GRZEGORZ KRAWCZYK *

CLOSED SUBGROUPS OF A QUADRATIC FORM SCHEME

Abstract. In the paper the number $c(S)$ of closed subgroups of a quadratic form scheme S is considered. We determine $c(S)$ for some classes of schemes. Schemes with small $c(S)$ are characterized and the behaviour of $c(S)$ under known operation on schemes are discussed, as well.

Introduction. Closed subgroups of the group of square classes $g(F) = F/F^2$ of a field F were introduced by K. Szymiczek in [10, Chapter V] as a byproduct of the Galois correspondence established between the subgroups of $g(F)$ and binary quadratic forms over F. We use his characterization of closed subgroups of g ([10, Theorem 1.6]) to generalize the concept to the context of quadratic form schemes in the sense of Cordes-Szczepanik. Thus if $S = (g, -1, d)$ is a quadratic form scheme we write $L(S)$ for the smallest set of subgroups of g with the following two properties:

(i) $d(a) \in L(S)$ for any $a \in g$,

(ii) if $X_t \in L(S)$ for any t in a set of indices T, then

$$\bigcap \{X_t : t \in T\} \in L(S).$$

The subgroups of g belonging to $L(S)$ are said to be *closed subgroups of the scheme S*. We write $c(S)$ for the cardinality of $L(S)$. Problem 8 proposed by K. Szymiczek in [10] consists in investigating the number of closed subgroups $c(S)$ of a scheme S and describing the connections with other scheme invariants.

In this paper we will determine $c(S)$ for a number of classes of schemes S. First we characterize the schemes with small numbers of closed subgroups and describe the behaviour of $c(S)$ under operations on schemes. This makes it possible to calculate $c(S)$ for any scheme S with $|g| \leqslant 32$, i.e. as far as the complete classifications of schemes are known at the moment (cf [1]). We also study $c(S)$ for schemes with only two 2-fold Pfister forms and for quasi-pythagorean schemes. One particular result (Corollary 4.4) seems to be new even in the classical case of pythagorean fields.

Notation and terminology. Let g be an elementary 2-group with distinguished element $-1 \in g$. (We permit $-1 = 1$). For every $a \in g$ the product $(-1)a$ will be written $-a$. Let d be any mapping from g into the set of all subgroups of g.

The triplet $S = (g, -1, d)$ is said to be a *quadratic form scheme* (or simply *scheme*) if it satisfies the following axioms:

C1. $a \in d(a)$ for any $a \in g$,

C2. $a \in d(b)$ iff $-b \in d(-a)$ for any $a, b \in g$,

C3. $\bigcup_{x \in bd(bc)} ad(ax) = \bigcup_{y \in ad(ac)} bd(by)$ for any $a, b, c \in g$.

Received July 5, 1982.

AMS (MOS) Subject classification (1980). Primary 10C03. Secondary 15A63.

Instytut Matematyki WSP, Opole, ul. Oleska 48, Poland.

The subgroup $R(S) = \bigcap \{d(a): a \in g\}$ is said to be the *radical of* the *scheme S*. The scheme $S = (g, -1, d)$ is said to be *radical* if $R(S) = g$, *quasi--pythagorean* if $R(S) = d(1)$ and *pythagorean* if $d(1) = \{1\}$.

The motivating example is the scheme $S(F)$ of a field F of characteristic not 2, with $g = g(F)$, $-1 = (-1)F^2$ and $d(a)$ the value group of the binary quadratic form $X^2 + aY^2$. A simple and often used consequence of C1 and C2 is this:

$$d(a) \cap d(b) \subset d(-ab) \text{ for any } a, b \in g.$$

Observe also that $a \in R(S)$ iff $d(-a) = g$ and that $g(x) = d(xr)$ for any $x \in g$, $r \in R(S)$.

1. Schemes with small number of closed subgroups. In the section we describe completely the schemes with $c(S) \leqslant 3$. We begin with the following observation.

LEMMA 1.1. *Let $S = (g, -1, d)$ be a quasi-pythagorean scheme. Then $d(a) = d(b)$ if and only if $ab \in R(S)$.*

Proof. If $d(a) = d(b)$, then $d(a) = d(a) \cap d(b) \subset d(-ab)$ and similarly $d(b) \subset d(-ab)$. Hence $ab \in d(-ab)$, hence also $-1 = ab(-ab) \in d(-ab)$ and $ab \in d(1) = R(S)$. Conversely, if $ab \in R(S)$, then $d(-ab) = g$ and so $d(a) = d(a) \cap d(-ab) \subset d(b)$ and similarly $d(b) \subset d(a)$.

We shall need the notion of a real scheme. We define the sets $D(n)$ for $n \in \mathbf{N}$ inductively as follows: $D(2) = d(1)$ and $D(n+1) = \bigcup \{d(a): a \in D(n)\}$. The scheme $S = (g, -1, d)$ is said to be *non-real* if there is an $n \in \mathbf{N}$ with $-1 \in D(n)$. Otherwise the scheme is said to be *real*.

We follow the terminology of [11] and say the scheme S is 1-*Hilbert* if the index of $d(a)$ in g is at most 2 for each $a \in g$ and equals 2 for at least one $a \in g$. As proved by Kaplansky [5], if $[g:R(S)] = 2$, the scheme is real 1-Hilbert (see [11] for a generalization).

Now we are ready to state the following result.

PROPOSITION 1.2. *Let $S = (g, -1, d)$ be a quadratic form scheme. Then*

(i) $c(S) = 1$ *if and only if S is a radical scheme,*

(ii) $c(S) = 2$ *if and only if S is a real* 1-*Hilbert scheme,*

(iii) $c(S) \neq 3$.

Proof. If $L(S)$ is the semilattice of closed subgroups of S, then certainly R and g both belong to $L(S)$. Hence $c(S) = 1$ requires $R = g$ and the scheme is radical.

To prove (ii), observe that $c(S) = 2$ means $L(S) = \{R, g\}$ and $R \neq g$. If $[g:R] = 2$, the scheme is real 1-Hilbert by the above mentioned result of Kaplansky. If $[g:R] > 2$ and $d(1) = R$, then by Lemma 1.1 there are at least $[g:R]$ pairwise distinct closed subgroups in g, contradicting $c(S) = 2$. The remaining case is $[g:R] > 2$ and $d(1) = g$. Now $-1 \in R$ and if $a \in g \backslash R$, then $d(a) \neq R$ and also $d(a) \neq g$, since otherwise $-a \in R$ and so $a = (-1)(-a) \in R$, a contradiction. Thus there are at least 3 closed subgroups: $R, d(a), g$, contrary to $c(S) = 2$. This proves (ii).

To prove (iii) observe that $c(S) = 3$ implies $L(S)$ is totally ordered by inclusion. K. Szymiczek ([10, Propositions 1.9 and 1.10]) proved that — in the field case — $L(S)$ is totally ordered if and only if $c(S) = 2$. His proof applies also in the abstract case thus giving $c(S) \neq 3$ for any scheme S.

REMARK. A complete characterization of the case $c(S) = 4$ is given in Proposition 4.5 below.

2. Behaviour of $c(S)$ under operations on schemes. We shall consider the following three operations on schemes: product of schemes, group extension of a scheme and factoring a scheme by the radical.

If $S = (g, -1, d)$ and $S' = (g', -1', d')$ are two schemes, their product $S \sqcap S'$ is defined to be $(g \times g', (-1, -1'), d \times d')$, where $(d \times d')((a, a')) = d(a) \times d'(a')$. A direct checking shows that $S \sqcap S'$ satisfies C1-C3 whenever S and S' do.

The group extension S^t of a scheme S is defined in the following way. Take a 2-element group $\{1, t\}$ and make $g^t = g \cup tg$ into a group in an obvious way. Define $d^t(a) = d(a)$ for $a \in g$, $a \neq -1$, $d^t(-1) = g^t$ and $d^t(at) = \{1, at\}$ for any $a \in g$. Then $S^t = (g^t, -1, d^t)$ is a scheme.

Finally, let $S = (g, -1, d)$ be a scheme and $R = R(S)$ its radical. Consider $S/R = (g_R, -1_R, d_R)$ where $g_R = g/R$, $-1_R = (-1)R$ and $d_R(aR) = d(a)R$. If S satisfies C1-C3, so does S/R, the factor scheme. More details on this subject can be found in [7], [8].

We want to know the behaviour of $c(S)$ under the three operations on shcmes. All the schemes considered are assumed to be finite.

PROPOSITION 2.1.

(i) $c(S \sqcap S') = c(S)c(S')$,

(ii) $c(S^t) = \begin{cases} c(S) + |g|, & \text{if } R(S) = \{1\}, \\ c(S) + |g| + 2, & \text{if } R(S) \neq \{1\}, \end{cases}$

(iii) $c(S/R) = c(S)$.

Proof. (i) For any two families of sets $\{A_i : i \in I\}$ and $\{B_j : j \in J\}$ we have

$$\bigcap_{i,j} A_i \times B_j = \bigcap_i A_i \times \bigcap_j B_j.$$

It follows $L(S \sqcap S') = L(S) \times L(S')$, hence (i).

(ii) If $R(S) = \{1\}$, then $g \notin L(S^t)$ and

$$L(S^t) = (L(S) \setminus g) \cup g^t \cup A$$

where A is the family of 2-element groups $\{1, at\}$, $a \in g$. Thus $c(S^t) = c(S) - 1 + 1 + |A| = c(S) + |g|$. If $R(S) \neq \{1\}$, then

$$L(S^t) = L(S) \cup g^t \cup \{1\} \cup A,$$

hence $c(S^t) = c(S) + 2 + |A| = c(S) + |g| + 2$.

(iii) L. Szczepanik ([8, Theorem 4.7]) has proved that for any scheme S there exists a radical scheme S' such that $S \cong S' \sqcap S/R$. Since isomorphic schemes have the same number of closed subgroups, we have $c(S) = c(S')c(S/R)$ and $c(S') = 1$ by Proposition 1.2.(i).

EXAMPLES. 2.2. Suppose $c = c(S)$ is the number of closed subgroups of a scheme $S = (g, -1, d)$ with $|g| = 2^n$. Then for any natural number $m \geqslant n$ there exists a scheme $S' = (g', -1', d')$ such that $|g'| = 2^n$ and $c(S') = c$.

Indeed, let $S'' = (g'', -1'', d'')$ be a radical scheme with $|g''| = 2^{m-n}$, $S'' = S(F_5) \sqcap \ldots \sqcap S(F_5)$ (m–n factors) for instance, then by Proposition 2.1.(i) the scheme $S' = S \sqcap S''$ satisfies the requirements.

2.3. Using the classification of schemes on groups of order $\leqslant 16$ carried over in [9] and Proposition 2.1 we have computed all the values of $c(S)$ actually taken on when S runs through the class.

$|g| = 1$: $c(S) = 1$.
$|g| = 2$: $c(S) = 1, 2$.
$|g| = 4$: $c(S) = 1, 2, 4, 5$.
$|g| = 8$: $c(S) = 1, 2, 4, 5, 7, 8, 9, 10, 16$.
$|g| = 16$: $c(S) = 1, 2, 4, 5, 7, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 20, 24, 25, 32, 67$.

2.4. For a non-real scheme S we define the u-invariant $u(S)$ to be the smallest positive integer u with the property that every $u+1$ dimensional form over S is isotropic. It is known that $u(S) \leqslant q(S)$, where $q(S)$ is the cardinality of the group g. For the schemes with largest possible u-invariant we are able to calculate $c(S)$ on using structure results of [3] and [8] and Proposition 2.1.

(i) If $4 \leqslant q(S) = u(S)$, then $c(S) = q(S)+1$.

(ii) If $8 \leqslant q(S) = 2u(S)$ and $s(S) \geqslant 4$, then $c(S) = q(S)+8$.

(iii) If $8 \leqslant q(S) = 2u(S)$ and $s(S) \leqslant 2$ and S is not a group extension of another scheme, then $c(S) = u(S)+1$.

Here $s(S)$ denotes the level of the scheme, that is, the minimal number n with $-1 \in D(n)$.

To prove (i) one uses L. Szczepanik's ([8, Theorem 5.4]) characterization of non-real schemes with $q(S) = u(S) \geqslant 4$. Any such scheme S is isomorphic to the scheme of the iterated power series field $F_3((t_1)) \ldots ((t_n))$ and to find $c(S)$ we use induction on n and Proposition 2.1.(ii).

Proofs for (ii) and (iii) are similar on using Theorem 3 in [3] and Lemma 5.5 and Theorem 5.6 in [8], respectively.

3. A characterization of non-real 2-local schemes. A scheme $S = (g, -1, d)$ is said to be 2-*local* if there are —up to isometry— exactly two 2-fold Pfister forms over g (cf. [11] for the motivation in the field case). We will characterize non-real 2-local schemes by means of the number of closed subgoups of the scheme. First note the following trivial bound for $c(S)$ of a finite scheme S.

PROPOSITION 3.1. *Let* $S = (g, -1, d)$ *be a scheme with* $|g| = 2^n$. *Then* $1 \leqslant c(S) \leqslant \alpha(2, n)$, *where* $\alpha(2, n)$ *is the number of all subgroups of an elementary 2-group of order* 2^n.

An explicit expression for $\alpha(2, n)$ is this (of Fuchs [4, § 15, Example 14]):

$$\alpha(2, n) = 1 + \sum_{k=1}^{n} \prod_{i=1}^{k} (2^{n-i+1}-1)/(2^i-1).$$

THEOREM 3.2. *Let S be a non-real scheme and $|g/R(S)| = 2^n$. Then S is 2-local if and only if $c(S) = \alpha(2, n)$.*

Proof. Suppose first S is a non-real 2-local scheme with $|g/R| = 2^n$. C. Cordes ([2, Corollary to Lemma 2]) proves —in the field case but his arguments work all right in the abstract case as well— that then for every subgroup A of index 2 in g containing R there is an element $a \in g$ such that $A = d(a)$. Thus all the subgroups of index 2 in g containing R belong to $L(S)$ and it follows that $c(S) = |L(S)| = \alpha(2, n)$.

Conversely, if S is a non-real scheme with $|g/R| = 2^n$ and $c(S) = \alpha(2, n)$, then necessarily every subgroup of index 2 in g containing R is of the form $d(a)$ for a certain $a \in g$ (recall that $L(S)$ consists of intersections of $d(a)$'s). Observe that $d(a) = d(ra)$ for any $r \in R$, hence the number of distinct subgroups of g of the form $d(a)$ is at most $2^n = |g/R|$. But in the elementary 2-group g/R of order 2^n there are exactly $2^n - 1$ subgroups of index 2 and as shown above each of them is of the form $d(a)$. It follows that $[g:d(a)] = 2$ for every $a \in g \backslash R$. Now we use Kaplansky's result ([5, Theorem 2]) to conclude that the scheme has only one anisotropic 2-fold Pfister form i.e., S is 2-local (cf. [11, Proposition 2.3] for a direct proof). This proves the theorem.

4. Closed subgroups in quasi-pythagorean schemes. In any scheme $R \subset d(1)$ and if $R = d(1)$, the scheme is said to be *quasi-pythagorean* (we follow the terminology of [6]). Every pythagorean scheme (satisfying $d(1) = \{1\}$) is quasi-pythagorean but there are also other examples. First, any real 1-Hilbert scheme is quasi-pythagorean since for such a scheme $|g/R| = 2$ and $R = d(1)$. Second, if S and S' are both quasi-pythagorean so is $S \sqcap S'$.

We determine here $c(S)$ for any finite quasi-pythagorean scheme and characterize this type of schemes in terms of closed subgroups.

We begin with the following result on pythagorean schemes.

PROPOSITION 4.1. *For any finite pythagorean scheme $S = (g, -1, d)$ we have $c(S) = |g|$.*

Proof. The structure of a finite pythagorean scheme S has been described by M. Kula. According to [7], S is built up from the scheme of real numbers $S(\mathbf{R})$ by iterating the operations of the product of schemes and group extensions. To prove $|c(S)| = |g|$ we use induction on the order of g. If $|g| = 2$, the scheme is isomorphic to $S(\mathbf{R})$ and $c = 2$. Assume $|g| = 2^n > 2$. By the structure theorem quoted above, either $S = S_1 \sqcap S_2$ or $S = S_1^t$, where S_1, S_2 are pythagorean schemes. Using induction hypothesis and Proposition 2.1.(i) and (ii), we get $c(S) = |g|$, as required.

