Journal für die reine und angewandte Mathematik

gegründet 1826 von

August Leopold Crelle

fortgeführt von
C. W. Borchardt, K. Weierstrass, L. Kronecker, L. Fuchs,
K. Hensel, L. Schlesinger, H. Hasse, H. Rohrbach

gegenwärtig herausgegeben von

Otto Forster · Willi Jäger · Martin Kneser
Horst Leptin · Samuel J. Patterson · Peter Roquette

unter Mitwirkung von
M. Deuring, P. R. Halmos, O. Haupt,
F. Hirzebruch, G. Köthe, K. Krickeberg, K. Prachar,
H. Reichardt, L. Schmetterer, B. Volkmann

JRMAA8

Band 336

Sonderdruck

Walter de Gruyter · Berlin · New York 1982

For English version, see Back Cover

Hinweise für die Autoren des Journals für die reine und angewandte Mathematik (Crelles Journal)

In das Journal werden nur **Originalarbeiten** aufgenommen, keine Buchbesprechungen, Referate oder dergl.
Der Verlag erwirbt durch die Veröffentlichung eines Beitrags das unbeschränkte **Verlagsrecht** für die Dauer des Urheberrechts, so daß ein anderweitiger Abdruck einschließlich der photomechanischen Wiedergabe oder einer sonstigen Vervielfältigung nicht statthaft ist. Für den Abdruck eines Beitrags in den Gesammelten Schriften eines verstorbenen Autors ist die Genehmigung beim Verlag zu beantragen.

Manuskripte sind, möglichst in 2 Exemplaren, an einen der Herausgeber zu senden, und zwar an denjenigen, der dem behandelten Thema am nächsten steht, im Zweifelsfall an den geschäftsführenden Herausgeber:

Prof. Dr. Otto Forster, Math. Inst. d. Univ., Theresienstr. 39, D-8000 München 2
Prof. Dr. Willi Jäger, Inst. f. Angew. Math. d. Univ., Im Neuenheimer Feld 294, D-6900 Heidelberg
Prof. Dr. Martin Kneser (geschäftsf. Herausgeber), Math. Inst. d. Univ., Bunsenstr. 3–5, D-3400 Göttingen
Prof. Dr. Horst Leptin, Fak. f. Math. d. Univ., Universitätsstraße, D-4800 Bielefeld 1
Prof. Dr. Samuel J. Patterson, Math. Inst. d. Univ., Bunsenstr. 3–5, D-3400 Göttingen
Prof. Dr. Peter Roquette, Math. Inst. d. Univ., Im Neuenheimer Feld 288, D-6900 Heidelberg

Die Autoren werden gebeten, ihre Manuskripte nach folgenden **Vorschriften** vorzubereiten. **Manuskripte, die den gestellten Anforderungen nicht genügen, können nicht angenommen werden.** Die Manuskripte sind in leserlicher Form in **Maschinenschrift** einzureichen. Unerwünscht sind schlecht lesbare Matrizenabzüge.

Für **mathematische Symbole** stehen zur Verfügung: die Alphabete lateinisch, gotisch (Fraktur), griechisch, grotesk, mit kleinen und großen, gewöhnlichen (Antiqua), kursiven oder halbfetten Buchstaben, neben diesen Buchstaben noch die Zeichen $\aleph$, ∇, $\wp$, sowie $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Lateinische Buchstaben als mathematische Symbole werden grundsätzlich *kursiv* gesetzt. Alle anderen, auch gewöhnlich (nicht-kursiv) zu setzende lateinische Buchstaben, sind als mathematische Symbole zu kennzeichnen, etwa durch verschiedenfarbiges Unterstreichen.

Da die großen griechischen Buchstaben zum Teil von großen lateinischen Buchstaben nicht zu unterscheiden sind, werden sie von der Druckerei grundsätzlich grotesk gesetzt: A, B, E, Z, H, I, K, M, N, O, P, T, Y, X. Für die von lateinischen Buchstaben verschiedenen großen griechischen Buchstaben stehen auch die kursiven Typen $\mathit{\Gamma}$, $\mathit{\Delta}$, $\mathit{\Theta}$, $\mathit{\Lambda}$, $\mathit{\Xi}$, $\mathit{\Pi}$, $\mathit{\Sigma}$, $\mathit{\Phi}$, $\mathit{\Psi}$, $\mathit{\Omega}$ zur Verfügung.

Die griechischen Großbuchstaben $\mathit{\Sigma}$, $\mathit{\Pi}$ sind nur zu kennzeichnen, wenn sie wie andere große griechische Buchstaben verwendet werden; als Zeichen für Summe bzw. Produkt bleiben sie ungekennzeichnet.

Das Zeichen für „ist Element von" soll $\in$, nicht ε **geschrieben werden**; das Zeichen für „ist Teiler von" ist *vertikal* zu schreiben, also $a|b$, nicht a/b.

Die lateinischen Buchstaben o, O bzw. l als mathematische Symbole sind zur Unterscheidung von der Zahl 0 bzw. 1 besonders zu kennzeichnen, ebenso das Zeichen $\emptyset$ für „leere Menge" zum Unterschied von der Form ϕ des kleinen griechischen φ sowie der Bindestrich (-) im Unterschied zum Minuszeichen (—).

Ähnliche Zeichen wie $\cap$, $\bigcap$; $\subset$, $<$, $\prec$, $\langle$; $\subseteqq$, $\leqq$; $'$, $'$ sind besonders deutlich zu schreiben.

Die Grenzen bei den Zeichen $\int$, $\sum$, $\prod$, $\bigcap$ usw. sollen *über* und *unter*, nicht neben dem Zeichen stehen.

In algebraischen und zahlentheoretischen Arbeiten sollen **Wurzelzeichen** nicht durch gebrochene Exponenten ersetzt werden.
Schräge Bruchstriche sollen nur ausnahmsweise in einem der beiden folgenden Fälle verwendet werden:

a) zur Hervorhebung der naturgemäßen mathematischen Assoziation, z. B.

$$\frac{\pi(x)}{x/\log x} \quad \text{statt} \quad \frac{\pi(x)\log x}{x}$$

b) falls Zähler und Nenner keine Summen oder Differenzen sind. In diesem Fall sollen im Manuskript Zähler bzw. Nenner deutlich *über* bzw. *unter* der Zeile und beide mit *kleineren* Typen als normal geschrieben sein, z. B. $|x| < {}^{2}/_{3}\,c$.

Dem Manuskript soll ein Blatt mit **Anweisungen für den Setzer** beiliegen. Darauf sind die farbigen Unterstreichungen zu erklären, durch die im Manuskript alle nichtlateinischen mathematischen Symbole gekennzeichnet sind, ebenso die verschiedenartigen Unterstreichungen, durch die im Manuskript *kursiver*, g e s p e r r t e r, **halbfetter** Textsatz gekennzeichnet ist.

Bei einem Satz, Hilfssatz, Lemma, Folgerung, Korollar ist dieses Wort und die etwa nachfolgende Nummer halbfett, der jeweilige Text kursiv auszuzeichnen, bei Definition, Bemerkung, Beispiel nur dieses Wort halbfett. **Eigennamen** sind nicht hervorzuheben. **Fußnoten** sind fortlaufend zu numerieren.

Im **Literaturverzeichnis** sind die Autornamen (namenalphabetisch geordnet) kursiv auszuzeichnen. Titel der Arbeit und Name der Zeitschrift bleiben ungekennzeichnet. Das Erscheinungsjahr ist in runden Klammern unmittelbar hinter der halbfett auszuzeichnenden Bandnummer anzugeben. Vor dem Autornamen steht die laufende Nummer des Verzeichnisses in eckigen Klammern, z. B.

[3] *Rudolf Lidl*, Tschebyscheffpolynome in mehreren Variablen, J. reine angew. Math. **273** (1975), 178—198.

Das Zitieren aus dem Literaturverzeichnis im Manuskript soll in der Form „R. Lidl [3], Satz 5", nicht in der Form „R. Lidl [3, Satz 5]" erfolgen.

Für etwaige **Figuren** sind reproduktionsfähige Reinzeichnungen mit Tusche auf Pergamentpapier erforderlich.

Der **Titel der Arbeit** soll in gewöhnlicher Schrift, nicht mit lauter Großbuchstaben geschrieben sein, bei nichtdeutscher Sprache auch nicht mit großen Anfangsbuchstaben der Haupt- und Eigenschaftswörter. Ist der Titel lang, so ist ein Vorschlag für einen kürzeren **Kolumnentitel** zu machen, der im endgültigen Druck über jeder Seite steht.

Am Ende des Manuskripts ist unter dem Literaturverzeichnis die **vollständige postalische Adresse** des Autors bzw. der Autoren anzugeben.

Für den Beitrag werden 100 **Sonderdrucke** kostenlos abgegeben, weitere gegen Berechnung. Die Gesamtzahl der gewünschten Sonderdrucke ist auf dem Laufzettel anzugeben, der jeder Korrektursendung beiliegt.

The Pythagoras number of some affine algebras and local algebras

By *M. D. Choi** at Toronto, *Z. D. Dai* at Peking, *T. Y. Lam*** at Berkeley, and *B. Reznick*** at Urbana

§ 1. Introduction

For a (commutative) ring A, the *pythagoras number*, $P(A)$, of A is the smallest number $n \leqq \infty$ such that any sum of squares in A can be expressed as a sum of at most n squares in A. For instance, $P(\mathbb{R}) = 1$, $P(\mathbb{F}_q) = 2$ (if $2 \nmid q$), and, by Lagrange's Theorem, $P(\mathbb{Z}) = P(\mathbb{Q}) = 4$. The number $P(A)$ is an interesting, but very delicate, arithmetic invariant of the ring A; the explicit computation of $P(A)$ is, in general, a difficult task. Given a ring, it is often far from easy even just to decide if $P(A)$ is finite of infinite. For some results on $P(A)$ in the recent literature, see, for example, [P], [P_2], [CEP], [HJ], [R], [Pe_1], [Pe_2], [EL], [Br], [Pr], etc. In some of these papers, the invariant $P(A)$ has appeared under an assortment of other names: for instance, "Pfister dimension" in [R], "Quadratstufe", in [Pe_2], and "reduced height" in [HJ] and [L]. In this paper, following [Br], [Pr], we shall call $P(A)$ the *pythagoras number* and hope that, in the future, other mathematicians will adopt the same terminology.

The motivation for the present work is Pfister's well-known result that if F is a function field of transcendence degree n over $\mathbb{R}$, then $P(F) \leqq 2^n$ ([P_2], [L], p. 301). Instead of working with function fields F, it seemed natural to us to also work with their finitely generated subrings $A \subsetneqq F$. This led us to the problem of computing the pythagoras number of affine $\mathbb{R}$-algebras (i.e., finitely generated algebras over $\mathbb{R}$). Each affine $\mathbb{R}$-algebra A corresponds to an affine variety V defined over $\mathbb{R}$, so $P(A)$ may be viewed as an arithmetic invariant of the variety V. Speaking loosely, we can say that $P(A)$ is the pythagoras number of the variety V.

The n-space $\mathbb{R}^n$ has, as its affine algebra, the real polynomial ring in n variables, $\mathbb{R}[x_1, \dots, x_n]$. Two of the present authors have announced in 1976 [CL] that this ring has pythagoras number $\geqq 2^n$, but the exact value of $P(\mathbb{R}[x_1, \dots, x_n])$ was not determined.

* Supported in part by NSERC of Canada.
** Supported in part by NSF.

0075-4102/82/0336-0003$02.00

In fact, it was not even known if $P(\mathbb{R}[x_1, \ldots, x_n])$ is finite or not. Note that if $P(\mathbb{R}[x_1, \ldots, x_n])$ were finite for all n, then *all* $\mathbb{R}$-affine algebras would also have finite pythagoras number. In this work, however, *we shall show that this is not the case: in fact,* $P(\mathbb{R}[x_1, \ldots, x_n]) = \infty$ if $n \geqq 2$ (Theorem 4. 1). We show, moreover, that the same result holds if the ground field $\mathbb{R}$ is replaced by any commutative ring A which admits a real ideal (Cor. 4. 19). (An ideal $\mathfrak{A} \subset A$ is called *real* if the quotient ring $R = A/\mathfrak{A}$ is formally real, i.e. if $\sum a_i^2 = 0$ in R implies that each $a_i = 0 \in R$.)

For affine varieties of dimension 1 (i.e. affine curves), the situation turns out to be quite different. Using the fact that $P(\mathbb{R}[x_1]) = 2$ [L], p. 302 (2nd printing), we show in § 3 that, *for any affine $\mathbb{R}$-algebra A of transcendence degree* 1, *we have* $P(A) < \infty$. (Thus, any affine curve defined over the real numbers has a finite pythagoras number.) Here, some explicit computations are possible; for instance, we show *if $A = \mathbb{R}[x, y]/(h)$ where $h(x, y)$ is any polynomial of degree 2, then* $P(A) = 2$ (Theorem 3. 7). On the other hand, one can construct affine $\mathbb{R}$-algebras A of transcendence degree 1 such that $P(A)$ is arbitrarily large, so there is no hope of getting a universal bound on $P(A)$ in general.

The result that $P(k[x, y]) = \infty$ for formally real field k has several important consequences. One consequence, as pointed out by A. Wadsworth, is that *there exists a principal ideal domain A (with 2 a unit) whose quotient field has pythagoras number* 4, *but A itself has infinite pythagoras number* (see (4. 6)). Moreover, it is possible that a unit $u \in A$ is a sum of (four) squares in the quotient field, but u is *not* a sum of squares in A (see (4. 8)). A second consequence of $P(k[x, y]) = \infty$ is that, by using the same kind of ideas, one also arrives at a computation of the pythagoras number of $\mathbb{Z}[x]$. In the literature it was only known, by a result of Peters [Pe_2], that $P(\mathbb{Z}[x]) \geqq 6$; we shall show that $P(\mathbb{Z}[x]) = \infty$. More generally, $P(R[x]) = \infty$ if R is any order in a totally real algebraic number field, or any commutative ring which admits a homomorphism into such an order (cf. (4. 14)).

In § 6, we consider an $\mathfrak{m}$-adic ring $(R, \mathfrak{m})$, where $\mathfrak{m}$ is an ideal in R with $\bigcap_{i \geqq 0} \mathfrak{m}^i = 0$. Let $A = G_{\mathfrak{m}}(R) = \bigoplus_{i \geqq 0} \mathfrak{m}^i/\mathfrak{m}^{i+1}$ be the associated graded ring with respect to $\mathfrak{m}$. Assuming that A is formally real, we show (in (6. 3)) that $P(R) \geqq hP(A)$, where $hP(A)$ denotes the "homogeneous" pythagoras number of A (defined by using the "length" of *homogeneous* elements of A). In the special case when $(R, \mathfrak{m})$ is a regular local ring with a residue field $k = R/\mathfrak{m}$, the associated graded ring A is a polynomial ring $k[x_1, \ldots, x_d]$ (with the usual grading), where $d = \dim R$. If $d \geqq 3$ and k is formally real, we have

$$hP(A) = P(k[x_2, \ldots, x_d]) = \infty .$$

Thus, any regular local ring $(R, \mathfrak{m})$ of dimension $\geqq 3$ has an infinite pythagoras number, provided that $R/\mathfrak{m}$ is formally real (Th. (6. 6)).

In § 7, we shall try to "globalize" the above result. In Theorem 7. 3, using the basic facts of real algebraic geometry, we develop a general criterion for an affine algebra A to be formally real. The "necessity" part of this criterion implies that, if A is formally real of Krull dimension d, then A has a real maximal ideal $\mathfrak{m}$ of height d such that the localization $A_{\mathfrak{m}}$ is regular. If $d \geqq 3$, it follows that $P(A) \geqq P(A_{\mathfrak{m}}) = \infty$, so we get the general result that *any formally real affine algebra of dimension $\geqq 3$ has an infinite pythagoras number* (Th. (7. 5)).

In § 5, we deal with various rings of dimension 2 and compute their pythagoras numbers. For instance *we show that the rings* $\mathbb{R}[[x, y]]$, $\mathbb{R}[x][[y]]$ and $\mathbb{R}[[y]][x]$ *all have pythagoras number* 2 (see (5. 10), (5. 14), (5. 18)). Together with the results of § 7, this enables us to compute the pythagoras numbers of

$$\mathbb{R}[[x_1, \ldots, x_n]][x_{n+1}, \ldots, x_{n+m}] \quad \text{and} \quad \mathbb{R}[x_1, \ldots, x_n][[x_{n+1}, \ldots, x_{n+m}]] \quad \text{for all } n, m.$$

(We have also complete results when $\mathbb{R}$ is replaced by $\mathbb{Z}$, and almost complete results when $\mathbb{R}$ is replaced by $\mathbb{Q}$.) One interesting by-product of the computation of $P(\mathbb{R}[[x, y]])$ is that it led to a proof that $\mathbb{C}((x, y))$ (*the quotient field of* $\mathbb{C}[[x, y]]$) *is a* C_2*-field for diagonal forms, in the sense of Lang* (cf. (5. 16)). In particular, $\mathbb{C}((x, y))$ provides a new example of a field with u-invariant 4 which seemed to have escaped earlier notice.

In § 8, we consider the affine algebra $A_n = \mathbb{R}[x_1, \ldots, x_n]/(1 + x_1^2 + \cdots + x_n^2)$, and its quotient field F_n. If $2^r \leqq n < 2^{r+1}$, it is known that $s(F_n) = 2^r$ [P₁], while $s(A_n) = n$ [DLP]. (Here, $s(R)$ denotes the *level* of a ring R, i.e. the smallest number $s \leqq \infty$ for which -1 is a sum of s squares in R.) In Theorem 8. 1, we compute the pythagoras number $P(F_n)$, showing that $P(F_n) = 2^r + 1$ if $n > 2$, while $P(F_2) = 2$. For the affine algebras A_n, however, we can compute $P(A_n)$ only in the case $n = 2^r$; namely, $P(A_2) = 2$, and $P(A_{2^r}) = 2^r + 1$ if $r \geqq 2$. It seems very likely that $P(A_n) = n + 1$ for any $n > 2$, but we have not been able to prove this.

The paper concludes with a final section, § 9, in which we collect a few interesting open problems in the hope of stimulating future work.

We want to thank J. Hsia for his helpful comments on Problem 1 in § 9. We are also indebted to A. Wadsworth for many stimulating conversations about this work; his help has been especially instrumental toward the inception and formulation of (4. 6), (4. 7), (5. 16), as well as (6. 3), (7. 3), and their applications.

§ 2. Some basic facts on the pythagoras number

Throughout this paper, we shall write $S_r(A)$ for the set of sums of r squares in a (commutative) ring A, and write $S(A) = \bigcup_{r \geqq 1} S_r(A)$ for the set of *all* sums of squares. In this section, we shall collect some basic facts on the pythagoras number. The first two facts are obvious so we shall omit their proofs.

(2. 0) *If there is a ring homomorphism* $A \to B$ *which is onto, then* $P(B) \leqq P(A)$.

(2. 1) *If* S *is a multiplicatively closed set in* A, *then* $P(S^{-1}A) \leqq P(A)$. In particular, if A is an integral domain and F is its quotient field, then

$$P(F) \leqq P(A).$$

(2. 2) *If* k *is a field, then by a theorem of Cassels* [C], $P(k[t]) = P(k(t))$.

Applying this to $k = \mathbb{R}(x_1, \ldots, x_n)$, for instance, we have

$$P(\mathbb{R}(x_1, \ldots, x_n)[t]) = P(\mathbb{R}(x_1, \ldots, x_n, t)) \leqq 2^{n+1},$$

by [P_2].

(2. 3) *If A is any valuation ring with $1/2 \in A$, and F is its quotient field, then* $P(A) = P(F)$.

This follows from a theorem of Kneser and Colliot-Thélène (see [CLRR], (4. 5)).

(2. 4) *Let A be a ring with $s = s(A) < \infty$. Then:*

(a) $s \leqq P(A) \leqq s + 2$.

(b) *If $2 \in U(A)$ (group of units in A), then $s \leqq P(A) \leqq s + 1$.*

The truth of (b) is well-known. In fact, if $2 \in U(A)$, then, for any $a \in A$, we can find $b, c \in A$ such that $a = b^2 - c^2$ (e.g. $b = (a+1)/2$, $c = (a-1)/2$). If $-1 = d_1^2 + \cdots + d_s^2$, then $a = b^2 + (d_1 c)^2 + \cdots + (d_s c)^2$ so $A = S_{s+1}(A)$. The fact (a) (without any assumption on the invertibility of 2) was pointed out by Joly [Jo] and Peters [Pe_2]. For the proof, consider $a = \sum a_i^2 \in S(A)$. We have

$$a = (1 + \sum a_i)^2 - 1 - 2b = (1 + \sum a_i)^2 + b^2 + (-1)(b+1)^2,$$

where $b = \sum_i a_i + \sum_{i<j} a_i a_j$. Since $-1 \in S_s(A)$, this implies that $a \in S_{s+2}(A)$. It is easy to see that the inequalities in (a) and (b) are the best possible. (For (b), take the ring

$$A = \mathbb{Z}[i][x] \quad (i^2 = -1).$$

A straightforward computation shows that $2x = (1+x)^2 + i^2 + (ix)^2 \notin S_2(A)$, so $P(A) = 3$.)

Lemma 2. 5. *Let $\mathfrak{A}$ be an ideal in A finitely generated by $a_1, \ldots, a_n$. Assume that $2 \in U(A)$, and that, for all i, $\pm a_i \in S(A)$ (for both signs). Let $B = A/\mathfrak{A}$. Then $P(A) < \infty$ iff $P(B) < \infty$.*

Proof. The "only if" part is clear from (2. 0). Conversely, assume $p = P(B) < \infty$. Consider any $c \in S(A)$. In B, we can write $\bar{c} = \bar{c}_1^2 + \cdots + \bar{c}_p^2$, for suitable $c_i \in A$. Lifting to A, we have therefore $c = c_1^2 + \cdots + c_p^2 + b_1 a_1 + \cdots + b_n a_n$, for suitable $b_i \in A$. As in (2. 4) (b), we can write $b_i = d_i^2 - e_i^2$ for suitable d_i, e_i. Choose a large number r such that $\pm a_i \in S_r(A)$, for both signs and for all i. Then

$$c = c_1^2 + \cdots + c_p^2 + a_1 d_1^2 + \cdots + a_n d_n^2 + (-a_1) e_1^2 + \cdots + (-a_n) e_n^2$$

is a sum of $p + 2rn$ squares, so $P(A) \leqq p + 2rn < \infty$. Q.E.D.

Corollary 2. 6. *Let R be any ring with $2 \in U(R)$ and let $b_1, \ldots, b_n \in R$. Then $P(R/(b_1^2 + \cdots + b_n^2)) < \infty$ iff $P(R/(b_1^2, \ldots, b_n^2)) < \infty$.*

Proof. Apply (2. 5) to $A = R/(b_1^2 + \cdots + b_n^2)$, with $a_i = \bar{b}_i^2$.

Let us now consider the following general situation, which will be fixed in the balance of this section: *Let k be a commutative ring with $P(k) < \infty$. Let A be a k-algebra which is finitely generated as a k-module.* The following two questions (Q_1) and (Q_2) arise naturally:

(Q_1) (Weak Question). *Is it true that $P(A) < \infty$?*

(Q_2) (Strong Question). *If A can be generated by n elements as a k-module, is it true that $P(A) \leqq n \cdot P(k)$?*

We have not been able to answer either of these questions in the general form stated above. However, in the sequel, we shall need to know the answers to (Q_1), (Q_2) only for some specific rings k. To be precise, what we need is the following:

Theorem 2. 7. *The answer to (Q_2) (and hence (Q_1)) is affirmative if*

(a) *k is a field, or*

(b) *$k = k_0[t]$ where k_0 is a real-closed field.*

Proof. First, assume that k is a field. If k has characteristic 2, every sum of squares in A is a single square, so $P(A) = 1$.

Now assume $\operatorname{char} k \neq 2$. Let $y_1, \ldots, y_n$ be k-module generators for A. Consider any $a \in S(A)$, say $a = \sum_{i=1}^{N} a_i^2$. Write $a_i = \alpha_{i1} y_1 + \cdots + \alpha_{in} y_n (\alpha_{ij} \in k)$, and consider the k-quadratic form

$$q(x_1, \ldots, x_n) = \sum_{i=1}^{N} (\alpha_{i1} x_1 + \cdots + \alpha_{in} x_n)^2. \tag{2. 8}$$

By the diagonalization theorem for quadratic forms over fields [L], p. 10, we can write

$$q(x_1, \ldots, x_n) = \sum_{j=1}^{n} \beta_j L_j(x)^2,$$

where $\beta_j \in k$ (possibly zero for some j's) and $L_j(x)$ $(1 \leqq j \leqq n)$ are n independent linear forms over k. Choosing $x = (x_1, \ldots, x_n) \in k^n$ such that $L_j(x) = 1$ and $L_i(x) = 0$ for $i \neq j$, we see that $\beta_j \in S(k)$ for all j. Say $\beta_j = \beta_{j1}^2 + \cdots + \beta_{jp}^2$ $(p = P(k), \beta_{ji} \in k)$. Substituting y_j for x_j in the identity (2. 8), we get

$$a = \sum_{i=1}^{N} (\alpha_{i1} y_1 + \cdots + \alpha_{in} y_n)^2 = q(y_1, \ldots, y_n) = \sum_{j=1}^{n} (\beta_{j1}^2 + \cdots + \beta_{jp}^2) L_j(y)^2 \in S_{pn}(A).$$

Therefore, $P(A) \leqq pn = nP(k)$. [1])

[1]) We thank the referee for a simplifying remark to an earlier version of this proof. Actually, the fact that q is a sum of $n \cdot P(k)$ squares of linear forms can also be proved by induction on n. We shall leave this inductive proof as an exercise for the reader. Moreover, the bound $P(A) \leqq nP(k)$ is not the best possible; for better bounds, see [CLR$_2$].

Next, we treat the case $k = k_0[t]$, where k_0 is a real-closed field. Using the same notation as above, we have now a quadratic form $q(x_1, \ldots, x_n)$ in (2. 8) with coefficients in $k_0[t]$. Viewed as a polynomial in $t, x_1, \ldots, x_n$, this q is certainly positive semidefinite, since it is a sum of squares of polynomials. By the theorem of Jakubović [J] and Rosenblum-Rovnyak [RR], p. 312, q is a sum of $2n$ squares in $k_0[t, y_1, \ldots, y_n]$ (see also [Po], [D]). Thus, the same substitution argument as in the first part of the proof shows that $a \in S_{2n}(A)$. Therefore, $P(A) \leqq 2n = P(k) \cdot n$.

Remark 2. 9. It would be of interest to extend (the quantitative part of) the theorem of Jakubović and Rosenblum-Rovnyak to base rings $k = k_0[t]$ with $P(k) < \infty$, but k_0 not necessarily real-closed. Unfortunately, we do not know how to do this. We note that a completely self-contained proof of the J-R-R theorem is available in [CLR$_1$], p. 22. This proof is valid as long as k_0 is real-clo ', but does not seem to generalize to other ground fields. If k_0 is a hereditarily pythagor) field, it is known that $P(k_0[t]) = 2$ [B$_1$], p. 95. In view of this, it seems likely that the (ntitative part of the) J-R-R theorem should remain valid for such k_0. However, it does no em easy to give a proof for this.

Reiterating (2. 7) (a), if A is a finite dimensional algebra over a field k, then $P(A) \leqq P(k) \dim_k A$. This result was first shown by A. Pfister (unpublished) when A is a field extension of finite degree over k. Pfister's proof (as shown to us by J. Hsia) works as long as A is a monogenic k-algebra, but our proof above works for any finite dimensional k-algebra. (Another proof, similar in spirit to ours, was noted independently by David Leep.) The proof, in fact, yields more precise information: *For any n, let $g_k(n)$ be the smallest number such that any sum of squares of n-ary k-linear forms can be written as a sum of $g_k(n)$ squares of such forms. Then, for any n-dimensional k-algebra A, we have $P(A) \leqq g_k(n)$.* At the cost of letting the dimension of A be larger than n (but no larger than $(n+1)^2$), we can, in fact, construct examples of algebras A with $P(A) = g_k(n)$. This is done in the following proposition:

Proposition 2. 10. *Let k be any form 'y real field and let $A = k[x_1, \ldots, x_n]/\mathfrak{A}$ where $\mathfrak{A}$ is the ideal generated by all cubic mono 's* (i.e. $\mathfrak{A} = (x_1, \ldots, x_n)^3$). *Then*

$$\dim_k A = (n+1)(n \quad 2 \text{ and } P(A) = g_k(n).$$

Proof. Any element f of A can be exp essed uniquely in the form $f = a + \lambda(\bar{x}) + q(\bar{x})$, where $\bar{x} = (\bar{x}_1, \ldots, \bar{x}_n)$, $a \in k$, λ is a linear form and q is a quadratic form. Thus

$$\dim_k A = \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2} \leqq (n+1)^2.$$

Now suppose $f \in S(A)$. Then clearly $a \in S(k)$. We may assume, in the following, that $p = P(k) < \infty$.

First assume $a \neq 0$. We claim, in this case, that $f \in S_p(A)$. In fact, write $a = a_1^2 + \cdots + a_p^2$ where, say, $a_1 \neq 0$. Then $a_1^2 + \lambda(\bar{x}) + g(\bar{x}) = f_1^2$ for some $f_1 \in A$. (To see this, let $f_1 = a_1 + \dfrac{\lambda(\bar{x})}{2a_1} + q'(\bar{x})$: then $f_1^2 = a_1^2 + \lambda(\bar{x}) + \dfrac{\lambda(\bar{x})^2}{4a_1^2} + 2a_1 q'(\bar{x})$. We can choose q'

[2]) A ring R is called a *pythagorean* ring if $P(R) = 1$. A *hereditarily pythagorean* field is a formally real field all of whose formally real finite field extensions are pythagorean.

such that $\frac{\lambda(\bar{x})^2}{4a_1^2}+2a_1 q'(\bar{x})=q(\bar{x})$ since $2a_1 \neq 0.$) Having chosen f_1, we have then

$$f=a_1^2+\lambda(\bar{x})+q(\bar{x})+a_2^2+\cdots+a_p^2=f_1^2+a_2^2+\cdots+a_p^2 \in S_p(A) \subsetneqq S_{g_k(n)}(A),$$

since $p=P(k) \leqq g_k(n)$.

Now assume $a=0$. We write

$$f=\lambda(\bar{x})+q(\bar{x})=\sum_i (a_i+\lambda_i(\bar{x})+q_i(\bar{x}))^2.$$

Since k is formally real, clearly all $a_i=0$, so the RHS boils down to $\sum_i \lambda_i(\bar{x})^2$, and hence $f=q(\bar{x})=\sum_i \lambda_i(\bar{x})^2$. The latter implies that $q(x)=\sum_i \lambda_i(x)^2$ in $k[x_1,\ldots,x_n]$. It is now clear that the pythagoras number $P(A)$ is precisely equal to $g_k(n)$. Q.E.D.

Corollary 2. 11 (cf. [DLP]). *There exist (local artinian) rings of any given pythagoras number.*

Proof. Choose k to be any formally real pythagorean field. Then the proof for (2. 7) (a) shows that $g_k(n)=n$ for any n. Now apply (2. 10). Note that, for the ring A in (2. 10), $(\bar{x}_1,\ldots,\bar{x}_n)$ is the unique maximal ideal, so A is an (artinian) local ring. Q.E.D.

The above results imply, in particular, that *the pythagoras numbers of finite dimensional algebras A over a field k cannot be bounded by a function of P(k).*[3]) It can also be shown that, *if A can be generated by n elements as a k-algebra, P(A) cannot be bounded by a function of n.* In fact, let k be a formally real field, and let $f \in k[x_1,\ldots,x_n]$ be a form of degree d. Arguing as in the proof of (2. 10), one can show that f is a sum of m squares in $k[x_1,\ldots,x_n]$ iff f is a sum of m squares in $A_r=k[x_1,\ldots,x_n]/(x_1,\ldots,x_n)^r$, where $r>d$. For $n \geqq 3$, our later results will show that, for any m, we can find a form f which is in

$$S_m(k[x_1,\ldots,x_n]), \text{ but not in } S_{m-1}(k[x_1,\ldots,x_n]).$$

Thus, the pythagoras numbers of the algebras A_r tend to infinity as $r \to \infty$.

In view of the above, it would be desirable to know more about the numbers $g_k(n)$. We note in passing that knowledge of $g_k(n)$ will also give information on sums of squares of higher degree forms. In fact, any sum of squares of n-ary forms of degree d over k can be written as a sum of squares of $g_k(r)$ such forms, where $r=\binom{n+d-1}{d-1}$ is the number of distinct n-ary monomials of degree d. For more refined results in this direction (when $k=\mathbb{R}$), we refer the reader to the forthcoming work [CLR_2].

The upper bound $g_k(n) \leqq nP(k)$ obtained above can probably be substantially improved, at least for specific fields. For example, L. Mordell [M_2] has shown that, for $k=\mathbb{Q}$, any n-ary positive semidefinite $\mathbb{Q}$-quadratic form can be expressed as a sum of $n+3$ squares of $\mathbb{Q}$-linear forms. This gives $g_{\mathbb{Q}}(n)=n+3$ (which implies that any finite dimensional $\mathbb{Q}$-algebra A has $P(A) \leqq \dim_{\mathbb{Q}} A+3$). Unfortunately, $g_k(n)$ has been determined for very few fields, let alone rings.

[3]) It is unknown, however, whether the pythagoras numbers of finite dimensional field extensions of k are bounded if $P(k)<\infty$: see the discussion after Problem 2 in § 9.

§ 3. Pythagoras number of real affine curves

We shall now show that any affine curve defined over a real-closed field k_0 has finite pythagoras number:

Theorem 3. 1. *Let k_0 be a real-closed field, and A be an affine k_0-algebra of transcendence degree* 1. *Then $P(A) < \infty$.*

Proof. By the Noether Normalization Theorem, there exists an element $t \in A$ transcendental over k_0 such that A is an integral extension of $k = k_0[t]$. Since A is finitely generated as a k_0-algebra, A is finitely generated as a k-module. Therefore, (2. 7) (b) applies, and we have $P(A) < \infty$. Q.E.D.

Corollary 3. 2. *Let k_0 be a real-closed field, and B be a k_0-algebra of finite k_0-dimension d. Then the polynomial algebra $A = B[t]$ has finite pythagoras number* $\;(A) \leqq 2d$.

We note in passing that, in Theorem 3. 1, the pythagoras numbers $P(A)$ *cannot* be bounded by a universal constant. In fact, given any integer n, take a finite dimensional k_0-algebra B with $P(B) = n$; this is possible by (2. 10). Then $A = B[t]$ has transcendence degree 1; by (2. 0), we have $P(A) \geqq P(B) = n$.

In the rest of this section, we shall compute explicitly the pythagoras number for various $\mathbb{R}$-affine ebras of transcendence degree 1 over $\mathbb{R}$.

Example 3. 3. Let $A = \mathbb{R}[x_1, \ldots, x_n]/\mathfrak{A}$, where $\mathfrak{A}$ is the ideal generated by $x_i x_j$, for all $i \neq j$. Let $\bar{x}_i$ be the image of x_i in A, and $t = \bar{x}_1 + \cdots + \bar{x}_n$. Then $\bar{x}_i t = \bar{x}_i^2$ so each $\bar{x}_i$ is integral over $\mathbb{R}[t]$. As an $\mathbb{R}[t]$-module, A is generated by $\bar{x}_1, \ldots, \bar{x}$ o our general method above gives $P(A) \leqq 2n$. We shall now use an ad hoc argumen show that, in fact, $) = 2$. Let $f(\bar{x}_1, \ldots, \bar{x}_n) \in S(A)$. We may assume that

$$f(\bar{x}_1, \ldots, \bar{x}_n) = a + \bar{x}_1 g_1(\bar{x}_1) + \cdots + \bar{x}_n g_n(\bar{x}_n),$$

where $a \in \mathbb{R}$ and the g_j's are polynomials in one variable. Mapping A to $\mathbb{R}[\bar{x}_i]$ by sending $\bar{x}_i$ to $\bar{x}_i$ and other $\bar{x}_j$'s to 0, we see that $a + \bar{x}_i g_i(\bar{x}_i) \in S(\mathbb{R}[\bar{x}_i])$. In particular, $a \geqq 0$. If $a \neq 0$, then

$$f = \frac{1}{a^{n-1}} (a + \bar{x}_1 g_1(\bar{x}_1)) \cdots (a + \bar{x}_n g_n(\bar{x}_n)).$$

Each factor is a sum of two squares, since $P(\mathbb{R}[\bar{x}_i]) = 2$. Hence, by the 2-square identity, f is a sum of 2 squares in A. Finally, suppose $a = 0$. Write $\bar{x}_i g_i(\bar{x}_i) = h_i(\bar{x}_i)^2 + k_i(\bar{x}_i)^2$. Clearly, h_i, k_i are divisible by $\bar{x}_i$, so

$$h_i(\bar{x}_i)\, h_j(\bar{x}_j) = 0 = k_i(\bar{x}_i)\, k_j(\bar{x}_j)$$

for $i \neq j$. In we have, therefore,

$$\begin{aligned} f &= h_1(\bar{x}_1)^2 + \cdots + h_n(\bar{x}_n)^2 + k_1(\bar{x}_1)^2 + \cdots + k_n(\bar{x}_n)^2 \\ &= (h_1(\bar{x}_1) + \cdots + h_n(\bar{x}_n))^2 + (k_1(\bar{x}_1) + \cdots + k_n(\bar{x}_n))^2, \end{aligned}$$

so $P(A) \leqq 2$. Clearly $1 + \bar{x}_i^2$ is not a square in A, so $P(A) = 2$.

The algebra considered above has, of course, a lot of zero-divisors. Now let us consider affine *domains* A of transcendence degree 1 over a real-closed field k_0. It will be of interest to obtain upper bounds on $P(A)$ which are more explicit and more efficient than the one given in (3. 1). Under very favorable circumstances, when one can apply the 2-square theorem of Choi-Lam-Reznick-Rosenberg [CLRR], (2. 5), one gets indeed a sharp result $P(A)=2$:

Theorem 3. 4. *Suppose the k_0-algebra A in* (3. 1) *is such that A and $A[\sqrt{-1}]$ are both* UFD's. *Then $P(A)=2$.*

Proof. In view of (2. 4) (b), we may assume that $\sqrt{-1}\notin A$. Let K be the quotient field of A. Since K is a function field of one variable over k_0, Witt's theorem [W] gives $P(K)=2$. Let $a\in S(A)$; then $a\in S(K)=S_2(K)$. By [CLRR], we get $a\in S_2(A)$ so $P(A)\leqq 2$. This must be an equality, by (2. 1). Q.E.D.

We record the following instance of (3. 4) because it provides an interesting exceptional case to the pythagoras number computations of the "generic rings" considered in § 8 below:

Proposition 3. 5. *Let $A=\mathbb{R}[x,y]/(1+x^2+y^2)$. Then $P(A)=2$.*

Proof. This ring A is known to be a UFD by [S], p. 36. If we adjoin $i=\sqrt{-1}$, the resulting ring is isomorphic to

$$\mathbb{C}[x,y]/(1+x^2+y^2)\cong\mathbb{C}[x,y]/(1-x^2-y^2),$$

which is the complex coordinate ring of the unit circle. This ring may be viewed as the localization $\mathbb{C}[t,t^{-1}]$ of the polynomial ring $\mathbb{C}[t]$, where $t=x+iy$, so it is a UFD. Thus, (3. 4) applies and we have $P(A)=2$. Q.E.D.

The same method, unfortunately, does not apply to $B=\mathbb{R}[x,y]/(1-x^2-y^2)$, the real coordinate ring of the circle. For this ring, $B[\sqrt{-1}]$ is a UFD, as pointed out above, but it is known that B itself is *not* a UFD (see [N], or [Sw], p. 273), so the theorem of [CLRR] does not apply here. Nevertheless, we have the following result:

Proposition 3. 6. *Let f be a real polynomial function which is everywhere nonnegative on the unit circle S^1. Then f is a sum of two squares of real polynomial functions on S^1. In particular, $P(B)=2$ for $B=\mathbb{R}[x,y]/(1-x^2-y^2)$.*

Proof. This is "plagiarized" from a result of F. Riesz and L. Fejér [F] on trigonometric polynomials! By [F], § 1, if a trigonometric polynomial

$$p(\theta)=c+\sum_{k=1}^{n}(a_k\cos k\theta+b_k\sin k\theta)$$

with real coefficients is nonnegative for all (real) angles θ, then $p(\theta)=|P(e^{i\theta})|^2$ for a suitable complex polynomial $P(z)\in\mathbb{C}[z]$ (see also [PS], Part 6, Problem 40). Now consider the given function $f\geqq 0$ on S^1. Suppose it is given by a polynomial $f(x,y)\in\mathbb{R}[x,y]$, and let $p(\theta):=f(\cos\theta,\sin\theta)$. As is well-known, the latter is convertible to a real trigonometric polynomial. By assumption, $p(\theta)\geqq 0$ for all angles θ, so we can write $p(\theta)=|P(e^{i\theta})|^2$ as above. Now write $P(e^{i\theta})=p_1(\theta)+ip_2(\theta)$ where p_j are real trigonometric polynomials. There exist real polynomials $f_j(x,y)$ such that

$$p_j(\theta)=f_j(\cos\theta,\sin\theta).$$

Therefore, we have

$$f(\cos\theta, \sin\theta) = p(\theta) = p_1(\theta)^2 + p_2(\theta)^2 = f_1(\cos\theta, \sin\theta)^2 + f_2(\cos\theta, \sin\theta)^2.$$

Since this holds for all θ, we must have $f = f_1^2 + f_2^2$ in the coordinate ring of S^1, as desired. Q.E.D.

In essence, the proof above depends on identifying the ring $B = \mathbb{R}[x, y]/(1 - x^2 - y^2)$ with the subring B' of $\mathbb{C}[z, z^{-1}]$ consisting of Laurent polynomials $F(z) = \sum_{k=-n}^{n} \alpha_k z^k$ such that $\alpha_{-k} = \bar{\alpha}_k$ for all k. (We identify x with $(z + z^{-1})/2$ and y with $(z - z^{-1})/2i$.) The Riesz-Féjer Theorem is proved by examining the distribution of the zeros of F in the complex plane when F is assumed to be nonnegative on the unit circle. By modifying this idea, we can also deal with the ring $A = \mathbb{R}[x, y]/(1 + x^2 + y^2)$ in (3. 5) by using complex (Laurent) polynomials instead of using the results in [CLRR]. Here, we identify A with the subring $A' \subset \mathbb{C}[z, z^{-1}]$ consisting of $G(z) = \sum_{k=-n}^{n} \alpha_k z^k$ such that $\alpha_{-k} = (-1)^k \bar{\alpha}_k$ for all k. (We identify x with $(z - z^{-1})/2$ and y with $(z + z^{-1})/2i$.) After analyzing the distribution of the zeros of G (without any positivity condition this time), we can see, just as in the proof of (3. 6), that any $g \in A$ is a sum of two squares in A. This gives a second proof for the fact that $P(A) = 2$.

Using (3. 5) and (3. 6), we can now obtain the following general result:

Theorem 3. 7. *Let* $R = \mathbb{R}[x, y]/(h)$, *where* $h(x, y)$ *is a quadratic polynomial. Then* $P(R) = 2$.

Proof. By elementary considerations, we see that the ring R has *nine* possible isomorphism types, corresponding to the following nine choices of $h(x, y)$:

$$h_1 = x^2 + y^2 + 1, \qquad h_2 = x^2 + y^2 - 1, \qquad h_3 = xy,$$
$$h_4 = xy - 1, \qquad h_5 = x^2 + 1, \qquad h_6 = x^2 + y,$$
$$h_7 = y^2, \qquad h_8 = y^2 - 1, \qquad h_9 = x^2 + y^2.$$

In all cases, it is easy to see that $1 + x^2$ is *not* a square in R, so we need only show that $P(R) \leqq 2$. The first two cases are covered by (3. 5) and (3. 6). The third case is a special case of (3. 3), and the fourth case follows from (2. 1) since $\mathbb{R}[x, y]/(h_4) \cong \mathbb{R}[x, x^{-1}]$. The fifth and sixth cases are clear since $\mathbb{R}[x, y]/(h_5) \cong \mathbb{C}[y]$ and $\mathbb{R}[x, y]/(h_6) \cong \mathbb{R}[x]$. For the seventh case, we use the fact that, for any positive strictly definite polynomial $F(x)$, there exist *relatively prime* polynomials $\phi(x)$ and $\psi(x)$ such that $F(x) = \phi(x)^2 + \psi(x)^2$. (The proof of this fact is left to the reader.) Given a sum of squares

$$S(x, y) = \sum (f_j(x) + g_j(x)y)^2 = \sum f_j(x)^2 + 2\sum f_j(x)g_j(x)y$$

in $\mathbb{R}[x, y]/(h_7)$, let $f(x)$ be the greatest common divisor of the f_j's. Then

$$\sum_j f_j(x)g_j(x) = f(x)g(x) \quad \text{and} \quad \sum f_j(x)^2 = f(x)^2 F(x),$$

where $g, F \in \mathbb{R}[x]$, and F is positive strictly definite. Writing $F(x) = \phi(x)^2 + \psi(x)^2$ as above and writing $1 = \phi(x)\phi_1(x) + \psi(x)\psi_1(x)$ for suitable $\phi_1(x)$ and $\psi_1(x)$, we have

$$S(x, y) = (f(x)\phi(x) + \phi_1(x)g(x)y)^2 + (f(x)\psi(x) + \psi_1(x)g(x)y)^2$$

in $\mathbb{R}[x, y]/(h_7)$, as desired. To treat h_8, let $S(x, y) = \phi_1(x) + \phi_2(x) y$ be a sum of squares in $\mathbb{R}[x, y]/(y^2 - 1)$. Setting $y = \pm 1$, we see that $\phi_1(x) \pm \phi_2(x)$ are positive semidefinite. Writing

$$\phi_1(x) + \phi_2(x) = g_1(x)^2 + h_1(x)^2,$$
$$\phi_1(x) - \phi_2(x) = g_2(x)^2 + h_2(x)^2,$$

a straightforward computation shows that

$$S(x, y) = \frac{1}{4}[g_1 + g_2 + y(g_1 - g_2)]^2 + \frac{1}{4}[h_1 + h_2 + y(h_1 - h_2)]^2$$

in $\mathbb{R}[x, y]/(y^2 - 1)$. Finally, to treat h_9, let $S(x, y) = a + xf(x, y) + yg(x, y)$ be a sum of squares in $\mathbb{R}[x, y]/(x^2 + y^2)$. If $a > 0$, we are done by writing

$$S(x, y) \equiv \frac{1}{4a}(2a + xf + yg)^2 + \frac{1}{4a}(yf - xg)^2 (\operatorname{mod} x^2 + y^2).$$

If, on the other hand, $a = 0$, then $S(x, y)$ cannot have linear terms and we can write $S \equiv x^2 F(x, y) + xyG(x, y) (\operatorname{mod} x^2 + y^2)$. But then

$$S(x, y) \equiv \frac{1}{4}(x + xF + yG)^2 + \frac{1}{4}(y + xG - yF)^2 (\operatorname{mod} x^2 + y^2),$$

so the pythagoras number is 2 in all cases. Q.E.D.

In contrast to (3. 7), there exist, however, many affine $\mathbb{R}$-algebras $R = \mathbb{R}[x, y]/(h)$ with $\deg h > 2$ such that $P(R) > 2$. We can even choose C such that both C and $C[\sqrt{-1}]$ are Dedekind domains (though not both PID's, in view of (3. 4)). An explicit example is the real coordinate ring of the elliptic curve $y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$ $(\lambda_i \in \mathbb{R})$. This can be deduced from the following:

Proposition 3. 8. *Let $k(x) \in \mathbb{R}[x]$ be a nonlinear polynomial of odd degree. Then the ring $R = \mathbb{R}[x, y]/(y^2 - k(x))$ has pythagoras number* 3 *or* 4.

Proof. In view of the proof of (3. 1), it suffices to show that $P(R) > 2$. *We claim that $1 + \bar{x}^2 + \bar{y}^2$ is not a sum of two squares in R.* In fact, if it is, we will have an equation

$$1 + \bar{x}^2 + \bar{y}^2 = (f_1(\bar{x}) + y g_1(\bar{x}))^2 + (f_2(\bar{x}) + y g_2(\bar{x}))^2 \in R,$$

which leads to a system of two equations:

$$(3.\ 9) \qquad f_1(x)^2 + f_2(x)^2 + k(x)(g_1(x)^2 + g_2(x)^2) = 1 + x^2 + k(x),$$

$$(3.\ 10) \qquad f_1(x) g_1(x) + f_2(x) g_2(x) = 0.$$

By an obvious degree consideration, (3. 9) implies that $g_1(x)$, $g_2(x)$ must be scalars with $g_1^2 + g_2^2 = 1$, and so, from (3. 10), $f_1(x)$, $f_2(x)$ are linearly dependent. If, say, $f_2 = \lambda f_1$ $(\lambda \in \mathbb{R})$, then (3. 9) leads to a contradiction $(1 + \lambda^2) f_1(x)^2 = 1 + x^2$. Q.E.D.

We shall now conclude this section by showing a class of nonreal $\mathbb{R}$-algebras (possibly *not* of finite level) which have arbitrary transcendence degrees and finite pythagoras numbers. By definition, we say that a ring A is *formally real* if $a_1^2+\cdots+a_r^2=0$ in A implies that all $a_i=0$ [4]). Otherwise, we say that A is *nonreal*. Note that, in the category of rings, this need not imply that A has finite level.

Example 3. 11. Let $f_1,\ldots,f_r \in \mathbb{R}[x_1,\ldots,x_n]$ be polynomials such that

$$\mathbb{R}[x_1,\ldots,x_n]/(f_1,\ldots,f_r)$$

has transcendence degree $\leqq 1$ over $\mathbb{R}$. Then $A=\mathbb{R}[x_1,\ldots,x_n]/(f_1^2+\cdots+f_r^2)$ has a finite pythagoras number.

(This follows from (2. 6), (3. 1), plus the simple observati[illegible] that the transcendence degree of $\mathbb{R}[x_1,\ldots,x_n]/(f_1^2,\ldots,f_r^2)$ equals the transcendence de[illegible]ee of

$$\mathbb{R}[x_1,\ldots,x_n]/(f_1,\ldots,f_r).)$$

For instance, [illegible] $=f_i(x_i)\neq 0$, and $A=\mathbb{R}[x_1,\ldots,x_n]/(f_1^2+\cdots+f_r^2)$ where $r=n$ or $n-1$, then (3. 11) app[illegible]s and we have $P(A)<\infty$.

§ 4. Sufficient conditions for $P(A[x])=\infty$

In the last section, we have shown that if k is a real-closed field, then any k-affine algebra of transcendence degree $\leqq 1$ has a finite pythagoras number. In this section, we shall show that the situation is quite different for affine algebras of transcendence degree $\geqq 2$. For instance, one of the main results in this section is the following:

Theorem 4. 1. *Let k be any formally real field, and $R=k[x_1,\ldots,x_n]$ $(n\geqq 2)$. Then $P(R)=\infty$.*

In fact, much more general results will be obtained. However, before we proceed to the formulation of these results, [illegible] will be useful to observe several consequences of Theorem 4. 1.

(4. 2) If A is a field, it is unknown whether $P(A)<\infty$ would imply $P(A[x])<\infty$ (see the discussion after Problem 2 in § 9). However, *if A is a ring (or even a PID), this implication is definitely false*; in fact, $A=\mathbb{R}[y]$ is a PID with $P(A)=2$, but $P(A[x])=\infty$ according to (4. 1).

(4. 3) ***A nonreal affine algebra need not have finite pythagoras number.***

For instance, consider $A=\mathbb{R}[u,v,x,y]/(u^2+v^2)$, which can be mapped by a ring homomorphism onto $\mathbb{R}[x,y]$. Since $P(\mathbb{R}[x,y])=\infty$, we must have $P(A)=\infty$ by (2. 0).

(4. 4) *It is possible that all proper quotients of a ring R have finite pythagoras number, but R itself has infinite pythagoras number.* (All proper quotients of $\mathbb{R}[x,y]$ have transcendence degree $\leqq 1$ over $\mathbb{R}$.)

(4. 5) *It is possible that the localizations at all prime ideals of a ring R have finite (and bounded) pythagoras numbers but R has an infinite pythagoras number.*

---

[4]) In case A is an integral domain, this means that the quotient field of A is formally real.

In fact, let $R = \mathbb{R}[x, y]$. By (4. 1), we have $P(R) = \infty$, but, by (2. 3) and (5. 2) below, the localization of R at each of its prime ideals $\mathfrak{p}$ has pythagoras number $\leqq 4$. (In fact, in view of (2. 1) and the theorem of Cassels-Ellison-Pfister [CEP], the localization $R_{\mathfrak{p}}$ all have pythagoras number *equal to* 4.)

(4. 6) *It is possible that a principal ideal domain R has a quotient field F with* $P(F) < \infty$, *but* $P(R) = \infty$.

The possibility of constructing such a PID from the result (4. 1) was pointed out to us by A. Wadsworth. To explain this construction, we need a definition: if $\mathfrak{A}$ is an ideal in a commutative ring A, we shall say that $\mathfrak{A}$ is *real* if the quotient ring $A/\mathfrak{A}$ is formally real.

Lemma 4. 7 (A. Wadsworth). *Let S be a multiplicative set in an integral domain A generated by a set* $\{s_i \neq 0 : i \in I\}$ *each of whose elements generates a real (principal) ideal. Then, for any element* $a \in A$, *the length of a in A is equal to the length of a in the localization* $S^{-1}A$. *In particular*, $P(A) = P(S^{-1}A)$.

Proof. Suppose $a \in S_r(S^{-1}A)$. Then for some $s \in S$, $s^2 a = a_1^2 + \cdots + a_r^2$ where $a_i \in A$. To show that $a \in S_r(A)$, it suffices to treat the case $s = s_i$. Going modulo (s), we see that $a_j = sb_j$ (for suitable $b_j \in A$), since A/sA is formally real. Cancelling s^2, we get $a = b_1^2 + \cdots + b_r^2 \in S_r(A)$. Q.E.D.

To construct a PID as in (4. 6), fix a real-closed field k. Let S_0 be the set of irreducible polynomials $s \in k[x_1, \ldots, x_n]$ $(n \geqq 2)$ such that s generates a real (prime) ideal [5]; let S be the multiplicative set generated by S_0, and $R = S^{-1}(k[x_1, \ldots, x_n])$. It is known that any prime ideal of height $\geqq 2$ in $k[x_1, \ldots, x_n]$ contains some $s \in S_0$ (see [DE_2], p. 114[6]), so upon localization at S, all such primes become the unit ideal. Thus, R has only height one primes; since these are all principal (and nonreal), R is a PID. By [P_2], the quotient field $F = k(x_1, \ldots, x_n)$ of R has $P(F) \leqq 2^n$, but by (4. 7) and (4. 1), $P(R) = P(k[x_1, \ldots, x_n]) = \infty$.

The same idea of construction also shows the following:

(4. 8) *If a unit in a principal ideal domain R' (with* $2 \in U(R')$*) is a sum of squares in the quotient field, it may not be a sum of squares in R'.*

(This contrasts with the theorems of Artin, Cassels, and known theorems about semilocal PID's [CLRR], (4. 1), as well as level theorems about Dedekind rings [Ba]. Such an example is also of interest in view of the fact that the Witt ring of R' injects into that of its quotient field [MH], p. 93). For the construction, let $n = 2$ and let R be as above. Let $f(x_1, x_2)$ be any positive semidefinite polynomial with the property that $f^{2r+1} \notin S(k[x_1, x_2])$ for any r. Such polynomials do exist: for instance, following Stengle [St], we can take

$$f(x_1, x_2) = x_1^3 + (x_1 x_2^2 - x_1^2 - 1)^2.$$

---

[5]) This condition is equivalent to $s(x_1, \ldots, x_n)$ being an *indefinite* polynomial: see the Sign-Changing Theorem in [DE_1], p. 125.

[6]) To avoid using this result from [DE_2], one can restrict this construction to the case $n = 2$. In this case, it is easy to see that any maximal ideal contains a linear polynomial $ax_1 + bx_2 + c \in S_0$. (Therefore, everything would have worked also if we localize $k[x_1, x_2]$ at the multiplicative set generated by the linear polynomials.)

(In fact, the better known Motzkin polynomial (cf. § 8) already has the desired property, though we will not digress to give the proof here.) We have $f \in S_4(k(x_1, x_2))$: this follows either by direct computation, or by the theorem of Hilbert [H]. Now let R' be the localization $R[f^{-1}]$, which is a PID. We claim that the unit $f \notin S(R')$. For, if otherwise, we will have $f^{2r+1} \in S(R)$ for some r, and therefore by (4. 7), $f^{2r+1} \in S(k[x_1, x_2])$, a contradiction. In this example, it is true, though, that $R' \cap S_2(k(x_1, x_2)) = S_2(R')$; this follows easily from the corresponding equation for $k[x_1, x_2]$, which holds by the 2-square theorem of [CLRR].

We shall now begin the proof of Theorem 4. 1. The idea of the proof is to study a polynomial ring $A[x]$ in one variable over a (formally real) integral domain A, and try to give sufficient conditions on A which would guarantee the infinitude of the pythagoras number of $A[x]$. It will be seen that these sufficient conditions are satisfied by $A = k[x_1, \ldots, x_{n-1}]$ $(n \geqq 2)$ as well as many other affine k-algebras, where k is any formally real field. In particular, Theorem 4. 1 will follow. The same sufficient conditions are also satisfied, for instance, by any order A in a totally real algebraic number field, so we also get, as a bonus, the infinitude of the pythagoras numbers of $A[x]$ for such orders. This contrasts with Pourchet's result [P] that $P(K[x]) \leqq 5$ for any number field K.

To facilitate the formulation of the results below, let us set up some general notations. For a ring A and a given integer n, we shall write $U_n = U_n(A)$ for the set of n-tuples over A of "unit length":

$$U_n(A) = \{(a_1, \ldots, a_n) \in A^n : a_1^2 + \cdots + a_n^2 = 1\}.$$

Further, we write $O_n(A)$ for the group of $n \times n$ orthogonal matrices over A, i.e.

$$O_n(A) = \{M \in M_n(A) : M^t M = I\}.$$

As is well-known, the group $O_n(A)$ acts on U_n. We shall work with rings A which satisfy the following two conditions:

$(1)_n$ *$O_n(A)$ acts transitively on $U_n = U_n(A)$.*

$(2)_n$ *There exists a nonzero element $\alpha \in A$ such [illegible] for any $(a_1, \ldots, a_n) \in U_n$, $\alpha \nmid a_i$ whenever $a_i \neq 0$.*

The following easy observation turns out to be useful later:

Lemma 4. 9. *Assume that A is an integral domain of characteristic $\neq 2$ satisfying $(2)_n$. Then A contains infinitely many elements $\alpha \nmid 2$ satisfying $(2)_n$.*

Proof. Fix any $\alpha \neq 0$ satisfying $(2)_n$. Clearly, α is a nonunit in A. Replacing α by 2α if necessary, we may assume that $\alpha \nmid 2$. Therefore, any nonzero $\alpha' \in A \cdot \alpha$ will not divide 2, and will satisfy $(2)_n$. Since A contains a nonunit α, it cannot be a field and therefore must have infinite cardinality. Since $\operatorname{Card} A \cdot \alpha = \operatorname{Card} A$, we see that there are infinitely many [illegible]s described in the lemma. Q.E.D.

Theorem 4. 10. *Let A be a formally real domain and n be a fixed integer. Assume that [illegible]fies $(1)_n$ and $(2)_n$ above. Let $\alpha_1 = 0$ and let $\{\alpha_j : j \geqq 2\}$ be a sequence of distinct elements [illegible]cribed in (4. 9). Suppose $f(x) \in A[x]$ is a polynomial of length n. Let $r \in \mathbb{N}$ be such that $\deg f < 2r$. Then $F(x) = \Delta_r(x)^2 f(x) + 1$ has length $n+1$, where $\Delta_r(x) := (x - \alpha_1) \cdots (x - \alpha_r)$.*

This theorem has the following immediate consequence:

Corollary 4. 11. *If a formally real domain A satisfies $(1)_n$ and $(2)_n$ for all n, then $P(A[x]) = \infty$.*

Proof of (4. 10). Clearly $F(x) \in S_{n+1}(A[x])$, so it is enough to show that $F(x) \notin S_n(A[x])$. Assume, on the contrary, that $F(x) = \sum_{i=1}^{n} \psi_i(x)^2$, $\psi_i \in A[x]$. Since A is formally real, $\deg \psi_i < 2r$ for all i. Setting $x = 0$, we have $1 = \sum_{i=1}^{n} \psi_i(0)^2$ (since $\alpha_1 = 0 \Rightarrow x \mid \Delta_r(x)$). Therefore, after an orthogonal transformation over A, we may assume, by $(1)_n$, that $\psi_1(0) = 1$ and $\psi_i(0) = 0$ $(i \geqq 2)$. Write $\psi_1(x) = 1 + x\phi_1(x)$ and $\psi_i(x) = x\phi_i(x)$ $(i > 2)$. Let α be any of $\alpha_2, \ldots, \alpha_r$ and evaluate $F(x)$ at α; we get

$$1 = (1 + \alpha\phi_1(\alpha))^2 + (\alpha\phi_2(\alpha))^2 + \cdots + (\alpha\phi_n(\alpha))^2.$$

The property of α in $(2)_n$ implies now that $\phi_2(\alpha) = \cdots = \phi_n(\alpha) = 0$, and so each $\psi_i(x)$ $(i \geqq 2)$ is divisible by $\Delta_r(x)$, say $\psi_i(x) = \Delta_r(x)\, \psi_i'(x)$ $(i \geqq 2)$. By transposition, we have

$$\Delta_r(x)^2 \left(f(x) - \sum_{i=2}^{n} \psi_i'(x)^2 \right) = \psi_1(x)^2 - 1 = (\psi_1(x) - 1)(2 + x\phi_1(x)).$$

Since none of $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ divides 2, this clearly implies that $\Delta_r(x)^2 \mid (\psi_1(x) - 1)$. But $\deg \psi_1 < 2r$ so we must have $\psi_1(x) \equiv 1$, and therefore $f(x) = \sum_{i=2}^{n} \psi_i'(x)^2$, contradicting the fact that $f(x)$ has length n. Q.E.D.

Corollary 4. 12. *Let A be a formally real domain which is not a field. Assume that, for any n, if $a_1^2 + \cdots + a_n^2 = 1$ in A, then all except one of the a_i's are zero. Then $P(A[x]) = \infty$.*

Proof. Here, $O_n(A)$ consists of all permutations of $(\pm 1, 0, \ldots, 0)$ so clearly $(1)_n$ is satisfied for all n. For $(2)_n$, we can take α to be any nonunit in A. Thus, Theorem 4. 10 applies. Q.E.D.

For A as in the Corollary, assume, say, 2 is not a unit. Then, in the construction of (4. 10), we can take $\alpha_1 = 0$ and $\alpha_i = 2^i$ $(i \geqq 2)$, and so $\Delta_r(x) = x \prod_{i=2}^{r} (x - 2^i)$. Starting with $f_1(x) = 1$, we can construct recursively a sequence of universal polynomials

(4. 13)
$$f_m(x) = \sum_{i=1}^{m} \prod_{j=2}^{i} \Delta_{2^{m-j}}(x)^2 \in S_m(\mathbb{Z}[x]),$$

such that, for each m, $f_m(x)$ has length m in $A[x]$. (For $i = 1$, the empty product is defined to be 1.) Note that $f_m(x)$ has degree $2^m - 2$.

Theorem 4. 14. *Let A be any commutative ring which admits a homomorphism into the ring of integers of a totally real algebraic number field K. Then, for each m, the polynomial $f_m(x)$ defined in* (4. 13) *has length m in $A[x]$. In particular, $P(A[x]) = \infty$.*

Proof. We may assume that A *is* the ring of algebraic integers in K. Suppose $a_1^2 + \cdots + a_n^2 = 1$ in A. Since all the imbeddings of K are real, the conjugates of each a_i must have absolute value $\leqq 1$. Thus $|N_{K/\mathbb{Q}}(a_i)| \leqq 1$. But $N_{K/\mathbb{Q}}(a_i) \in \mathbb{Z}$ so it must be 0 or ± 1. This clearly implies that all except one of the a_i's are zero. Now apply (4. 12). Q.E.D.

As a special case of (4. 14), we have $P(\mathbb{Z}[x]) = \infty$. This improves (and completes) an earlier result of Peters [Pe₂] which gave $P(\mathbb{Z}[x]) \geqq 6$.

To get other applications of Theorem 4. 10, we state the following variation of (4. 11):

Corollary 4. 15. *Let A be a formally real domain which is not a field. Assume that A contains a field k such that, for any n, if $a_1^2 + \cdots + a_n^2 = 1$ in A, then each $a_i \in k$. Then $P(A[x]) = \infty$.*

Proof. By Witt's Theorem [L], p. 19, the field k satisfies the property $(1)_n$. This and the given hypothesis clearly imply that A also satisfies $(1)_n$. For $(2)_n$, we can take α (as before) to be any nonunit of A. Q.E.D.

From (4. 15), we get immediately the following result (which the reader should compare with (3. 2)):

Theorem 4. 16. *Let k be a formally real field, and let A be any subalgebra of $k[x_1, \ldots, x_r]$ not equal to k. Then $P(A[x]) = \infty$.*

Consider, for instance, the case $A = k[y]$. In the construction in the proof of (4. 10) we can take $\alpha_1 = 0$, and $\alpha_i = iy$ $(i \geqq 2)$, and so $\Delta_r(x, y) = x \prod_{i=2}^{r} (x - iy)$. Starting with $f_1(x, y) = 1$ and proceeding by recursion, we get the universal polynomials

$$(4. 17) \qquad f_m(x, y) = \sum_{i=1}^{m} \prod_{j=2}^{i} \Delta_{2^{m-j}}(x, y)^2 \in S_m(\mathbb{Z}[x, y]),$$

such that, for each m, $f_m(x, y)$ has length m in $k[x, y]$ for any formally real field k. Again, the total degree of $f_m(x, y)$ is $2^m - 2$.

Corollary 4. 18. *Let R be any commutative ring with infinite level. Then*

$$P(R[x_0, \ldots, x_r]) = \infty \quad \textit{for any} \quad r \geqq 1.$$

Proof. By a well-known result, if R has infinite level, then it has a real prime ideal $\mathfrak{p}$. We have a natural homomorphism $R[x_0, \ldots, x_r] \to k[x_0, \ldots, x_r]$, where k is the (formally real) quotient field of $R/\mathfrak{p}$. Since $f_m(x_0, x_1)$ has length m in $k[x_0, \ldots, x_r]$, it must have length m in $R[x_0, \ldots, x_r]$. This being true for all $m \geqq 1$, we must have

$$P(R[x_0, \ldots, x_r]) = \infty. \quad \text{Q.E.D.}$$

Using (4. 18), we can also construct affine algebras with an infinite pythagoras number which are not polynomial algebras over some subalgebra. For instance, consider the quadric defined by a real quadratic form $q(x_1, \dots, x_n) \in \mathbb{R}[x_1, \dots, x_n]$, with the associated coordinate ring $B = \mathbb{R}[x_1, \dots, x_n]/(q)$. If rank $q \leqq n-2$, then B has a homomorphism onto $\mathbb{R}[x, y]$, so $P(B) = \infty$. If rank $q \geqq n-1$ and q is semidefinite, then $P(B) < \infty$ by (3. 11). Now assume rank $q \geqq n-1$ and q is indefinite. If $n = 2$, B has transcendence degree 1 so $P(B) < \infty$ by (3. 1). If $n = 3$, we have essentially two cases: $q = x_1^2 - x_2^2$ and $q = x_1^2 + x_2^2 - x_3^2$. In the first case, B maps onto $\mathbb{R}[x, y]$ again and we get $P(B) = \infty$. In the second case $B = \mathbb{R}[x_1, x_2][\sqrt{x_1^2 + x_2^2}]$ and we see easily that $P(\mathbb{R}[x_1, x_2]) = \infty \Rightarrow P(B) = \infty$ (cf. [EL], (3. 10) (1)). Finally, if $n \geqq 4$, then rank $q \geqq 3$ and B has a homomorphism onto $\mathbb{R}[x_1, x_2, x_3]/(x_1^2 + x_2^2 - x_3^2)$ so again $P(B) = \infty$.

In summary, the only cases where we get finite pythagoras numbers are the following:

$$\mathbb{R}[x_1, x_2]/(x_1^2 - x_2^2),$$
$$\mathbb{R}[x_1, \dots, x_n]/(x_1^2 + \cdots + x_{n-1}^2),$$
$$\mathbb{R}[x_1, \dots, x_n]/(x_1^2 + \cdots + x_n^2).$$

In all other cases, we get infinite pythagoras numbers.

Another class of examples is given by the 2-dimensional algebras

$$R = k[x, y, z]/(z^a - x^b y^c),$$

where a, b, c are nonnegative integers (not all zero). Using the methods in this section, it can be shown that, for any formally real field k, $P(R) = \infty$; the details will be left to the reader.

§ 4 bis. Quantitative improvements of the results

In $\mathbb{Z}[x]$, we have shown that there exist polynomials of any prescribed length m. It is of interest to ask the following question: *what is the smallest integer $d = d(m)$ such that there exists a polynomial of degree d having length m?* As we have observed before, the polynomial $f_m(x)$ of length m constructed in (4. 13) has degree $2^m - 2$, which is essentially exponential in m. We shall now show that, by a more careful construction, we can replace $f_m(x)$ by some $g_m(x)$ whose degree is *linear* in m.

Proposition 4. 1'. *Suppose $g(x) \in \mathbb{Z}[x]$ has length m. Then, for sufficiently large integers t, $G(x) := 1 + (x-t)^2 g(x)$ has length $m+1$.*

Proof. Say $\deg g < 2r$. Let $N = \max\{g(i) : 1 \leqq i \leqq r\}$ and let t be any integer such that

(4. 2') $\quad t > r \quad and \quad (t-r)^2 > 2 + N.$

We claim that $G(x)=1+(x-t)^2 g(x)$ has length $m+1$. Indeed, assume $G(x)=\sum_{i=1}^{m} g_i(x)^2$ in $\mathbb{Z}[x]$; clearly, each g_i has degree $<r$. Write $g_i(x)=a_i+(x-t)\,h_i(x)$, where $0\leqq a_i<t$ and $h_i\in\mathbb{Z}[x]$. Then $a_1^2+\cdots+a_m^2=1$; upon reindexing, we may assume that

$$(a_1,\ldots,a_m)=(1,0,\ldots,0),$$

so

$$G(x)=\left(1+(x-t)\,h_1\right)^2+(x-t)^2\sum_{i=2}^{m} h_i^2,$$

or

$$(x-t)^2 g(x)=2(x-t)\,h_1+(x-t)^2\sum_{i=1}^{m} h_i^2.$$

This implies that $(x-t)|h_1$. Writing $h_1(x)=(x-t)\,h(x)$ and cancelling $(x-t)^2$, we get

$$g(x)=2h+(x-t)^2h^2+\sum_{i=2}^{m} h_i^2. \tag{4. 3'}$$

Let i be any integer such that $1\leqq i\leqq r$. *We claim that* $h(i)=0$. In fact, if $a=|h(i)|\neq 0$, then $a\geqq 1$, and evaluation of (4. 3′) at $x=i$ gives

$$\begin{aligned} g(i) &\geqq 2h(i)+(i-t)^2\,h(i)^2\geqq -2a^2+(t-i)^2a^2\\ &=a^2[(t-i)^2-2]>N=\max\{g(j):1\leqq j\leqq r\}, \end{aligned}$$

which is a contradiction. This proves the claim, and so $h(x)=\prod_{i=1}^{r}(x-i)\,h'(x)$ for sor If $h'\neq$ hen $\deg h\geqq r$ and so $\deg g_1=\deg\left(1+(x-t)^2h\right)\geqq r+2$, a contradiction. T fore h – $a=0$. But then (4. 3′) gives $g(x)=\sum_{i=2}^{m} h_i^2$, again a contradiction. Q.E.D.

Starting with the (constant) polynomial $g(x)=7$ of length 4 and using (4. 1′) recursively, we get

Corollary 4. 4′. *For any $m\geqq 4$, there exists a polynomial $g_m(x)$ in $\mathbb{Z}[x]$ of length m such that* $\deg g_m=2(m-4)$.

The proof of (4. 1′) used very special properties of the ring of integers and does not seem to generalize to other rings of coefficients. On the other hand, as we ha e seen already, the methods of § 4 apply to a much larger class of rings. Thus, (4.1′) shoul t be viewed as a substitute for (4. 10), but rather, only as a technical device which gi uantitative impro ents for lengths in $\mathbb{Z}[x]$.

A similar improvement is possible for lengths in $k[x, y]$ where k is rmally real field. In (4. 17), we have constructed a polynomial $f_m(x, y)\in k[x, y]$ of len , with total degree 2^m-2. By using an alternative construction, we can replace $f_m(x,$ y a suitable $g_m(x, y)$ with total degree of the order of magnitude $2^{m/2}$.

Proposition 4. 5′. *Suppose $g(x,y)\in k[x,y]$ has length m, with $\deg_x g<2r$. Then $G(x,y)=1+(y-x^r)^2 g(x,y)$ has length $m+1$.*

Proof. Suppose, instead, that $G=\sum_{i=1}^{m} g_i^2$. Write each $g_i=a_i+(y-x^r)h_i$ where $h_i\in k[x,y]$ and $a_i\in k[x]$. Setting $y=x^r$, we have $1=\sum a_i^2$. Thus, all $a_i\in k$ so, after an orthogonal transformation over k, we may assume that $(a_1,\ldots,a_m)=(1,0,\ldots,0)$. Proceeding as in the proof of (4. 1′), we can write $h_1(x,y)=(y-x^r)h(x,y)$, with an equation

$$g=2h+(y-x^r)^2h^2+\sum_{i=2}^{m} h_i^2.$$

If $h\not\equiv 0$, the RHS will clearly have x-degree $\geqq 2r$, a contradiction. Thus we must have $h\equiv 0$ and $g=\sum_{i=2}^{m} h_i^2$, also a contradiction. Q.E.D.

The advantage of (4. 5′) over its counterpart in § 4 is that, in the passage from $g(x)$ to $G(x)$, although the x-degree goes up by $2r$, the y-degree goes up only by 2. Thus, in the next step of the construction, we can take $1+(x-y^s)^2G(x,y)$ for a relatively "small" s such that $2s>\deg_y G$. If we start with $g_1(x,y)=1$, $g_2(x,y)=1+x^2$, and $g_3(x,y)=1+x^2+y^2$ (of lengths, respectively, 1, 2 and 3), and construct $g_4, g_5, \ldots$, etc. two at a time (using alternately $y-x^r$ and $x-y^s$), we shall get a sequence $\{g_m(x,y)\}$ such that, for $m\geqq 4$:

$$\text{(4. 6′)}\quad \text{total degree of } g_m=\begin{cases}2^{i+2}+2^i-4i-6 & \text{if } m=2i,\\ 2^{i+2}+2^{i+1}+2^i-4i-8 & \text{if } m=2i+1.\end{cases}$$

This degree has the order of magnitude of $2^{m/2}$.

For a more systematic (quantitative) study of the length of polynomials of a *given* total degree, see the forthcoming work [CLR_2].

§ 5. Regular local rings of dimension $\leqq 2$

In this section, we shall compute the pythagoras number of certain types of regular local rings and power series rings of (Krull) dimension $\leqq 2$. The study of the case of dimension >2 requires different techniques and will be postponed to the next section. Basically, in the case of dimension $\leqq 2$, we try to get results on the *finiteness* of the pythagoras number, while in the case of dimension >2, we try to get results on the *infinitude* of the pythagoras number. Note that the "threshold" value 2 is one higher than in the case of polynomial rings; this shows a clear distinction between the "local" situation and the "global" situation.

If R is a regular local ring of dimension 1, then R is a discrete valuation ring. Assuming that 2 is invertible in R, we have by (2. 3) $P(R)=P(F)$ ($F=$quotient field of R), so the computation of $P(R)$ is reduced to the computation of the pythagoras number of a field. This case is, therefore, not of particular interest. For a large class of examples, we can mention the following:

Theorem 5. 1. (1) *Let k be any formally real field. Then $P(k[[x]])=P(k)$.*

(2) *Let k be a real-closed field and R be the local ring at any point (not necessarily regular) on a curve defined over k, then $P(R)<\infty$.*

Proof. In (2), R is the localization of a k-affine algebra of dimension 1 at a maximal ideal, so $P(R) < \infty$ follows from (2. 1) and (3. 1). For (1), consider any $f \in S(k[[x]]) \setminus \{0\}$, say $f = a_0 x^{2d} + a_1 x^{2d+1} + \cdots$, where $a_i \in k$, $a_0 \in S(k) \setminus \{0\}$. Writing

$$f = a_0 x^{2d}(1 + a_0^{-1} a_1 x + \cdots),$$

we see that $f \in a_0 S_1(k[[x]])$ since we can take a "formal" square root of $1 + a_0^{-1} a_1 x + \cdots$. This clearly shows that $P(k[[x]]) = P(k)$. Q.E.D.

We c… …er next the case of dimension 2. The following result pro… … a large class of …egular … rings of dimension 2 which have a finite pythagoras nu…

The… …. 2. *Let K be a function field of transcendence degree d … … real-closed field k. L… …e any prime ideal of height 2 in the polynomial algebra $K[$… … $\ldots x_n]$. Then $P(K[x_1, \ldots, x_n]_{\mathfrak{p}}) \leqq 2^{d+n}$.*

Proof. Let $R = K[x_1, \ldots, x_n]_{\mathfrak{p}}$, a regular local ring of dimension 2. By a result of H. Lindel [Ld], Lemma 1 [7]), R is isomorphic to $K'[y, z]_{\mathfrak{m}}$, where $K' = K(x_1, \ldots, x_{n-2})$, and $\mathfrak{m}$ is a maximal ideal in $K'[y, z]$. Thus, it is sufficient to show that, if $d' = \mathrm{tr.d}_k K'$, then $P(K'[y, z]_{\mathfrak{m}}) \leqq 2^{d'+2}$. Exploiting the well-known maximal ideal structure in polynomial rings over fields, we may assume that $\mathfrak{m} = (y, p(z))$, where $p(z)$ is an irreducible polynomial in $K'[z]$. Let $R' = K'[y, z]_{\mathfrak{m}}$, and let $f/g \in S(R')$, where $f, g \in K'[y, z]$, with $g \notin \mathfrak{m}$. Then $gf \in S(R') \subset S(K'(y, z))$. By Pfister's Theorem $[\mathrm{P}_2]$, $P(K'(y, z)) \leqq r := 2^{d'+2}$, so, by Cassels' Theorem [C], $gf \in S_r(K'(y)[z])$. Thus, there exists a nonzero polynomial $h(y) \in K'[y]$ such that $h^2 gf = f_1^2 + \cdots + f_r^2$, where $f_i \in K'[y, z]$. If $y \mid h$, then clearly $y \mid f_i$ for all i. After dividing out by enough powers of y, we may therefore assume that $y \nmid h$. But then $h(y) \notin \mathfrak{m}$, so $f/g = h^2 gf (h^{-1} g^{-1})^2 \in S_r(R')$. This shows that $P(R') \leqq r = 2^{d'+2}$. Q.E.D.

The above considerations seem to suggest that if R is a regular local ring obtained by localizing a k-affine algebra (k real-closed) at a height 2 prime, then $P(R)$ should be finite. It would be possible to prove that this is the case, if, for instance, we knew that the "Weak Question" (Q_1) in Section 2 has an affirmative answer when the bottom ring is a local ring. Unfortunately, the correct answer to (Q_1) seems to be unknown even in this special case. (Cf. Problem 1 and Problem 5 in § 9.)

Another important example of a 2-dimensional regular local ring with a finite pythagoras number is the power series ring $\mathbb{R}[[x, y]]$: we shall show below that $P(\mathbb{R}[[x, y]]) = 2$. The proof of this depends heavily on the Weierstrass' Preparation Theorem. In the following, we shall reformulate the underlying ideas of Weierstrass' Theorem in a slightly more general context. The advantage of this generalized formulation is that, using it, we can compute not only $P(\mathbb{R}[[x, y]])$, but also $P(\mathbb{R}[x][[y]])$, $P(\mathbb{R}[x, x^{-1}][[y]])$, and many others. In addition, our methods will allow us to replace the real field $\mathbb{R}$ by any h.p. (hereditarily pythagorean) field k: for the definition of an h.p. field, see (2. 9).

[7]) We are indebted to M. Ojanguren who brought Lindel's Lemma to our attention.

Weierstrass' Lemma 5. 3. *Let B be any commutative ring and*

(5. 4) $$p(y)=p_0+p_1y+p_2y^2+\cdots\in A:=B[[y]]$$

be a power series over B. Let C be an additive subgroup of B such that $B=B\cdot p_0+C$. Then

(1) $A=A\cdot p+C[[y]]$. (*Here, $C[[y]]$ means the additive group of all power series with coefficients in C.*)

(2) *If the sum for B is direct and p_0 is not a zero-divisor in B, then the sum for A is also direct.*

(3) *Suppose B is a k-algebra, where k is a commutative ring. If $B/(p_0)$ is a finitely generated (resp. free) k-module, then $A/(p)$ is a finitely generated (resp. free) $k[[y]]$-module.*

Proof. Let $h(y)=\sum_{i=0}^{\infty} h_iy^i\in A$. We want to find $q(y)=\sum_{i=0}^{\infty} q_iy^i\in A$ and $r(y)=\sum_{i=0}^{\infty} r_iy^i\in C[[y]]$ such that $h=pq+r$. This amounts to the following system of equations in B:

(5. 5)
$$\begin{aligned} h_0 &= p_0q_0+r_0,\\ h_1-p_1q_0 &= p_0q_1+r_1,\\ h_2-p_2q_0-p_1q_1 &= p_0q_2+r_2,\\ &\vdots \end{aligned}$$

Since $B=B\cdot p_0+C$, we can solve for $q_0\in B$, $r_0\in C$ from the first equation, and then solve for $q_1\in B$, $r_1\in C$ from the second equation, and so on down. This enables us to construct $q(y)$ and $r(y)$, which proves (1). For (2), if $B=B\cdot p_0\oplus C$ and p_0 is not a zero-divisor in B, then clearly the q_i's and the r_i's in (5. 5) are (inductively) uniquely determined. Hence $A=A\cdot p_0\oplus C[[y]]$. For (3), let $b_1,\dots,b_n\in B$ be such that their images in $B/(p_0)$ generate the latter as a k-module. The conclusion in (3) follows by applying (1) with $C=\sum_{i=1}^{n} k\cdot b_i$. Q.E.D.

Corollary 5. 6. *Let k be a field and let B be a k-algebra of one of the following types:*

(1) *B is a k-affine domain of transcendence degree 1 over k; or*

(2) *B is a discrete valuation ring whose residue field k' is a finite extension of k.*

Then, for any $p(y)\in A=B[[y]]$ as in (5. 4) with $p_0\neq 0$ in B, the quotient $A/(p)$ is a finitely generated free $k[[y]]$-module.

Proof. In the case (1), $B/(p_0)$ is a k-affine algebra of Krull dimension 0, so it is a finite dimensional k-vector space, so (5. 3) (3) applies. In the case (2), we may assume that p_0 is a nonunit in B (for otherwise p is a unit in A and $A/(p)=0$). Then p_0 is an associate of a power, π^d, of the uniformizer π of B, and so

$$\dim_k B/(p_0) = \dim_k B/(\pi^d) = d \cdot \dim_k B/(\pi) = d \cdot [k' : k] < \infty .$$

Again, the conclusion about $A/(p)$ follows from (5. 3) (3). Q.E.D.

Remark 5. 7. Case (2) above is applicable to $B = k[[x]]$, or to B, the local ring at a simple point of a curve defined over a perfect field k.

Proposition 5. 8. *Let k be any h.p. (hereditarily pythagorean) field, and let B be a formally real k-domain as in* (1) *or* (2) *in* (5. 6). *In the case* (1), *assume also that B and $B[\sqrt{-1}]$ are both* PID's. *Let $p(y)$ in* (5. 4) *be a nonzero prime element in $A = B[[y]]$ which generates a nonreal ideal. Then $p(y)$ is associate in A to an element in $S_2(A)$ (sums of two squares in A).*

Proof. The constant term p_0 in p must be nonzero. For otherwise p is associate to y and $A/(p) = B[[y]]/(y) \cong B$ is formally real, contradicting the hypothesis on p. Clearly, $A/(p)$ contains (a copy of) $k[[y]]$ and by (5. 6), $A/(p)$ is a finitely generated (free) module over $k[[y]]$. Thus, the quotient field F of $A/(p)$ is a finite extension of $k((y))$. Since k is h.p., so is $k((y))$, and therefore, *the finite nonreal extension $F \supset k((y))$* must have level 1. (For the relevant facts used about h.p. fields, see [B_1], Ch. 3.) At this point, we shall appeal to the main results of [CLRR]. If we can apply [CLRR], (2. 5) (3), the above fact the level of F will imply that p is associate in A to a sum of two squares. We shall now check the hypotheses for [CLRR], (2. 5) (3) to make sure it applies here. *First, we need* $\sqrt{-1} \notin A$; this is clear because B (and hence A) is formally real. Next, we must check that $A = B[[y]]$ is a UFD: this follows from the fact that B is a *regular* UFD (see [S], p. 90). *Finally, we must check that $A[\sqrt{-1}]$ is also a* UFD. If B is as in Case (1) then $A[\sqrt{-1}] = B[\sqrt{-1}][[y]]$, so we can apply [S], p. 90 again. If B is as in Case (2), then A is a regular local ring (with 2 a unit), and so $A[\sqrt{-1}]$ is a UFD as observed in the proof of [CLRR], (3.). Q.E.D.

Proposition 5. 9. *Keep the hypotheses in* (5. 8) *and let $f \in S(A)$. Then there exists a unit u_0 of B and two elements $h_1, h_2 \in A$ such that $f = u_0 \cdot (h_1^2 + h_2^2)$; moreover, u_0 is a sum of squares in the quotient field of B.*

Proof. Since A is a UFD, we can write $f = g^2 h$ where h has no repeated prime factors. We may, of course, assume that $f \neq 0$. *We claim that any nonzero prime $p | h$ generates a nonreal ideal in A.* In fact, write $f = f_1^2 + \cdots + f_m^2$ and $h = h' \cdot p$. If the f_i's are not all divisible by p, then $f_1^2 + \cdots + f_m^2 = g^2 h' \cdot p$ implies that $A \cdot p$ is nonreal. On the other hand, if $f_i = f_i' \cdot p$ for all i, then $p^2 | g^2 h$ and so $g = g' \cdot p$ for some $g' \in A$ since $p^2 \nmid h$. Cancelling p^2, we get $f_1'^2+\cdots+f_m'^2=g'^2h'\cdot p$, and we can carry out the same argument again. Since this process must terminate in a finite number of steps, we have proved our claim. Hence, by (5. 8), p is associate to an element of $S_2(A)$. Using the 2-square identity, we can therefore write $f=u(g_1^2+g_2^2)$, where $u=\sum_{i=0}^{\infty} u_i y^i$ is a unit in A (i.e. u_0 is a unit in B). Since $1+u_0^{-1}u_1 y+u_0^{-1}u_2 y^2+\cdots$ is a perfect square in A, we can rewrite the equation for f in the form $f=u_0(h_1^2+h_2^2)$ with $h_1, h_2\in A$. Comparing the coefficients of the lowest degree terms in y on both sides, we see that u_0 is a sum of squares in the quotient field of B. Q.E.D.

The above proposition gives the main tool for computing the pythagoras number of $A=B[[y]]$ for rings B of the two types specified in (5. 6). For convenience of exposition, we shall state the results separately for the two different types of B.

Theorem 5. 10. *Let k be a real-closed field and B be a formally real k-affine domain of transcendence degree 1. Assume that B and $B[\sqrt{-1}]$ are both* PID's. *Let B' be the localization of B at any multiplicative set S. Then $P(B'[[y]])=2$.*

Proof. If b is any nonunit in B', it is easy to see that b^2+y^2 has length two in $B'[[y]]$. Thus, it suffices to show that $P(B'[[y]])\leqq 2$. In the following, we shall write $A=B[[y]]$ and $A'=B'[[y]]$.

Let us first show that $P(A)\leqq 2$. Note that by Witt's Theorem, the quotient field K of B has pythagoras number 2 since K is the function field of a curve defined over k. Let $f\in S(A)$ and keep the notations in (5. 8). The element u_0 is a sum of squares in K, so $u_0\in B\cap S_2(K)=S_2(B)$ by [CLRR], (2. 5). By the 2-square identity, we get then $f=u_0(h_1^2+h_2^2)\in S_2(A)$.

Finally, we show $P(A')\leqq 2$. By an easy direct limit argument, we can reduce this to the case when the multiplicative set $S\subset B$ is generated by a finite number of elements $s_1,\ldots,s_m$. But then $B'=B[s_1^{-1},\ldots,s_m^{-1}]$ is also a k-affine domain of transcendence degree 1; moreover B' and $B'[\sqrt{-1}]=B[\sqrt{-1}][s_1^{-1},\ldots,s_m^{-1}]$ remain PID's. Therefore, $P(B')\leqq 2$ follows as in the last paragraph. Q.E.D.

Corollary 5. 11. *Let k be an h.p. field, and B' be the localization of $B=k[x]$ at any multiplicative set S. Then $P(B'[[y]])=2$.*

Proof. The reason we need k to be real-closed in the argument above is that we used Witt's Theorem to get $P(K)=2$, where K is the quotient field of B'. But if $B'=k[x]_S$, we know that $P(K)=P(k(x))=2$ as long as k is h.p. [B₁], p. 95. Therefore, the hypothesis that k be real-closed can be weakened in this case. (Note also that here we do not need to use the result in [CLRR], since we can use instead Cassels' Theorem, and the fact that $P(B')\leqq P(B)=2$.) Q.E.D.

Next, we shall treat the case when B is a discrete valuation ring.

Theorem 5. 12. *Let k be an h.p. field contained in a formally real discrete valuation ring B such that the residue field of B is a finite extension of k.*

(1) *If $P(B)\leqq 2n$, then $P(B[[y]])\leqq 2n$.*

(2) *If B is 2-henselian (i.e., if $1+\mathfrak{m}\subseteq B^2$ where $\mathfrak{m}$ is the maximal ideal of B), then $P(B[[y]])=2$.*

we get $f_1'^2 + \cdots + f_m'^2 = g'^2 h' \cdot p$, and we can carry out the same argument again. Since this process must terminate in a finite number of steps, we have proved our claim. Hence, by (5. 8), p is associate to an element of $S_2(A)$. Using the 2-square identity, we can therefore write $f = u(g_1^2 + g_2^2)$, where $u = \sum_{i=0}^{\infty} u_i y^i$ is a unit in A (i.e. u_0 is a unit in B). Since $1 + u_0^{-1} u_1 y + u_0^{-1} u_2 y^2 + \cdots$ is a perfect square in A, we can rewrite the equation for f in the form $f = u_0(h_1^2 + h_2^2)$ with $h_1, h_2 \in A$. Comparing the coefficients of the lowest degree terms in y on both sides, we see that u_0 is a sum of squares in the quotient field of B. Q.E.D.

The above proposition gives the main tool for computing the pythagoras number of $A = B[[y]]$ for rings B of the two types specified in (5. 6). For convenience of exposition, we shall state the results separately for the two different types of B.

Theorem 5. 10. *Let k be a real-closed field and B be a formally real k-affine domain of transcendence degree 1. Assume that B and $B[\sqrt{-1}]$ are both* PID's. *Let B' be the localization of B at any multiplicative set S. Then $P(B'[[y]]) = 2$.*

Proof. If b is any nonunit in B', it is easy to see that $b^2 + y^2$ has length two in $B'[[y]]$. Thus, it suffices to show that $P(B'[[y]]) \leqq 2$. In the following, we shall write $A = B[[y]]$ and $A' = B'[[y]]$.

Let us first show that $P(A) \leqq 2$. Note that by Witt's Theorem, the quotient field K of B has pythagoras number 2 since K is the function field of a curve defined over k. Let $f \in S(A)$ and keep the notations in (5. 8). The element u_0 is a sum of squares in K, so $u_0 \in B \cap S_2(K) = S_2(B)$ by [CLRR], (2. 5). By the 2-square identity, we get then $f = u_0(h_1^2 + h_2^2) \in S_2(A)$.

Finally, we show $P(A') \leqq 2$. By an easy direct limit argument, we can reduce this to the case when the multiplicative set $S \subset B$ is generated by a finite number of elements $s_1, \ldots, s_m$. But then $B' = B[s_1^{-1}, \ldots, s_m^{-1}]$ is also a k-affine domain of transcendence degree 1; moreover B' and $B'[\sqrt{-1}] = B[\sqrt{-1}][s_1^{-1}, \ldots, s_m^{-1}]$ remain PID's. Therefore, $P(B') \leqq 2$ follows as in the last paragraph. Q.E.D.

Corollary 5. 11. *Let k be an h.p. field, and B' be the localization of $B = k[x]$ at any multiplicative set S. Then $P(B'[[y]]) = 2$.*

Proof. The reason we need k to be real-closed in the argument above is that we used Witt's Theorem to get $P(K) = 2$, where K is the quotient field of B'. But if $B' = k[x]_S$, we know that $P(K) = P(k(x)) = 2$ as long as k is h.p. [B$_1$], p. 95. Therefore, the hypothesis that k be real-closed can be weakened in this case. (Note also that here we do not need to use the result in [CLRR], since we can use instead Cassels' Theorem, and the fact that $P(B') \leqq P(B) = 2$.) Q.E.D.

Next, we shall treat the case when B is a discrete valuation ring.

Theorem 5. 12. *Let k be an h.p. field contained in a formally real discrete valuation ring B such that the residue field of B is a finite extension of k.*

(1) *If $P(B) \leqq 2n$, then $P(B[[y]]) \leqq 2n$.*

(2) *If B is 2-henselian (i.e., if $1 + \mathfrak{m} \subseteq B^2$ where $\mathfrak{m}$ is the maximal ideal of B), then $P(B[[y]]) = 2$.*

In view of (5. 15), it will be of interest to characterize the set

$$S(k[[x,y]]) = S_2(k[[x,y]])$$

(and, if possible, its intersection with $k[x,y]$). We have not been able to find such characterizations. As a partial result, we shall mention the following without proof: Let

$$h(x,y) = h_d(x,y) + h_{d+1}(x,y) + \cdots \in k[[x,y]],$$

where h_i is homogeneous of degree i, and $h_d \not\equiv 0$. Then $h \in S(k[[x,y]])$ *if* h_d is positive definite, and *only if* h_d is positive semidefinite. (Unfortunately, neither condition will be both necessary and sufficient.)

Some of the methods used above to study the power series ring $k[[x,y]]$ can also be adapted to give information on the field $\bar{k}((x,y))$ over an algebraically closed ground field $\bar{k}$. In the literature, it seems to be unknown whether the field $\bar{k}((x,y))$ is a C_2-field in the sense of Lang (see [G], p. 36). The following offers a partial result in this direction; we thank Adrian Wadsworth for collaboration on the proof below.

Theorem 5. 16. *Let $\bar{k}$ be an algebraically closed field, and $F = \bar{k}((x,y))$. Then* (1) *F is a C_2-field for diagonal forms, i.e. any diagonal form $f_1 t_1^d + \cdots + f_n t_n^d$ over F with $n > d^2$ has a nontrivial zero.* (2) *F has u-invariant* 4. (For the definition of the u-invariant, see [L], p. 315.)

Proof. Recall that a power series $f \in \bar{k}[[x,y]]$ is said to be *regular in y of degree d* if f contains a term ay^d ($a \in \bar{k} \setminus \{0\}$) but does not contain any term $a'y^i$ ($a' \in \bar{k} \setminus \{0\}$) with $i < d$ (see [ZS], p. 147). An important special case of such a power series is one of the form

(5. 17) $$g = h_0(x) + h_1(x)y + \cdots + h_{d-1}(x)y^{d-1} + y^d,$$

where $h_i(x) \in \bar{k}[[x]]$ with $h_i(0) = 0$, for all i. Such a power series g is called a *Weierstrass polynomial (in y) of degree d*. By Weierstrass' Preparation Theorem [ZS], p. 139, any $f \in \bar{k}[[x,y]]$ regular in y of degree d is associate to a (unique) Weierstrass polynomial g as in (5. 17). Now consider a diagonal form

$$f_1 t_1^d + \cdots + f_n t_n^d \quad \text{over} \quad F = \bar{k}((x,y)).$$

We may assume that all f_i are in $\bar{k}[[x,y]]$ and are nonzero. After "moving" the set $\{f_i\}$ by a suitable $\bar{k}$-automorphism of $\bar{k}[[x,y]]$, we may assume that *each* f_i is regular in y (of some degree d_i) [ZS], p. 147. By Weierstrass' Preparation Theorem, we can write $f_i = u_i g_i$, where $g_i \in \bar{k}[[x]][y]$ is a Weierstrass polynomial in y of degree d_i, and $u_i \in \bar{k}[[x,y]]$ with $u_i(0,0) \neq 0$. Since $\bar{k}$ is algebraically closed, the latter implies that $u_i = v_i^d$ for suitable power series $v_i \in \bar{k}[[x,y]]$. Consider $g_1 s_1^d + \cdots + g_n s_n^d$, viewed as a form (in the indeterminates s_i) over the field $\bar{k}((x))(y)$. Since $\bar{k}((x))$ is a C_1-field, $\bar{k}((x))(y)$ is a C_2-field [G], p. 22, p. 35. Thus, if $n > d^2$, there exist $s_i \in \bar{k}((x))(y)$, not all zero, such that $g_1 s_1^d + \cdots + g_n s_n^d = 0$. But then $f_1(v_1^{-1}s_1)^d + \cdots + f_n(v_n^{-1}s_n)^d = 0$, so $f_1 t_1^d + \cdots + f_n t_n^d$ has a nontrivial zero in $F = \bar{k}((x,y))$. This proves (1) in the theorem. Since every *quadratic* form over a field (of characteristic not 2) can be diagonalized, (1) implies that F has u-invariant $u(F) \leqq 4$. The form $t_1^2 + xt_2^2 + yt_3^2 + xyt_4^2$ is easily seen to be anisotropic over $\bar{k}((x))((y)) \supset F$ (by using Springer's Theorem), so it must be anisotropic over F. Therefore $u(F) = 4$. Q.E.D.

For a real-closed field k, we do not know whether the quotient field $k((x_1, \dots, x_n))$ of $k[[x_1, \dots, x_n]]$ has a finite pythagoras number when $n \geqq 3$. The computation of $P(k((x_1, \dots, x_n)))$ is closely related to the computation of the u-invariant of $\bar{k}((x_1, \dots, x_n))$, where $\bar{k}$ denotes the algebraic closure of k. For a discussion of this point, see § 9.

We shall now conclude this section by considering the pythagoras number of rings of the type $R = k[[y]][x]$, where k is a field. Note that this ring is *not the same* as $k[x][[y]]$, although it may be viewed as a subring of the latter. For the pythagoras number $P(R)$, we have the following result:

Theorem 5.18. *Let k be a formally real field all of whose finite nonreal extensions k' have level $s(k') \leqq 2^n$. Then, for $R = k[[y]][x]$, we have $P(R) \leqq 2^{n+1}$.*

Proof. We first claim that $P(k((y))(x)) \leqq 2^{n+1}$. From Milnor's exact sequence for the Witt ring of a rational function field, this will follow if we can show that any nonreal finite extension E of $k((y))$ has $s(E) \leqq 2^n$ [L], p. 314. But, by valuation theory, any such E is isomorphic to a power series field $k'((y'))$, where k' is a finite extension of k. Since E is nonreal, so must be k' and so $s(E) = s(k'((y))) = s(k') \leqq 2^n$. This proves our claim.

To get $P(R) \leqq 2^{n+1}$, let $f \in S(R)$. View f as a sum of squares in $F[x]$, where $F = k((y))$. By (2.2) (Cassels' Theorem), $P(F[x]) = P(F(x))$, which, by the last paragraph, is $\leqq m := 2^{n+1}$. Thus, $f \in S_m(F[x])$. But $F = k[[y]][y^{-1}]$, so there exists $e \geqq 0$ such that $y^{2e} f = f_1^2 + \dots + f_m^2$, for suitable $f_i \in k[[y]][x] = R$. Clearly, if $e > 0$, all f_i must be divisible by y. Thus, after cancelling y^2 e-times, we get the desired conclusion that $f \in S_m(R)$. Q.E.D.

This theorem, combined with the following one, gives an alternative method for computing the pythagoras numbers of $k[[x, y]]$ and $k[x][[y]]$.

Theorem 5.20. *For any formally real field k, let*

$$A' = k[[x, y]], \qquad A = k[x][[y]], \qquad R = k[[y]][x],$$

and view $R \subset A \subset A'$. Then, for any natural number n, we have $S_n(A) = A^2 \cdot S_n(R)$ and $S_n(A') = A'^2 \cdot S_n(R)$.

Proof. In both cases, we need only prove the inclusion "$\subseteqq$". We shall first treat the ring A, so consider $f(x, y) = \sum_{i=1}^{n} g_i^2(x, y)$ where $g_i \in A$. If $y \mid f$, then $y \mid g_i$ for each i, and we can cancel y^2 from the equation. Thus, we may assume that $y \nmid f$, or that $f(x, 0) \neq 0$. If $f(x, 0)$ is a constant, say α, then $\alpha \in S_n(k)$, and $f = (\alpha^{-1} f) \cdot \alpha \in A^2 \cdot S_n(k)$. We may, therefore, assume that $f(x, 0)$ has degree $2d > 0$ in $k[x]$. By Weierstrass' Division Theorem (cf. [ZS], p. 139), we can write $g_i = h_i f + r_i$ where $h_i \in A$, and $r_i \in R = k[[y]][x]$ with $\deg_x r_i(x, y) < 2d$. From $g_i(x, 0) = h_i(x, 0) f(x, 0) + r_i(x, 0)$, and the fact that $\deg g_i(x, 0) \leqq d$, we see that $h_i(x, 0) \equiv 0$, i.e. $y \mid h_i(x, y)$ for each i. Now

$$\sum r_i^2 = \sum (g_i - h_i f)^2 = \sum g_i^2 - 2f \sum g_i h_i + f^2 \sum h_i^2 = f \cdot f_0$$

where $f_0 = 1 - 2 \sum g_i h_i + f \sum h_i^2 \in A$, since $y \mid h_i$ for all i, f_0 is a unit and is a square in A. Therefore, $f \in A^2 \cdot S_n(R)$. The proof for the case $A' = k[[x]][[y]]$ is similar, by considering the order of $f(x, 0)$ instead of $\deg_x f(x, 0)$. (Here, the argument is even simpler: in the case where $f(x, 0)$ has a positive order $2e > 0$, each $g_i(x, 0)$ will have order $\geqq e > 0$ so $f_0 = 1 - 2 \sum g_i h_i + f \sum h_i^2 \equiv 1 \pmod{xA' + yA'}$ is a unit and is a square in A'.) Q.E.D.

Corollary 5. 21. *In the notation of the theorem, we have* $P(A') \leqq P(A) \leqq P(R)$. *If* k *satisfies the hypothesis of* (5. 18), *then* $P(A') \leqq P(A) \leqq 2^{n+1}$.

Corollary 5. 22. *If* k *is an h.p. field, then* $P(A) = P(A') = P(R) = 2$. *If* k *is a number field, then* $P(A') \leqq P(A) \leqq P(R) \leqq 8$. *If* k *is a (formally real) function field of transcendence degree* n *over a real closed field, then* $P(A') \leqq P(A) \leqq P(R) \leqq 2^{n+1}$.

(For the last case, use [P_2], or [L], p. 301. Note that, for the rings A and A', the first case has been obtained before in (5. 11) and (5. 14). However, the present method also covers the second and the third case which are inaccessible by the earlier method.)

§ 6. Regular local rings of dimension $\geqq 3$

In this section we shall compute the pythagoras number of regular local rings A of (Krull) dimension $\geqq 3$ whose residue fields are formally real. This includes, in particular, power series rings in three or more variables over any formally real field. The key to this computation is the observation that the associated graded ring of a regular local ring is isomorphic to a polynomial ring over its residue field. In order to formulate the ideas in the proper perspective, it is convenient to first make some remarks on sums of squares in graded rings. The proof of the following proposition is routine and will be omitted.

Proposition 6. 1. *Let* $A = A_0 \oplus A_1 \oplus A_2 \oplus \cdots$ *be a commutative graded ring. Then*

(1) *A is formally real iff, for any n and* $\{a_1, \ldots, a_m\} \subset A_n$, $\sum a_j^2 = 0$ *implies that all* $a_j = 0$.

(2) *Assume that A is formally real, and* $a \in A_n - \{0\}$. *Then* $a \in S_m(A)$ *iff* $n = 2r$ *for some r and* $a = \sum_{i=1}^{m} a_i^2$ *for some* $a_i \in A_r$.

Definition 6. 2. Let A be a commutative graded ring. We define the *homogeneous pythagoras number*, $hP(A)$, to be the supremum of $\{\text{length}_A(a) : a \in h(A) \cap S(A)\}$ where $h(A)$ denotes the set $A_0 \cup A_1 \cup A_2 \cup \cdots$ of homogeneous elements of A. (Clearly, $hP(A) \leqq P(A)$.)

We shall now prove the following Proposition which was prompted by a remark of A. Wadsworth:

Proposition 6. 3. *Let* $\mathfrak{m}$ *be an ideal in a ring R with* $\bigcap_{i \geqq 0} \mathfrak{m}^i = 0$. *Let*

$$A = G_{\mathfrak{m}}(R) = \bigoplus_{i \geqq 0} \mathfrak{m}^i/\mathfrak{m}^{i+1}$$

be the associated graded ring with respect to $\mathfrak{m}$.

(1) *If A is formally real, then R is also formally real.*

(2) *Assume that A is formally real. Let $a \in \mathfrak{m}^n - \mathfrak{m}^{n+1}$ and $\bar{a} = a + \mathfrak{m}^{n+1} \in A$. Then* $h_A \bar{a} \leqq \text{length}_R a$. *In particular, $hP(A) \leqq P(R)$.*

Proof. (1) Suppose $\sum a_i^2 = 0$ in R. Since $A = G_m(R)$ is formally real, we see that if all a_j are in some $\mathfrak{m}^i$, then they are all in $\mathfrak{m}^{i+1}$. Thus by induction on i, we get $a_j \in \bigcap_{i \geqq 0} \mathfrak{m}^i = 0$.

(2) If $a \notin S(R)$, we take $\text{length}_R a = \infty$ by convention so there is nothing to prove. Next, assume $a = a_1^2 + \cdots + a_m^2$. Let r be the largest integer such that all a_j lie in $\mathfrak{m}^r$. Then $a_j + \mathfrak{m}^{r+1}$ are not all zero in A, and $\sum (a_j + \mathfrak{m}^{r-1})^2 = a + \mathfrak{m}^{2r+1}$. If $n > 2r$, we would have $\sum (a_j + \mathfrak{m}^{r+1})^2 = 0 \in A$, contradicting the formal reality of A. Thus $n \leqq 2r$; this must be an equality since $a = \sum a_j^2 \in \mathfrak{m}^{2r}$. We have then $\bar{a} = a + \mathfrak{m}^{n+1} = \sum (a_j + \mathfrak{m}^{r+1})^2$, so $\text{length}_A \bar{a} \leqq \text{length}_R a$. Finally, to prove $hP(A) \leqq P(R)$, let $\alpha \neq 0$ be a homogeneous element of A, say of length k. By (6. 1), we must have $\alpha \in A_{2r}$ (for some r) and $\alpha = \alpha_1^2 + \cdots + \alpha_k^2$ where $\alpha_i \in A_r$. Write $\alpha_j = a_j + \mathfrak{m}^{r+1}$ ($a_j \in \mathfrak{m}^r$) and let $a := a_1^2 + \cdots + a_k^2 \in \mathfrak{m}^{2r}$. Since

$$a + \mathfrak{m}^{2r+1} = \sum_j (a_j + \mathfrak{m}^{r+1})^2 = \sum_j \alpha_j^2 = \alpha \neq 0,$$

we have $a \notin \mathfrak{m}^{2r+1}$. By the first part of (2), we see that $\text{length}_R(a) = k$, so $P(R) \geqq hP(A)$. Q.E.D.

Remark 6. 4. In general, we may not have $P(R) \geqq P(A)$. In fact, if $R = \mathbb{R}[[x, y]]$ and $\mathfrak{m} = (x, y)$, then by (5. 14), $P(R) = 2$, but the associated graded ring is $A = k[x, y]$, with pythagoras number $P(A) = \infty$. Here $hP(A) = 2$ so the inequality $hP(A) \leqq P(R)$ in (6. 3) (2) turns out to be an equality. In general, however, this may not be the case. For instance, let $R = \mathbb{R}[[x, y]]$, $R' = R[[z]]$ and $\mathfrak{m}' = R' \cdot z$. The associated graded ring for R' with respect to $\mathfrak{m}'$ is $A' = G_{\mathfrak{m}'}(R') \cong R[z]$, with R having degree 0 in the grading. Clearly $hP(A') = P(R) = 2$ (by (5. 14)), but $P(R') = P(\mathbb{R}[[x, y, z]]) = \infty$ by (6. 7) below.

At this point, it will be convenient to prove the following lemma on the behavior of the length of forms upon dehomogenization:

Lemma 6. 5. *Let $g(x_0, \ldots, x_n)$ be a form of degree $2r$ over a formally real ring R, and let $\tilde{g}(x_1, \ldots, x_n) = g(1, x_1, \ldots, x_n)$. Then*

$$\text{length of } \tilde{g} \text{ in } R[x_1, \ldots, x_n] = \text{length of } g \text{ in } R[x_0, \ldots, x_n]$$
$$= \text{length of } g \text{ in } R[[x_0, \ldots, x_n]].$$

Proof. The last equality follows from (6. 3) (2) since the associated graded ring of $R[[x_0, \ldots, x_n]]$ with respect to $\mathfrak{m} = (x_0, \ldots, x_n)$ is $R[x_0, \ldots, x_n]$. For the first equality, we only need to show that $\text{length}(g) \leqq \text{length}(\tilde{g})$. Suppose $\tilde{g} = \sum_{i=1}^m h_i^2$ in $R[x_1, \ldots, x_n]$. Since R is formally real, it is easy to see that each h_i must have total degree $\leqq r$. Thus

$$H_i(x_0, x_1, \ldots, x_n) := x_0^r h_i(x_1/x_0, \ldots, x_n/x_0)$$

are forms of degree r in $R[x_0, \ldots, x_n]$. Now we have

$$\sum_{i=1}^m H_i^2 = x_0^{2r} \tilde{g}(x_1/x_0, \ldots, x_n/x_0) = x_0^{2r} g(1, x_1/x_0, \ldots, x_n/x_0) = g(x_0, x_1, \ldots, x_n)$$

so $\text{length}(g) \leqq \text{length}(\tilde{g})$, as desired. Q.E.D.

In the above argument, it is important that we assume g to be a *form*. In fact, the lemma is clearly false without this assumption.

Theorem 6. 6. *Let* $(R, \mathfrak{m})$ *be a regular local ring with a formally real residue field* $k=R/\mathfrak{m}$. *Then*

(1) *R is formally real.*

(2) *If* $\dim R \geqq 3$, *then* $P(R)=\infty$.

Proof. Let $x_1, \ldots, x_d \in \mathfrak{m}$ be a regular system of parameters for R, where $d=\dim R$. If we write $\bar{x}_i = x_i + \mathfrak{m} \in G_{\mathfrak{m}}(R)$, then $G_{\mathfrak{m}}(R)$ is the polynomial ring $k[\bar{x}_1, \ldots, \bar{x}_n]$ graded in the usual way. Since k is formally real, so is $k[\bar{x}_1, \ldots, \bar{x}_n]$. Thus (1) follows from (6. 3) (1) (see also [CT₁], Prop. 2. 1). Now assume $d \geqq 3$. Let $F_m(x, y, z)$ be the homogenization of the polynomial $f_m(x, y)$ in (4. 17). By (6. 5), $F_m(\bar{x}_1, \bar{x}_2, \bar{x}_3)$ has length m in $k[\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_d]$, so by (6. 3) (2), $F_m(x_1, x_2, x_3)$ has length m in R. Since this holds for any m, we see that $P(R)=\infty$. Q.E.D.

Corollary 6. 7. *Let A be any ring which has infinite level. Then, for any* $d \geqq 3$, $P(A[[x_1, \ldots, x_d]])=\infty$.

Proof. As in the proof of (4. 18), we can reduce this to the case of A being a formally real field. But then $A[[x_1, \ldots, x_d]]$ is a regular local ring of dimension d with residue field A, so we are done by Theorem (6. 6). Q.E.D.

If we combine this Corollary with the results of § 4, 5 we will be able to compute even the pythagoras number of all power series rings of "mixed types":

$$R_{n,m}=k[[x_1, \ldots, x_n]][x_{n+1}, \ldots, x_{n+m}],$$
$$R'_{n,m}=k[x_1, \ldots, x_n][[x_{n+1}, \ldots, x_{n+m}]],$$

at least when $k=\mathbb{R}$ or $k=\mathbb{Z}$. The results are stated in (6. 8), (6. 8′) and (6. 9) below.

Theorem 6. 8. *Let k be any formally real field. Then* $P(R_{n,m})=\infty$ *unless*

$$(n, m)=(0, 0),\ (1, 0),\ (0, 1),\ (1, 1) \quad \textit{or} \quad (2, 0).$$

In these five special cases, if k is an h.p. field, we have, respectively,

$$P(R_{n,m})=1,\ 1,\ 2,\ 2 \ \textit{and}\ 2.$$

Proof. The last statement follows from [B₁], p. 95, (5. 1), (5. 14) and (5. 19). Now assume $(n, m) \neq (0, 0), (1, 0), (0, 1), (1, 1)$ or $(2, 0)$. If $(n, m)=(0, 2)$, we have $R_{n,m}=k[x_1, x_2]$ so $P(R_{n,m})=\infty$ by (4. 18). In the remaining cases, we have $n+m \geqq 3$. View $R_{n,m}$ as a subring of $R_{n+m}=k[[x_1, \ldots, x_{n+m}]]$. Since $F_i(x_1, x_2, x_3) \in S_i(R_{n,m})$ has length i in R_{n+m}, it must have length i in $R_{n,m}$. This being true for all i, we have clearly $P(R_{n,m})=\infty$. Q.E.D.

Theorem 6.8′. *Let k be any [illegible]ally real field. Then $P(R'_{n,m})=\infty$ unless*

$$(n,m)=(0,0),\ (0,1),\ (1,0),\ (1,1)\ \text{or}\ (0,2).$$

In these five special cases, if k is an h.p. field, we have, respectively

$$P(R'_{n,m})=1,\ 1,\ 2,\ 2\ \text{and}\ 2.$$

Proof. If (n,m) is not one of the five special cases, the same argument as in the proof of (6.8) works. Among the five special cases, the only one not covered by (6.8) is $R'_{1,1}=k[x_1][[x_2]]$. This case, however, is covered by (5.11). Q.E.D.

If k is not an h.p. field, but say $k=\mathbb{Q}$, then the "finite" cases to be considered are $\mathbb{Q}$, $\mathbb{Q}[[x]]$, $\mathbb{Q}[x]$, $\mathbb{Q}[[x,y]]$, $\mathbb{Q}[x][[y]]$ and $\mathbb{Q}[[y]][x]$. Of course, $P(\mathbb{Q})=4$ by Lagrange's Theorem, and hence $P(\mathbb{Q}[[x]])=4$ by (5.1) (1). Also, $P(\mathbb{Q}[x])=5$ by Pourchet's Theorem [P] combined with Cassels' Theorem [C]. For the remaining rings we have

$$5\leqq P(\mathbb{Q}[[x,y]])\leqq P(\mathbb{Q}[x][[y]])\leqq P(\mathbb{Q}[[y]][x])\leqq 8$$

by (5.22), but, unfortunately, we do not know the exact values of these pythagoras numbers. For $k=\mathbb{Z}$, however, we do have a complete result:

Theorem 6.9. *Let $k=\mathbb{Z}$ and $(n,m)\neq(0,0)$. Then $P(R_{n,m})=\infty$ unless $(n,m)=(1,0)$, and $P(R'_{n,m})=\infty$ unless $(n,m)=(0,1)$. Moreover, $P(R_{1,0})=P(R'_{0,1})=P(\mathbb{Z}[[x]])=5$.*

Proof. The last statement is a theorem of H. Liese [Li]. (We thank W. Scharlau and M. Peters for pointing out to us Liese's result.) In all other cases, the ring in question will have a surjection onto either $\mathbb{Z}[x]$ or $\mathbb{Z}[[x,y]]$, so by (2.0), it suffices to show that $P(\mathbb{Z}[x])=P(\mathbb{Z}[[x,y]])=\infty$. The first case is covered by (4.12). The second case follows from the observation that the associated graded ring of $\mathbb{Z}[[x,y]]$ with respect to the ideal (x,y) is the polynomial ring $\mathbb{Z}[x,y]$: in view of (6.3) (2) and (6.5), this implies that

$$P(\mathbb{Z}[[x,y]]\geqq hP(\mathbb{Z}[x,y])=P(\mathbb{Z}[x])=\infty \qquad \text{Q.E.D.}$$

§ 7. Formally real affine algebras

In this section we shall utilize the results on local algebras developed in § 5, 6 to compute the pythagoras numbers of some formally real affine algebras. The main result here is that *any such algebra of (Krull) dimension $\geqq 3$ has an infinite pythagoras number*: see (7.5) below.

Recall that a prime ideal $\mathfrak{p}$ in a ring A is called *real* if the quotient ring $A/\mathfrak{p}$ is formally real. Let us call $\mathfrak{p}$ *regular* if the localization $A_{\mathfrak{p}}$ is a regular local ring. Using this terminology, we can restate a result in § 6 in the following convenient global form:

Theorem 7.1. *Let A be a ring which has a regular real prime ideal $\mathfrak{p}$ of height $d\geqq 3$. Then $P(A)=\infty$. In fact, let $x_1,\ldots,x_d\in\mathfrak{p}$ be a regular system of parameters for $A_{\mathfrak{p}}$. Then $P(B)=\infty$ for any subring $B\subseteq A$ containing at least three of $x_1,\ldots,x_d$.*

Proof. Consider the regular local ring $A_{\mathfrak{p}}$. Its residue field $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ is the quotient field of $A/\mathfrak{p}$ which is formally real. For any m, let $F_m(x,y,z)$ be the homogenization of the polynomial $f_m(x,y)$ in (4.17). Let B be any subring of A containing, say x_1,x_2,x_3. By the proof of (6.6) (2), $F_m(x_1,x_2,x_3)$ has length m in $A_{\mathfrak{p}}$, so it must also have length m in B. Since this holds for any m, $P(B)=\infty$. Q.E.D.

Our next goal is to develop some criteria for an arbitrary affine algebra (over some field) to be formally real. One of these criteria, when combined with (7. 1), will enable us to prove the infinitude of the pythagoras number for formally real affine algebras of dimension $\geqq 3$. The following results (7. 2), (7. 3) and (7. 4) are obtained in collaboration with Adrian Wadsworth; we want to thank him for permitting us to include these results here.

Lemma 7. 2. *If a ring A is formally real, then any localization $S^{-1}A$ is also formally real.*

The proof of this is routine and will be omitted.

Theorem 7. 3 (with A. Wadsworth). *For any commutative ring A, the following two statements are equivalent:*

(1) *A is formally real;*

(2) *A is reduced and each minimal prime of A is real.*

Moreover, each of (3), (4), (5) *below implies* (1) *and* (2):

(3) *A is reduced and each minimal prime of A lies in a real regular prime.*

(4) *A is reduced and each minimal prime of A lies in a real regular maximal ideal.*

(5) *A has a real regular prime, and A satisfies the following condition:*

(†) *For any minimal prime $\mathfrak{p}_0 \subset A$, if $\sum_{j=0}^{r} a_j^2 = 0$, $a_j \in \mathfrak{p}_0$ $(1 \leqq j \leqq r)$, then all $a_j = 0$.*

If A is an affine algebra over some field k, then all five conditions are equivalent.

Proof. (1) $\Rightarrow$ (2) (cf. [DE$_1$], Lemma 1. 1) Let $\mathfrak{p}$ be a minimal prime of A; then $\mathfrak{p}A_\mathfrak{p}$ is the nilradical of $A_\mathfrak{p}$. By (7. 2), $A_\mathfrak{p}$ is formally real, so $\mathfrak{p}A_\mathfrak{p} = 0$, i.e. $A_\mathfrak{p}$ is a field. This field is the quotient field of $A/\mathfrak{p}$, so $\mathfrak{p}$ is real.

(2) $\Rightarrow$ (1) Suppose $\sum a_j^2 = 0$. Then, by (2), each a_j lies in all minimal primes of A, so a_j is nilpotent. Since A is reduced, we have $a_j = 0$ for all j.

(4) $\Rightarrow$ (3) $\Rightarrow$ (2) The first implication is trivial, so assume (3). Let $\mathfrak{p}_0$ be a minimal prime of A, and (by (3)) let $\mathfrak{p}$ be a real regular prime containing $\mathfrak{p}_0$. Then $A_\mathfrak{p}$ is a regular local ring, in particular a domain. Since the primes in $A_\mathfrak{p}$ are in one-one correspondence with the primes of A lying in $\mathfrak{p}$, we see easily that $\mathfrak{p}_0 = \ker(A \rightarrow A_\mathfrak{p})$. To show that $\mathfrak{p}_0$ is real, it is therefore enough to show that $A_\mathfrak{p}$ is formally real. But $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$, being the quotient field of $A/\mathfrak{p}$, is formally real, so $A_\mathfrak{p}$ is indeed formally real by (6. 3) (1).

(5) $\Rightarrow$ (2) Let $\mathfrak{p}$ be a real regular prime. Then, as above, $\mathfrak{p}_0 := \ker(A \rightarrow A_\mathfrak{p})$ is a minimal prime of A and $\mathfrak{p}_0$ is also real. Thus, if $\sum a_j^2 = 0$ in A, then all $a_j \in \mathfrak{p}_0$ and therefore $a_j = 0$ by (†).

For the rest of the proof, *assume that A is an affine algebra $k[x_1, \ldots, x_n]/\mathfrak{A}$, where k is some field.* To complete the proof, it is enough to show that

(2) $\Rightarrow$ (4)[10]) Take any minimal prime $\mathfrak{p}_0/\mathfrak{A}$ of A and let $B = k[x_1, \ldots, x_n]/\mathfrak{p}_0$. By (2), this is a formally real domain; let K be a real closure of its quotient field. The algebraic closure k' of k inside K is then a real closure of k and we have a natural surjection $\lambda\colon k' \otimes_k B \to k' \cdot B \subseteq K$. Note that $k' \otimes_k B$ is an integral extension of $k \otimes_k B = B$, and the prime ideal $\ker \lambda \subset k' \otimes_k B$ contracts to zero in B. Therefore, by the Cohen-Seidenberg Theorem, $\ker \lambda$ is a minimal prime ideal in $k' \otimes_k B$; this prime is real since $k' \cdot B \subseteq K$ is formally real. Now $k' \otimes_k B$ is isomorphic to $k'[x_1, \ldots, x_n]/(\mathfrak{p}_0)$ where $(\mathfrak{p}_0)$ denotes the ideal generated by $\mathfrak{p}_0$ in $k'[x_1, \ldots, x_n]$. Thus, $\ker \lambda$ corresponds to a *real* prime $\mathscr{P}_1$ of $k'[x_1, \ldots, x_n]$ which is minimal over $(\mathfrak{p}_0)$ (and therefore minimal over

$$(\mathfrak{A}) = \mathfrak{A} \cdot k'[x_1, \ldots, x_n]).$$

Let $\mathscr{P}_2, \ldots, \mathscr{P}_r$ be the other minimal primes over $(\mathfrak{A})$. Let V_i $(1 \leqq i \leqq r)$ be the algebraic set defined by $\mathscr{P}_i$ in the algebraic closure $\bar{k}$ of k', and let $(V_i)_{k'} = V_i \cap k'^n$ be its k'-points. Let $\mathscr{S}(V_1)$ be the singular locus of V_1; then $\mathscr{S}(V_1)$ is Zariski-closed of codimension $\geqq 1$ in V_1. Also, none of the V_i $(i \geqq 2)$ can contain V_1. Therefore, $V_1 - \mathscr{S}(V_1) \cup V_2 \cup \cdots \cup V_r$ is a nonempty Zariski open set in V_1. Now use the fact that $\mathscr{P}_1$ is *real*. By the Realnullstellensatz [DE₁], this implies that $(V_1)_{k'}$ is Zariski dense in V_1. Hence, there exists a point

$$a \in (V_1)_{k'} - \mathscr{S}(V_1) \cup V_2 \cup \cdots \cup V_r.$$

Let M (resp. M') be the maximal ideal in $k[x_1, \ldots, x_n]$ (resp. $k'[x_1, \ldots, x_n]$) corresponding to a (so $M = M' \cap k[x_1, \ldots, x_n]$). Then

$$k[x_1, \ldots \quad]/M \subseteq k'[x_1, \ldots, x_n]/M' \cong k',$$

so [illegible] real. We claim that the [illegible]al) maximal ideal $\mathfrak{m} = M/\mathfrak{A}$ in A is *regular*. To prove this, [illegible]der the localization $A_\mathfrak{m} = k[x_1, \ldots, x_n]_M/\mathfrak{A}_M$. Since the point a lies on exactly one o[illegible]e $\bar{k}$-irreducible components[11]) of the zero-set of $\mathfrak{A}$, $(\mathfrak{p}_0)_M/\mathfrak{A}_M$ is the unique minimal prime of $A_\mathfrak{m}$, and hence is its nilradical. But since we assumed A to be reduced, so is $A_\mathfrak{m}$ and hence $(\mathfrak{p}_0)_M = \mathfrak{A}_M$. This gives $A_\mathfrak{m} = k[x_1, \ldots, x_n]_M/(\mathfrak{p}_0)_M$, which is the k-local ring at a of the (unique) irreducible component of V_1 containing a. Since a is a simple point on this component, the k-local ring at a is a regular local ring [Lg], p. 201, as desired.[12]) Q.E.D.

---

[10]) The truth of this implication, usually attributed to Artin-Lang, seems to be part of the folklore in real algebraic geometry. However, a complete proof of it, especially in the case of a *non-real-closed* ground fie[illegible]es not seem to be available in the literature. We have, therefore, included the necessary arguments here to [illegible]s gap.

[11]) By choice, a avoids all of $V_2, \ldots, V_r$, and, since a is a simple point of V_1, it lies on only one irreducible c[illegible]ent of V_1. (In fact, $\mathscr{P}_1$ being a real prime implies that V_1 is irreducible (cf. [DE₁], Thm. 1. 11); however, w[illegible]t need to use this fact here.)

[12]) Note that throughout this proof we are working in characteristic zero, so we need not worry about subtleties such as inseparability or ramification of primes. In particular, there is no problem in applying the classical characterization of simple points in terms of regular local rings.

Remarks 7. 4. In conditions (3) and (4) of the theorem, the assumption that A be reduced cannot be removed, i.e. it does not follow from the fact that every minimal prime of A lies in a real regular prime (or maximal) ideal. For example, $A = \mathbb{R}[x, y]/(x^2, xy)$ has a unique minimal (real) prime $(\bar{x})$, which lies in the real regular maximal ideal $(\bar{x}, \bar{y}+1) = (\bar{y}+1)$, but A is not reduced (and therefore not formally real). In a similar vein, the assumption (†) cannot be removed from condition (5). For, if A_1 is a k-affine algebra with a real regular prime $\mathfrak{p}_1$, then for any nonreal finite extension $k_1 \supset k$, the k-affine algebra $A := k_1 \times A_1$ has a real regular prime $k_1 \times \mathfrak{p}_1$ (of the same height as $\mathfrak{p}_1$), but the minimal prime $\mathfrak{p}_0 = k_1 \times \{0\}$ of A does not satisfy the condition (†). Of course A cannot be formally real since $A \supset k_1$.

We can now combine (7. 3) ((1) $\Rightarrow$ (4)) with Theorem 7. 1 to get the following general result:

Theorem 7. 5. *Let A be a formally real affine algebra (over some field) of Krull dimension $d \geqq 3$. Then $P(A) = \infty$.*

Proof. Take a minimal prime $\mathfrak{p}_0 \subset A$ of coheight d. By (1) $\Rightarrow$ (4) in Theorem 7. 3, there exists a real regular maximal ideal $\mathfrak{m} \subset A$ containing $\mathfrak{p}_0$. Since $A/\mathfrak{p}_0$ is an affine domain of dimension d, the maximal ideal $\mathfrak{m}/\mathfrak{p}_0$ must have height d. This clearly implies that $\mathfrak{m}$ itself has height d in A; since $d \geqq 3$, the hypothesis of Theorem 7. 1 is satisfied. Therefore, $P(A) = \infty$. Q.E.D.

§ 8. Pythagoras number of same generic fields

In this section, we shall study the affine algebra $A_n = \mathbb{R}[x_1, \ldots, x_n]/(1 + x_1^2 + \cdots + x_n^2)$ and its quotient field F_n. Let r be the unique integer such that $2^r \leqq n < 2^{r+1}$. It is known that $s(F_n) = 2^r$ [P₁], while $s(A_n) = n$ [DLP]. Therefore, by (2. 4) (b), $2^r \leqq P(F_n) \leqq 2^r + 1$ and $n \leqq P(A_n) \leqq n + 1$. Our goal in this section is to try to determine the precise values of these two pythagoras numbers. We have complete success for $P(F_n)$, but only partial success for $P(A_n)$, as the following result shows:

Theorem 8. 1.

(1)
$$P(F_n) = \begin{cases} 2 & \textit{if } n = 2; \\ 2^r + 1 & \textit{if } n > 2. \end{cases}$$

(2) *Let $n = 2^r$. Then*

$$P(A_n) = \begin{cases} 2 & \textit{if } n = 2; \\ n + 1 & \textit{if } n > 2. \end{cases}$$

The computations for $P(F_2)$ and $P(A_2)$ have already been given in (3. 4) and (3. 5) (see also the discussion following the proof of (3. 6)). Therefore, *in the following, we shall assume that $n > 2$.*

Suppose we have shown that $P(F_n) = 2^r + 1$. Then, by (2. 1), $P(A_{2^r}) \geqq P(F_{2^r}) = 2^r + 1$. Since we have already pointed out the reversed inequality, it follows that $P(A_{2^r}) = 2^r + 1$, as claimed.

We shall now try to prove that $P(F_n)=2^r+1$ (when $n>2$). This is related to, but not identical with, the fact pointed out in Footnote (6) of [Pr], p. 289. The field discussed in the latter is F_n', the quotient field of $\mathbb{R}[x_0, x_1, \dots, x_n]/(x_0^2+\cdots+x_n^2)$, which is the "bigger" generic field; the relationship between F_n and F_n' is given by $F_n' \cong F_n(x_0)$. From $s(F_n)=2^r$, it is easy to see that x_0 is not a sum of 2^r squares in $F_n(x_0)$, so $P(F_n')$ is clearly 2^r+1. However, the fact that $P(F_n)=2^r+1$ ($n>2$), which we are about to prove, is considerably harder. We begin with a lemma which is crucial for the proof:

Lemma 8. 2. *There exists a rational function $g(x_1, x_2)\in\mathbb{R}(x_1, x_2)$ such that $1+x_1^2+\cdots+x_r^2+g^2(x_1, x_2)$ has length $r+2$ in $\mathbb{R}(x_1, \dots, x_r)$ for every $r\geqq 2$.*

Proof. In view of Cassels' Theorem [C], it is enough to construct $g(x, y)\in\mathbb{R}(x, y)$ such that $1+x^2+y^2+g^2(x, y)$ has length 4 in $\mathbb{R}(x, y)$. By the main result of [CEP], $\mathbb{R}(x, y)$ does have an element of length 4, namely, the Motzkin polynomial:

$$M(x, y)=x^2y^2(x^2+y^2-3)+1,$$

though this does not have the desired form $1+x^2+y^2+g^2(x, y)$. By straightforward computation, we have

$$(x^2+y^2)\,M(x, y)=x^2(y^2-1)^2+y^2(x^2-1)^2+x^2y^2(x^2+y^2-2)^2.$$

Multiplying this by x^2+y^2 and using the 2-square identity, we get

$$\begin{aligned}(x^2+y^2)^2\,M(x, y)&=[x\cdot x(y^2-1)-y\cdot y(x^2-1)]^2+[x\cdot y(x^2-1)+y\cdot x(y^2-1)]^2\\&\quad+x^2y^2(x^2+y^2)(x^2+y^2-2)^2\\&=(x^2-y^2)^2+(xy(x^2+y^2-2))^2+x^2y^2(x^2+y^2)(x^2+y^2-2)^2.\end{aligned}$$

Thus, letting $h=(x^2+y^2)/xy(x^2+y^2-2)$ and $g=(x^2-y^2)/xy(x^2+y^2-2)$, we have

$$h^2(x, y)\,M(x, y)=1+x^2+y^2+g^2(x, y).$$

Since this rational function has the same square class as $M(x, y)$ in $\mathbb{R}(x, y)$, the RHS has length 4 in $\mathbb{R}(x, y)$, as desired. Q.E.D.

We shall now resume the proof of $P(F_n)=2^r+1$ ($n>2$). Consider F_n as a quadratic extension of the rational function field $K=\mathbb{R}(x_1, \dots, x_{n-1})$, by adjunction of $x_n=\sqrt{f}$ where $f=-(1+x_1^2+\cdots+x_{n-1}^2)$. For $g=g(x_1, x_2)$ as in the Lemma, consider the element $g+\sqrt{f}\in F_n=S(F_n)$. (Note that since $n-1\geqq 2$, g is an element of K; this is essential for the argument below.) Computing the norm with respect to the extension F_n/K, we have

$$N_{F_n/K}(g+\sqrt{f})=g^2-f=1+x_1^2+\cdots+x_{n-1}^2+g^2(x_1, x_2).$$

By the Lemma, this norm has K-length $n+1\geqq 2^r+1$. It follows that $g+\sqrt{f}$ must have F_n-length $\geqq 2^r+1$, for, if $g+\sqrt{f}\in S_{2^r}(F_n)$, then by Knebusch's Norm Principle [L], p. 208, we would have $N_{F_n/K}(g+\sqrt{f})\in S_{2^r}(K)$, which is not the case. We have therefore shown that $P(F_n)=2^r+1$. Q.E.D.

§ 9. Open problems

As we have said before, the computation of the pythagoras number of a ring is in general a very difficult task. Many problems in this area have remained unsolved. In this section, we shall collect a few of these open problems to indicate the rich possibilities for future work.

Problem 1. *In the category of (commutative) rings, find the answers to the questions* (Q_1) *and* (Q_2) *posed in* § 2 *(after* (2. 7)).

More ambitiously, given a ring k with $P(k) < \infty$, and any integer n, one may try to get qualitative and quantitative results on the invariant $g_k(n)$, the smallest number ($\leqq \infty$) such that any sum of squares of n-ary k-linear forms can be written as a sum of at most $g_k(n)$ squares of such forms. Very little work has been done in this direction. For instance the values of $g_k(n)$ do not seem to be known for all n even for $k = \mathbb{Z}$. The case $n = 2$ is classical: L. Mordell [M_1] had shown that every positive semidefinite binary form $ax^2 + 2bxy + cy^2$ over $\mathbb{Z}$ is a sum of 5 squares of $\mathbb{Z}$-linear forms, which implies that $g_{\mathbb{Z}}(2) = 5$. John Hsia has pointed out to us that, using the method of [Hs], Mordell's result can be extended to positive semidefinite forms $\sum a_{ij} x_i x_j$ ($a_{ij} = a_{ji} \in \mathbb{Z}$) to (at least) the case of $n \leqq 5$ variables, leading to $g_{\mathbb{Z}}(n) = n + 3$ for $n \leqq 5$. Hsia further commented that, in view of the results of [HKK], it seems likely that, in general, $g_{\mathbb{Z}}(n)$ is bounded by a polynomial function of n, though the explicit computation of $g_{\mathbb{Z}}(n)$ would probably be difficult. If we pass from $\mathbb{Z}$ to $k = \mathbb{Z}[1/p]$ by inverting a prime p, the computation becomes easier; in fact, one has an analog of Mordell's theorem for any number of variables over k, which gives $g_k(n) \leqq n + 3$, according to John Hsia.

Problem 2. *Let k_0 be a field with $P(k_0) < \infty$, and A be a k_0-affine algebra of transcendence degree* 1, *is it true that $P(A) < \infty$?*

If the answer to the "Weak Question" (Q_1) is yes, we can reduce Problem 2 (by the Noether Normalization Theorem, as in (3. 1)) to the purely transcendental case: $A = k_0[t]$. In view of (2. 2), the question in this case can be restated strictly within the category of fields:

If $P(k_0) < \infty$, does it follow that $P(k_0(t)) < \infty$?

It is known that this conclusion will follow iff all finite field extensions of k_0 have bounded pythagoras numbers, iff all nonreal finite field extensions of k_0 have bounded levels [P_2], [L], p. 314. However, whether this is indeed the case has remained for many years a difficult open problem in the theory of quadratic forms over fields.

In § 3 (cf. the paragraph following (3. 2)), we have remarked that there exist algebras A of transcendence degree 1 over $\mathbb{R}$ with arbitrarily large pythagoras numbers. However, the algebras we constructed there are more or less of an "unpleasant" type—for instance, they are not integral domains. In this connection, it would seem natural to consider the following:

Problem 3. *If A is the real coordinate ring of an absolutely irreducible affine curve C over $\mathbb{R}$, is $P(A)$ bounded by a universal constant?*

We do not know the answer to this problem even in the case when the curve C in question is assumed to be nonsingular.

The methods of Section 7 have led to large families of affine algebras of transcendence degree $\geqq 3$ (over the base field) which have an infinite pythagoras number. However, our results are conclusive for affine algebras of transcendence degree two, i.e. for the case of affine spaces. We pose as the next problem the following:

Problem 4. *Study the pythagoras number of affine algebras of transcendence degree 2 over a real closed field.*

It will also be useful to study a "local" version of this problem, i.e., to try to compute the pythagoras number of affine algebras over real-closed fields localized at height 2 primes. The solution to this, even if only for regular primes of height 2, will be of considerable interest. In this regard, we raise a somewhat more general question:

Problem 5. *Let A be a regular local ring of dimension 2 whose quotient field has a finite pythagoras number. Does it follow that A has a finite pythagoras number?*

To motivate the assumption that A has dimension 2, we recall that the problem has a positive answer for dimension 1 (cf. (2. 3)), but has a negative answer for dimension $\geqq 3$ (cf. (6. 6), (6. 7)).

Our next problem concerns the field $k((x_1, \ldots, x_n))$, which is the quotient field of the power series ring $k[[x_1, \ldots, x_n]]$.

Problem 6. *For k any real-closed field, compute $P(k((x_1, \ldots, x_n)))$ for $n \geqq 3$.* (Cf. (5. 1) and (5. 14) if $n \leqq 2$.)

Note that $F_n = k((x_1, \ldots, x_n))$ is a much smaller field than the iterated power series field $K_n = k((x_1)) \cdots ((x_n))$. The latter is known to have many remarkable properties, e.g. K_n is hereditarily pythago ean [B$_1$] and $K_n(\sqrt{-1})$ is a C_n-field in the sense of Lang [G], p. 35. It seems to be unknown, however, whether $F_n(\sqrt{-1})$ is a C_n-field (cf. [G], p. 36), or even a C_n^q-field in the sense of Pfister [P$_3$]. If we know that $F_n(\sqrt{-1})$ is a "C_n-field for quadratic forms" (or more weakly, if any n-fold Pfister form over $F_n(\sqrt{-1})$ is universal), then the usual descent argument (cf. [P$_2$], [L], p. 301) will show that $P(F_n) \leqq 2^n$, as in the case of the rational function field $k(x_1, \ldots, x_n)$. For $n=2$, we do know (from (5. 16)) that $F_2(\sqrt{-1})$ is C_2 for diagonal forms and hence for quadratic forms: the descent argument implies $P(F_2) \leqq 4$, while it turns out that $P(F_2) = 2$ by (5. 14). Based on this, it may seem tempting to conjecture that $P(F_n) \leqq 2^{n-1}$.

In field theory, there is a well-known theorem of Springer on the behavior of quadratic forms under an odd degree field extension: *If $[K: k]$ is odd and if q is an anisotropic quadratic form over k, then q remains anisotropic over K* [L], p. 198. Applying this to the forms $q = a x_0^2 - x_1^2 - \cdots - x_n^2$, we see easily that $P(k) \leqq P(K)$. It would be interesting to find out to what extent this could be generalized to rings (or at least to unique factorization domains):

Problem 7. *If R is a* UFD *and A is an R-algebra which, as an R-module, is finitely generated of odd rank, is it true that $P(R) \leqq P(A)$?*

Finally, it will be of interest to try to generalize the results of this paper from sums of squares to sums of higher powers in rings. For any natural number $d \in \mathbb{N}$, one can define the (higher) pythagoras number $P_d(A)$, for a ring A, to be the smallest number $n \leqq \infty$ such that any sum of d-th powers in A can be written as a sum of at most n d-th powers. In this notation, the usual pythagoras number $P(A)$ is just $P_2(A)$. A couple of the results in this paper concerning $P(A)$ can be extended to $P_{2^r}(A)$ by just making formal changes in the proofs. The most notable example is the proof for (4. 10) and (4. 12), which extends easily to give $P_{2r}(\mathbb{Z}[x]) = \infty$ for any $r \in \mathbb{N}$. Unfortunately, the proof for

$$P(\mathbb{R}[x_1, \ldots, x_n]) = \infty \qquad (n \geqq 2)$$

does not seem to generalize to give $P_{2r}(\mathbb{R}[x_1, \ldots, x_n]) = \infty$. We propose as the last problem the following

Problem 8. *For any $n \geqq 1$ and $r \geqq 2$, compute $P_{2r}(\mathbb{R}[x_1, \ldots, x_n])$.*

E. Becker has shown recently [B_2] that $P_{2r}(\mathbb{R}(x_1, \ldots, x_n))$ is finite for all n and all r. However, we do not know if $P_{2r}(\mathbb{R}[x_1, \ldots, x_n])$ is finite even for $n = 1$ and $r = 2$. Thus, an important special case for Problem 8 is the determination of $P_4(\mathbb{R}[x])$.

Note added in proof. Concerning Problem 3, E. Becker and M. Ojanguren have shown us the construction of subrings of the type $\mathbb{R}[t^{n_1}, \ldots, t^{n_r}]$ in $\mathbb{R}[t]$ which have unbounded pythagoras numbers (private communication). After receiving this communication, we have further shown that rings of the type $\mathbb{R}[t^a, t^{2a-1}]$ (arising from *plane* curves) already have unbounded pythagoras numbers. However, since these curves do have singularities, the case of Problem 3 for *nonsingular* curves remains open.

References

[A] *M. Artin*, On the solutions of analytic equations, Invt. Math. **5** (1968), 277—291.

[B_1] *E. Becker*, Hereditarily Pythagorean Fields and Orderings of Higher Level, Monografias de Matemática, No. 29, I.M.P.A. Rio de Janeiro, 1978.

[B_2] *E. Becker*, Summen n-ter Potenzen in Körpern und der reelle Holomorphiering, to appear.

[Ba] *R. Baeza*, Über die Stufe von Dedekind Ringen, Archiv Math. **33** (1979), 226—231.

[Br] *L. Bröcker*, Über die Pythagoraszahl eines Körpers, Archiv Math. **31** (1978), 133—136.

[C] *J. W. S. Cassels*, On the representation of rational functions as sums of squares, Acta Arithm. **9** (1964), 79—82.

[CEP] *J. W. S. Cassels, W. J. Ellison* and *A. Pfister*, On sums of squares and on elliptic curves over function fields, J. Number Theory **3** (1971), 125—149.

[CL] *M. D. Choi* and *T. Y. Lam*, An old question of Hilbert, in Proc. of Quadratic Form Conference (ed. G. Orzech), Queen's Papers in Pure and Applied Math. **46** (1977), 385—405.

[CLR_1] *M. D. Choi, T. Y. Lam* and *B. Reznick*, Real zeros of positive semidefinite forms. I, Math. Zeit. **171** (1980), 1—26.

[CLR_2] *M. D. Choi, T. Y. Lam* and *B. Reznick*, A combinatorial theory of sums of squares of polynomials, in preparation.

[CLRR] *M. D. Choi, T. Y. Lam, B. Reznick* and *A. Rosenberg*, Sums of squares in some integral domains, J. Algebra **65** (1980), 234—256.

[CT_1] *J.-L. Colliot-Thélène*, Formes quadratiques multiplicatives et variétés algébriques, Bull. Soc. Math. France **106** (1978), 113—151.

[CT_2] *J.-L. Colliot-Thélène*, Formes quadratiques sur les anneaux semilocaux réguliers, Bull. Soc. Math. France Mém. **59** (1979), 13—31.

[D] *D. Ž. Djoković*, Hermitian matrices over polynomial rings, J. Algebra **43** (1976), 359—374.

[De] *C. Delzell*, A constructive, continuous solution to Hilbert's 17th Problem, and other results in semi-algebraic geometry, Thesis, Stanford University 1980.

[DE_1] *D. Dubois* and *G. Efroymson*, