PARIS 7 LOGIQUE
CNRS

N° 60

On forms whose total signature is zero mod 2^n. Solution to a problem of M. Marshall

M. Dickmann and F. Miraglia

Février 1997

ÉQUIPE DE LOGIQUE MATHÉMATIQUE

Prépublications

Équipe de Logique. Université Paris VII. Tour 45-55. 5ème étage.
2, Place Jussieu. 75251 PARIS Cedex 05. FRANCE
Tél. (33-1) 43 29 77 26

N° 60

On forms whose total signature is zero mod 2^n. Solution to a problem of M. Marshall

M. Dickmann and F. Miraglia

Février 1997

On forms whose total signature is zero mod 2^n. Solution to a problem of M. Marshall.

M. A. Dickmann * and F. Miraglia †

February, 1997

We give here an affirmative answer to the following problem, posed by M. Marshall in 1974 :

Let F be a formally real, Pythagorean field. Is it true that for every quadratic form φ over F and any integer $n \geq 1$, the following holds :

[MC] *If $sgn_P(\varphi) \equiv 0 \pmod{2^n}$ for every order P of F, then $\varphi \in I^n(F)$.*

Here $sgn_P(\varphi)$ denotes the signature of φ under the order P and $I^n(F)$ is the n^{th} power of the ideal $I(F)$ of the Witt ring $W(F)$ of F, consisting of all even dimensional forms.

As far as we know, the above question first appeared in print in Marshall's 1977 paper ([Ma]; Open question 2; p. 575) where it is posed for the more general context of abstract spaces of orders, as well as in Lam's lectures [L2] in the same volume, where it occurs as Open Problem B, p. 49, for the field case. The aforementioned date (1974) was communicated to us by M. Marshall.

Our proof is divided in two parts, whose main points are outlined below.

Part I : In the framework of special groups and the related Boolean-theoretic techniques introduced in [DM1], it is shown that [MC] is equivalent to

[WMC] If $2\varphi \in I^{n+1}(F)$, then $\varphi \in I^n(F)$, for every integer $n \geq 1$.

As a matter of fact, both [MC] and [WMC] make sense in the context of formally real special groups. Here [MC] takes the following form : for every integer $n \geq 1$ and every quadratic form φ over such a group G

[MC] If $sgn_\sigma(\varphi) \equiv 0 \pmod{2^n}$ for every $\sigma \in X_G$, then $\varphi \in I^n(G)$,

where X_G denotes the space of orders of G – i.e., the set of special group homomorphisms from G to the 2-element special group $\mathbf{Z}_2$, suitably topologized – and $W(G)$, $I(G)$ have definitions similar to the field case.

We prove the equivalence of [MC] and [WMC] for formally real special groups G with the property that $2^n\langle 1 \rangle \notin I^{n+1}(G)$, for every integer $n \geq 1$; we call these groups $\mathcal{AP}$ (for Arason-Pfister). By the Arason-Pfister Hauptsatz, reduced special groups and the special groups of formally real fields are $\mathcal{AP}$ groups (Lemma 1.7). Since reduced special groups and abstract order spaces are (dually) equivalent notions ([Li]; [DM1], § 3), this part of the proof also works for Marshall's original formulation of the problem.

*Équipe de Logique Mathématique, University of Paris VII, Paris, France
†Dept. of Mathematics, University of São Paulo, São Paulo, Brazil

The reduction of $[MC]$ to $[WMC]$ proceeds through the following steps :

(a) First we show that, whenever G is $\mathcal{AP}$, the inductive limit $W(G)$ of the groups $\overline{I^n}(G) = I^n(G)/I^{n+1}(G)$ (under the operation induced by the sum of forms in $I^n(G)$), with transition functions induced by multiplication (i.e., tensor product) by $2 = \langle 1, 1 \rangle$, is a non-trivial Boolean ring. This is also the case, when F is a formally real field, for the inductive limit $k(F)$ of Milnor's mod 2 K-theoretic groups k_nF, with transition functions induced by multiplication by $l(-1)$ (Theorem 2.9.(a)). As Boolean algebras, these inductive limits possess a natural structure of reduced special groups, cf. § 4 in [DM1].

(b) Furthermore, the natural group homomorphisms $\rho : G \longrightarrow W(G)$ and $\kappa : G(F) \longrightarrow k(F)$, are, in addition, morphisms of special groups, which are injective iff G is reduced and F is Pythagorean, respectively (Theorem 2.9.(b), (c)). Owing to the universal property of the Boolean hull B_G of G (Theorem 5.7 in [DM1]), these maps extend to Boolean algebra morphisms $B(\rho) : B_G \longrightarrow W(G)$ and $B(\kappa) : B(F) \longrightarrow k(F)$, respectively (Corollary 2.13).

(c) The next step is the proof that these Boolean homomorphisms are **isomorphisms**. Indeed, they have inverses $M : W(G) \longrightarrow B_G$ and $\varepsilon : k(F) \longrightarrow B(F)$, respectively.

The homomorphism M is defined on the image of $\overline{I^n}$ in $W(G)$ (by the homomorphism α_n given by the inductive limit construction) to be the clopen in X_G

$$\{\sigma \in X_G : sgn_\sigma(\varphi) \not\equiv 0 \ (\text{mod } 2^{n+1})\} \qquad\qquad (\varphi \in I^n(G)).$$

M is a Boolean analogue of a map considered by Milnor (§ 3 in [Mi]), induced by the Stiefel-Whitney invariant of order 2^{n-1} on forms in I^n. The map ε, defined on the image of k_nF in $k(F)$ sends (the image of) a generator $l(a_1)l(a_2)\ldots l(a_n)$ to the element $a_1 \wedge a_2 \wedge \ldots \wedge a_n$ in $B(F)$.

(d) It follows from the definition of the map M that $[MC]$ holds for a given integer $n \geq 1$ if and only if the map $M \circ \alpha_n : \overline{I^n} \longrightarrow B_G$ is injective. And this is the case, if and only if, $[WMC]$ holds at level n (equivalently, the transition homomorphism $\overline{I^n}(G) \xrightarrow{2\,\cdot} \overline{I^{n+1}}(G)$ induced by multiplication by 2 is injective). A similar statement holds for the map ε.

Part II : In the second step of the proof we deal with (formally real) Pythagorean fields properly. We establish the injectivity of the map $\overline{I^n}(G) \xrightarrow{2\,\cdot} \overline{I^{n+1}}(G)$ as follows :

(a) If F is such a field and $n \geq 1$ is an integer, write $H^n(F)$ for the n^{th} cohomology group of F, with coefficients in $\mathbf{Z}/2\mathbf{Z}$. In Proposition 5.4 we show that the map $(-1) \cup : H^n(F) \longrightarrow H^{n+1}(F)$ is injective. This comes from, among other things, the long exact sequence in cohomology associated to quadratic extensions of F, due to Arason, together with Voevodsky's recent and celebrated result ([V]) that the Milnor homomorphisms $h_n^F : k_nF \longrightarrow H^n(F)$ are isomorphisms for all $n \geq 1$.

(b) The commutativity of the diagram

$$\begin{array}{ccc} k_nF & \xrightarrow{\ l(-1)\cdot\ } & k_{n+1}F \\ \Big\downarrow h_n^F & & \Big\downarrow h_{n+1}^F \\ H^n(F) & \xrightarrow[\ (-1)\cup\ ]{} & H^{n+1}(F) \end{array}$$

where the map in upper row is induced by multiplication by $l(-1)$, yields at once that this homomorphism is injective for all $n \geq 1$ and every formally real, Pythagorean field F (Corollary 5.5). It follows that every such field verifies Milnor's conjecture for the graded Witt ring, i.e., the homomorphism $s_n : k_n F \longrightarrow \overline{I^n}(F)$ is an isomorphism for all $n \geq 1$.

(c) Finally, the commutativity of the diagram

$$\begin{array}{ccc} k_n F & \xrightarrow{\;l(-1)\cdot\;} & k_{n+1} F \\ \downarrow s_n & & \downarrow s_{n+1} \\ \overline{I^n} & \xrightarrow[\;2\cdot\;]{} & \overline{I^{n+1}} \end{array}$$

proves $[WMC]$ and hence, $[MC]$ for all formally real Pythagorean fields.

Acknowledgements : The research leading to the present results was carried out from April 1996 to January 1997 at Louisiana (USA), São Paulo (Brazil), Santander (Spain) and Paris (France). It would not have been possible without the support of the exchange program between the Universities of São Paulo and Paris VII.

The authors wish to thank E. Becker and M. Marshall for helpful, sometimes illuminating, discussions on quadratic form theory – particularly about points in [DM1]. They also express their gratitude to B. Kahn for his generous help with matters cohomological.

1 Introduction

We shall here set down the basic tools needed for the constructions that follow. We work in the context of **special groups (SG)**, following all notational conventions set down in [DM1].

In all that follows a Pythagorean field will always be considered to be formally real.

The Witt ring of a special group appears in [D], but we recall the main points for the convenience of the reader.

Let $\langle G, \equiv_G, -1 \rangle$ be a special group, where $\equiv_G$ denotes isometry in G. Whenever clear from context, we drop the reference to G in the notation of isometry. Although G is a group of exponent 2 ($\forall\, x \in G$, $x^2 = 1$), being therefore commutative, the group operation in G is written multiplicatively. Thus, we write 1 for the neutral element of G. For $a \in G$, $-a$ stands for $-1 \cdot a$.

For an integer $n \geq 1$, a n-form φ over G is a n-tuple $\varphi = \langle a_1, \ldots, a_n \rangle$ of elements of G; n is the dimension of φ, $dim\, \varphi$.

A special group G is **reduced** if $1 \neq -1$ and

[red] For all $a \in G$, $\langle a, a \rangle \equiv_G \langle 1, 1 \rangle$ implies $a = 1$.

A morphism of special groups $\langle G, \equiv_G, -1 \rangle \xrightarrow{f} \langle H, \equiv_H, -1 \rangle$ is a group homomorphism, such that $f(-1) = -1$ and for all a, b, c, $d \in G$

$$\langle a, b \rangle \equiv_G \langle c, d \rangle \quad \text{implies} \quad \langle f(a), f(b) \rangle \equiv_H \langle f(c), f(d) \rangle.$$

If $\varphi = \langle a_1, \ldots, a_n \rangle$ is a n-form over G, write $f \star \varphi$ for the form $\langle f(a_1), \ldots, f(a_n) \rangle$ over H, called **the image form** of φ by f.

For forms φ, ψ over G, φ is **Witt-equivalent** to ψ, written $\varphi \approx_G \psi$, if there are integers n, $m \geq 0$ such that

$$\varphi \oplus n\langle 1, -1 \rangle \equiv_G \psi \oplus m \langle 1 - 1 \rangle.$$

By Witt cancellation (Proposition 1.6.(b) in [DM1]), this relation can always be written as

$$\varphi \oplus k\langle 1, -1 \rangle \equiv \psi \quad \text{or} \quad \varphi \equiv \psi \oplus k\langle 1, -1 \rangle,$$

where $k = |dim\, \varphi \; - \; dim\, \psi|$. It is easily verified that $\approx_G$ is an equivalence relation on the set of forms over G. For forms φ, ψ, write $\varphi - \psi$ for $\varphi \oplus -\psi$.

Let $\mathcal{W}(G)$ be the set of equivalence classes of forms over G under equivalence relation determined by Witt-equivalence. Write $\overline{\varphi}$ for the class of the form φ in $\mathcal{W}(G)$. We have

Lemma 1.1 *: Let G be a special group and φ a form over G.*

a) $\varphi \otimes \langle 1, -1 \rangle \equiv dim\, \varphi \cdot \langle 1, -1 \rangle = \sum_{i=1}^{dim\, \varphi} \langle 1, -1 \rangle$.

b) Witt-equivalence is a congruence with respect to sum and product of forms.

c) With the operations $\overline{\varphi} + \overline{\psi} = \overline{\varphi \oplus \psi}$ *and* $\overline{\varphi}\, \overline{\psi} = \overline{\varphi \otimes \psi}$, *$\mathcal{W}(G)$ is a commutative ring with identity $\overline{\langle 1 \rangle}$, and whose zero is the class of the hyperbolic forms.*

d) The set $I(G)$ of (classes of) even dimensional forms is a maximal ideal in $\mathcal{W}(G)$ (the fundamental ideal of $\mathcal{W}(G)$). Moreover, $\mathcal{W}(G)/I(G)$ is the two element field. $\diamond$

To keep notation straight, we shall denote

- By $\mathbb{F}_2 = \{0, 1\}$, the two element field.
- By $\mathbb{Z}_2 = \{1, -1\}$, the 2-element special group, whose isometry relation is defined by the condition

$$\langle a, b \rangle \equiv_{\mathbb{Z}_2} \langle c, d \rangle \;\; \text{iff} \;\; a + b = c + d \text{ (sum in } \mathbb{Z}),$$

for a, b, c, $d \in \{1, -1\}$. $\mathbb{Z}_2$ is a reduced special group.

Let $n \geq 0$ be an integer. A **Pfister form** over G is a form of the type $\bigotimes_{i=1}^{n} \langle 1, a_i \rangle$, where $a_i \in G$. The integer n is called the **degree** of $\mathcal{P}$. Write 2^k for the Pfister form $\bigotimes_{i=1}^{k} \langle 1, 1 \rangle$. Note that $2^0 = \langle 1 \rangle$.

Observe that every element of the fundamental ideal I is a linear combination of Pfister forms of degree 1. For an integer $n \geq 0$, set $I^0 = \mathcal{W}(G)$ and let I^n be the n^{th} power of I, $n \geq 1$. Note that I^n is generated, as an abelian group, by multiples of Pfister forms of degree n, that is, every element of I^n is a linear combination of Pfister forms of degree n. Clearly, I^{n+1} is an ideal in I^n.

The **Weak Marshall Conjecture** is the following statement :

[WMC] For all forms φ and all integers $n \geq 1$, $2\varphi \in I^{n+1}$ implies $\varphi \in I^n$.

For a special group G, $Sat(G)$ is the saturated subgroup consisting of the elements represented by 2^n, for some $n \geq 1$ (see section 2 in [DM1]). If G is reduced, then $Sat(G) = \{1\}$. The quotient $G/Sat(G)$ is a special group and the canonical projection, $\pi : G \longrightarrow G/Sat(G)$, is a morphism of special groups (Propositions 2.22 and 2.19, [DM1]).

A special group G is **formally real** if $-1 \notin Sat(G)$. In this case, $1 \neq -1$ in $G/Sat(G)$ and this quotient is a **reduced** special group, indicated by G_{red}. It follows from the preceding observations that every reduced special group is formally real.

Remark 1.2 : We here recall some results which appear in Example 1.7 in [DM1] in a more general setting. Let F be a field of characteristic $\neq 2$. As usual, for a subset $S \subseteq F$

$\dot{S} = \{x \in S : x \neq 0\}$, $\dot{S}^2 = \{x^2 : x \in \dot{S}\}$ and $\Sigma\dot{S}^2$ is the set of sums of squares of elements in $\dot{S}$.

Recall that if T is a pre-order on F and $a, b \in \dot{F}$, then

$$D_T(a, b) = \{x \in \dot{F} : \exists\, s, t \in T \text{ such that } x = as + bt\},$$

is the set of elements represented by $\langle a, b \rangle$ over T.