COROLLARY 4.2. *For any finite quasi-pythagorean scheme S we have $c(S) = |g/R(S)|$.*

Proof. $c(S) = c(S/R(S))$ by Proposition 2.1.(iii). On the other hand, $S/R(S)$ is pythagorean, hence Proposition 4.1 applies.

THEOREM 4.3. *A finite scheme S is quasi-pythagorean if and only if every closed subgroup of S is of the form $d(a)$ for $a \in g$.*

Proof. Suppose first S is quasi-pythagorean. By Lemma 1.1 there are exactly $|g/R|$ pairwise distinct subgroups $d(a)$, $a \in g$. Each of them is closed and by Corollary 4.2 the number of all closed subgroups is g/R. Hence the result.

Now assume the only closed subgroups of g are $d(a)$, $a \in g$. Then $R = d(b)$ for a certain $b \in g$. Hence for any $x \in g$,

$$d(b) = R \subset d(x) = d(-b) \cap d(x) \subset d(bx).$$

Putting $x = 1$ we get $R = d(1)$, i.e. the scheme is quasi-pythagorean.

An interesting corollary to this seems not to have been recorded in the literature even in the case of pythagorean fields.

COROLLARY 4.4. *A finite scheme S is quasi-pythagorean if and only if for any two elements $a, b \in g$ there is a $c \in g$ such that $d(a) \cap d(b) = d(c)$.*

PROPOSITION 4.5. *For any scheme S, $c(S) = 4$ if and only if $S/R(S) \cong$ $\cong S(\mathbf{R}) \sqcap S(\mathbf{R})$.*

Proof. The "if" part follows immediately from Proposition 2.1.(i) and 2.1.(iii).

To prove the converse we may assume $R(S) = \{1\}$ (Proposition 2.1.(iii)). If $c(S) = 4$, the set of closed subgroups cannot be totally ordered by inclusion (cf. Corollary 1.11 in [10]), hence there are $a, b \in g$, $a \neq b$, such that $d(a) \cap d(b) =$ $= \{1\}$. It follows

$$1 \neq ab \notin d(a) \cup d(b)$$

and since $ab \in d(ab)$ we get $d(ab) = g$. Hence $-ab \in R = \{1\}$ and since $a \neq b$ it follows $1 \neq -1$ and $d(1) \neq g$. Also $d(1) \neq d(a)$ since otherwise $d(a) = d(1) \cap$ $\cap d(a) \subset d(-a) = d(b)$, a contradiction. Similarly $d(1) \neq d(b)$ and so $d(1) =$ $= \{1\}$. Thus the scheme is pythagorean and by Proposition 4.1, $|g| = c(S) = 4$.

Now the only pythagorean scheme with $|g| = 4$ is $S(\mathbf{R}) \sqcap S(\mathbf{R})$, as required.

REFERENCES

[1] A. B. CARSON, M. A. MARSHALL, *Decomposition of Witt rings*, preprint.

[2] C. M. CORDES, *Quadratic forms over non-formally real fields with a finite number of quaternion algebras*, Pacific J. Math. 63 (1976), 357—365.

[3] C. M. CORDES, J. R. RAMSEY, *Quadratic forms over fields with $u = q/2 < +\infty$*, Fund. Math. 99 (1978), 1—10.

[4] L. FUCHS, *Infinite Abelian Groups*, vol. I, New York and London 1970, Academic Press.

[5] I. KAPLANSKY, *Frohlich's local quadratic forms*, J. Reine Angew. Math. 239/240 (1969), 74—77.

[6] D. KIJIMA, M. NISHI, *Kaplansky's radical and Hilbert Theorem* 90, II, preprint.

[7] M. KULA, *Fields with prescribed Quadratic form schemes*, Math. Z. 167 (1979), 201—212.

[8] L. SZCZEPANIK, *Quadratic form schemes with non-trivial radical*, Fund. Math.

[9] L. SZCZEPANIK, *Fields and quadratic form schemes with the index of radical not exceeding 16*, Annales Mathematicae Silesianae 1 (1985), 23—46.

[10] K. SZYMICZEK, *Quadratic forms over fields*, Dissertationes Math. 152.

[11] K. SZYMICZEK, *Generalized Hilbert fields*, J. Reine Angew. Math. 329 (1981), 58—65.