JAN G. PĘKAŁA*

ON THE AXIOMS OF QUADRATIC FORM SCHEMES

Abstract. We show that the generally accepted axioms C1, C2 and C3 of quadratic form schemes can be replaced by two simply axioms S1 and S2. Several operations on schemes and the notion of a complete scheme are introduced in the paper. A proof is given that every elementary scheme is complete.

Introduction. A quadratic form scheme is a triple S = (g, V, -1), where g is an elementary 2-group, -1 is a distinguished element of g and V is a mapping assigning to each $a \in g$ a subgroup V(a) of g. We require that the following three axioms hold:

C1. $a \in V(a)$,

C2. $b \in V(a)$ implies $-a \in V(-b)$,

C3. D(a, b, c) = D(b, a, c).

Here $-a = (-1) \cdot a$ and D(a, b, c) is defined for a, b, c in g as follows:

$$D(a, b, c) = \bigcup \{aV(ax): x \in bV(bc)\}.$$

When F is a field of characteristic different from 2, put $g = \dot{F}/\dot{F}^2$, $-1 = (-1)\cdot\dot{F}^2$ and $V(a\dot{F}^2) = D(1, a)$, the value group in g of the binary quadratic form $X^2 + aY^2$. Then $S(F) = (F/\dot{F}^2, V, (-1)\cdot\dot{F}^2)$ is a quadratic form scheme.

The notion of a scheme was introduced by C. Cordes in [3] who demended only the axioms C1 and C2. Then L. Szczepanik [7] observed that C1 and C2 are not sufficient to characterize schemes coming from fields and introduced the axiom C3.

In Section 1 of this paper we show that the axioms C2 and C3 can be substituted by a single axiom S2 avoiding the necessity of using D(a, b, c). The axiom looks as follows:

S2. $-t \in V(a) \cdot V(sa)$ implies $-a \in V(t) \cdot V(ta)$, $a, s, t \in g$.

In Section 2 we consider a generalized version of S2:

GS2. for any subgroup A of g

 $-t \in \Box \{V(sa): a \in A\}$ implies $-s \in \Box \{V(ta): a \in A\}, s, t \in g.$

Taking here $A = \{1, a\}$ one gets S2. Any scheme satisfying GS2 is said to be a *complete scheme*. We prove that every elementary scheme is complete (here *elementary scheme* is defined to be one obtained from some basic simple schemes by taking products and finite group extensions of schemes; for a precise statement see Section 2).

1. New axioms for a scheme. In this section we show to replace the axioms C2 and C3 by a new axiom S2. In the field case C3 is a consequence of the

Received February 8, 1984.

AMS (MOS) Subject classification 1980. Primary 10C02. Secondary 15A63.

^{*}Instytut Matematyki Uniwersytetu Śląskiego, Katowice, ul. Bankowa 14, Poland.

commutativity of addition while connection of S2 with this property is less transparent.

LEMMA 1.1. Suppose (g, V, -1) satisfies C1 and C2. Then for any a, b, c, s, t in g we have

(1.1.1) $y \in D(a, b, c)$ iff $-ab \in V(bc) \cdot V(-ay)$,

(1.1.2)
$$-a \in D(s, st, t) \text{ iff } -t \in V(s) \cdot V(sa).$$

Proof. We have

$$D(a, b, c) = \bigcup \{aV(au): u \in bV(bc)\} = \bigcup \{aV(abx): x \in V(bc)\}.$$

Hence $y \in D(a, b, c)$ if and only if there is an $x \in V(bc)$ such that $ay \in V(abx)$. By C2 this holds if and only if $-abx \in V(-ay)$ or equivalently $-ab \in xV(-ay)$, with x in V(bc). This proves (1.1.1) and (1.1.2) follows directly from (1.1.1).

COROLLARY 1.2. Suppose (g, V, -1) satisfies C1 and C2. Then C3 is satisfied if and only if for every a, s, t in g,

(1.2.1)
$$-t \in V(s) \cdot V(sa) \text{ implies } -s \in V(t) \cdot V(ta).$$

Proof. Assume C3 and $-t \in V(s) \cdot V(sa)$. Then $-a \in D(s, st, t)$, by (1.1.2). Since always D(a, b, c) = D(a, c, b), we conclude $-a \in D(s, t, st)$ and by C3, $-a \in D(t, s, st) = D(t, st, s)$. Hence by (1.1.2) we get $-a \in V(t) \cdot V(ta)$. Now assume (1.2.1) holds. Then

$$D(a, b, c) = abc \cdot D(bc, ac, ab) = abc \cdot D(bc, ab, ac)$$

and similarly

$$D(b, a, c) = abc \cdot D(ac, ab, bc).$$

On combining (1.1.2) and (1.2.1) we get D(bc, ab, ac) = D(ac, ab, bc). This proves C3.

THEOREM 1.3. Let g be an elementary 2-group, -1 a distinguished element of g and V a mapping assigning to each $a \in g$ a subgroup V(a) of g. Then S = (g, V, -1) satisfies C1, C2 and C3 if and only if satisfies the following two conditions S1 and S2:

S1. $a \in V(a), a, s, t \in g$,

S2. $-t \in V(s) \cdot V(sa)$ implies $-s \in V(t) \cdot V(ta)$, $a, s, t \in g$.

Proof. We have proved already that C1, C2 and C3 imply S1 and S2 (Corollary 1.2). Conversely, if S satisfies S1 and S2, then C2 holds, since taking a = 1 we get $V(s) \cdot V(sa) = V(s) \cdot V(s) = V(s)$ and S2 becomes C2. By Corollary 1.2, C1, C2 and S2 imply C3, as required.

2. Elementary and complete schemes. The axiom S2 says that for any 2-element subgroup $A = \{1, a\}$ (and also for $A = \{1\}$) the following property holds

$$(2.0.0) -t \in \prod \{V(sa): a \in A\} \text{ implies } -s \in \prod \{V(ta): a \in A\}.$$

One may ask whether or not (2.0.0) holds, for any subgroup A of g. If this is a case we say S = (g, V, -1) satisfies GS2, the generalized S2. If S satisfies S1 and GS2 it

satisfies also S2 and is said to be a *complete quadratic form scheme*. We are unable to prove that for any field F of characteristic not 2 the scheme S(F) is complete but we shall prove the completeness of any elementary scheme. To define elementary schemes we need to recall some basic facts and terminology.

Let S = (g, V-1) be a scheme. We write g(S) for g and R(S) for the radical of S, that is, for the set $\{a \in g: V(x) = V(ax) \text{ for every } x \in g\}$. R(S) is a subgroup of g. If $ab \in R(S)$, then V(a) = V(b), but not necessarily the other way.

There are two basic operations on schemes. If $\{1, t\}$ is a 2-element group, we write $S^{t} = (g^{t}, V^{t}, -1)$, where $g^{t} = g \oplus \{1, t\}$ and $V^{t}(x) = g^{t}$ for x = -1, $V^{t}(x) = V(x)$ for $x \in g, x \neq -1$ and $V^{t}(x) = \{1, x\}$ elsewhere. S^{t} turns out to be a scheme and is said to be group extension of S. The other operation on schemes is the product of schemes. If $S_{i} = (g_{i}, V_{i}, -1_{i})$. i = 1, 2, are two schemes, then $S = (g_{1} \times g_{2}, V_{1} \times V_{2}, (-1_{1}, -1_{2}))$, where $(V_{1} \times V_{2})(x, y) = V_{1}(x) \times V_{2}(y)$, is also a scheme. S is said to be the product of S_{1} and S_{2} and is denoted $S_{1} \sqcap S_{2}$. The details can be found in [4] and [7].

A scheme S is said to be radical scheme if V(a) = g for every $a \in g$, or equivalently, if R(S) = g. A scheme S is said to be 1-Hilbert if the index of V(a) in g is at most 2 and equals 2 in special cases. The schemes of p-adic fields Q_p and of real numbers are 1-Hilbert. Now we are ready to define elementary schemes.

DEFINITION 2.1. The class \mathfrak{M}_e of elementary schemes is the smallest class of schemes containing all the radical and 1-Hilbert schemes and closed with respect to the operations of the product and group extensions of schemes.

The subclass \mathfrak{M}_{fe} of finite elementary schemes (i.e., those with finite group g(S)) is known to be contained in the class \mathfrak{M}_{fields} of schemes of fields.