Set $G(F) = \dot{F}/\dot{F}^2$, $G_{red}(F) = \dot{F}/\Sigma\dot{F}^2$ and let $\bar{\cdot} : \dot{F} \longrightarrow G(F)$ and $\pi : G(F) \longrightarrow G_{red}(F)$ be the canonical projections. However, for $1, -1 \in \dot{F}$, we shall indicate their class in $G(F)$ and $G_{red}(F)$ by 1 and -1, respectively.

The following facts follow from the results in Example 1.7 in [DM1] :

Fact A : *a) $G(F)$ and $G_{red}(F)$ are special groups, such that for all $a, b, c, d \in \dot{F}$, the following conditions are equivalent, where $T = \Sigma\dot{F}^2$ (resp., $\dot{F}^2$) :*

1. $\langle \pi(\overline{a}), \pi(\overline{b}) \rangle \equiv_{G_{red}(F)} \langle \pi(\overline{c}), \pi(\overline{d}) \rangle$ *(resp.,* $\langle \overline{a}, \overline{b} \rangle \equiv_{G(F)} \langle \overline{c}, \overline{d} \rangle$*).*
2. $\pi(\overline{ab}) = \pi(\overline{cd})$ *and* $D_T(a, b) = D_T(c, d)$ *(resp.,* $\overline{ab} = \overline{cd}$ *and* $D_T(a, b) = D_T(c, d)$*).*
3. $\pi(\overline{ab}) = \pi(\overline{cd})$ *and* $D_T(a, b) \cap D_T(c, d) \neq \emptyset$ *(resp.,* $\overline{ab} = \overline{cd}$ *and* $D_T(a, b) \cap D_T(c, d) \neq \emptyset$*).*

Thus, $\pi(\overline{a}) \in D_{G_{red}(F)}(1, \pi(\overline{b}))$ *iff* $a \in D_T(1, b)$ *(resp.,* $\overline{a} \in D_{G(F)}(1, \overline{b})$ *iff* $a \in D_T(1, b)$*).*

b) $Sat(G(F)) = \Sigma\dot{F}^2/\dot{F}^2$.

c) $G(F)$ is reduced iff F is Pythagorean. F is formally real iff $G_{red}(F)$ is reduced iff $G(F)$ is formally real. ◇

This example is at the origin of the notion of formally real special group.

Definition and Remarks 1.3 : (SG-characters; signature; Boolean hull)

a) An **SG-character** *of a special group G is a morphism of special groups from G to $\mathbb{Z}_2$.*

An SG-character σ has the following property :

[ker] For all $a \in G$, $a \in \ker\sigma$ implies $D_G(1, a) \subseteq \ker\sigma$.

Write X_G for the space of characters of G. With the topology induced by the product topology on $2^{|G|}$, it is a Boolean space, that is, Hausdorff and compact, with a basis of clopens constituted by finite intersections of sets of the type

$$[a = \delta] =_{def} \{\sigma \in X_G : \sigma(a) = \delta\},$$

where $a \in G$ and $\delta \in \{1, -1\} = 2$.

Fact A : *Any formally real special group has a SG-character.*

To see this, we first register that, by Corollary 2.7 and Theorem 2.10 in [DM1], any reduced special group has a SG-character τ. Now, $\sigma = \tau \circ \pi$ is a SG-character of G, where π is the canonical projection $G \xrightarrow{\pi} G_{red}$.

b) If $\varphi = \langle a_1, \ldots, a_n \rangle$ is a n-form over G and $\sigma \in X_G$, the **signature** *of φ at σ is the integer $\sigma(\varphi) = \sum_{i=1}^{n} \sigma(a_i)$ ($\in \mathbf{Z}$).*

Signature commutes with sum and product of forms, that is,

For all forms φ, ψ over G and all $\sigma \in X_G$,

$$\sigma(\varphi \oplus \psi) = \sigma(\varphi) + \sigma(\psi) \quad \text{and} \quad \sigma(\varphi \otimes \psi) = \sigma(\varphi)\sigma(\psi). \tag{*}$$

Fact B : *If $\mathcal{P}$ is a Pfister form of degree $n \geq 1$, then $\sigma(\mathcal{P})$ is either 0 or 2^n. If $\mathcal{Q}$ is a linear combination of Pfister forms of degree $n \geq 1$, then $\sigma(\mathcal{Q})$ is a multiple of 2^n.*

c) The **Boolean hull** of G is the Boolean algebra of clopens in X_G, written B_G. Note that in B_G, $\bot = \emptyset$ and $\top = X_G$. When dealing directly with clopens in X_G, we use standard set-theoretic notation for the operations in B_G. When dealing with generic elements of B_G, we shall use $\wedge$, $\vee$ to indicate meet and join, while $\triangle$ will always stand for symmetric difference. The complement of $b \in B_G$ will be denoted by $-b$ ($= \top \triangle b$).

There is a complete embedding (Corollary 6.4 in [DM1]) $\varepsilon_G : G \longrightarrow B_G$ defined by

$$\varepsilon_G(a) = [a = -1],$$

by which we may **identify** G with its image in B_G. Moreover, for all a, $b \in G$:

I. ε_G is injective and $\varepsilon_G(ab) = \varepsilon_G(a) \triangle \varepsilon_G(b)$.

II. $\varepsilon_G(1) = \bot$ and $\varepsilon_G(-1) = \top$;

III. $a \in D_G(1, b)$ iff $\varepsilon_G(a) \leq \varepsilon_G(b)$ ($\leq$ is the order in B_G).

(I) and (II) imply that for $a \in G$ $\varepsilon_G(-a) = -\varepsilon_G(a)$ (complement in B_G). $\diamond$

Lemma 1.4 : *For a formally real special group G, the following conditions are equivalent :*

1. *G verifies $[WMC]$.*
2. *For all forms φ and all integers k, $n \geq 1$,*

$$2^k\varphi \in I^{n+k} \quad \textit{implies} \quad \varphi \in I^n.$$

3. *For all forms φ over G and all integers $n \geq 1$,*

$$\varphi \in I^{n-1} \textit{ and } 2\varphi \in I^{n+1} \quad \textit{implies} \quad \varphi \in I^n.$$

Proof : It is clear that 1. $\Leftrightarrow$ 2. $\Rightarrow$ 3. It remains to verify that 3. $\Rightarrow$ 1. Suppose that φ is a form over G such that $2\varphi \in I^{n+1}$, for some $n \geq 1$. Our first observation is

Fact 1 : *If, for some $n \geq 1$, $2\varphi \in I^{n+1}$, then $dim\,\varphi$ is even, that is, $\varphi \in I$.*

Proof : For integers p, $q \geq 0$, we have

$$2\varphi \oplus p\langle 1, -1 \rangle \equiv_G \mathcal{Q} \oplus q\langle 1, -1 \rangle, \tag{I}$$

where $\mathcal{Q}$ is a linear combination of Pfister forms of degree $n+1$ over G. Thus, applying any SG-character σ (see Fact 1.3.A) on both sides of (I) and recalling Fact 1.3.B, yields

$$2\sigma(\varphi) = \sigma(\mathcal{Q}) = \alpha\, 2^{n+1},$$

for some integer $\alpha \in \mathbf{Z}$. Thus, $\sigma(\varphi) = \alpha\, 2^n$ is even, since $n \geq 1$. Write $\varphi = \langle a_1, \ldots, a_m \rangle$ and set $\beta =$ the cardinal of $\{j \leq m : \sigma(a_j) = -1\}$. Then,

$$\sigma(\varphi) = \sum_{i=1}^{m} \sigma(a_i) = - \ \beta + (m - \beta) = m - 2\beta,$$

which clearly forces $m = dim\,\varphi$ to be even.

To end the proof that 3. $\Rightarrow$ 1., we shall verify by induction on $1 \leq k \leq n$, that $\varphi \in I^k$. Fact 1 takes care of the case $k = 1$. Suppose our contention is true for $k < n$. Then, $k + 2 \leq n + 1$ and so $\varphi \in I^k$, with $2\varphi \in I^{k+2}$. By 3., we conclude that $\varphi \in I^{k+1}$, completing the induction step. $\diamond$

Lemma 1.5 : *Let G be a formally real special group and $G \xrightarrow{\pi} G_{red}$ be the canonical special group quotient map. Let φ be a form over G and $\pi \star \varphi$ the image form in G_{red}. Then,*

a) If $\sigma \in X_G$, then $Sat(G) \subseteq ker\ \sigma$. Thus, σ factors through π to give a character $\overline{\sigma}$ in G_{red}. Moreover, $\sigma(\varphi) = \overline{\sigma}(\pi \star \varphi)$.

b) The map $\tau \mapsto \tau \circ \pi$ is a homeomorphism from $X_{G_{red}}$ onto X_G.

c) If G verifies [WMC], then G_{red} verifies [WMC].

Proof : a) The property [ker] of Definition 1.3(a) says that ker σ is a **saturated** subgroup of G (Def. 2.3 in [DM1]). Lemma 2.4(b) of [DM1] shows, by induction on degree, that :

If $\mathcal{P}$ is a Pfister form with coefficients in ker σ, then $D_G(\varphi) \subseteq$ ker σ.

It follows that $Sat(G) \subseteq$ ker σ. Hence, the functional equation $\overline{\sigma} \circ \pi = \sigma$ defines a map $\overline{\sigma} : G_{red} \longrightarrow \{\pm 1\}$. Routine checking shows that $\overline{\sigma}$ is a SG-morphism in $\mathbf{Z}_2$, i.e., $\overline{\sigma} \in X_{G_{red}}$. Using the preceding equation componentwise gives $\sigma(\varphi) = [\overline{\sigma} \circ \pi](\varphi) = \overline{\sigma}(\pi \star \varphi)$.

b) Since π is a morphism of special groups, $\tau \circ \pi$ is a SG-character of G, for all $\tau \in X_{G_{red}}$. Moreover, because π is surjective, $\tau \mapsto \tau \circ \pi$ is injective. That it is also surjective follows directly from (a). Since we are dealing with compact Hausdorff spaces, $\tau \mapsto \tau \circ \pi$ will be a homeomorphism if it is continuous. To verify continuity, just note that, for $a \in G$ and $\sigma \in X_G$, the inverse image of the clopen $[a = 1]$ in X_G is the clopen $[\pi(a) = 1]$ in $X_{G_{red}}$.

c) Since π is a SG-morphism, $\varphi \in I^n(G)$ implies $\pi \star \varphi \in I^n(G_{red})$. Since it is surjective, every form ψ over G_{red} <u>lifts</u> to G, i.e., there is a form φ over G such that $\pi \star \varphi = \psi$.

Assume that $2\psi \in I^{n+1}(G_{red})$, ψ a form over G_{red}. Thus, there are integers p, q, ≥ 0 and a linear combination, $\mathcal{Q}$, of Pfister forms of degree $n + 1$ over G_{red}, such that

$$2\psi \oplus p\langle 1, -1 \rangle \equiv_{G_{red}} \mathcal{Q} \oplus q\langle 1, -1 \rangle. \tag{I}$$

Thus, we may consider a lifting φ of ψ to G and a linear combination $\mathcal{T}$ of Pfister forms of degree $n + 1$ over G, that is a lifting of $\mathcal{Q}$. By Proposition 2.19 in [DM1], (I) implies that there is $k \geq 0$ such that

$$2^k(2\varphi \oplus p\langle 1, -1 \rangle) \equiv_G 2^k(\mathcal{T} \oplus q\langle 1, -1 \rangle),$$

and so $2^{k+1}\varphi \in I^{k+n+1}(G)$. Since G verifies [WMC], we conclude that $\varphi \in I^n(G)$, which in turn implies $\pi \star \varphi = \psi \in I^n(G_{red})$, as desired. $\diamond$

A formally real special group G satisfies **Marshall's conjecture** if for all integers $n \geq 1$ and all forms $\varphi = \langle a_1, \ldots, a_n \rangle$ over G

[MC] If for all SG-characters σ of G, $\sigma(\varphi) \equiv 0 \bmod 2^n$, then $\varphi \in I^n$.

Definition 1.6 : *A special group G is said to be $\mathcal{AP}$ if it is formally real and for all integers $k \geq 1$, $2^k \notin I^{k+1}$.*

Lemma 1.7 : *If G is reduced, or is formally real and verifies $[WMC]$, or is the special group of a formally real field, then G is $\mathcal{AP}$.*

Proof : If $2^k \in I^{k+1}$ and G is the special group of a formally real field or a reduced special group, we apply the classical version of the Arason-Pfister Haupsatz (see Theorem 3.1 in [L1]), or its reduced special group version (Theorem 7.30 in [DM1]), respectively, to conclude that 2^k is hyperbolic. But then -1 is represented by 2^k, a contradiction.

If G is formally real and satisfies $[WMC]$, $2^k \in I^{k+1}$ implies $\langle 1 \rangle \in I$, a contradiction. $\diamond$

2 The inductive limit of graded rings of exponent 2

Recall that a **graded ring** is a sequence of abelian groups

$$\mathcal{H} = (H_1, H_2, \ldots, H_n, \ldots),$$

with an associative operation

$$H_n \times H_m \longrightarrow H_{n+m}, \quad (x, y) \mapsto x * y, \qquad n, m \geq 1$$

such that for all $x, x' \in H_n$ and $y \in H_m$,

$$(x + x') * y = (x * y) + (x' * y) \quad \text{and} \quad y * (x + x') = (y * x) + (y * x').$$

$\mathcal{H}$ is **commutative** if $*$ is commutative. The group H_n is called the group of degree n of $\mathcal{H}$.

Definition 2.1 : *A sequence $\mathcal{H} = (H_1 \xrightarrow{h_1} H_2 \xrightarrow{h_2} \ldots H_n \xrightarrow{h_n} H_{n+1} \ldots)$ is an* **inductive graded ring of exponent two (IGR)** *if it satisfies, for all $n, m \geq 1$*

1. *H_n is a group of exponent 2, with a distinguished element $\top_n$.*
2. *h_n is a group homomorphism, such that $h_n(\top_n) = \top_{n+1}$.*
3. *$\mathcal{H}$ is a commutative graded ring.*
4. *For $1 \leq s \leq t$, define*

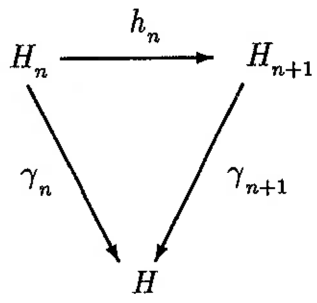
$$h_s^t = \begin{cases} Id_{H_s} & \text{if } s = t \\ h_{t-1} \circ \ldots \circ h_{s+1} \circ h_s & \text{if } s < t. \end{cases}$$

Then, if $p \geq n$ and $q \geq m$, for all $x \in H_n$ and $y \in H_m$, $h_n^p(x) * h_m^q(y) = h_{n+m}^{p+q}(x * y)$.

If $\mathcal{H}$ is an IGR, let $\underrightarrow{lim}\, \mathcal{H} = \langle H; \{\gamma_n : n \geq 1\} \rangle$ be its inductive limit. For ease of reference, we register the (well-known) basic properties of this construction in

Remark 2.2 : For each $n \geq 1$, we have a group homomorphism $\gamma_n : H_n \longrightarrow H$, satisfying :

1. For all $n \geq 1$, the following diagram is commutative :



It follows readily that for all $1 \leq n \leq m$, $\gamma_n = \gamma_m \circ h_n^m$.

2. $H = \bigcup_{n \geq 1} \gamma_n(H_n)$.

   If $w = \gamma_n(x)$, we say that $x \in H_n$ is a **representative** of $w \in H$.

3. For all $n, m \geq 1$ and all $x \in H_n$, $y \in H_m$, the following conditions are equivalent :

   (i) $\gamma_n(x) = \gamma_m(y)$; (ii) There is $k \geq n, m$ such that $h_n^k(x) = h_m^k(y)$.

   Note that the h_n's are injective iff the γ_n's are injective.

   Write $\perp$ for the zero of H. It has $0 \in H_n$ as representatives. $\diamond$

By Remark 2.2, addition in H can be described by representatives as follows :

For w, $z \in H$, let $x \in H_n$ and $y \in H_m$ be representatives of w and z, respectively, and let k be an integer greater than n and m. Then,

[sum] $$w + z = \gamma_k(h_n^k(x) + h_m^k(y)) = \gamma_k(h_n^k(x)) + \gamma_k(h_m^k(y)).$$

In particular, k may taken to be $\max\{n, m\}$. As an inductive limit of groups of exponent 2, H is an group of exponent 2.

Remarks 2.3 : a) Recall that a Boolean ring (cf. § 1.6 in [HBA]) is a commutative ring, R, with identity, such that for all $x \in R$, $x + x = 0$ and $x \cdot x = x$. R is **non-trivial** if $0 \neq 1$.

There is a well-known bijective correspondence between non-trivial Boolean rings and Boolean algebras, where meet ($\wedge$) and join ($\vee$) and complement are defined, in terms of the ring operations in R, by

$$a \wedge b = a \cdot b, \quad a \vee b = a + b + (a \cdot b) \quad \text{and} \quad -a = 1 + a. \qquad (a, b \in R)$$

Order is defined by

$$a \leq b \text{ iff } a \cdot b = a \quad (\text{or iff } a \vee b = b),$$

in which 0 is the least element of R (bottom, $\perp$) and 1 is its largest element (top, $\top$). For all a, b in R, we have

$$a + b = (a \wedge -b) \vee (-a \wedge b), \tag{I}$$

the usual notion of "symmetric difference". Conversely, a Boolean algebra $B = \langle B, \vee, \wedge, \perp, \top \rangle$ gives rise to a Boolean ring by defining product as meet and sum as "symmetric difference", that is, by the formula (I). Since in a Boolean algebra $\perp \neq \top$, B is a non-trivial Boolean ring.

When dealing with Boolean algebras, we shall use Δ for the operation of symmetric difference.

If A, B are Boolean algebras and $A \xrightarrow{f} B$ is a map, then f is a Boolean algebra homomorphism iff it is a Boolean ring homomorphism.

b) It is shown in section 4 of [DM1], that any non-trivial Boolean ring (or algebra) R carries a natural structure of **reduced** special group, namely (cf. Def. 4.1 in [DM1])

– Its domain is the additive group of R, with $1 = \bot$ and $-1 = \top$;

– For $u, v, w, z \in R$, $\quad \langle u, v \rangle \equiv_R \langle w, z \rangle$ iff $u + v = w + z$ and $u \cdot v = w \cdot z$. **[iso]**

Alternatively, the representation relation $a \in D_R(1, b)$ is given by the order of $R : a \leq b$.

Item (a) and Corollary 4.4 in [DM1] imply that R is a reduced special group. $\diamond$

We now prove

Theorem 2.4 : *Suppose that $\mathcal{H}$ is an IGR such that*

[*br* 0] : *For all $n \geq 1$, $\top_n \notin \ker h_n$.*

[*br* 1] : *For all $n \geq 1$ and all $x \in H_n$, there is $k \geq n+1$ such that $h^k_{n+1}(\top_1 * x) = h^k_n(x)$.*

[*br* 2] : *For all $n \geq 1$ and all $x \in H_n$, there is $k \geq 2n$ such that $h^k_n(x) = h^k_{2n}(x * x)$.*

Then, $H = \varinjlim \mathcal{H}$ is a non-trivial Boolean ring, that is, $\bot \neq \top =_{def} \gamma_1(\top_1)$ (its multiplicative identity) and for all $w \in H$, $w + w = \bot$ and $w \cdot w = w$.

Proof : We start by verifying that H is a ring with identity $\top = \gamma_1(\top_1)$.

The graded ring structure in $\mathcal{H}$ induces a product in H, as follows :

For w, $z \in H$, let $x \in H_n$, $y \in H_m$ be representatives of w, z, respectively. Now set

[prd] $$w \cdot z = \gamma_{n+m}(x * y).$$

To show that this is well defined, let $x' \in H_p$ and $y' \in H_q$ be representatives of w, z, respectively. By Remark 2.2.(3), there must be $k \geq n, m, p, q$ such that

$$h^k_n(x) = h^k_p(x') \quad \text{and} \quad h^k_m(y) = h^k_q(y').$$

By condition 4 in Definition 2.1, we have

$$h^{2k}_{n+m}(x * y) = h^k_n(x) * h^k_m(y) = h^k_p(x') * h^k_q(y') = h^{2k}_{p+q}(x' * y'),$$

and so Remark 2.2.(3) yields $\gamma_{n+m}(x * y) = \gamma_{p+q}(x' * y')$, proving that formula [prd] is independent of representatives. Since $\mathcal{H}$ is commutative, the same will be true of the product in H.

A similar reasoning will show that H is a ring, that is, its product is associative and distributes over sum, with $\bot$ being its zero. [*br* 1] and Remark 2.2.(3) show that $\top = \gamma_1(\top_1)$ is the multiplicative identity in H, while [*br* 0] guarantees $\bot \neq \top$. Note that by condition 2 in Definition 2.1, the $\top_n$'s are representatives of $\top$.

Since the additive group of H is of exponent two, we have $w + w = \bot$, for all $w \in H$. That the product in H is idempotent follows from Remark 2.2.(3) and [*br* 2]. $\diamond$

We register the following consequence of the proof of Theorem 2.4

Corollary 2.5 : *For integers $n, m \geq 1$ and $x \in H_n$, $y \in H_m$, in $H = \varinjlim \mathcal{H}$ we have,*

$$\gamma_n(x) \cdot \gamma_m(y) = \gamma_{n+m}(x * y). \qquad \diamond$$

We shall apply Theorem 2.4 to two situations, namely the mod 2 K-theory of a field of characteristic $\neq 2$, and the graded Witt ring of a special group.

The contents of Remark 1.2 will be used without further notice. We shall assume that the reader is familiar with the contents of [Mi]. If F is a field of characteristic $\neq 2$, let

$$k_*F = (k_1F, k_2F, \ldots, k_nF, \ldots),$$

be the graded algebra over $\mathbb{F}_2$ corresponding to the mod 2 K-theory of F as in section 3 of [Mi]. It follows directly from the definition of the k_nF that they are additive groups of exponent 2.

A generator of k_nF will be written $l(a_1)l(a_2)\ldots l(a_n)$, with $a_j \in \dot{F}$. Recall that k_1F is $G(F)$ written additively, that is $l : G(F) \longrightarrow k_1F$ is an isomorphism such that $l(ab) = l(a) + l(b)$.

Lemma 2.6 : *With notation as above,*

a) $\forall\, a \in \dot{F},\ \ l(a)l(-a) = 0$ *and* $l(a)^2 = l(a)l(-1)$.

b) If $a_1, \ldots, a_n,\ x \in \dot{F}$, *then in* k_nF, $\ l(a_1)\ldots l(x^2a_i)\ldots l(a_n) = l(a_1)\ldots l(a_n)$.

c) If $a_1, \ldots, a_n \in \dot{F}$ *and* σ *be a permutation of* $\{1, \ldots, n\}$, *then in* k_nF,

$$l(a_1)\ldots l(a_n) = l(a_{\sigma(1)})\ldots l(a_{\sigma(n)}).$$

d) If $a_1, \ldots, a_n \in \dot{F}$ *and* $\sum_{i=1}^{n} a_i = 0$ *or* 1, *then* $\ l(a_1)\ldots l(a_n) = 0$ *in* k_nF.

Proof : Item (a) comes from Lemmas 1.1 and 1.2 in [Mi], while (b) and (c) appear in Lemma 1.6 in [EL 1]; (d) is Lemma 1.3 in [Mi]. $\diamond$

Note that Lemma 2.6.(b) assures that $l(a)$ depends only on the square class of a in F. Thus, we may write $l(c)$, for $c \in G(F)$, or $l(\overline{a})$, for $a \in \dot{F}$.

It follows from Lemma 2.6.(c) that k_*F is a commutative graded ring. For each $n \geq 1$, there is a group homomorphism

$$\omega_n : k_nF \longrightarrow k_{n+1}F,$$

defined on generators as multiplication by $l(-1)$. For each $n \geq 1$, we set $\top_n = l(-1)^n$ as the distinguished element of k_nF. Thus, it is clear that the system

$$\mathcal{K}(F) = (k_1F \xrightarrow{\omega_1} k_2F \xrightarrow{\omega_2} \ldots k_nF \xrightarrow{\omega_n} k_{n+1}F \ldots),$$

satisfies conditions 1, 2 and 3. in Definition 2.1. Note that for $1 \leq n \leq m$, ω_n^m is multiplication by $l(-1)^{m-n}$; since graded multiplication is commutative, condition 4 in Definition 2.1 is also satisfied and so we have

Lemma 2.7 : *If F is a field of characteristic $\neq 2$, then $\mathcal{K}(\mathcal{F})$ is an IGR.* $\diamond$

If G is a special group, consider the sequence

$$\mathcal{W}(G) = (I/I^2, I^2/I^3, \ldots I^n/I^{n+1}, \ldots),$$

where I^n is the n^{th} power of the fundamental I of G, as in section 1. Note that if $\varphi \in I^n$, then $\varphi \oplus \varphi = 2 \otimes \varphi \in I^{n+1}$, showing that I^n/I^{n+1} is a group of exponent two under addition. To ease exposition, we set $\overline{I^n} = I^n/I^{n+1}$ and write x/n for an element of $\overline{I^n}$.

$\mathcal{W}(G)$ inherits a graded multiplication from the tensor product of forms. For $x/n \in \overline{I^n}$ and $y/m \in \overline{I^m}$, define

$$x/n * y/m = (x \otimes y)/n + m.$$

To show that this is well defined, suppose that $x - x' \in I^{n+1}$ and $y - y' \in I^{m+1}$. Then,

$$(x \otimes y) - (x' \otimes y') \approx_G [(x \otimes y) - (x \otimes y')] \oplus [(x \otimes y') - (x' \otimes y')]$$
$$= [x \otimes (y - y')] \oplus [y' \otimes (x - x')] \in I^{n+m+1},$$

as needed. It follows directly from the analogous properties of sum and product of forms that $\mathcal{W}(G)$ is a commutative graded ring. For each $n \geq 1$, we have group homomorphisms

$$f_n : \overline{I^n} \longrightarrow \overline{I^{n+1}}, \text{ given by } f_n(x/n) = (2x)/n + 1 = (\langle 1, 1 \rangle \otimes x)/n + 1.$$

Note that for $1 \leq n \leq m$, f_n^m is multiplication by 2^{m-n}. Thus, setting $\top_n = 2^n/n \in \overline{I^n}$, it is straightforward to see that we have

Lemma 2.8 : *If G is a special group, then $\mathcal{W}(G)$ is an IGR.* $\diamond$

Write $\langle W(G); \{\alpha_n : n \geq 1\} \rangle = \varinjlim \mathcal{W}(G)$ and $\langle k(F); \{\beta_n : n \geq 1\} \rangle = \varinjlim \mathcal{K}(F)$.

We now state

Theorem 2.9 : *If F is a formally real field and G is an $\mathcal{AP}$ group, then*

a) $k(F)$ and $W(G)$ are non-trivial Boolean rings.

b) The maps $\rho : G \longrightarrow W(G)$ and $\kappa : G(F) \longrightarrow k(F)$, defined for $a \in G$ and $b \in G(F)$ by

$$\rho(a) = \alpha_1(\langle 1, -a \rangle/1) \quad \text{and} \quad \kappa(b) = \beta_1(l(b)),$$

are morphisms of special groups, where $k(F)$ and $W(G)$ have the natural special group structure of a Boolean ring (cf. Remark 2.3(b)).

c) κ and ρ are injective iff F is Pythagorean and G is reduced, respectively.

The proof of Theorem 2.9 will require a number of results. We start with the relation between the IGR $\mathcal{K}(F)$ and the Boolean hull of $G_{red}(F)$, to be described in Theorem 2.11.

Remarks 2.10 : a) For a formally real field F, let $G_{red}(F) \xrightarrow{\varepsilon_F} B(F)$ be the Boolean hull of the reduced special group $G_{red}(F)$, as in Definition and Remarks 1.3.(c).

b) The Stiefel-Whitney invariants and the multiplicative Horn-Tarski invariants, appearing in the statement of the next result, can be found in section 3 of [Mi] and section 7 of [DM1], respectively. We recall the definition of the latter.

Let $\varphi = \langle a_1, \ldots, a_n \rangle$ be a form over a reduced SG, G. For each $1 \leq k \leq n$, $\mathcal{HT}_k(\varphi)$ and $\mathcal{HT}_k^*(\varphi)$ are defined as the following elements **of $\mathbf{B_G}$**, where G is identified with its image in B_G via ε_G and $S^{n,k}$ is the set of all strictly increasing k-sequences $p = \{p_1 < p_2 < \ldots < p_k\}$ of elements of $\{1, \ldots, n\}$:

$$\mathcal{HT}_k(\varphi) = \bigvee_{p \in S^{n,k}} \bigwedge_{i=1}^{k} a_{p_i}. \qquad \text{(additive Horn-Tarski invariants)}$$

$$\mathcal{HT}_k^*(\varphi) = \mathop{\triangle}_{p \in S^{n,k}} \bigwedge_{i=1}^{k} a_{p_i}. \qquad \text{(multiplicative Horn-Tarski invariants)}$$

Theorem 7.1 in [DM1] shows that these are complete invariants for isometry of forms over G. $\diamond$

Theorem 2.11 : *Let F be a formally real field. Then there is a unique graded ring homomorphism $(\varepsilon_n)_{n\geq 1} : k_*F \longrightarrow B(F)$, such that*

1. For all $n \geq 1$ and all $a_1, \ldots, a_n \in \dot{F}$,

$$\varepsilon_n(l(a_1)\ldots l(a_n)) = \varepsilon_F(\pi(\overline{a}_1)) \wedge \varepsilon_F(\pi(\overline{a}_2)) \wedge \ldots \wedge \varepsilon_F(\pi(\overline{a}_n)).$$

2. For all $\eta \in k_nF$ and $\zeta \in k_mF$, $\varepsilon_{n+m}(\eta * \zeta) = \varepsilon_n(\eta) \wedge \varepsilon_m(\zeta)$.

3. For all $n \geq 1$, $\varepsilon_{n+1} \circ \omega_n = \varepsilon_n$.

4. For all forms $\varphi = \langle a_1, \ldots, a_n \rangle$ over $\dot{F}$ and all $1 \leq i \leq n$, $\varepsilon_i(w_i(\varphi)) = \mathcal{HT}_i^*(\varepsilon_F \star \pi \star \overline{\varphi})$, where $w_i(\varphi)$ is the i^{th} K-theoretic Stiefel-Whitney invariant of φ and $\mathcal{HT}_i^*(\varepsilon_F \star \pi \star \overline{\varphi})$ is the i^{th} multiplicative Horn-Tarski invariant of the image form $\varepsilon_F \star \pi \star \overline{\varphi}$.

Proof : Notation is as in Remark 1.2 and [Mi]. We shall borrow freely from section 1 in [Mi]. To simplify exposition, write f for $\varepsilon_F \circ \pi$.

Recall that $\dot{F} \xrightarrow{l} K_1F$ is an isomorphism, such that $l(a\ b) = l(a) + l(b)$, $a, b \in \dot{F}$.

Define a map α_n from $(K_1F)^n$ to $B(F)$ by the following rule :

$$\alpha_n(l(a_1), \ldots, l(a_n)) = f(\overline{a}_1) \wedge f(\overline{a}_2) \wedge \ldots \wedge f(\overline{a}_n).$$

Recalling that $\triangle$ distributes over meets in $B(F)$ and the properties of the map ε_F (see 2.10 and 1.3.(c)), we have

$$\begin{aligned}\alpha_n(l(a_1), \ldots, l(a_i) + l(c_i), \ldots, l(a_n)) &= \alpha_n(l(a_1), \ldots, l(a_i \cdot c_i), \ldots, l(a_n)) = \\ &= f(\overline{a}_1) \wedge \ldots \wedge [f(\overline{a}_i \cdot \overline{c}_i)] \wedge \ldots \wedge f(\overline{a}_n) = f(\overline{a}_1) \wedge \ldots \wedge [f(\overline{a}_i) \triangle f(\overline{c}_i)] \wedge \ldots \wedge f(\overline{a}_n) \\ &= (f(\overline{a}_1) \wedge \ldots \wedge f(\overline{a}_i) \wedge \ldots \wedge f(\overline{a}_n)) \triangle (f(\overline{a}_1) \wedge \ldots \wedge f(\overline{c}_i) \wedge \ldots \wedge f(\overline{a}_n)) \\ &= \alpha_n(l(a_1), \ldots, l(a_i), \ldots, l(a_n)) \triangle \alpha_n(l(a_1), \ldots, l(c_i), \ldots, l(a_n)),\end{aligned}$$

verifying the n-linearity of α_n. Thus, α_n induces a homomorphism $\widehat{\alpha}_n$ from the n-fold tensor product $\bigotimes_{i=1}^n K_1F$ to B_F, such that $l(a_1)l(a_2)\ldots l(a_n)$ is taken to $f\overline{a}_1 \wedge f\overline{a}_2 \wedge \ldots \wedge f\overline{a}_n$.

To show that $\widehat{\alpha}_n$ factors through K_nF, it must be verified that if $\eta = l(a_1)l(a_2)\ldots l(a_n)$ is such that $a_i + a_{i+1} = 1$, for some $i \leq n-1$, then $\widehat{\alpha}_n(\eta) = \perp$ ($= 1$ in $B(F)$).

But if $a_i = 1 - a_{i+1}$, then $a_i \in D_T(1, -a_{i+1})$, where $T = \Sigma\dot{F}^2$. It follows from Remarks 2.10 and Definition 1.3.(c), that $f(\overline{a}_i) \leq f(-(\overline{a}_{i+1})) = -f(\overline{a}_{i+1})$. Thus, $f(\overline{a}_i) \wedge f(\overline{a}_{i+1}) = \perp$, which in turn implies $\widehat{\alpha}_n(\eta) = \perp$, as needed.

Thus, $\widehat{\alpha}_n$ induces a homomorphism $g_n : K_nF \longrightarrow B(F)$, taking a generator $l(a_1)l(a_2)\ldots l(a_n)$ to $f(\overline{a}_1) \wedge f(\overline{a}_2) \wedge \ldots \wedge f(\overline{a}_n)$ in $B(F)$.

It is clear from the definition of g_n, that for all $\eta \in K_nF$, $\zeta \in K_mF$, $n, m \geq 1$,

$$g_{n+m}(\eta * \zeta) = g_n(\eta) \wedge g_m(\zeta), \qquad (*)$$

and so $g = (g_n) : K_*F \longrightarrow B(F)$ is a homomorphism of graded rings.

For all $n \geq 1$, Remarks 2.10 and Definition 1.3.(c) imply that

$$g_n(l(-1)^n) = \bigwedge_{i=1}^n f(-1) = \bigwedge_{i=1}^n \top = \top \text{ (top in } B(F)). \qquad (**)$$

If $\eta = l(a_1)l(a_2)\dots l(a_n)$ is such that $a_i = c^2 \in \dot{F}^2$, then

$$g_n(\eta) = f(\overline{a}_1) \wedge \dots \wedge [f(\overline{c}) \triangle f(\overline{c})] \wedge \dots \wedge f(\overline{a}_n) = \perp,$$

showing that $2K_nF \subseteq \ker g_n$, for all $n \geq 0$. Since $k_*F = K_*F/2K_*F$, g_n induces a homomorphism

$$\varepsilon_n : k_nF \longrightarrow B(F),$$

that maps a generator $l(a_1)l(a_2)\dots l(a_n)$ to $f(\overline{a}_1) \wedge f(\overline{a}_2) \dots \wedge f(\overline{a}_n)$ in $B(F)$.

Item (2) comes directly from (*), while (**) yields (3). With respect to (4), it is clear from the values of ε_i on the generators of k_iF, that $\varepsilon_i(w_i(\varphi)) = \mathcal{HT}_i^*(f \star \overline{\varphi})$. $\diamond$

Proposition 2.12 : *Let F be a field and G a special group. For an integer $n \geq 1$, let $\eta \in k_nF$ and $x \in I^n$. Then,*

a) $2^n x - (x \cdot x) \in I^{2n+1}$. *b) In* $k_{2n}F$, $l(-1)^n\eta = \eta \cdot \eta$.

Proof : a) Fix $x \in I^n$; x is the Witt-equivalence class of a linear combination of Pfister forms of degree n, say $\mathcal{Q} = \sum_{i=1}^k a_i\mathcal{P}_i$, with $a_i \in G$, $1 \leq i \leq k$. Thus, (a) amounts to proving that

$$2^n\mathcal{Q} - (\mathcal{Q} \otimes \mathcal{Q}) \text{ is in } I^{2n+1}. \tag{I}$$

Now define $\mathcal{T} = \sum_{i=1}^k \mathcal{P}_i$ and $\mathcal{R} = \mathcal{Q} - \mathcal{T}$.

Fact I : *If assertion (I) holds for $\mathcal{T}$, then it holds for $\mathcal{Q}$.*

Proof : Note that $\mathcal{R} = \sum_{i=1}^k \langle a_i, -1\rangle\mathcal{P}_i \in I^{n+1}$. We also have $\mathcal{Q} \approx \mathcal{T} \oplus \mathcal{R}$. Thus,

$$2^n\mathcal{Q} - (\mathcal{Q} \otimes \mathcal{Q}) \approx (2^n\mathcal{T} \oplus 2^n\mathcal{R}) - ((\mathcal{T} \oplus \mathcal{R}) \otimes (\mathcal{T} \oplus \mathcal{R}))$$
$$= (2^n\mathcal{T} - (\mathcal{T} \otimes \mathcal{T})) \oplus 2^n\mathcal{R} - 2(\mathcal{T} \otimes \mathcal{R}) - (\mathcal{R} \otimes \mathcal{R}).$$

Since $2^n\mathcal{R} \in I^{2n+1}$, while $(\mathcal{R} \otimes \mathcal{R})$, $2(\mathcal{T} \otimes \mathcal{R}) \in I^{2n+2}$, we conclude that $\mathcal{Q}$ also satisfies (I).

Fact I tells us that it is enough to verify (I) for sums $\mathcal{Q} = \sum_{i=1}^k \mathcal{P}_i$ of Pfister forms of degree n. The proof will proceed by induction on the integer $k \geq 1$.

Part I : $k = 1$. Then, $\mathcal{Q}$ is $\mathcal{P} = \bigotimes_{j=1}^n \langle 1, c_i\rangle$, with $c_i \in G$.

The proof of Part I will be by induction on $n \geq 1$. For $n = 1$, we have

$$2\langle 1,c\rangle - (\langle 1,c\rangle \otimes \langle 1,c\rangle) = \langle 1,c\rangle \oplus \langle 1,c\rangle - \langle 1,c\rangle - \langle 1,c\rangle, \tag{II}$$

showing that in this case $2\mathcal{Q} - (\mathcal{Q} \otimes \mathcal{Q})$ is in fact hyperbolic. Now suppose the conclusion holds for n and let $\mathcal{Q} = \mathcal{P} \otimes \langle 1,c\rangle$, with $\mathcal{P}$ a Pfister form of degree n. Then, using (II), we get

$$2^{n+1}\mathcal{Q} - (\mathcal{Q} \otimes \mathcal{Q}) = 2^{n+1}\mathcal{P} \otimes \langle 1,c\rangle - (\mathcal{P} \otimes \langle 1,c\rangle \otimes \mathcal{P} \otimes \langle 1,c\rangle)$$
$$= 2^n\mathcal{P} \otimes 2\langle 1,c\rangle - (\mathcal{P} \otimes \mathcal{P} \otimes \langle 1,c\rangle \otimes \langle 1,c\rangle$$
$$= 2^n\mathcal{P} \otimes 2\langle 1,c\rangle - (\mathcal{P} \otimes \mathcal{P} \otimes 2\langle 1,c\rangle) = 2\langle 1,c\rangle(2^n\mathcal{P} - (\mathcal{P} \otimes \mathcal{P})) \in I^{2n+3}.$$

Part II : Induction step. Let $\mathcal{Q} = \mathcal{P} \oplus \mathcal{T}$, where $\mathcal{P}$ is a Pfister form of degree n and $\mathcal{T}$ is the sum of less than k Pfister forms of degree n. Then,

$$2^n\mathcal{Q} - (\mathcal{Q} \otimes \mathcal{Q}) = (2^n\mathcal{P} \oplus 2^n\mathcal{T}) - ((\mathcal{P} \oplus \mathcal{T}) \otimes (\mathcal{P} \oplus \mathcal{T}))$$
$$= (2^n\mathcal{P} - (\mathcal{P} \otimes \mathcal{P})) \oplus (2^n\mathcal{T} - (\mathcal{T} \otimes \mathcal{T})) - 2(\mathcal{P} \otimes \mathcal{T}).$$

Since $2(\mathcal{P} \otimes \mathcal{T}) \in I^{2n+1}$, the induction hypothesis and Part I yield (I) for $\mathcal{Q}$, proving (a).

b) We first prove that (b) holds on generators $\eta = l(a_1) \ldots l(a_n)$ of k_nF. Since k_nF is commutative, Lemma 2.6.(a) yields

$$l(-1)^n l(a_1) \ldots l(a_n) = [l(-1)l(a_1)][l(-1)l(a_2)] \ldots [l(-1)l(a_n)] = l(a_1)^2 l(a_2)^2 \ldots l(a_n)^2 = \eta \cdot \eta,$$

showing that (b) is verified on generators. If we assume that (b) holds for sums of $k \geq 1$ generators, let $\eta = \zeta + \xi$ where ζ is a generator of k_nF and ξ is a sum of at most k generators. Then, the induction hypothesis and the fact that k_nF is an additive group of exponent two yields

$$l(-1)^n\eta = l(-1)^n[\zeta + \xi] = l(-1)^n\zeta + l(-1)^n\xi = (\zeta \cdot \zeta) + (\xi \cdot \xi) = (\zeta + \xi) \cdot (\zeta + \xi),$$

completing the proof. $\diamond$

Proof of (a) in Theorem 2.9 : We shall verify conditions [*br i*] in Theorem 2.4, $0 \leq i \leq 2$.

For each $n \geq 1$, $\top_n = \begin{cases} l(-1)^n & \text{in } \mathcal{K}(F) \\ 2^n & \text{in } \mathcal{W}(G). \end{cases}$

Thus, [*br* 0] is equivalent to $\begin{cases} l(-1)^{n+1} \neq 0 & \text{for } \mathcal{K}(F) \\ 2^{n+1} \notin I^{n+2} & \text{for } \mathcal{W}(G). \end{cases}$

If $l(-1)^{n+1} = 0$ in $k_{n+1}F$, then, by Theorem 2.11, we would have

$$\varepsilon_{n+1}(l(-1)^{n+1}) = \bigwedge_{i=1}^{n} \varepsilon_F(\pi(-1)) = \varepsilon_F(\pi(-1)) = \perp \text{ in } B(F).$$

Since ε_F is injective, we conclude that $\pi(-1) = 1$; but then $-1 \in \Sigma\dot{F}^2$ and F is not formally real. Since G is an $\mathcal{AP}$ group, it is clear that $2^{n+1} \notin I^{n+2}$. This proves [*br* 0] for $\mathcal{K}(F)$ and $\mathcal{W}(G)$.

We register that Theorem 3.2 in [EL 1] will give another proof of [*br* 0] for the ring $\mathcal{K}(F)$.

For [*br* 1], just notice that if $x/n \in I^n$ and $\eta \in k_nF$, then

$$f_{n+1}^{n+2}(\langle 1, 1 \rangle * x/n) = f_n^{n+2}(x/n) \quad \text{and} \quad \omega_{n+1}^{n+2}(l(-1) * \eta) = \omega_n^{n+2}(\eta).$$

The last condition to be verified, [*br* 2], is a direct consequence of Proposition 2.12. This proves that $k(F)$ and $W(G)$ are non-trivial Boolean rings. $\diamond$

Proof of (b) in Theorem 2.9.

I. The case of $\mathcal{W}(G)$. The proof will be done in 2 steps :

1. ρ is a group homomorphism, with $\rho(-1) = \top$: For $a, b \in G$, we have

$$(\langle 1, -a \rangle \oplus \langle 1, -b \rangle) - \langle 1, -ab \rangle = \langle 1, -a, -b, ab \rangle \oplus \langle 1, -1 \rangle$$
$$= (\langle 1, -a \rangle \otimes \langle 1, -b \rangle) \oplus \langle 1, -1 \rangle,$$

proving that $\overline{\langle 1, -a \rangle}/1 + \overline{\langle 1, -b \rangle}/1 = \overline{\langle 1, -ab \rangle}/1$ in $\overline{I^1}$. Since α_1 is a group homomorphism, this shows that $\rho(ab) = \rho(a) + \rho(b)$. Finally,

$$\rho(1) = \alpha_1(\overline{\langle 1, -1 \rangle}/1) = \perp \quad \text{and} \quad \rho(-1) = \alpha_1(\overline{\langle 1, 1 \rangle}/1) = \top.$$

2. ρ is a special group morphism : For a, b, c, $d \in G$, let $u = \rho(a)$, $v = \rho(b)$, $w = \rho(c)$ and $z = \rho(d)$. For ρ to be a morphism of special groups, it must be shown that

$$\langle a, b \rangle \equiv_G \langle c, d \rangle \text{ implies } \langle u, v \rangle \equiv_{\mathcal{W}(G)} \langle w, z \rangle. \tag{I}$$

According to equivalence **[iso]** in Remark 2.3(b), (I) is equivalent to

$$\langle a,b\rangle \equiv_G \langle c,d\rangle \quad \text{implies} \quad u+v=w+z \quad \text{and} \quad u\cdot v = w\cdot z. \tag{II}$$

It follows from [SG 3] in Definition 1.1 of [DM1] (the discriminant axiom) that $ab = cd$. Since ρ is a group homomorphism, this equation implies $u + v = w + z$. By the definition of product in $W(G)$, to prove $u \cdot v = w \cdot z$ it is enough to verify that

$$(\langle 1,-a\rangle \otimes \langle 1,-b\rangle) - (\langle 1,-c\rangle \otimes \langle 1,-d\rangle) \in I^3. \tag{III}$$

Because if (III) holds, then $(\overline{\langle 1,-a\rangle}\cdot\overline{\langle 1,-b\rangle})/2 = (\overline{\langle 1,-c\rangle}\cdot\overline{\langle 1,-d\rangle})/2$, and so the value of α_2 at this point will give $u\cdot v = w\cdot z$.

To prove (III), compute as follows, recalling that $\langle a,b\rangle \equiv_G \langle c,d\rangle$ and $ab = cd = t$:

$$\begin{aligned}(\langle 1,-a\rangle \otimes \langle 1,-b\rangle) - (\langle 1,-c\rangle \otimes \langle 1,-d\rangle) &= \langle 1,-a,-b,ab\rangle - \langle 1,-c,-d,cd\rangle \\ &= \langle 1,-1\rangle \oplus (\langle c,d\rangle - \langle a,b\rangle) \oplus \langle t,-t\rangle,\end{aligned}$$

which is hyperbolic, ending the proof that $\rho : G \longrightarrow W(G)$ is a SG-morphism.

II. The case of $\mathcal{K}(F)$. Since l takes product in $G(F)$ to sum in k_1F and β_1 is a homomorphism, it is clear that κ is a homomorphism from $G(F)$ to $k(F)$. For the preservation of -1, just notice that $l(-1)$ in k_1F is a representative of $\top \in k(F)$. It remains to prove that κ is a morphism of special groups. Just as above, this reduces to verifying that for a, b, c, d in $\dot{F}$,

$$\langle \overline{a}, \overline{b}\rangle \equiv_{G(F)} \langle \overline{c}, \overline{d}\rangle \quad \Rightarrow \quad \kappa(a)+\kappa(b) = \kappa(c)+\kappa(d) \quad \text{and} \quad \kappa(a)\cdot\kappa(b) = \kappa(c)\cdot\kappa(d). \tag{I}$$

Since $G(F)$ is a special group, Lemma 1.5.(a) in [DM1] yields

$$\langle \overline{a}, \overline{b}\rangle \equiv_{G(F)} \langle \overline{c}, \overline{d}\rangle \quad \text{iff} \quad \overline{ab} = \overline{cd} \quad \text{and} \quad \overline{ac} \in D_{G(F)}(1, \overline{cd}).$$

By item (a) of Fact 1.2.A, we may restate this equivalence as

$$\langle \overline{a}, \overline{b}\rangle \equiv_{G(F)} \langle \overline{c}, \overline{d}\rangle \quad \text{iff} \quad \exists\, x \in \dot{F} \text{ and } y,\, z \in F \text{ such that } ab = cdx^2 \quad \text{and} \quad ac = y^2 + cdz^2. \tag{II}$$

It follows from the first equation in (II) and Lemma 2.6.(b) that

$$l(a) + l(b) = l(ab) = l(cdx^2) = l(cd) = l(c) + l(d). \tag{III}$$

Since β_1 is a homomorphism, the first equation in (I) is verified.

To complete the proof of (b), note that either y or z in the last equation in (II) must be in $\dot{F}$. The case of $z \neq 0$ is left to the reader, and we treat the case in which $y \neq 0$. It follows from (II) that $ac\ (1/y)^2 + -cd\,(z/y)^2 = 1$. Thus, (b) and (d) in Lemma 2.6 yield $l(ac)l(-cd) = 0$ in k_2F. Now, (III) and Lemma 2.6.(a) yield,

$$\begin{aligned} 0 = l(ac)l(-cd) &= [l(a) + l(c)]\,[l(-1) + l(c) + l(d)] \\ &= l(a)l(-1) + l(a)[l(c) + l(d)] + l(c)l(-1) + l(c)[l(c) + l(d)] \\ &= l(a)l(-1) + l(a)[l(a) + l(b)] + l(c)l(-1) + l(c)^2 + l(c)l(d) \\ &= l(a)l(-1) + l(a)^2 + l(a)l(b) + l(c)l(d) = l(a)l(b) + l(c)l(d). \end{aligned}$$

Since $\kappa(a)\cdot\kappa(b) = \beta_2(l(a)l(b))$, it is clear that $\kappa(a)\kappa(b) = \kappa(c)\kappa(d)$, as desired. $\diamond$

Proof of (c) in Theorem 2.9. Since any subgroup of a reduced special group must be reduced, it is enough to show the "only if" part of the equivalence in (c). So assume that F is Pythagorean and G is a reduced special group.

Note that, because F is Pythagorean, the morphism $G(F) \xrightarrow{\pi} G_{red}(F)$ is the identity.

Suppose that $a,\ b \in \dot{F}$ are such that $\kappa(a) = \kappa(b)$ in $k(F)$. By Remark 2.2.(3), there is $n \geq 1$ such that $l(-1)^n l(a) = l(-1)^n l(b)$ in $k_{n+1}F$. By Theorem 2.11, $\varepsilon_{n+1}(l(-1)^n l(a)) = \varepsilon_F(\overline{a})$; thus, we have $\varepsilon_F(\overline{a}) = \varepsilon_F(\overline{b})$. Since ε_F is injective (Remarks 2.10 and Definition 1.3), we conclude that κ must be injective. It should perhaps be mentioned that Theorem 3.2 in [EL 1] can also be used to prove that κ is injective.

Now assume that for $a,\ b \in G$, $\rho(a) = \rho(b)$. Just as above, there is an integer $k \geq 1$ such that $2^{k-1}\langle 1, -a \rangle - 2^{k-1}\langle 1, -b \rangle \in I^{k+1}$. Note that

$$2^{k-1}\langle 1, -a \rangle - 2^{k-1}\langle 1, -b \rangle = 2^{k-1}\langle 1, -1 \rangle \oplus 2^{k-1}\langle -a, b \rangle,$$

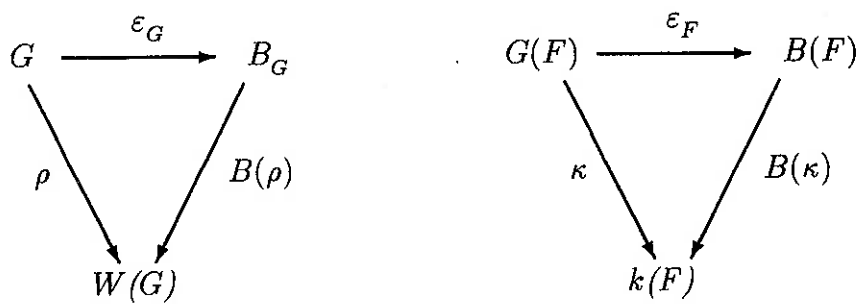
and so $2^{k-1}\langle -a, b \rangle \in I^{k+1}$. It follows from the reduced special group version of the Arason-Pfister Hauptsatz (Theorem 7.30 in [DM1]) that $2^{k-1}\langle -a, b \rangle$ must be hyperbolic. In Proposition 1.6.(e) of [DM1] it is shown that the following condition is equivalent to G being reduced :

– For all forms ψ of even dimension over G, $\psi \oplus \psi$ hyperbolic $\Rightarrow$ ψ hyperbolic.

This result and straightforward induction shows that $\langle -a, b \rangle$ must be hyperbolic, that is, $\langle -a, b \rangle \equiv_G \langle 1, -1 \rangle$. It follows from the discriminant axiom [SG 3] in Definition 1.1 of [DM1] that $-ab = -1$; thus, $a = b$, ending the proof the proof of Theorem 2.9. $\diamond$

As a direct consequence of Theorem 5.7.(3) in [DM] and Theorem 2.9 we get the important

Corollary 2.13 : *Let G be a reduced special group and let F be a Pythagorean field. Then, the SG-embeddings $G \xrightarrow{\rho} W(G)$ and $G(F) \xrightarrow{\kappa} k(F)$ of Theorem 2.9 have unique extensions to Boolean algebra homomorphisms $B(\rho) : B_G \longrightarrow W(G)$ and $B(\kappa) : B(F) \longrightarrow k(F)$, such that the following diagrams are commutative :*



Moreover,

1. If $\{a_{ij} : 1 \leq i \leq k,\ 1 \leq j \leq n\} \subseteq G$ and $a = \triangle_{i=1}^{k} \bigwedge_{j=1}^{n} \varepsilon_G(a_{ij})$, then

$$B(\rho)(a) = \alpha_n(\overline{\varphi}/n), \tag{SG}$$

where $\varphi = \sum_{i=1}^{k} \bigotimes_{j=1}^{n} \langle 1, -a_{ij} \rangle \in I^n$.

2. If If $\{a_{ij} : 1 \leq i \leq k,\ 1 \leq j \leq n\} \subseteq G(F)$ and $a = \triangle_{i=1}^{k} \bigwedge_{j=1}^{n} \varepsilon_F(a_{ij})$, then

$$B(\kappa)(a) = \beta_n(\eta), \tag{KT}$$

where $\eta = \sum_{i=1}^{k} l(a_{i1})l(a_{i2})\ldots l(a_{in}) \in k_nF$.

Proof : Only formulas (SG) and (KT) remain to be checked. By Remark 2.3.(a), $B(\rho)$ and $B(\kappa)$ take symmetric difference to sum and meet to product in $W(G)$ and $k(F)$, respectively.

To verify (SG), set $\mathcal{P}_i = \otimes_{j=1}^{n} \langle 1, -a_{ij} \rangle$; then Corollary 2.5 yields

$$B(\rho)(\varepsilon_G(a)) = \triangle_{i=1}^{k} \prod_{i=1}^{n} B(\rho)(\varepsilon_G(a_{ij})) = \sum_{i=1}^{k} \prod_{i=1}^{n} \rho(a_{ij})$$
$$= \sum_{i=1}^{k} \prod_{i=1}^{n} \alpha_1(\overline{\langle 1, -a_{ij} \rangle}/1) = \sum_{i=1}^{k} \alpha_n(\overline{\mathcal{P}_i}/n) = \alpha_n(\overline{\varphi}/n).$$

For (KT), write $\eta_i = l(a_{i1})l(a_{i2})\ldots l(a_{in})$; by Corollary 2.5,

$$B(\kappa)(\varepsilon_F(a)) = \triangle_{i=1}^{k} \prod_{i=1}^{n} B(\kappa)(\varepsilon_F(a_{ij})) = \sum_{i=1}^{k} \prod_{i=1}^{n} \kappa(a_{ij})$$
$$= \sum_{i=1}^{k} \prod_{i=1}^{n} \beta_1(l(a_{ij})) = \sum_{i=1}^{k} \beta_n(\eta_i) = \beta_n(\eta). \quad \diamond$$

Remark 2.14 : In [DM2] we have a basic version of an algebraic K-theory for special groups, showing that it is possible to live without addition. We also show that if a special group comes from a field, then our K-theory is isomorphic to Milnor's. With the results in [DM2] it would be possible to phrase Theorems 2.11 and 2.9, as well as Corollary 2.13, in the language of special groups. We chose to deal directly fields in the case of K-theory in order to avoid having to spell out the constructions in [DM2] at this time. $\diamond$

3 The isomorphisms $\mathbf{k(F) \approx B(F)}$ and $\mathbf{W(G) \approx B_G}$

In this section we prove the isomorphisms in title for Pythagorean fields and reduced special groups. In this section F will stand for a Pythagorean field and G for a reduced special group.

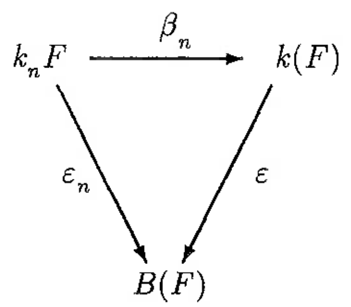
We first treat the case of a Pythagorean field F. One should keep in mind that $G(F) = G_{red}(F)$, that is, the canonical projection π is the identity.

Since $k(F) = \varinjlim \mathcal{K}(F)$, Theorem 2.11.(b) implies that the sequence of homomorphisms $(\varepsilon_n)_{n \geq 1}$ induces a homomorphism $\varepsilon : k(F) \longrightarrow B(F)$, that can be described as follows :

For $z \in k(F)$, let $\eta = \sum_{i=1}^{k} l(a_{i1})l(a_{i2})\ldots l(a_{in}) \in k_nF$ be a representative of z. Then,

$$\varepsilon(z) = \varepsilon_n(\eta) = \triangle_{i=1}^{k} \bigwedge_{j=1}^{n} \varepsilon_F(a_{ij}).$$

The map ε also makes the following diagram commutative, for all $n \geq 1$:



Theorem 3.1 : *Let F be a Pythagorean field. Then, the map $\varepsilon : k(F) \longrightarrow B(F)$ is a Boolean algebra isomorphism, whose inverse is the map $B(\kappa)$ of Corollary 2.13.*

Proof : We shall show that (I) $\varepsilon \circ B(\kappa) = Id_{B(F)}$ and (II) $B(\kappa) \circ \varepsilon = Id_{k(F)}$.

Proof of (I) : Since

- $B(\kappa)$ and ε are Boolean algebra homomorphisms;
- $B(\kappa)$ extends κ (Corollary 2.13); and
- $G(F)$ generates $B(F)$ as a Boolean algebra (Proposition 5.1 in [DM1]), that is, for all $u \in B(F)$,

There is $n \geq 1$ and finite subsets $F_i \subseteq G(F)$, $1 \leq i \leq n$, such that $u = \bigvee_{i=1}^{n} \bigwedge_{a \in F_i} \varepsilon_F(a)$,

it is enough to show that for all $a \in G(F)$, $\varepsilon(\kappa(a)) = \varepsilon_F(a)$. But we have, by the commutative diagram above and Theorem 2.11,

$$\varepsilon(\kappa(a)) = \varepsilon(\beta_1(l(a)) = \varepsilon_1(l(a)) = \varepsilon_F(a).$$

Proof of (II) : For $z \in k(F)$, let $\eta \in k_n F$ be a representative of z, that is, $z = \beta_n(\eta)$. Write $\eta = \sum_{i=1}^{k} l(a_{i1})l(a_{i2}) \ldots l(a_{in})$. To prove (II), it is enough to show that $B(\kappa)(\varepsilon(z)) = \beta_n(\eta)$. But this follows directly from formula (KT) in Corollary 2.13. $\diamond$

We now turn to the case of a reduced special group G. Notation will be as in sections 3 and 4 of [DM1]. To ease exposition, we include the following :

Facts 3.2 : By Fact 1.3.B, for any Pfister form $\mathcal{P} = \otimes_{i=1}^{n} \langle 1, a_i \rangle$ we have :

Fact A : $\{\sigma \in X_G : \sigma(\mathcal{P}) = 0\} = \bigcup_{i=1}^{n} [a_i = -1] = \bigvee_{i=1}^{n} \varepsilon_G(a_i)$, a **clopen** in X_G.

Fact B : $\{\sigma \in X_G : \sigma(\mathcal{P}) = 2^n\} = - \bigvee_{i=1}^{n} \varepsilon_G(a_i)$, a **clopen** in X_G.

Note that for $\varphi = \langle a_1, \ldots, a_n \rangle$,

Fact C : $\mathcal{HT}_1(\varphi) = \bigvee_{i=1}^{n} a_i$ and $\mathcal{HT}_1^*(\varphi) = \triangle_{i=1}^{n} a_i$ (= the discriminant of φ).

For Pfister forms of degree $n \geq 1$, $\mathcal{P} = \bigotimes_{i=1}^{n} \langle 1, a_i \rangle$ we have, by Theorem 7.18 in [DM] :

Fact D : $\mathcal{HT}_1(\mathcal{P}) = \bigvee_{i=1}^{n} a_i$.

In this notation, we can rewrite Facts C and D as :

Fact E : If $\mathcal{P} = \bigotimes_{i=1}^{n} \langle 1, a_i \rangle$ is a Pfister form of degree n, then

$\{\sigma \in X_G : \sigma(\mathcal{P}) = 0\} = \mathcal{HT}_1(\mathcal{P})$ and $\{\sigma \in X_G : \sigma(\mathcal{P}) = 2^n\} = - \mathcal{HT}_1(\mathcal{P}) = \bigwedge_{i=1}^{n} -a_i$.

Let $n \geq 1$ be an integer. If φ and ψ are Witt-equivalent forms in G, then for all $\sigma \in X_G$, $\sigma(\varphi) = \sigma(\psi)$. Thus, if $x \in I^n$ and $\sigma \in X_G$, we may define the **signature** of x at σ, $\sigma(x)$, as the signature of any form φ such that $\overline{\varphi} = x$.

Formula (*) and Fact 1.3.B, yield

Fact F : *For all $n \geq 1$, all $x \in I^n$ and all $\sigma \in X_G$, $\sigma(x) \equiv 0 \bmod 2^n$.* $\diamond$

For $x \in I^n$, define

$$\mu_n(x) = \{\sigma \in X_G : \sigma(x) \text{ is not congruent to } 0 \bmod 2^{n+1}\}.$$

Lemma 3.3 : *With notation as above,*

a) For all $n \geq 1$ and $x \in I^n$, $\mu_n(x) \in B_G$.

b) For all integers $1 \leq n, m \leq k$ and all $x \in I^n$ and $y \in I^m$

$$2^{k-n}x - 2^{k-m}y \in I^{k+1} \quad \textit{implies} \quad \mu_n(x) = \mu_m(y).$$

c) Let $\mathcal{P}$ be a Pfister form of degree $n \geq 1$. For $a \in G$ and $x = \overline{a\mathcal{P}} \in I^n$,

$$\mu_n(x) = -\mathcal{HT}_1(\mathcal{P}).$$

Proof : a) Let $x = \overline{\mathcal{Q}}$, with $\mathcal{Q} = \sum_{i=1}^{p} a_i \mathcal{P}_i$, where $a_i \in G$ and $\mathcal{P}_i = \bigotimes_{j=1}^{n} \langle 1, b_{ij} \rangle$ are Pfister forms of degree n. Suppose $\sigma \in \mu_n(x)$, that is, $\sigma(\mathcal{Q}) \not\equiv 0 \bmod 2^{n+1}$. Consider the clopen

$$U = \bigcap \{[b_{ij} = \sigma(b_{ij})] : 1 \leq i \leq p, 1 \leq j \leq n\} \ \cap \ \bigcap \{[a_i = \sigma(a_i)] : 1 \leq i \leq p\}.$$

It is clear that $\sigma \in U$, as well as that for all $\tau \in U$ we have $\tau(\mathcal{Q}) = \sigma(\mathcal{Q})$. But this means that U is a clopen neighbourhood of σ contained in $\mu_n(x)$. The same reasoning will show that the complement of $\mu_n(x)$ is open.

b) It must be shown that for all $\sigma \in X_G$,

$$\sigma(x) \equiv 0 \bmod 2^{n+1} \quad \text{iff} \quad \sigma(y) \equiv 0 \bmod 2^{m+1}.$$

For $\sigma \in X_G$, formula (*) and Fact 1.3.B yield, together with our hypothesis, that for some integer $p \geq 0$ the following equation holds in $\mathbf{Z}$:

$$2^{k-n}\sigma(x) - 2^{k-m}\sigma(y) = p2^{k+1}. \tag{I}$$

Now suppose that $\sigma(x)$ is a multiple of 2^{n+1}, say $\sigma(x) = q2^{n+1}$. Then, (I) gives

$$q2^{k+1} - 2^{k-m}\sigma(y) = p2^{k+1},$$

which clearly implies $\sigma(y) \equiv 0 \bmod 2^{m+1}$. A similar reasoning will show that $\sigma(y) \equiv 0 \bmod 2^{m+1}$ implies $\sigma(x) \equiv 0 \bmod 2^{n+1}$.

c) Since $\mathcal{P} - a\mathcal{P} \in I^{n+1}$, (c) yields $\mu_n(\overline{\mathcal{P}}) = \mu_n(x)$. By Fact 1.3.B and Fact 3.2.E we have

$$\mu_n(\overline{\mathcal{P}}) = \{\sigma \in X_G : \sigma(\mathcal{P}) \not\equiv 0 \bmod 2^{n+1}\} = \{\sigma \in X_G : \sigma(\mathcal{P}) = 2^n\} = -\mathcal{HT}_1(\mathcal{P}). \qquad \diamond$$

It follows from Lemma 3.3 that for each $n \geq 1$ we have a map $\mu_n : \overline{I^n} \longrightarrow B_G$, defined by

$$\mu_n(x/n) = \mu_n(x).$$

We now define a map $M : W(G) \longrightarrow B_G$ as follows :

For $w \in W(G)$, let x/n be a representative of w. Then

$$M(w) = \mu_n(x).$$

It follows from Remark 2.2.(3) and Lemma 3.3.(b) that the definition of M is independent of representatives. The main result of this section reads

Theorem 3.4 *: The map $M : W(G) \longrightarrow B_G$ is an isomorphism of Boolean algebras, whose inverse is the homomorphism $B(\rho)$ of Corollary 2.13.*

As part of the proof of Theorem 3.4, we first establish :

Proposition 3.5 *: With notation as above, let $n \geq 1$ be an integer.*

a) M is a Boolean algebra homomorphism.

b) For $x/n \in \overline{I^n}$, let $w = \alpha_n(x/n)$ and $x = \overline{\mathcal{Q}}$, where $\mathcal{Q} = \sum_{i=1}^{p} a_i \mathcal{P}_i$ is a linear combination of Pfister forms of degree n. Then,

$$M(w) = \triangle_{i=1}^{p} -\mathcal{HT}_1(\mathcal{P}_i) = (-1)^p \triangle_{i=1}^{p} \mathcal{HT}_1(\mathcal{P}_i).$$

Proof : a) By Lemma 3.3.(c), we have

$M(\top) = \mu_1(\langle 1,1 \rangle) = -\mathcal{HT}_1(\langle 1,1 \rangle) = -\perp = \top$ and $M(\perp) = \mu_1(\langle 1,-1 \rangle) = -\top = \perp$.

By Remark 2.3, we have to show that for w, $z \in W(G)$,

$$M(w + z) = M(w) \triangle M(z) \quad \text{and} \quad M(w \cdot z) = M(w) \wedge M(z). \tag{I}$$

Let x/n, y/m be representatives of w and z, respectively. We may suppose that $m \geq n$. Then, $M(w + z) = \mu_m(2^{m-n}x + y)$.

In any Boolean algebra $-(a \triangle b) = (a \wedge b) \vee (-a \wedge -b)$. Thus, if $t = 2^{m-n}x + y$, the verification the first equation in (I) reduces to showing that for all $\sigma \in X_G$,

$$\sigma(t) \equiv 0 \bmod 2^{m+1} \quad \Leftrightarrow \quad \sigma \in (\mu_n(x) \cap \mu_m(y)) \cup (-\mu_n(x) \cap -\mu_m(y)). \tag{II}$$

The proof of (II) is in two steps. For $\sigma \in X_G$, write $\sigma(x) = \alpha 2^n$ and $\sigma(y) = \beta 2^m$, for integers α, $\beta \geq 0$ (Fact 3.2.F). Then,

– If $\sigma(t) = p2^{m+1}$, then

$$p2^{m+1} = \sigma(t) = 2^{m-n}\sigma(x) + \sigma(y) = 2^{m-n}\alpha 2^n + \beta 2^m = (\alpha + \beta)2^m,$$

and so $\alpha + \beta = 2p$. Thus, α, β are both even or both odd. If α, β are even, then $\sigma \in -\mu_n(x) \cap -\mu_m(y)$. If they are both odd, then $\sigma \in \mu_n(x) \cap \mu_m(y)$, proving part ($\Rightarrow$) of the equivalence.

– It is clear that if $\sigma \in -\mu_n(x) \cap -\mu_m(y)$, then $\sigma(t) \equiv 0 \bmod 2^{m+1}$. If $\sigma \in \mu_n(x) \cap \mu_m(y)$, then the integers α, β are both odd, say $\alpha = 2s + 1$, $\beta = 2r + 1$. Then,

$$\sigma(t) = 2^{m-n}(2s + 1)2^n + (2r + 1)2^m = 2^{m+1}s + 2^m + 2^{m+1}r + 2^m \equiv 0 \bmod 2^{m+1},$$

ending the proof of (II).

For the second equation in (I), we have $M(w \cdot z) = \mu_{m+n}(x \cdot y)$. Set $t = x \cdot y$; by the same argument as above, the desired conclusion is equivalent to verifying that for all $\sigma \in X_G$,

$$\sigma(t) \equiv 0 \bmod 2^{m+n+1} \quad \Leftrightarrow \quad \sigma \in -\mu_n(x) \cup -\mu_m(y). \tag{III}$$

Fix $\sigma \in X_G$; as above, $\sigma(x) = \alpha 2^n$ and $\sigma(y) = \beta 2^m$. Then,

– If $\sigma(t) = \sigma(x)\sigma(y) = p2^{m+n+1}$, let r, s be the largest integers ≥ 0 such that 2^r divides $\sigma(x)$ and 2^s divides $\sigma(y)$. We have $r + s \geq m + n + 1$; thus, either $r \geq n + 1$ or $s \geq m + 1$, showing that $\sigma \in -\mu_n(x) \cup -\mu_m(y)$.

– If $\sigma \in -\mu_n(x)$, then α must be even, say $\alpha = 2p$. Consequently,

$$\sigma(t) = \sigma(x)\sigma(y) = 2p2^n\beta 2^m = p\beta 2^{n+m+1}.$$

Similarly, if $\sigma \in -\mu_m(y)$, then $\sigma(t)$ is a multiple of 2^{n+m+1}.

b) Lemma 3.3.(c) gives $\mu_n(a_i\mathcal{P}_i) = -\mathcal{HT}_1(\mathcal{P}_i)$. For $1 \leq i \leq p$, set $x_i = \overline{a_i\mathcal{P}_i}$ and $w_i = \alpha_n(x_i)$. Then, $x = \sum_{i=1}^{p} x_i$ and $w = \sum_{i=1}^{p} w_i$. Since M is a homomorphism, we get

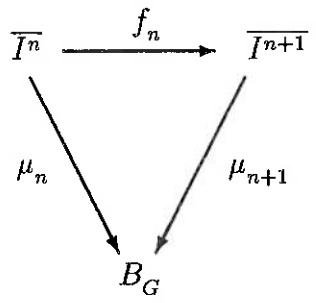
$$M(w) = \textstyle\sum_{i=1}^{p} M(w_i) = \sum_{i=1}^{p} \mu_n(x_i) = \triangle_{i=1}^{p} -\mathcal{HT}_1(\mathcal{P}_i).$$ ◇

The method of proof of Proposition 3.5 will also give

Proposition 3.6 : *Let G be a reduced special group. Then, for all $n \geq 1$,*

a) μ_n is a group homomorphism from $\overline{I^n}$ to B_G, such that $\mu_n(2^{n-1}\langle 1,1\rangle/n) = \top$.

b) The following diagram is commutative :



c) For all $x/n \in \overline{I^n}$ and $y/m \in \overline{I^m}$, $\mu_{n+m}(xy/n+m) = \mu_n(x) \wedge \mu_m(y)$.

d) If $x = \overline{\mathcal{Q}}$ where $\mathcal{Q} = \sum_{i=1}^{p} a_i \mathcal{P}_i$ is a linear combination of Pfister forms of degree n, then

$$\mu_n(x) = \triangle_{i=1}^{p} -\mathcal{HT}_1(\mathcal{P}_i) = (-1)^p \triangle_{i=1}^{p} \mathcal{HT}_1(\mathcal{P}_i).$$

e) G satisfies $[WMC]$ iff for all $n \geq 1$, f_n is injective. $\diamond$

Proposition 3.6 can be used to give an alternative proof of Proposition 3.5.

Proof of Theorem 3.4 : We prove that (I) $M \circ B(\rho) = Id_{B_G}$ and (II) $B(\rho) \circ M = Id_{W(G)}$.

Proof of (I) : Exactly as in the proof of (I) in Theorem 3.1, it is enough to show that for all $a \in G$, $M(\rho(a)) = \varepsilon_G(a)$. But Lemma 3.3.(c) yields

$$M(\rho(a)) = M(\overline{\langle 1,-a\rangle}/1) = \mu_1(\langle 1,-a\rangle) = -\ \mathcal{HT}_1(\langle 1,-a\rangle) = -\varepsilon_G(-a) = \varepsilon_G(a),$$

as needed.

Proof of (II) : For $w \in W(G)$, let x/n be a representative of w, that is, $w = \alpha_n(x/n)$.

Let $\mathcal{Q} = \sum_{i=1}^{p} a_i \mathcal{P}_i$ be a linear combination of Pfister forms of degree n, such that $x = \overline{\mathcal{Q}}$. Let $y = \overline{\mathcal{T}}$, with $\mathcal{T} = \sum_{i=1}^{p} \mathcal{P}_i$. Since $\mathcal{Q} - \mathcal{T} \in I^{n+1}$, $y/n = x/n$. Thus, Lemma 3.3.(c) gives

$$M(w) = \mu_n(x) = \mu_n(y).$$

To prove (II), it is therefore enough to show that $B(\rho)(M(w)) = \alpha_n(y/n)$. For $1 \leq i \leq p$, write $\mathcal{P}_i = \bigotimes_{j=1}^{n} \langle 1, b_{ij}\rangle$, with $b_{ij} \in G$. By Fact 3.2.E,

$$-\ \mathcal{HT}_1(\mathcal{P}_i) = \bigwedge_{i=1}^{n} -b_{ij}.$$

By Proposition 3.5.(b), we have

$$M(w) = \triangle_{i=1}^{p} -\mathcal{HT}_1(\mathcal{P}_i) = \triangle_{i=1}^{p} \bigwedge_{i=1}^{n} -b_{ij}.$$

Now, formula (SG) in Corollary 2.13 yields

$$B(\rho)(M(w)) = B(\rho)(\triangle_{i=1}^{p} \bigwedge_{i=1}^{n} -b_{ij}) = \alpha_n(\overline{\mathcal{T}}/n) = \alpha_n(y/n) = w,$$

ending the proof of Theorem 3.4. $\diamond$

4 The equivalence of Marshall's conjecture to the Weak Marshall conjecture for $\mathcal{AP}$ groups.

We start with a result for reduced special groups.

Theorem 4.1 : *Let G be a reduced special group. The following conditions are equivalent :*

1. *G satisfies $[MC]$.*
2. *For all $n \geq 1$ and for all $\varphi \in I^n$,*

$$\text{If for all } \sigma \in X_G,\ \ \sigma(\varphi) \equiv 0 \bmod 2^{n+1}, \quad \text{then} \quad \varphi \in I^{n+1}.$$

3. *For all $n \geq 1$, $\mu_n : \overline{I^n} \longrightarrow B_G$ is injective.*
4. *G satisfies $[WMC]$.*

Proof : It is clear that 1. $\Rightarrow$ 2.

2. $\Rightarrow$ 1. : Let φ be a form over G such that $\sigma(\varphi) \equiv 0 \bmod 2^n$, for all $\sigma \in X_G$. If $n = 1$, Fact 1 in the proof of Lemma 1.4 tells us that $\varphi \in I$, verifying $[MC]$. So assume that $n \geq 2$. We shall verify by induction that for all $1 \leq k \leq n-1$, $\varphi \in I^{k+1}$. For $k = 1$, since $\varphi \in I$ and $n \geq 2$, we have

$$\forall\, \sigma \in X_G\ (\sigma(\varphi) \equiv 0 \bmod 2^n) \quad \text{implies} \quad \forall\, \sigma \in X_G\ (\sigma(\varphi) \equiv 0 \bmod 4),$$

and so 2. implies $\varphi \in I^2$. Now assume that that $\varphi \in I^k$, for $k \leq n-1$. But then, just as above,

$$\forall\, \sigma \in X_G\ (\sigma(\varphi) \equiv 0 \bmod 2^n) \quad \text{implies} \quad \forall\, \sigma \in X_G\ (\sigma(\varphi) \equiv 0 \bmod 2^{k+1}),$$

and so another application of 2. yields $\varphi \in I^{k+1}$.

2. $\Rightarrow$ 3. : If G verifies 2., suppose that for $x/n \in \overline{I^n}$, we have $\mu_n(x/n) = 0$. This means that for all $\sigma \in X_G$, $\sigma(x) \equiv 0 \bmod 2^{n+1}$ and so 2. guarantees that $x/n \in I^{n+1}$, that is, $x/n = 0$ in $\overline{I^n}$. Since μ_n is a homomorphism (Proposition 3.6.(a)), μ_n must be injective.

3. $\Rightarrow$ 4. : By the commutativity of the diagram in Proposition 3.6.(b), if μ_n is injective for all n, the same is true of all the f_n's. But this is equivalent to $[WMC]$, according to Proposition 3.6.(e).

4. $\Rightarrow$ 2. : For an integer $n \geq 1$, assume that $\varphi \in I^n$ satisfies $\sigma(\varphi) \equiv 0 \bmod 2^{n+1}$, for all $\sigma \in X_G$. Let $w \in W(G)$ be given by $\alpha_n(x/n)$, where $x = \overline{\varphi}$. Then, $M(w) = \perp$ in B_G; since M is injective (Theorem 3.4), we conclude that $w = \perp$ in $W(G)$. Thus, $\alpha_n(x/n) = \perp = \alpha_n(2^{n-1}\langle 1, -1 \rangle)$. By Remark 2.2.(3), there must be $k \geq n$ such that

$$2^{k-n}\varphi - 2^{k-n}2^{n-1}\langle 1, -1 \rangle = 2^{k-n}\varphi - 2^{k-1}\langle 1, -1 \rangle \in I^{k+1}.$$

Thus, $2^{k-n}\varphi \in I^{k+1}$. By Lemma 1.4.(2), $[WMC]$ yields $\varphi \in I^{n+1}$, as needed. $\diamond$

Theorem 4.2 : *If G is an $\mathcal{AP}$ special group, then*

$$G \text{ verifies } [MC] \quad \text{iff} \quad G \text{ verifies } [WMC].$$

Proof : It is readily verified that $[MC]$ implies $[WMC]$.

Now suppose G satisfies $[WMC]$ and φ is a form over G such that $\sigma(\varphi) \equiv 0 \bmod 2^n$, for all σ in X_G. By items (a) and (b) of Lemma 1.5, we conclude that

$$\text{For all } \tau \in X_{G_{red}},\quad \tau(\pi \star \varphi) \equiv 0 \bmod 2^n. \tag{I}$$

Lemma 1.5.(c) guarantees that G_{red} also verifies $[WMC]$, and so by Theorem 4.1, G_{red} satisfies $[MC]$. Thus, (I) implies that $\pi \star \varphi \in I^n(G_{red})$. With the same argument as in the proof of part (c) of Lemma 1.5, there is a linear combination $\mathcal{T}$ of Pfister forms of degree n over G such that $\pi \star \varphi$ is Witt equivalent, in G_{red}, to $\pi \star \mathcal{T}$. By Proposition 2.19 in [DM1], there is $k \geq 0$ such that $2^k\varphi$ is Witt equivalent to $2^k\mathcal{T}$, that is, $2^k\varphi \in I^{n+k}(G)$. Since G verifies $[WMC]$, we get $\varphi \in I^n(G)$, as desired. $\diamond$

Note that a formally real field satisfying $[WMC]$ must be Pythagorean. To see this, it is enough to verify that $G(F)$ is reduced (Fact 1.2.A(c)). Let ψ be a form of dimension $2p$ over $G(F)$, such that 2ψ is hyperbolic. Then, $2\psi \in I^{2p+2}$, and so $[WMC]$ yields $\psi \in I^{2p+1}$. Now the Arason-Pfister Hauptsatz implies that ψ must be hyperbolic. This implies that $G(F)$ is reduced (Proposition 1.6.(e) in [DM1]; see also proof of 2.9.(c)). In spite of this observation, we state the application of our results to fields as

Corollary 4.3 *: A formally real field verifies $[MC]$ iff it verifies $[WMC]$.* $\diamond$

5 Marshall's conjecture for Pythagorean fields

In this section we show that all Pythagorean fields verify Marshall's conjecture (Theorem 5.6).

We start with a result on the K-theory of quadratic extensions. This result is a consequence of Corollary 5.3 in [BT], which in turn comes from Theorem 2.3 in [Mi]. However, since the part that we need has a simple proof, we include it.

Lemma 5.1 *: Let F be a field of characteristic $\neq 2$ and $E = F(d^{1/2})$ be a quadratic extension of F. Let n be an integer ≥ 2. Then, for each $\eta \in k_nE$, there is a finite set of indices I together with $a_1^i, \ldots, a_{n-1}^i \in \dot{F}$ and $b^i \in \dot{E}$, $i \in I$, such that*

$$\eta = \textstyle\sum_{i \in I} l(a_1^i) \ldots l(a_{n-1}^i) l(b^i)$$

Proof : Clearly, it is enough to prove the statement for generators $l(z_1)l(z_2)\ldots l(z_n)$ in k_nE. We show that the result holds for $n = 2$ and a straightforward induction will give the desired conclusion for all $n \geq 2$.

Let $w = a + b\sqrt{d}$ and $z = x + y\sqrt{d}$ be elements of $F(d^{1/2})$, with $a, x \in F$ and $b, y \in \dot{F}$. Then,

Claim : *There are $s, t \in \dot{F}$ such that $sw + tz$ is either* 0 *or* 1.

Proof : We have $w/b - z/y = a/b - x/y = \alpha \in F$. If $\alpha = 0$, we are done, with $s = 1/b$ and $t = -1/y$; if $\alpha \in \dot{F}$, then set $s = 1/\alpha b$ and $t = -1/\alpha y$, to get $sw + tz = 1$.

The Claim and Lemma 2.6.(d) yield

$$0 = l(sw)l(tz) = [l(s) + l(w)][l(t) + l(z)],$$

from which it follows that $l(w)l(z)$ can writen in the desired form. $\diamond$

In section 6 of [Mi], Milnor presents the construction, due to H. Bass and J. Tate, of a graded ring homomorphism from the mod 2 K-theory of a field F to the mod 2 cohomology ring of F. We recall the main points succintly.

For a field F, let F_s be the separable closure of F and G be the Galois group of F_s over F. F_s is a G-module under the operation $x \mapsto \sigma(x)$, for $\sigma \in G$. The exact sequence of G-modules

$$1 \longrightarrow \{\pm 1\} \longrightarrow \dot{F}_s \xrightarrow{(\cdot)^2} \dot{F}_s \longrightarrow 1, \tag{I}$$

leads to a long exact sequence in Galois cohomology (Proposition II.4.4, p. 115 in [Ri]) whose first terms are

$$H^0(G, \dot{F}_s) \xrightarrow{(\cdot)^2} H^0(G, \dot{F}_s) \xrightarrow{\delta} H^1(G, \{\pm 1\}) \longrightarrow H_1(G, \dot{F}_s), \tag{II}$$

where δ is the connecting homomorphism associated to the exact sequence (I). By Hilbert's Theorem 90 (Proposition V.1.2, p. 246 in [Ri]), $H^1(G, \dot{F}_s) = 0$. Moreover, since H^0 is the subgroup of fixed points of the G operation on $\dot{F}_s$, the sequence in (II) yields, with $\mathbf{Z}/2\mathbf{Z}$ in place of $\{\pm 1\}$, the exactness of

$$\dot{F} \xrightarrow{(\cdot)^2} \dot{F} \xrightarrow{\delta} H^1(G, \mathbf{Z}/2\mathbf{Z}) \longrightarrow 0. \tag{III}$$

Since $\dot{F}/\dot{F}^2$ may be identified with k_1F via l, the map $l(a) \in k_1F \mapsto \delta(a) \in H^1(G, \mathbf{Z}/2\mathbf{Z})$ is an isomorphism. We shall conform to standard practice and write (a) for $\delta(a)$. Note that for all $x \in \dot{F}$, $(ax^2) = (a)$ (compare Lemma 2.6.(b)).

By Lemma 6.1 in [Mi], the isomorphism $l(a) \mapsto (a)$ extends to a graded ring homomorphism

$$h^F = (h_n^F)_{n \geq 1} : k_*F \longrightarrow H^*(G, \mathbf{Z}/2\mathbf{Z}),$$

that sends a generator $l(a_1)l(a_2)\ldots l(a_n)$ to $(a_1) \cup (a_2) \cup \ldots \cup (a_n) =_{def} (a_1, \ldots, a_n)$, the cup product of the a_i's in $H^n(G, \mathbf{Z}/2\mathbf{Z})$.

To simplify exposition, write $H^n(F)$ for $H^n(G, \mathbf{Z}/2\mathbf{Z})$ and $H^*(F)$ for $H^*(G, \mathbf{Z}/2\mathbf{Z})$.

At the end of 1995, V. Voevodsky announced the proof of

Theorem 5.2 *(Theorem 1.1 in [V]) : If F is a field of characteristic $\neq 2$, then h_n^F is an* **isomorphism**, *for all $n \geq 1$.* ◇

Among the many consequences of this beautiful result, we register

Corollary 5.3 *: Let F be a field of characteristic $\neq 2$. Then*

a) $H^*(F)$ is generated, as a graded ring, by $H^1(F)$, that is, for all $n \geq 1$, if $\eta \in H^n(F)$, there is a finite set of indices J and elements $a_1^j, \ldots, a_n^j \in \dot{F}$ such that

$$\eta = \textstyle\sum_{j \in J} (a_1^j, \ldots, a_n^j)$$

b) Let $E = F(d^{1/2})$ be a quadratic extension of F. Then, for all $n \geq 1$ and all $\beta \in H^n(E)$, there is a finite set of indices I together with $a_1^i, \ldots, a_{n-1}^i \in \dot{F}$ and $b^i \in \dot{E}$, $i \in I$, such that

$$\beta = \textstyle\sum_{i \in I} (a_1^i, \ldots, a_{n-1}^i, b^i).$$

Proof : Item 1 follows directly from the fact that h_n^F is an isomorphism and that every element in k_nF is a sum of generators of the type $l(a_1)l(a_2)\ldots l(a_n)$, taken by h_n^F to $(a_1, \ldots, a_n)$ in $H^n(F)$. Item 2 follows from Lemma 5.1 and the fact that h_n^E is an isomorphism. ◇

We now prove

Proposition 5.4 *: Let F be a Pythagorean field. Then, $(-1) \cup (\cdot) : H^n(F) \longrightarrow H^{n+1}(F)$ is an injection, for all $n \geq 1$.*

Proof : Let $E = F(d^{1/2})$ be a quadratic extension of F. By Corollary 4.6 in [A], there is a long exact sequence of mod 2 cohomology, which for each $n \geq 0$ consists of

$$\cdots H^n(F) \xrightarrow{Res} H^n(E) \xrightarrow{Cor} H^n(F) \xrightarrow{\mu} H^{n+1}(F) \xrightarrow{Res} \cdots, \qquad (Q)$$

where μ stands for cup product with (d), while *Res* and *Cor* are the restriction and corestriction maps in Galois cohomology , respectively. We have (see paragraph before Theorem 4.1 and paragraphs before Theorem 4.4 in [A]) :

1. With the identification originating from the sequence (III) above, $Res : H^1(F) \longrightarrow H^1(E)$ is given, for each $a \in \dot{F}$, by $(a) \mapsto (a)$;

2. The corestriction $Cor : H^1(E) \longrightarrow H^1(F)$ is given, for each $b \in \dot{E}$, by $(b) \mapsto (N_{E/F}(b))$, where $N_{E/F}$ is the field norm, that is, if $b = x + y\sqrt{d}$, then $N_{E/F}(b) = x^2 - y^2 d \in \dot{F}$.

Moreover, the maps *Res* and *Cor* have the following properties :

3. For $\eta \in H^p(F)$ and $\zeta \in H^q(F)$, $Res(\eta \cup \zeta) = Res(\eta) \cup Res(\zeta)$.

(Proposition III.7.3, p. 191 in [Ri] or § 2.6.(a), p. I-14 in [S]).

4. For $\eta \in H^p(F)$ and $\zeta \in H^q(E)$, $Cor(Res(\eta) \cup \zeta) = \eta \cup Cor(\zeta)$.

(See paragraph before Theorem 4.4 in [A], Proposition III.7.5, p. 192 in [Ri], or § 2.6.(a), p. I-14 in [S]).

For $\beta \in H^n(E)$, we may write, by Corollary 5.3.(b),

$$\beta = \textstyle\sum_{i \in I} (a_1^i, \ldots, a_{n-1}^i, b^i),$$

with $a_k^i \in \dot{F}$, for $1 \leq k \leq n-1$ and all $i \in I$. Write $\eta_i = (a_1^i, \ldots, a_{n-1}^i)$ Then, recalling items 1., 2., 3. and 4. above

$$\begin{aligned} Cor(\beta) &= Cor(\textstyle\sum_{i \in I} \mathrm{Res}(\eta_i) \cup b^i) = \sum_{i \in I} Cor(Res(\eta_i) \cup b^i) \\ &= \textstyle\sum_{i \in I} \eta_i \cup Cor(b^i) = \sum_{i \in I} \eta_i \cup (N_{E/F}(b^i)). \end{aligned}$$

Now notice that if $d = -1$, then, for each $i \in I$, $N_{E/F}(b^i)$ is a non-zero sum of squares in F. Since F is Pythagorean, there is $x_i \in \dot{F}$ such that $N_{E/F}(b^i) = x_i^2$, for all $i \in I$. But, for each $i \in I$, we have $(x_i^2) = (1)$, the zero of $H^1(F)$. It follows that *Cor* is the zero map from $H^n(E)$ to $H^n(F)$. Now, the exactness of the sequence (Q) yields that cup product with (-1) is an injection from $H^n(F)$ to $H^{n+1}(F)$, as claimed. $\diamond$

Recall that in section 2 we defined the homomorphisms $\omega_n : k_n F \longrightarrow k_{n+1} F$, consisting of multiplying by $l(-1)$. It is clear from the above considerations that the following diagram is commutative, for all $n \geq 1$:

$$\begin{array}{ccc} k_n F & \xrightarrow{\omega_n} & k_{n+1} F \\ {\scriptstyle h_n^F}\downarrow & & \downarrow{\scriptstyle h_{n+1}^F} \\ H^n(F) & \xrightarrow[\mu]{} & H^{n+1}(F) \end{array}$$

where μ is cup product by (-1). Thus, Theorem 5.2 and Proposition 5.4 yield

Corollary 5.5 : *$k_nF \xrightarrow{\omega_n} k_{n+1}F$ is injective, for all Pythagorean fields F and all $n \geq 1$.* $\diamond$

We now prove

Theorem 5.6 : *Every Pythagorean field verifies $[MC]$.*

Proof : In section 4 of [Mi], Milnor constructs, for each $n \geq 1$, a group homomorphism $s_n : k_nF \longrightarrow I^n/I^{n+1} = \overline{I^n}$, that sends a generator $l(a_1)l(a_2)\ldots l(a_n)$ to the class of the Pfister form $\otimes_{i=1}^{n} \langle 1, -a_i \rangle$ modulo I^{n+1}.

Since the ω_n are injective for all n, it follows from Remark 4.2 in [Mi] that s_n is an isomorphism, for all $n \geq 1$. Now notice that, for each $n \geq 1$, the following diagram is commutative :

$$\begin{array}{ccc} k_nF & \xrightarrow{\omega_n} & k_{n+1}F \\ {\scriptstyle s_n}\downarrow & & \downarrow{\scriptstyle s_{n+1}} \\ \overline{I^n} & \xrightarrow[f_n]{} & \overline{I^{n+1}} \end{array}$$

where f_n is multiplication by $2 = \langle 1, 1 \rangle$, as in section 2. Corollary 5.5 and the fact that the s_n's are bijective imply that f_n is injective for all n, i.e., F satisfies $[WMC]$. But then Theorem 4.1 (or Corollary 4.3) guarantees that F verifies $[MC]$. $\diamond$

For a Pythagorean field F, let $B(F)$ be the Boolean hull of $G(F)$ as in Remark 2.10. For each $n \geq 1$, write $B(F)(n)$ for the subgroup of $B(F)$ (under $\triangle$), generated by the meets of at most n elements of $G(F)$. We can then state

Corollary 5.7 : *Let F be a Pythagorean field. Then, for all integers $n \geq 1$,*

a) The homomorphism ε_n of Theorem 2.11 is an isomorphism from k_nF onto $B(F)(n)$.

b) The homomorphism μ_n of Proposition 3.6 is an isomorphism from $\overline{I^n}$ onto $B(F)(n)$.

c) $H^n(F)$ is isomorphic to $B(F)(n)$.

Proof : a) It follows from the construction of ε_n that its image is $B(F)(n)$. With notation as in sections 2 and 3, we have a commutative diagram

$$\begin{array}{ccc} k_nF & \xrightarrow{\beta_n} & k(F) \\ & {\scriptstyle \varepsilon_n}\searrow \quad \swarrow{\scriptstyle \varepsilon} & \\ & B(F) & \end{array}$$

Now, each β_n is injective, because the same is true of each ω_n (Corollary 5.5). Since ε is an isomorphism (Theorem 3.1), we conclude that ε_n is also injective, as asserted.

b) By Facts 3.2.D and E and Proposition 3.6.(d), the image of μ_n is precisely $B(F)(n)$. But Theorems 5.6 and 4.1.(3) tell us that μ_n is injective for all $n \geq 1$.

c) Clear, by Theorem 5.2 and item (b). ◇

In [AEJ] the question was raised of characterizing, for a Pythagorean field F and a given integer $n \geq 1$, the kernel of the "total signature" map :

$$\tau : I^n(F) \longrightarrow \prod_{\sigma \in \chi(F)} \overline{I^n}(F_\sigma),$$

given by :

$$\tau(\varphi) = \langle \varphi \otimes F_\sigma / I^{n+1}(F_\sigma) \ : \ \sigma \in \chi(F) \rangle,$$

where $\chi(F)$ is the space of orders of F, and F_σ denotes the real closure of $\langle F, \sigma \rangle$. Marshall's conjecture for F obviously entails that $\ker(\tau) = I^{n+1}(F)$, proving this "local-global" principle as well. Thus, Theorem 5.2 implies that it also holds for the graded cohomology ring of F.

References

[A] J. Kr. Arason, *Cohomologische Invarianten quadratischer Formen*, J. Algebra, **36**, 448-491 (1975).

[AEJ] J. Kr. Arason, R. Elman, B. Jacob, *On Quadratic Forms and Galois Cohomology*, Rocky Mountain Journal Math. **19**, 575 - 588 (1989).

[BT] H. Bass, J. Tate, *The Milnor ring of a global field*, in **Algebraic K-Theory II**, Lecture Notes in Math., **342**, 349 - 446, Springer Verlag, 1973.

[D] M. Dickmann, *Anneaux de Witt abstraits et groupes speciaux*, Séminaire de Structures Algébriques Ordonnées, 1991-92, (F. Delon, M. Dickmann, D. Gondard, eds.), Paris VII-CNRS Logique, Prépublications **42**, 1993.

[DM1] M. Dickmann, F. Miraglia, *Special Groups, application of boolean algebras to the theory of quadratic forms*, October 1996, submitted.

[DM2] M. Dickmann, F. Miraglia *Algebraic K-theory and Special Groups*, preprint, March 1996.

[EL 1] R. Elman, T. Y. Lam, *Pfister forms and K-theory of fields*, J. Algebra **23**, 181-213 (1972).

[EL 2] R. Elman, T. Y. Lam, *Quadratic forms over formally real and pythagorean fields*, Amer. J. Math. **94**, 1155-1194 (1972).

[HBA] **Handbook of Boolean Algebras**, vol.1 by S. Koppelberg, (J. Donald Monk, R. Bonnet, eds.), North-Holland Publ. Co., Amsterdam, 1989.

[L 1] T. Y. Lam, **The Algebraic Theory of Quadratic Forms**, W.A.Benjamin, Mass., 1973.

[L 2] T. Y. Lam, **Ten Lectures on Quadratic Forms over Fields**, in Conf. on Quadratic Forms (G. Orzech, ed.), Queen's Papers on Pure and Applied Math. **46**, Queen's University, Ontario, Canada, 1 - 102, 1977.

[Li] A. Lira de Lima, *Les Groupes Spéciaux*, Doctoral dissertation, University of Paris VII, 1995.

[Ma] M. Marshall, *A reduced theory of quadratic forms*, in Conf. on Quadratic Forms (G. Orzech, ed.), Queen's Papers on Pure and Applied Math. **46**, Queen's University, Ontario, Canada, 569 - 579, 1977.

[Mi] J.Milnor, *Algebraic K-theory and Quadratic Forms*, Inventiones Math. **9** (1970), 318-344.

[Ri] L. Ribes, **Introduction to Profinite Groups and Galois Cohomology**, Queen's Papers in Pure and Applied Math. **24**, Queen's University, Ontario, 1970.

[S] J. P. Serre, **Cohomologie Galoisienne**, Lecture Notes in Math. **5**, Springer-Verlag, 3rd edition, 1965.

[V] V. Voevodsky, *List of Results*, preprint of november 1995, distributed by e-mail.

M. Dickmann
Equipe de Logique Mathématique
U.R.A. 753
2, Place Jussieu – Case 7012
75251 PARIS CEDEX 05, France
e-mail : dickmann@logique.jussieu.fr

F. Miraglia
Instituto de Matemática e Estatística
Universidade de São Paulo
C. P. 66.281 (Ag. Cidade São Paulo)
05389-970 S.Paulo, S.P., Brasil
e-mail : miraglia@ime.usp.br

Prépublications de l'Equipe de Logique.

N° 1 **D. Lascar.**
Les beaux automorphismes, janvier 1990.

N° 2 **F. Delon, M. A. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques Ordonnées (1988-89), janvier 1990.

N° 3 **J.-L. Krivine.**
Opérateurs de mise en mémoire et traduction de Gödel, janvier 1990.

N° 4 **M. Giraudet.**
Groupes à moitié ordonnés. Première partie : Présentation axiomatique des groupes de permutations monotones de chaînes, février 1990.

N° 5 **M. Giraudet** et **F. Lucas.**
Groupes à moitié ordonnés. Deuxième partie : Sous-groupes de groupes à moitié réticulés, février 1990.

N° 6 **C. Michaux.**
Ordered rings over which output sets are recursively enumerable sets, février 1990.

N° 7 **V. Danos.**
Lambda-calculus and its dynamic algebra 1 : basic results, février 1990.

N° 8 **L. Régnier**
A propos de l'équivalence opérationnelle, avril 1990.

N° 9 **Ch. Berline.**
Rétractions et interprétation interne du polymorphisme : Le problème de la rétraction universelle, mai 1990.

N° 10 **D. Gondard-Cozette.**
Axiomatisations simples des théories des corps de Rolle, mai 1990.

N° 11 **A. Fleury** et **C. Rétoré.**
The MIX rule : a proofnet syntax for multiplicatives, their units and $(A\otimes B)$-0$(A\&B)$, septembre 1990.

N° 12 **P. Malacaria** et **L. Régnier.**
Lambda-calculus and its dynamic algebra 3 : Weak Nilpotency, septembre 1990.

N° 13 **D. Lascar.**
Les automorphismes d'un ensemble fortement minimal, octobre 1990.

N° 14 **D. Gluschankof** et **M. Tilli.**
On some extension theorems in functional analysis and the theory of boolean algebras, novembre 1990.

N° 15 **U. Gropp.**
There is no sharp transitivity on q^6 when q is a type of Morley rank 2, décembre 1990.

N° 16 **M.A. Dickmann.**
A combinatorial geometric structure on the space of orders of a field, décembre 1990.

N° 17 **F. Delon, M. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques Ordonnées 1989-90, décembre 1990.

N° 18 **J.-Y. Girard.**
Logic and exceptions : A few remarks, décembre 1990.

N° 19 **J.-Y. Girard.**
Quantifiers in linear logic II, janvier 1991.

N° 20 **T. Jech.**
Singular cardinal problem : Shelah's theorem on $2^{\aleph_\omega}$, janvier 1991.

N° 21 **G. Amiot.**
Sémantique des phases de la Logique Linéaire du second ordre, février 1991.

N° 22 **T. Ehrhard, P. Malacaria.**
Stone duality for stable functions, février 1991.

N° 23 **Z. Chatzidakis, L. van den Dries, A. Macintyre.**
Definable sets over finite fields, mars 1991.

N° 24 **J.-Y. Girard.**
A new constructive logic : classical logic, mai 1991.

N° 25 **P. Rozière.**
Règles admissibles en calcul propositionnel intuitionniste, mai 1991.

N° 26 **J.-Y. Girard.**
On the unity of logic, juin 1991.

N° 27 **S. Kuhlmann.**
Quelques propriétés des espaces vectoriels valués en théorie des modèles, juin 1991.

N° 28 **U. Gropp.**
Action d'un groupe ω-stable sur un ensemble de rang de Morley 2, juin 1991.

N° 29 **A.A. Voronkov.**
On completeness of program synthesis systems, juin 1991.

N°30 **D. Gondard-Cozette.**
Sur les ordres de niveau 2^n et sur une extension du 17ème problème de Hilbert, octobre 1991.

N°31 **P. Michel.**
Busy Beaver Competition and Collatz-like Problems, janvier 1992.

N° 32 **F. Delon, M. A. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques Ordonnées (1990-91), janvier 1992.

N° 33 **M. A. Dickmann, K. Keimel** (eds).
Workshop « PROCOPE » - Paris, 8-10 novembre 1990, janvier 1992.

N° 34 Comptes-Rendus au Colloque Franco-Exsoviétique de Théorie des Modèles C.I.R.M., 27 janvier-1er février 1992, mai 1992.

N° 35 **J.-B. Joinet.**
Une preuve combinatoire de forte normalisation (du fragment multiplicatif et exponentiel) des réseaux de preuves pour la logique linéaire (PN1), mai 1992.

N° 36 **E. Bouscaren** et **E. Hrushovski.**
Interpreting groups in stable one-based theories, mai 1992.

N° 37 **F. Miraglia** et **U. Solitro.**
Sheaves over right side indempotent Quantales, juin 1992.

N° 38 **Ch. Berline.**
λ-calcul, systèmes de typages et modélisations, octobre 1992.

N° 39 **F. Métayer.**
Homology of Proof-nets, octobre 1992.

N° 40 **J.-L. Krivine.**
Classical logic, storage operators and second order lambda-calculus, décembre 1992.

N° 41 **V. Danos, J.-B. Joinet** et **H. Schellinx.**
On the Linear Decoration of Intuitionistic Derivations, janvier 1993.

N° 42 **F. Delon, M.A. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques ordonnées (1991-92), février 1993.

N° 43 **Z.I. Abud** et **F. Miraglia.**
The Measurability of Pettis integrable Functions and Applications, février 1993.

N° 44 **X. Gouy** et **Y. Jiang.**
Universal retractions on DI-domains, juin 1993.

N° 45 **C. Zylberajch.**
A model-theoretic method to prove ease in lambda-calculus (Types, Models, Ease), juin 1993.

N° 46 **S. Malecki.**
A survey about polymorphic type systems from the typability point of view, juin 1993.

N° 47 **C. Rétoré.**
Graph theory from linear logic : AGREGATES, octobre 1993.

N° 48 **M.R. Darnel, M. Giraudet, S.J. McCleary.**
Uniqueness of the group operation on the lattice of order-automorphisms of the real line, décembre 1993.

N° 49 **F. Delon, M.A. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques Ordonnées (1992-93), février 1994.

N° 50 **Ch. Berline** et **K. Grue.**
A simple semantic consistency proof for Map Theory based on ξ-denotational semantics, septembre 1994.

N° 51 **V. Danos, J.-B. Joinet** et **H. Schellinx.**
LKQ and LKT : Sequent calculi for second order logic based upon dual linear decompositions of classical implication, octobre 1994.

N° 52 **V. Danos, J.-B. Joinet et H. Schellinx.**
A new deconstructive logic : linear logic, octobre 1994.

N° 53 **L. Tortora de Falco.**
Strong normalisation property for heterostytle $Lk^{t;q}$ and Free Deduction, décembre 1994.

N° 54 **F. Delon, M.A. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques Ordonnées (1993-94), février 1995.

N° 55 **M. Dickmann et F. Miraglia.**
SPECIAL GROUPS. Applications of Boolean algebras to the theory of quadratic forms, mars 1995.

N° 56 **F. Delon, M.A. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques Ordonnées (1994-95), janvier 1996.

N° 57 **M. Giraudet** et **J. Rachùnek.**
Varieties of half lattice-ordered groups of monotonic permutations of chains.

N° 58 **Z. Chatzidakis et E. Hrushovski.**
Model theory of difference fields.

N° 59 **Z. Chatzidakis.**
Théorie des modèles des corps finis et pseudo-finis.

N° 60 **M. Dickmann et F. Miraglia.**
On forms whose total signature is zero mod 2^n. Solution to a problem of M. Marshall, février 1997.

N° 61 **F. Delon, M.A. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques Ordonnées (1995-96), février 1997.

Certaines prépublications d'articles par des membres de l'Equipe de Logique Mathématique sont aussi disponibles à:

Some preprints of papers by members of the Equipe de Logique Mathématique are also electronically available at:

`http://www.logique.jussieu.fr`