PACIFIC JOURNAL OF MATHEMATICS
Vol. 93, No. 1, 1981

FANS, REAL VALUATIONS, AND HEREDITARILY-PYTHAGOREN FIELDS

BILL JACOB

In this paper we give an explicit description of valuation rings compatible with certain infinite preprimes of a field. These results are essentially constructive versions of the results of L. Brocker and E. Becker relating fans and valuations. We discuss a number of examples in detail, including the higher orderings recently introduced by E. Becker. One of several applications is a generalization of the theorem of Brocker-Brown charactorizing superpythagorean fields.

1. The main theorem. We begin by introducing the main definitions and notation of this subject. Let K be any field.

DEFINITION 1. (Harrison [7].) If $P \subseteqq K$ satisfies $-1 \notin P$, $P + P \subseteqq P$, $P \cdot P \subseteqq P$, then P called a *preprime* of K. In case $1 \in P$, P is called an *infinite* preprime of K. The maximal preprimes of K are called the Harrison primes of K.

Harrison primes were introduced as a possible generalization to arbitrary fields of the notion of a "prime" that arises in algebraic number fields. Throughout this paper we shall be concerned only with infinite preprimes. Following E. Becker [1], [2], [3] we give:

DEFINITION 2. An infinite preprime P is called a *preordering* if $P^{\cdot} = P - \{0\}$ is a subgroup of $K^{\cdot}$. A preordering P is called a *fan*, if whenever $U \subseteqq K^{\cdot}$ is a subgroup with $P^{\cdot} \subseteqq U$ and $-1 \notin U$, $U \cup \{0\}$ is a preorder of K. Finally, a preorder P is said to be *complete* if whenever $a^2 \in P$ it happens that $a \in P$ or $-a \in P$.

In [1], [2], [3] Becker shows that in many cases complete preorderings give rise to valuation rings. Very often, these complete preorderings are not Harrison primes. Thus it becomes interesting to know precisely when a preprime induces a valuation on a field. With this in mind we give:

DEFINITION 3. A preordering P is called a *strong fan* if whenever $a \notin \pm P$ it happens that $1 + a \in P \cup a \cdot P$. We shall call a strong fan P a *valuation fan* if in addition, whenever $a \notin \pm P$ but $1 + a \in P$, then $1 - a \in P$.

Finally, one more definition:

DEFINITION 4. A valuation ring $O \subsetneqq K$, with maximal ideal I, is said to be *compatible* with an infinite preprime P if $1 + I \subseteqq P$.

We now give the main result of this section:

THEOREM 1. *An infinite preprime P is a valuation fan only if there is a valuation ring $O \subsetneqq K$ compatible with P for which $\bar{P}^{\cdot} = P^{\cdot}/I$ is the positive cone of a linear order of the residue field $O/I = \bar{K}$.*

Proof. First, let P be an infinite preprime, and assume such a valuation ring O exists. Suppose $a \notin \pm P$. Then as $P^{\cdot}/I$ is the positive cone of a linear of O/I, we see that a cannot be a unit of O. Thus as either $a \in I$ or $a^{-1} \in I$, we have by compatibility that $1 + a \in P$ or $1 + a^{-1} \in P$. From this we that $1 + a \in P \cup aP$. We also see that in case $1 + a \in P$, we must have that $a \in I$, so that as $-a \in I$ we have $1 - a \in P$. This shows that P is a valuation fan.

Conversely, we now assume that P is a valuation fan. For $x \in K^{\cdot}$ we shall denote by $[x]$ the coset of x in $K^{\cdot}/P^{\cdot}$. It follows that whenever $x, y \in K^{\cdot}$ are such that $[x] \neq -[y]$, it happens that $[x + y] = [x]$ or $[x + y] = [y]$. We also see that if $[x] \neq \pm[y]$, then $[x + y] = [x]$ if and only if $[x - y] = [x]$.

Next we define $O_1(K, P) = \{x \in K^{\cdot} : [x] \neq \pm P^{\cdot} \text{ but } [1 + x] = P^{\cdot}\}$, and $O_2(K, P) = \{x \in K^{\cdot} : [x] = \pm P^{\cdot} \text{ and } x \cdot O_1(K, P) \subseteqq O_1(K, P)\}$. Our task is to show that $O(K, P) = O_1(K, P) \cup O_2(K, P) \cup \{0\}$ is the desired valuation ring of K. We now check many facts:

(1) $\qquad x \in O(K, P)$ if and only if $-x \in O(K, P)$.

Proof. As P is a valuation fan we clearly have that $x \in O_1(K, P)$ if and only if $-x \in O_1(K, P)$. It now immediately follows by the definition of $O_2(K, P)$, that $x \in O_2(K, P)$ if and only if $-x \in O_2(K, P)$.

