-v)$.

We are able to apply Theorem 4 to above system of diophantine equations. Using Theorem 4 for $a = -1$, $b = 4$, $c = -1$, $\lambda = -5/2$, we see that the quadratic form $q(\mathbf{X}) = X_1^2 + 125X_2^2 + 50X_3^2 + 50X_4^2$ is multiplicative on $V : X_1X_2 = X_3^2 - 4X_3X_4 - X_4^2$. The bilinear map $\varphi : \mathbf{Z}^4 \times \mathbf{Z}^4 \to \mathbf{Z}^4$ such that $q(\mathbf{X})q(\mathbf{Y}) = q(\varphi(\mathbf{X},\mathbf{Y}))$ is given as follows:

$$\begin{aligned}
\varphi(\mathbf{X},\mathbf{Y}) = \\
&(X_1Y_1 + 125X_2Y_2 + 50X_3Y_3 + 50X_4Y_4, \\
&X_2Y_1 + X_1Y_2 - 2X_3Y_3 \\
&\qquad + 4X_4Y_3 + 4X_3Y_4 + 2X_4Y_4, \\
&X_3Y_1 - 5X_3Y_2 + 10X_4Y_2 \\
&\qquad - X_1Y_3 + 5X_2Y_3 - 10X_2Y_4, \\
&X_4Y_1 + 10X_3Y_2 + 5X_4Y_2 \\
&\qquad - 10X_2Y_3 - X_1Y_4 - 5X_2Y_4).
\end{aligned} \tag{6}$$

Using this φ, we obtain the following extended result of Dickson's system.

Theorem 7. *Let N be an integer such that $N = p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$, where $p_i \equiv 1 \pmod 5$ is a prime for each i. Then the system of diophantine equations* (3)–(5) *with N instead of p has integer solutions.*

Let p_1 and p_2 be primes such that $p_1 \equiv p_2 \equiv 1 \pmod 5$. Let $(x_{p_1}, w_{p_1}, v_{p_1}, u_{p_1})$ (resp. $(x_{p_2}, w_{p_2}, v_{p_2}, u_{p_2})$) be one of integer solutions of the system of (3)–(5) which belongs to p_1 (resp. p_2). For the product p_1p_2, we define $(x_{p_1p_2}, w_{p_1p_2}, v_{p_1p_2}, u_{p_1p_2}) \in \mathbf{Z}[1/2]^4$ by

$$\begin{aligned}
&(x_{p_1p_2}, w_{p_1p_2}, v_{p_1p_2}, u_{p_1p_2}) \\
&\quad := \frac{\varphi((x_{p_1}, w_{p_1}, v_{p_1}, u_{p_1}), (x_{p_2}, w_{p_2}, v_{p_2}, u_{p_2}))}{4},
\end{aligned} \tag{7}$$

where φ is the bilinear map in (6). Furthermore, we define $(x_N, w_N, v_N, u_N) \in \mathbf{Z}[1/2]^4$, for $N = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, each p_i is prime $\equiv 1 \pmod 5$, by repeating and using the definition (7). We see that the 4-tuple (x_N, w_N, v_N, u_N) is the solution of the Dickson's system (3)–(5) which belongs to N. Therefore to prove Theorem 7 we have to show that the 4-tuple is integral: $(x_N, w_N, v_N, u_N) \in \mathbf{Z}^4$.

Lemma 8. *Let p be a prime $\equiv 1 \pmod 5$. Then the solution $(x_p, w_p, v_p, u_p) \in \mathbf{Z}^4$ of the system* (3)–(5) *satisfies the following congruences.*

$$(8) \qquad \begin{cases} -x_p + w_p + 2u_p \equiv 0 \pmod 4, \\ -x_p - w_p + 2v_p \equiv 0 \pmod 4. \end{cases}$$

Proof. See, for example, [6, Lemma 1 (d)]. □

Lemma 9. *Let $N_1 = l_1^{a_1} l_2^{a_2} \cdots l_m^{a_m}$ and $N_2 = q_1^{b_1} q_2^{b_2} \cdots q_n^{b_n}$, each l_j, q_k is prime $\equiv 1 \pmod 5$. If $(x_{N_i}, w_{N_i}, v_{N_i}, u_{N_i}) \in \mathbf{Z}^4$ and it satisfies* (8) *for $i = 1, 2$ then $(x_{N_1N_2}, w_{N_1N_2}, v_{N_1N_2}, u_{N_1N_2}) \in \mathbf{Z}^4$ and it also satisfies* (8).