If we write \mathfrak{M}_c for the class of complete schemes, then our main result proved further on in this section says that $\mathfrak{M}_e \subset \mathfrak{M}_c$.

We shall introduce now further operations on shemes. So assume S = (g, V, -1) is the usual triple (satisfying at least C1; for a while we do not need any more). In this case $R(S) \subset \bigcap \{V(x): x \in g\}$.

DEFINITION 2.2. For any subgroup A of g put $S_A = (g, U_A, -1)$ where $U_A(s) = \prod \{V(sa): a \in A\}$. S_A is said to be A-completion of S.

Observe that $A \subset R(S_A)$ and $S_{R(S)} = S$.

DEFINITION 2.3. For any subgroup A of R(S) put $S/A = (g/A, V/A, (-1) \cdot A)$, where (V/A)(sA) = V(s)/A. S/A is said to be A-factor of S.

DEFINITION 2.4. For any subgroup A of g put $S_A^* = S_A/A$. S_A^* is the A-factor of A-completion of S.

DEFINITION 2.5. For any subgroup A of g put $T_s(A) = (A, V', e)$ where V'(a) = A for every $a \in A$ and e = -1 if $-1 \in A$ and otherwise e = 1.

Now we will generalize a result of L. Szczepanik [7]. Here is the case A = R(S).

PROPOSITION 2.6. For any subgroup A of R(S),

$$S \cong S/A \sqcap T_S(A).$$

Proof. Recall that $S_1 = (g_1, V_1, -1_1)$ and $S_2 = (g_2, V_2, -1_2)$ are isomorphic if there exists a group isomorphism $f:g_1 \to g_2$ such that $f(-1_1) = -1_2$ and $f(V_1(x)) = V_2(f(x))$, for any $x \in g$. In our case S = (g, V, -1) and $S/A \sqcap T_S(A) =$ $= (g/A \times A, V/A \times V', (-A, e))$. Since g is an elementary 2-group, there exists a subgroup B of g such that $g = B \oplus A$. If $-1 \notin A$, we can choose B to satisfy $-1 \in B$. Now let us define

$$f:g \to g/A \times A$$

by putting f(xy) = (xA, y), for $x \in B$ and $y \in A$. Then f is a well defined group isomorphism and f(-1) = (-A, e). We will prove $f(V(z)) = (V/A \times V')(f(z))$. So let $z = xy \in g$ with $x \in B$ and $y \in A$. Since $A \subset R(S)$, we have V(xy) = V(x) and $A \subset V(x)$. Thus for $h = B \cap V(x)$ we have $V(x) = h \oplus A$. Hence

$$f(V(z)) = f(V(xy)) = f(h \cdot A) = h \cdot A/A \times A =$$

= V(x)/A \times A = V/A(xA) \times V'(y) =
= (V/A \times V')(xA, y) = (V/A \times V')(f(xy)),

as required.

COROLLARY 2.7. $S_A \cong S_A^* \sqcap T_S(A)$. Proof. Indeed, $T_S(A) = T_S(A)$. LEMMA 2.8. If $A^A < B < R(S)$ is a chain of groups, then

B/A < R(S/A) and $S/A/B/A \cong S/B$.

Proof. The required isomorphism is defined as follows:

 $f:g/A/B/A \rightarrow g/B, f((xA)B/A) = xB.$

Suppose now S_1 and S_2 are two triples and g_1, g_2 are the two elementary 2-groups. We write $pr_i:g_1 \times g_2 \rightarrow g_i$, i = 1, 2 for the projections, $pr_i(x_1, x_2) = x_i$, i = 1, 2. If $C \subset g_1 \times g_2$, we write C^p for $pr_1(C) \times pr_2(C)$.

In the lemma below the groups A_1, A_2, C, A, B are assumed to satisfy the obvious conditions making the formulae sensible.

LEMMA 2.9. For any triples S, S_1 and S_2 (satisfying C1) we have:

 $(2.9.1) (S_1 \sqcap S_2)_{A_1 \times A_2} \cong S_{1A_1} \sqcap S_{2A_2},$

$$(2.9.2) (S_1 \sqcap S_2)_C = (S_1 \sqcap S_2)_{C^p} \cong S_{1pr_1(C)} \sqcap S_{2pr_2(C)}.$$

(2.9.3)
$$S_1 \sqcap S_2/A_1 \times A_2 \cong S_1/A_1 \sqcap S_2/A_2,$$

 $(2.9.4) (S_1 \sqcap S_2)^*_{A_1 \times A_2} \cong S^*_{1A_1} \sqcap S^*_{2A_2},$

(2.9.5)
$$S_1 \sqcap S_2/C \cong S_1/pr_1(C) \sqcap S_2/pr_2(C) \sqcap T_{S_1 \sqcap S_2/C}(C^p/C),$$

$$(2.9.6) (S_1 \sqcap S_2)^*_C \cong S^*_{1pr_1(C)} \sqcap S_{2pr_2(C)} \sqcap T_{(S_1 \sqcap S_2)^*_C}(C^p/C),$$

(2.9.7)
$$(S')^*_A \cong \begin{cases} (S^*_A)^t, & A \subset g(S), \\ S^*_A \circ_{\sigma(S)}, A \subset g(S), \end{cases}$$

(2.9.8)
$$(S^t)^*_{\{1,t\}} \cong S.$$

Proof. Here everything is easy or follows from the preceding statements except for (2.9.5) and (2.9.7). These will be given full proofs.

Proof of (2.9.5). Let C be a subgroup of $R(S_1 \sqcap S_2) = R(S_1) \times R(S_2)$ and $C^p = A_1 \times A_2$, $A_i = pr_i(C)$, i = 1, 2. From (2.9.3) and Lemma 2.8 we get

 $S_1/A_1 \sqcap S_2/A_2 \cong S_1 \sqcap S_2/A_1 \times A_2 = S_1 \sqcap S_2/C^p \cong S_1 \sqcap S_2/C/C^p/C.$

We use this and Proposition 2.6 to finish the proof:

$$S_{1} \sqcap S_{2}/C \cong S_{1} \sqcap S_{2}/C/C^{p}/C \sqcap T_{S_{1} \sqcap S_{2}/C}(C^{p}/C)$$
$$\cong S_{1}/A_{1} \sqcap S_{2}/A_{2} \sqcap T_{S_{1} \sqcap S_{2}/C}(C^{p}/C).$$
(2.9.7). Let $S = (g, V, -1)$ and $S^{t} = (g^{t}, V^{t}, -1)$ where

$$V'(x) = \begin{cases} g^t, & x = -1, \\ V(x), & x \neq -1 \text{ and } x \in g, \\ \{1, x\} & x \in g^t \setminus g. \end{cases}$$

Let A be a subgroup of g^t . Then $(S^t)_A = (g^t, U_A^t, -1)$ where

$$U_A^t(s) = \prod \{ V^t(sa) : a \in A \}$$
 and $(S^t)_A^* = (g^t/A, U_A^t/A, -A).$

Case I. Let $A \subset g(S) = g$. We consider three subcases.

(1) $-s \in A$. Then $U_A^t(s) = g^t$.

Proof of

(2) $-s \in g \setminus A$.

Then $U_A^t(s) = \prod \{V(sa): a \in A\} = :U_A(s)$ where $S_A^* = (g/A, U_A/A, -A)$. (3) $-s \in g^t \setminus g$.

Then $U_A^{t}(s) = \prod \{\{1, sa\}: a \in A\} = \{1, s\} \oplus A$. Thus

$$U_{A}^{t}(s) = \begin{cases} g^{t}, & -s \in A, \\ U_{A}(s), & -s \in g \setminus A, \\ \{1, s\} \oplus A, & -s \in g^{t} \setminus g, \end{cases}$$

and

$$U_{A}^{t}/A(sA) = \begin{cases} g^{t}/A, & sA = -A, \\ U_{A}/A(sA), & sA \neq -A \text{ and } sA \in g/A, \\ \{A, sA\}, & sA \in g^{t}/A \setminus g/A. \end{cases}$$

Thus the mapping $f:g^t/A \to g/A \times \{1, t\}, f((xy)A) = (xA, y)$, for $x \in g$ and $y \in \{1, t\}$ establishes an isomorphism between $(S')^*_A$ and $(S^*_A)^t$.

Case II. Suppose $A \subseteq g$. Take $B = A \cap g$ and choose an $a_0 \in A \setminus g = A \setminus B$. Then $A = B \cup a_0 B = \{1, a_0\} \oplus B$. Recall that $U_A^t(s) = \bigcap \{V^t(sa): a \in A\}$. Consider now three subcases:

(1)
$$-s \in A$$
.

Then $U_A^t(s) = g^t$. (2) $-s \in g \setminus A$. Then

$$U_{A}^{i}(s) = \prod \{V(sa): a \in B\} \cdot \prod \{V^{i}(sa_{0}a): a \in B\} =$$

= $U_{B}(s) \cdot \prod \{\{1, sa_{0}a\}: a \in B\} =$
= $U_{B}(s) \cdot B \cdot \{1, sa_{0}\} = U_{B}(s) \cdot \{1, a_{0}\}$

where $S_B^* = (g/B, U_B/B, -B)$. (3) $-s \in g^t \setminus (g \cup A)$.

Then $-sa_0 \in g \setminus A$ and $U_A^t(s) = U_A^t(sa_0) = U_B(sa_0) \{1, a_0\}$ by the subcase (2). Hence

$$U_{\boldsymbol{A}}^{t}(s) = \begin{cases} g^{t}, & -s \in A, \\ U_{\boldsymbol{B}}(s) \oplus \{1, a_{0}\}, & -s \in g \setminus A, \\ U_{\boldsymbol{B}}(sa_{0}) \oplus \{1, a_{0}\}, & -s \in g^{t} \setminus (A \cup g), \end{cases}$$

and

$$U_A^t/A(sA) = \begin{cases} g^t/A, & sA = -A, \\ U_B(s) \oplus \{1, a_0\}/B \oplus \{1, a_0\}, & sA \neq -A \text{ and } s \in g, \\ U_B(sa_0) \oplus \{1, a_0\}/B \oplus \{1, a_0\}, & sA \neq -A \text{ and } a \in g^t \setminus g. \end{cases}$$

Also $g^t = g \oplus \{1, t\} = g \oplus \{1, a_0\}$ and $A = B \oplus \{1, a_0\}$. Let $f:g^t/A \to g/B$, f((xy)A) = xB, for $x \in g$ and $y \in \{1, a_0\}$. Then f is a well defined group isomorphism and f(-A) = -B. Moreover,

$$f(U_A^t/A(sA)) = \begin{cases} g/B, & sA = -A, \\ U_B(s)/B, & sA \neq -A \text{ and } s \in g, \\ U_B(sa_0)/B, & sA \neq -A \text{ and } s \in g^t \setminus g, \end{cases}$$
$$= \begin{cases} g/B, & sA = -A, \\ U_B/B(sB), & sA \neq -A \text{ and } s \in g, \\ U_B/B(sa_0 \cdot B), & sA \neq -A \text{ and } s \in g, \\ U_B/B(sa_0 \cdot B), & sA \neq -A \text{ and } sa_0 \in g, \end{cases}$$
$$= U_B/B(f(sA)).$$

Thus f is the required isomorphism of $(S')_A^*$ and S_B^* . This proves the lemma.

The final lemma needed assumes again S is a scheme. In the case of fields it was first proved by C. Cordes [3].

LEMMA 2.10. Suppose S = (g, V, -1) is either radical or 1-Hilbert quadratic form scheme. Then for any $a, b \in g$,

$$V(a) = V(b)$$
 iff $ab \in R(S)$.

Proof. The implication \Leftarrow is trivial and has been remarked earlier on. To prove \Rightarrow , let us assume V(a) = V(b) and let x be an arbitrary element of g. If $x \in V(a) = V(b)$, then $-a, -b \in V(-x)$ and $ab \in V(-x)$, hence $x \in V(-ab)$. If $x \notin V(a) = V(b)$, then $-a, -b \notin V(-x)$. Since $|g/V(-x)| \leq 2$, we conclude $ab \in V(-x)$ and so $x \in V(-ab)$. In both cases $x \in V(-ab)$, that is, V(-ab) = gand so $ab \in R(S)$.

Now we come to the main result of this section.

THEOREM 2.11. Any elementary scheme S has the property that for each subgroup A of g(S) the A-factor of A-completion of S (i.e. S_A) is again an elementary scheme.

Proof. Let \mathfrak{N} be the class of schemes S with the property that for each subgroup A of g(S) the S_A^* is an elementary scheme. The definition of the class \mathfrak{M}_e (Definition 2.1) suggests that it is sufficient to prove the following three statements:

- (1) If S is radical or 1-Hilbert scheme, then $S \in \mathfrak{N}$.
- (2) If $S_1, S_2 \in \mathfrak{N}$, then $S_1 \sqcap S_2 \in \mathfrak{N}$.
- (3) $S \in \mathfrak{N}$ implies $S^t \in \mathfrak{N}$.

Proof of (1). Suppose S is a radical or 1-Hilbert scheme. Then obviously the same is true of S_A and $S_A/A = S_A^*$, for any subgroup A of g, because

$$S_A = \begin{cases} S, & A \subset R(S), \\ T_S(g(S)), & A \subset / R(S), \end{cases}$$

by Lemma 2.10. Thus $S \in \mathfrak{N}$.

Proof of (2). Suppose $S_1, S_2 \in \mathfrak{N}$ and let C be any subgroup of $g(S_1 \sqcap S_2) = g(S_1) \times g(S_2)$. Then (2.9.6) asserts that

 $(S_1 \sqcap S_2)_C^* \cong S_{1\,pr_1(C)}^* \sqcap S_{2\,pr_2(C)}^* \sqcap T_{(S_1 \sqcap S_2)_C}^* (C^p/C)$

and all the three factors of the product on the right hand side belong to \mathfrak{M}_e (the first two because of $S_1, S_2 \in \mathfrak{N}$). Hence also the whole product belongs to \mathfrak{M}_e . This shows that $S_1 \sqcap S_2 \in \mathfrak{N}$.

Proof of (3). Suppose $S \in \mathfrak{N}$ and A is any subgroup of g(S'). From (2.9.7) and from $S \in \mathfrak{N}$ we conclude that $(S')^*_A \in \mathfrak{M}_e$. Hence $S' \in \mathfrak{N}$, as required. This proves the theorem.

As a corollary to 2.11 we obtain the result mentioned in the Introduction. THEOREM 2.12. Every elementary scheme is complete.

Proof. Let S be an elementary scheme. By Theorem 2.11, for any subgroup A of g, S_A^* is an elementary scheme. According to Corollary 2.7, $S_A \cong S_A^* \sqcap T_S(A)$, and since $T_S(A)$ in certainly elementary scheme, so is S_A . This implies S is complete, as required.

As we have remarked earlier on it is an open question as to $\mathfrak{M}_{fields} \subset \mathfrak{M}_{c}$. In a series of papers C. Cordes [2], K. Szymiczek [8], M. Kula [5], M. Kula, L. Szczepanik and K. Szymiczek [6], L. Szczepanik [7], A. B. Carson and M. Marshall [1] have proved that any scheme S, with the index of radical R(S) in the group g(S) not exceeding 32, is elementary and so, by Theorem 2.12, is complete. Moreover, all the schemes with $[g(S):R(S)] \leq 32$ are realizable as schemes of fields (M. Kula [4]). All this shows that there is no simple counterexample to the conjecture $\mathfrak{M}_{\text{fields}} \subset \mathfrak{M}_{c}$.

REFERENCES

- [1] A.B. CARSON and M. MARSHALL, Decomposition of Witt rings, preprint.
- [2] C. CORDES, The Witt group and the equivalence of fields with respect to quadratic forms, J. Algebra 26 (1973), 400-421.
- [3] C. CORDES, Quadratic forms over nonformally real fields with a finite number of quaternion algebras. Pacific J. Math. 63 (1976), 357–366.
- [4] M. KULA, Fields with prescribed quadratic form schemes, Math. Z. 167 (1979), 201-212.
- [5] M. KULA, Fields with non-trivial Kaplansky's radical and finite square class number. Acta Arith. 38 (1981), 411–418.
- [6] M. KULA, L. SZCZEPANIK and K. SZYMICZEK, Quadratic forms over formally real fields with eight square classes, Manuscripta Math. 29 (1979), 295–303.
- [7] L. SZCZEPANIK, Klasyfikacja pierścieni Witta w aksjomatycznej teorii form kwadratowych. Praca doktorska, Uniwersytet Śląski, Katowice 1979.
- [8] K. SZYMICZEK, Quadratic forms over fields with finite square class number, Acta Arith. 28 (1975), 195–221.