(2) If $[x] \neq \pm P^{\cdot}$, then $x \in O_1(K, P)$ if and only if $x^{-1} \notin O_1(K, P)$.

Proof. Note that $x \in O_1(K, P)$ if and only if $[1 + x] = P^{\cdot}$ if and only if $[1 + x^{-1}] = x^{-1}P$ if and only if $x^{-1} \notin O_1(K, P)$.

(2′) $\qquad$ If $[x] = P^{\cdot}$, then at least one of $x, x^{-1} \in O_2(K, P)$.

Proof. Suppose we have $z, w \in O_1(K, P)$ such that $xz, x^{-1}w \notin O_1(K, P)$. Then $[1 + xz] = [xz]$ and $[1 + x^{-1}w] = [x^{-1}w]$ so that $[x + w] = [w]$. Thus, $[1 + xz + x + w] = [xz]$ or $[w]$. But note that $[(1 + w) + x(1 + z)] = P^{\cdot}$ as both $z, w \in O_1(K, P)$. This contradiction gives (2′).

(3) Suppose that $x, y \in O_1(K, P)$, and that $[xy] \neq \pm P^\cdot$. Then $xy \in O_1(K, P)$.

Proof. We have that $[1 + x] = [1 - y] = P^\cdot$. Thus $[(1 + x) - x(1 - y)] = P^\cdot$ or $-[x]$. But as $[y] \neq -P^\cdot$, $[xy] \neq -[x]$. It follows that $[1 + xy] = P^\cdot$.

(4) Suppose that $x, y \in O_1(K, P)$ and that $[xy] = P^\cdot$. Then $xy \in O_2(K, P)$.

Proof. Let $z \in O_1(K, P)$. In view of (1), replacing z by $-z$ if necessary, we may assume that $[z] \neq -[x]$, $-[y]$. It then follows that $[x(1 + y) + y(1 + z) + z(1 + x)] = [x]$, $[y]$, or $[z]$. But further, as $[(1 + x)(1 + y)(1 + z)] = [1 + xyz + x + y + z + xy + yz + xz] = P^\cdot$, subtraction yields that $[1 + xyz] = P^\cdot$, $-[x]$, $-[y]$, or $-[z]$. As $[xyz] = [z] \neq -[x]$, $-[y]$, $-[z]$, we see that $[1 + xyz] = P^\cdot$, which proves (4).

(5) $O(K, P)$ is closed under multiplication.

Proof. (i) If $x, y \in O_1(K, P)$ then $x \cdot y \in O(K, P)$ follows from (3) and (4).

(ii) If $x \in O_1(K, P)$ and $y \in O_2(K, P)$, then $xy \in O_1(K, P)$ follows immediately from the definition of $O_2(K, P)$.

(iii) If $x, y \in O_2(K, P)$, then for any $z \in O_1(K, P)$ we have that $yz \in O_1(K, P)$, and hence that $xyz \in O_1(K, P)$. It follows that $xy \in O_2(K, P)$.

(6) If $[x] \neq \pm P^\cdot$, and either $[2 + x] = P^\cdot$ or $[4 + x] = P^\cdot$, then $[1 + x] = P^\cdot$.

Proof. First suppose that $[2 + x] = P^\cdot$, but $[1 + x] = [x]$. Then as $[1 + (1 + x)] = P^\cdot$, we have that $[1 - (1 + x)] = P^\cdot$, clearly a contradiction. Thus if $[2 + x] = P^\cdot$, it happens that $[1 + x] = P^\cdot$. Next suppose that $[4 + x] = P^\cdot$, but $[2 + x] = [x]$. As above we have that $[2 + (2 + x)] = P^\cdot$, so that $[2 - (2 + x)] = P^\cdot$, a contradiction which proves (6).

(7) If $x, y \in O_1(K, P)$ and $[x + y] \neq \pm P^\cdot$, then $x + y \in O_1(K, P)$.

Proof. As $[1 + x] = [1 + y] = P^\cdot$, we have that $[1 + x + 1 + y] = P^\cdot$, so that $[1 + (x + y)] = P^\cdot$ by (6).

(8) If $x, y \in O_1(K, P)$ and $[x + y] = P^\cdot$, then $x + y \in O_2(K, P)$.

Proof. As $[x] \neq \pm P^{\cdot}$, $[y] \neq \pm P^{\cdot}$, but $[x+y] = P^{\cdot}$, we must have that $[x] = [-y]$. Let $z \in O_1(K, P)$. Replacing z by $-z$ if necessary we may assume that $[z] \neq [-x]$. Then we have $P^{\cdot} = [(1+x)(1+z) + (1-y)(1-z)] = [2 + (x+y)z + (x-y)]$. As $[x-y] = [x]$, subtraction gives $[2+(x+y)z] = P^{\cdot}$ or $-[x]$. As $[(x+y)z] \neq -[x]$, we conclude that $[2+(x+y)z] = P^{\cdot}$, so that by (6), $[1+(x+y)z] = P^{\cdot}$, proving (8).

(9) If $x \in O_2(K, P)$, $y \in O_1(K, P)$, then $x + y \in O(K, P)$.

Proof. We may assume that $[x] = P^{\cdot}$. First suppose that $[x+y] = [x]$. Let $z \in O_1(K, P)$. Then $P^{\cdot} = [1+xy] = [1+xz] = [(1+y)(1+z)]$ implies that $P^{\cdot} = [1 + xy + 1 + xz + (1+y)(1+z)] = [3 + (x+y)z + z + y + xy]$. We may assume that $[z] \neq [-y]$. Then subtraction shows that $[3+(x+y)z] = P^{\cdot}$, $[-z]$ or $[-y]$. But as $[(x+y)z] \neq [-z]$ or $[-y]$, we have $[3+(x+y)z] = P^{\cdot}$, so by (6) $x + y \in O_2(K, P)$.

Secondly, suppose that $[x+y] = [y]$. As $[1+y] = P^{\cdot}$, we have that $[1+y+x] = P^{\cdot}$, so that $x + y \in O_1(K, P)$.

(10) If $x, y \in O_2(K, P)$, then $x + y \in O(K, P)$.

Proof. Suppose that $[x+y] = \pm P^{\cdot}$ Then for $z \in O_1(K, P)$ we have $[1+xz] = [1+yz] = P^{\cdot}$, so by (6), $x + y \in O_2(K, P)$.

Next suppose that $[x+y] \neq \pm P^{\cdot}$. If $x + y \notin O_1(K, P)$, then by (2), $(x+y)^{-1} \in O_1(K, P)$. But now as x^2, xy, $y^2 \in O_2(K, P)$ we have that $[1 + x^2(x+y)^{-1}] = [1 + xy(x+y)^{-1}] = [1 + y^2(x+y)^{-1}] = P^{\cdot}$. Thus $[4 + (x^2 + 2xy + y^2)(x+y)^{-1}] = P^{\cdot}$, from which it follows by (6) that $[1 + (x+y)] = P^{\cdot}$. This proves (10).

We have now shown that $O(K, P)$ is a valuation subring of K. It is clear by (2) that if x is a unit of $O(K, P)$ then $x \in P \cup -P$. Further, let $x, y \in P^{\cdot}$ be units of $O(K, P)$. Then for any $z \in O_1(K, P)$ we have that $[x+z] = [y+z] = P^{\cdot}$. Thus we have $[(x+y) + 2z] = P^{\cdot}$, from which it follows that $[(x+y)+z] = P^{\cdot}$. In particular $x + y$ is a unit of $O(K, P)$. We thus have: $\bar{P} \cap -\bar{P} = \{0\}$, $\bar{K} = \bar{P} \cup -\bar{P}$, $\bar{P} + \bar{P} \subseteq \bar{P}$, and $\bar{P} \cdot \bar{P} \subseteq \bar{P}$. Hence $\bar{P}^{\cdot}$ is the positive cone of a linear order of $\bar{K}$.

Finally we must see that $O(K, P)$ is compatible with P. If $x \in O_1(K, P)$, then $1 + x \in P^{\cdot}$, by the definition of $O_1(K, P)$. Assume that $x \in O_2(K, P)$ is not a unit. If $[x] = P^{\cdot}$, then clearly $1 + x \in P^{\cdot}$. If $[x] = -P^{\cdot}$, then let $y \in O_1(K, P)$ be such that $[-x+y] = [y]$. Then as $[(1+x) + (-x+y)] = P^{\cdot}$, we conclude that $[1+x] = P^{\cdot}$ or $[-y]$. As $1 + x$ is a unit of $O(K, P)$ we have that $[1+x] = P^{\cdot}$. This proves Theorem 1. □

The following is an immediate consequence of Theorem 1.

COROLLARY 1. *A field K is formally real if and only if K has a valuation fan.* □

REMARK 1. It is clear that every strong fan is a fan. E. Becker has also recently proved that the converse is also true. However, as this result depends upon the nonconstructive results of his paper [3], we omit a discussion of this result here.