Proof. If $(x_{N_i}, w_{N_i}, v_{N_i}, u_{N_i}) \in \mathbf{Z}^4$ and it satisfies (8) for $i = 1, 2$ then there are $s_1, t_1, s_2, t_2 \in \mathbf{Z}$ such that

$$(9) \qquad \begin{cases} x_{N_i} = w_{N_i} + 2u_{N_i} + 4s_i, \ (i = 1, 2), \\ v_{N_i} = w_{N_i} + u_{N_i} + 2t_i, \quad (i = 1, 2). \end{cases}$$

By the definition (7) and using (9) we see that the 4-tuple $(x_{N_1N_2}, w_{N_1N_2}, v_{N_1N_2}, u_{N_1N_2})$ is equal to

$$\begin{aligned}
(&4s_1s_2 + 50t_1t_2 + 2s_2u_1 + 25t_2u_1 \\
&\quad + 2s_1u_2 + 25t_1u_2 + 26u_1u_2 + s_2w_1 + 25t_2w_1 \\
&\quad + 13u_2w_1 + s_1w_2 + 25t_1w_2 + 13u_1w_2 + 44w_1w_2, \\
&s_2w_1 - 2t_1t_2 + t_2u_1 + t_1u_2 \\
&\quad + 2u_1u_2 - t_2w_1 + u_2w_1 + s_1w_2 - t_1w_2 + u_1w_2, \\
&2s_2t_1 - 2s_1t_2 + s_2u_1 - t_2u_1 - s_1u_2 + t_1u_2 \\
&\quad + s_2w_1 + 2t_2w_1 - u_2w_1 - s_1w_2 - 2t_1w_2 + u_1w_2, \\
&s_2u_1 - s_1u_2 - 5t_2w_1 - 4u_2w_1 + 5t_1w_2 + 4u_1w_2),
\end{aligned}$$

where $(w_i, u_i) = (w_{N_i}, u_{N_i})$ for $i = 1, 2$.
Hence $(x_{N_1N_2}, w_{N_1N_2}, v_{N_1N_2}, u_{N_1N_2}) \in \mathbf{Z}^4$. Using this it is easily verified that this 4-tuple satisfies (8). □

Proof of Theorem 7. By the definition (7), the system of diophantine equations (3)–(4) which belongs to N has solutions $(x_N, w_N, v_N, u_N) \in \mathbf{Z}[1/2]^4$. By Lemma 8 and Lemma 9, we obtain that this 4-tuple (x_N, w_N, v_N, u_N) is in $\mathbf{Z}^4$. It remains to show that $x_N \equiv -1 \pmod 5$. This follows from (6) and (7). □

It is well known that the Dickson's system (3)–(5) is related very deeply to the Jacobi sums. In fact for a prime $p \equiv 1 \pmod 5$ the solution of Dickson's system (3)–(5) give the coefficients of Jacobi sum for $\mathbf{F}_p$. We can study the Jacobi sum for $\mathbf{F}_q$, $q = p^\alpha$ in detail by using Theorem 4. We shall discuss it in separate paper because it is much more elaborate.

Acknowledgement. The author thanks Professor K. Hashimoto who gave him various suggestions during this study.

References

[1] Dickson, L. E.: Cyclotomy, higher congruences and Waring's problem. Amer. J. Math., **57**, 391–424 (1935).

[2] Pfister, A.: Zur Darstellung von −1 als Summe von Quadraten in einem Körper. J. London Math. Soc., **40**, 159–165 (1965).

[3] Pfister, A.: Multiplikative quadratische Formen. Arch. Math., **16**, 363–370 (1965).

[4] Pfister, A.: Quadratic forms with applications to algebraic geometry and topology. London Mathematical Society Lecture Note Series, no. 217, Cambridge University Press, Cambridge (1995).

[5] Schafer, R. D.: An Introduction to Nonassociative Algebras. Dover Publications, Inc., New York (1995).

[6] Katre, S. A., and Rajwade, A. R.: Unique determination of cyclotomic numbers of order five. Manuscripta Math., **53**, 65–75 (1985).

[7] Rajwade, A. R.: Squares. London Mathematical Society Lecture Note Series, no. 171, Cambridge University Press, Cambridge (1993).