2. Examples. Let $P \subseteqq K$ be a strong fan. We define $R(P, K) = \{x \in K^{\cdot} : \exists\, p \in P^{\cdot} \text{ with } [1 + px] = P^{\cdot} \text{ and } [1 - px] \neq P^{\cdot}\}$. We have:

LEMMA 1. *If $x, y \in R(P, K)$, then either $x \in \pm P^{\cdot}$, $y \in \pm P^{\cdot}$, or $xy \in \pm P^{\cdot}$.*

Proof. Assume to the contrary. Then for some $x, y \in K^{\cdot}$, $p_1, p_2 \in P^{\cdot}$, we have that $[1 + p_1x] = [1 + p_2y] = P^{\cdot}$, $[1 - p_1x] = [-x]$, $[1 - p_2y] = [-y]$, with $[x]$, $[y]$, $[xy] \neq \pm P^{\cdot}$. But then as $[1 - (p_1x)^2] = [-x]$, $[(p_1x)^2 - (p_1xp_2y)^2] = [-x^2y]$ we conclude that $[1 - (p_1x)^2 + (p_1x)^2 - (p_1xp_2y)^2] = [1 + p_1p_2xy][1 - p_1p_2xy] = [-x]$ or $[-x^2y]$. But as $[1 + p_1p_2xy] = P^{\cdot}$ or $[xy]$, and $[1 - p_1p_2xy] = P^{\cdot}$ or $[-xy]$ we have a contradiction which proves the lemma. □

We next see that whenever one has strong fan, one can easily find a valuation fan.

LEMMA 2. *If $P \subseteqq K$ is a strong fan, then either P is a valuation fan, or for any $x \in R(P, K) - \pm P^{\cdot}$, $P \cup x \cdot P$ is a valuation fan.*

Proof. In case $R(P, K) \subseteqq \pm P^{\cdot}$, than as $1 \in P$, we see immediately that P is a valuation fan. Now let $x \in R(P, K) - \pm P^{\cdot}$. It is easy to see that $P \cup x \cdot P$ is a strong fan. Now suppose that $y \notin \pm P \cup \pm x \cdot P$. Then by Lemma 1, $y \notin R(P, K)$. Thus if $[1 + y] = P$, we must have that $[1 - y] = P$. Also, as P is a strong fan, we note that $[1 + y] = x \cdot P$ is impossible. This shows that $P \cup x \cdot P$ is a valuation fan. □

In [1], [2], [3] the valuations compatible with complete fans are studied. Along these lines we give:

LEMMA 3. *Let $P \subseteqq K$ be a complete strong fan. Then P is a valuation fan.*

Proof. Suppose that $x \notin \pm P$. Then as P is complete, $x^2 \notin P$.

Thus if $[1 + x] = P^{\cdot}$, we must also have that $[1 - x] = P^{\cdot}$, for otherwise $[1 - x^2] = [1 + x][1 - x] = [-x]$, a contradiction. □

Complete strong fans are nice for many reasons. One such reason is:

LEMMA 4. *Let K be any field with a valuation subring O, whose residue class field can be ordered. Then there is a complete strong fan $P \subseteqq K$ for which $O = O(K, P)$, and such that $\bar{P}$ is any given order of the residue field.*

Proof. Take $P^{\cdot}$ to be the positive units of $O \subseteqq K$. The result is then an easy application of valuation theory. □

This lemma shows that the complete strong fans (respectively the complete fans in view of Remark 1 of the last section) of a field K, give all the order and valuation theoretic information of the field K. This fact has led E. Becker and the author to suggest that the notion of "complete fans" be the appropriate generalization of the "real infinite primes" of number theory.

Let $P \subseteqq K$ be a complete preprime, and suppose that $K^{\cdot}/P^{\cdot}$ is a torsion group. Then the results of [3] show that P is a strong fan. This appears to be an extremely deep result, and does not (yet) have an elementary proof. Of special interest is the case where $K^{\cdot}/P^{\cdot} \cong Z/nZ$, with n even which are called orders of level n. (See [1] and [2] for more details.) In some cases it is possible to give an elementary proof that these higher orders are strong fans. Along these lines we give:

LEMMA 5. *If P is an order of level* 2, 4, 6, *or* 8, *then P is a strong fan.*

Proof. If P has level 2, the result is trivial. If P has level 4, then we may express $K^{\cdot} = \pm P^{\cdot} \cup \pm x \cdot P^{\cdot}$ for some $x \in K$. For such x, suppose that $1 + x = -p$ or $-px$ for some $p \in P$. In either case we find that $-x \in P$, a contradiction. Thus P is a strong fan.

Next suppose P has level 6. Then $K^{\cdot} = P^{\cdot} \cup xP^{\cdot} \cup x^2P^{\cdot} \cup x^3P^{\cdot} \cup x^4P^{\cdot} \cup x^5P^{\cdot}$ for some $x \in K$. As P is complete, $-P^{\cdot} = x^3P^{\cdot}$. Now suppose that for $p_1, p_2 \in P$, we have $1 + xp_1 = x^2p_2$. Then $x^3p_2 = x + x^2p_1 = x + p_1p_2^{-1}(1 + xp_1)$. But then we see that for some $p_3 \in P$, $1 + xp_3 \in -P$, a contradiction. Thus, $P + xP$ does not represent any elements of x^2P.

It is clear that $P + xP$ does not represent any elements of $x^3 \cdot P$ or $x^4 \cdot P$. Next assume that $1 + xp_1 = x^5p_2$ for $p_1, p_2 \in P$. Then as $xp_1 +$

$x^2p_1^2 \in P$, we have that $1/4 + xp_1 + x^2p_1^2 \in P$. Since P is complete, $1/2 + xp_1 \in \pm P$, from which it follows that $1/2 + xp_1 \in P$. Thus $1/2 + 1/2 + xp_1 \in P$, a contradiction. Thus $P + xP \subseteqq P \cup xP$, for all x such that $xP^{\cdot}$ generates $K^{\cdot}/P^{\cdot}$.

We now see in addition, that $P + x^2P$ does not represent x^3P, x^4P, or x^5P. So assume that $1 + x^2p_1 = xp_2$ for some $p_1, p_2 \in P$. It then must happen that for $p_3 \in P$, $1 - x^2p_1 = p_3$ or x^5p_3, as $(1 + x^2p_1)(1 - x^2p_1) \in P \cup xP$. If $1 - x^2p_1 = p_3$, then $(1 + x^2p_1)^3 - (1 - x^2p_1)^3 \in -P$, i.e., $6x^2p + 2x^6p^3 \in -P$, a contradiction. If $1 - x^2p_1 = x^5p_3$, then $(1 + x^2p_1)^3 + (1 - x^2p_1)^3 \in -P$, i.e., $2 + 6x^4p^2 \in -P$, a contradiction. This shows that if P has level 6, then P is a strong fan.

Finally we suppose that P has level 8. We identify $K^{\cdot}/P^{\cdot}$ with $\{P, xP, x^2P, \cdots, x^7P\}$, where $x^4P = -P$. We first claim that $P + x^2P = P \cup x^2P$. For assume that $p_1 + x^2p_2 = x^3p_3$. Then as $p_1^2 - x^4p_2^2 = (p_1 + x^2p_2)(p_1 - x^2p_2) \in P$ we must have that $p_1 - x^2p_2 \in x^5P$. But now since $(p_1 + x^2p_2)^2 - (p_1 - x^2p_2)^2 = 4x^2p_1p_2$, it follows that $x^6P - x^2P$ represents an element of x^2P, clearly a contradiction. A similar contradiction results if we assume that $P + x^2P$ represents x^7P.

Next we assume that $P + x^2P$ represents x^5P. As $xP = -x^5P$, it cannot happen that $P + x^2P$ also pepresents xP, as then it would represent 0. Thus $P + x^2P$ represents only P, x^2P, and x^5P. As in the above paragraph we find that $P - x^2P$ represents only P, $-x^2P$, and x^3P. But now, as $P + x^2P$ represents x^5P, we have that $P - x^5P$ represents $-x^2P$. Thus as $P - x^2P$ represents x^3P we conclude that $P - x^5P$ represents x^3P, i.e., $P + xP$ represents x^3P.

Suppose that $p_1 + xp_2 \in x^3P$. Then as $p_1^2 - x^2p_2^2 \in P$, $-x^2P$, or x^3P, we conclude that $p_1 - xp_2 \in P$, x^3P or x^5P. Clearly $p_1 - xp_2 \notin x^3P$, for otherwise $(p_1 + xp_2) + (p_1 - xp_2) \in x^3P$. If $p_1 - xp_2 \in x^5P$, then both $(p_1 + xp_2)^4$, $(p_1 - xp_2)^4 \in -P$, while $(p_1^2 - x^2p_2^2) \in P$. Thus: $(p_1 + xp_2)^4 + (p_1 - xp_2)^4 - 2(p_1^2 - x^2p_2^2)^2 = 16x^2p_1^2p_2^2 \in -P$, a contradiction. Finally, if $p_1 - xp_2 \in P$, then $(p_1 + xp_2)^4 - (p_1 - xp_2)^4 = 8(xp_1^3p_2 + x^3p_1p_2^3) \in -P$, which says that $P + xP$ represents $-x^3P$. This contradicts the fact that $P + xP$ already represents x^3P.

Thus $P + x^2P$ cannot represent x^5P. A similar argument shows that $P + x^2P$ cannot represent xP. Thus $P + x^2P = P \cup x^2P$, and also $P - x^2P = P \cup -x^2P$. It is now clear that P is a strong fan, for if $P + xP$ represents x^jP for some $j \neq 0, 1$, subtraction in one way or another will contradict what we know about $P \pm x^2P$. This proves the lemma. □

REMARK 2. An elementary proof of the analogue of Lemma 5 for all higher orders would be very nice, for then it should enable us to give an effective procedure for finding expressions for the "Hilbert identities", which Becker proves in [1] and [2]. Unifortunately, we have not been able to find such proofs.

3. Higher Pythagorean fields.

Recall that a formally real field is called Pythagorean in case $K^{\cdot 2} + K^{\cdot 2} = K^{\cdot 2}$. If $K^{\cdot 2}$ is a (strong) fan, then K is called Superpythagorean in [6] or strictly-Pythagorean in [1]. Generalizing these definitions we give:

DEFINITION 5. K is called *m-Pythagorean* if $K^{\cdot 2m} + K^{\cdot 2m} = K^{\cdot 2m}$, and K is called *strictly m-Pythagorean* in case $K^{\cdot 2m}$ is a strong fan.

LEMMA 6. *If K is strictly m-Pythagorean and if K is 2-Pythagorean, then $K^{\cdot 2m}$ is a valuation fan.*

Proof. We denote by $[x]_n$ the class of x in $K^{\cdot}/K^{\cdot n}$. Fix $x \notin \pm K^{\cdot 2m}$, and suppose that $[1 + x]_{2m} = K^{\cdot 2m}$, while $[1 - x]_{2m} = [-x]_{2m}$. In case $[x]_2 \neq \pm K^{\cdot 2}$, then we have that $[1 - x^2]_4 = [-xy^2]_4$, for some $y \in K^{\cdot}$. But as $K^{\cdot 4} + K^{\cdot 4} = K^{\cdot 4}$, we conclude that $K^{\cdot 4} - x^2 K^{\cdot 4}$ represents a multiplicative subgroup of $K^{\cdot}$. This implies $K^{\cdot 4} - x^2 K^{\cdot 4}$ represents x^2, a contradiction.

Now suppose that $[x]_2 = \pm K^{\cdot 2}$. If $x = y^2$, we have that $[1 - y^2]_{2m} = [-y^2]_{2m}$, so that $[1 + y]_{2m} = [y]_{2m}$, and $[1 - y]_{2m} = [-y]_{2m}$. But then $[(1 + y)^2 + 2(1 - y)]_{2m} = [y^2]_{2m}$ or $[-y]_{2m}$. However, $[3 + y^2]_{2m} = [2 + (1 + y^2)]_{2m} = K^{\cdot 2m}$, a contradiction. If $x = -y^2$, we have a similar contradiction. This proves Lemma 6. □

Let S be a set of primes, where for convenience we always include $1 \in S$.

DEFINITION 6. We shall say that K is *strictly S-Pythagorean* if for all distinct $p, q \in S$, K is strictly $p \cdot q$-Pythagorean.

THEOREM 2. *A field K is strictly S-Pythagorean if and only if K carries a valuation with residue field $\bar{K}$, such that whenever $n \in N$ with the primes dividing n in S, $\bar{K}^{\cdot}/\bar{K}^{\cdot 2n}$ has at most four elements, and Hensel's Lemma holds for all equations of the form $X^{2n} - a$ with $a \in K$. Further, if K is 2-Pythagorean, we can require that $\bar{K}$ be Euclidean.*

Proof. We first assume that for some $p \in S$, $K^{\cdot 2p}$ is not a valuation fan. Then by Lemma 2, for some $x \notin \pm K^{\cdot 2p}$ we have $[1 + x]_{2p} = K^{\cdot 2p}$, $[1 - x]_{2p} = [-x]_{2p}$ and $K^{\cdot 2p} \cup x \cdot K^{\cdot 2p}$ is a valuation fan. We also note that as $[1 - x^2]_{2p} \neq K^{\cdot 2p}$ or $[-x^2]_{2p}$, it must happen that $x^2 \in K^{\cdot 2p}$. Thus, as $x \notin K^{\cdot 2p}$, $x \notin \pm K^{\cdot 2}$, which shows that for all $q \in S$ that $[1 + x]_{2q} = K^{\cdot 2q}$ and $[1 - x]_{2q} = [-x]_{2q}$. In particular, for all distinct

$p, q \in S$ we have that $P_{pq} = \dot{K}^{2pq} \cup x \cdot \dot{K}^{2pq}$ is a valuation fan.

We next note that $O(K, P_{pq}) \subseteqq O(K, P_p) \cap O(K, P_q)$. First, it is immediate from the definitions that $O_1(K, P_p) \subseteqq O_1(K, P_{pq})$, and thus that $O_2(K, P_{pq}) \subseteqq O_2(K, P_p)$. But also, if $a \in O_1(K, P_{pq}) - O_1(K, P_p)$, we claim that $a \in O_2(K, P_p)$. For we cannot have $a^{-1} \in O_1(K, P_p)$, as then we would have $a^{-1} \in O_1(K, P_{pq})$, a contradiction. Thus $a \in \pm P_p$. Let $b \in O_1(K, P_p)$. As $ab \notin \pm P_p$, and as $a \cdot b \in O_1(K, P_{pq})$, we must have that $a \cdot b \in O_1(K, P_p)$. Thus $a \in O_2(K, P_p)$, showing what we wanted.

Now consider the ring $O(K, S, x) = \bigcap_{p \in S} O(K, P_p)$. We see that $O(K, S, x)$ is a valuation subring of K. For if $a \notin O(K, P_p)$ and $a^{-1} \notin O(K, P_q)$ for $p, q \in S$, we would have $a, a^{-1} \notin O(K, P_{pq}) \subseteqq O(K, P_p) \cap O(K, P_q)$, a contradiction.

Next, we observe that if $a \in O(K, S, x)$ is a unit, then it must happen that $a \in \pm \dot{K}^{2p} \cup \pm x \cdot \dot{K}^{2p}$ for all $p \in S$. As x is a pth power for all $p \in S$, a must also be a p^2th power which shows that $a \in \pm \dot{K}^{2p^2} \cup \pm x \cdot \dot{K}^{2p^2}$ by applying the preceding to the unit $\sqrt[p]{a}$. We thus see that whenever $n \in N$ with all primes dividing n in S, that $a \in \pm \dot{K}^{2n} \cup \pm x \cdot K^{2n}$. It is now clear that $\dot{\bar{K}}/\dot{\bar{K}}^{2n}$ has at most four elements.

Now suppose that $a, b \in O(K, S, x)$ are units, and that $a \notin \dot{K}^{2n}$. As $b^2 \in \dot{K}^{2n}$, we have that $a - b^2 \in \pm \dot{K}^{2n} \cup \pm x \cdot \dot{K}^{2n}$. For $p \in S$, let $c \in O_1(K, P_p)$. Then as $[a + c/2]_{2p} = [a]_{2p}$, and $[b^2 - c/2]_{2p} = \dot{K}^{2p}$, we conclude that $[(a + c/2) - (b^2 - c/2)]_{2p} = [(a - b^2) + c]_{2p} = [a]_{2p}$ or $-\dot{K}^{2p}$. Thus $[(a - b^2) + c]_{2p} = [a - b^2]_{2p}$ which shows $a - b^2$ is a unit of $O(K, P_p)$, and hence is a unit of $O(K, S, x)$. It now follows that for such $a, \bar{a} \notin \dot{\bar{K}}^{2n}$, which shows that Hensel's Lemma holds for the equation $X^{2n} - a$.

Next we note that in case $\dot{K}^{2p}$ is a valuation fan for all $p \in S$, then so is $\dot{K}^{2pq}$ for all $p, q \in S$. In this case we may replace $O(K, S, x)$ by the ring $O(K, S) = \bigcap_{p \in S} O(K, \dot{K}^{2p})$, and the above argument applies. By Lemma 6, this is precisely what happens when K is 2-Pythagorean.

Conversely, we now assume a field K carries a valuation as described above. We must see that for all distinct $p, q \in S$, that $\dot{K}^{2pq}$ is a strong fan. Clearly $\dot{\bar{K}}^{2pq}$ is a strong fan of $\bar{K}$ as $\dot{\bar{K}}/\dot{\bar{K}}^{2pq}$ has at most four elements. Now suppose that $a \notin -\dot{K}^{2pq}$, and assume that a is integral under our valuation. Clearly $\bar{a} \notin -\dot{\bar{K}}^{2pq}$ by our Henselian property, so that $1 + a$ is a unit. As $\overline{1 + a} \in \dot{\bar{K}}^{2pq}$ or $\bar{a} \cdot \dot{\bar{K}}^{2pq}$, it follows again by the Henselian property that $1 + a \in \dot{K}^{2pq}$ or $1 + a \in a \cdot \dot{K}^{2pq}$. In particular, we now have shown that for all $a \notin -\dot{K}^{2pq}$, one of $1 + a$, $1 + a^{-1}$ lies in $\dot{K}^{2pq}$. This proves Theorem 2. □

COROLLARY 2. *If K is strictly S-Pythagorean, then K is strictly*

n-Pythagorean, for all n with the primes dividing n in S.

Proof. The Henselian properties of our valuation give the result, exactly as proven at the end of the proof of Theorem 2. □

REMARK 3. In case $S = \{1\}$, Theorem 2 reduces to the well known result of Bröcker and Brown characterizing Superpythagorean fields. See [4] and [5] for details. Also, in case K is 2-Pythagorean, we see by the Euclidean residue fields that K must be strictly 2-Pythagorean, so our Corollary 2 reduces to Corollary 2 of Theorem 27 of [1], p. 68.

A field K is called *Hereditarily-Pythagorean* if every formally real algebraic extension is Pythagorean. These fields, which have been studied closely in [1], [4], and elsewhere, have many remarkable properties. To mention a few, we give the following:

THEOREM 3. (E. Becker, [1].) *The following are equivalent for a real field K:*

(i) *K is Hereditarily-Pythagorean.*

(ii) *The absolute Galios group* $\mathrm{Gal}(\tilde{K}/K[i])$ *is abelian.*

(iii) *Every algebraic extension of K is of the form*

$$K[\sqrt[t_1]{a_1}, \sqrt[t_2]{a_2}, \cdots, \sqrt[t_n]{a_n}] \quad \textit{for some} \quad t_1, \cdots, t_n \in N\,, \quad a_1, \cdots, a_n \in K\,.$$

Suppose that K is an n-Pythagorean field. Then we shall say that K is *Hereditarily n-Pythagorean* if every formally real algebraic extension of K is n-Pythagorean. It follows from Theorem 9 p. 109 of [1] that if K is a Hereditarily-Pythagorean field which is 2^n-Pythagorean, then K is Hereditarily 2^n-Pythagorean. Our last result is a generalization of this fact.

THEOREM 4. *Let K be a Hereditarily-Pythagorean field. If $K^{\cdot 2n}$ is a strong fan, then K is Hereditarily n-Pythagorean.*

Proof. Let $O \subsetneqq K$ be the valuation ring given by Theorem 2, and let $\bar{K}$ be its residue field. We have that $\bar{K}/{}^{\cdot}\bar{K}^{\cdot 2n}$ has at most four elements, and according to Theorems 17 and 18 of [1], Chapter 3, we see that $\bar{L}^{\cdot}/\bar{L}^{\cdot 2n}$ has at most four elements for any real algebraic extension $\bar{L}$ of $\bar{K}$. It is now clear that in any such $\bar{L}$, $\bar{L}^{\cdot 2n}$ is a strong fan.

Now let $L = K[\sqrt[p]{a}\,]$ be a real extension where p is a prime, and let $O' \subsetneqq L$ extend the valuation ring $O \subsetneqq K$. We show that Hensel's Lemma holds for equations of the form $X^q - b$ in this valuation of L, whenever q is a prime dividing $2n$. Note that as $M = L[\sqrt[q]{b}\,]$ is a radical extension of K, we have that $M = K[\sqrt[p]{a}, \sqrt[q]{c}\,]$ or $M = K[{}^{p}\sqrt[q]{c}\,]$ for $c \in K$. By the Henselian property of O, we see that in any extension of O to $O'' \subseteqq K[\sqrt[q]{c}\,]$, that either the value group or the residue field must extend by a power of q. In particular, as the same now must be true in the extension O' of O to M, we see that Hensel's Lemma must hold for $X^q - b$ over L.

We now see that Hensel's Lemma holds for equations of the form $X^{2n} - b$ in this valuation of L. Together with the fact that $\bar{L}^{\cdot 2n}$ is a strong fan of $\bar{L}$, this shows that $L^{\cdot 2n}$ is strong fan of L. As every real algebraic extension of K is obtained by successive extensions as the above, it is now clear that K is Hereditarily n-Pythagorean. □

REFERENCES

1. E. Becker, *Hereditarily Pythagorean Fields and Orderings of Higher Level,* IMPA Lecture Notes, Rio de Janeiro, 1978.
2. ———, *Summen n-ter Potenzen in Korpen,* J. Reine Angew. Math., **307/308** (1979), 8-30.
3. ———, *Partial orders on a field and valuation rings,* Communications in Algebra, **7** (18) (1979), 1933-1976.
4. L. Brocker, *Characterization of fans and hereditarily Pythagorean fields,* Math. Zeit., **151** (1976), 149-163.
5. R. Brown, *Superpythagorean fields,* J. Algebra, **42** (1976), 483-494.
6. R. Elman and T. Y. Lam, *Quadratic forms over formally real fields and Pythagorean fields,* Amer. J. Math., **94** (1972), 1155-1194.
7. D. K. Harrison, *Finite and infinite primes for rings and fields,* Memoirs of the Amer. Math. Soc. #68, Providence, R. I., 1966.

Received March 2, 1980. Much of this work appeared as part of the author's Doctoral Thesis, Princeton, 1979. The author would like to thank his advisor, Simon Kochen, and Eberhard Becker for their advice during the preparation of this work.

UNIVERSITY OF CALIFORNIA
LOS ANGELES, CA 90024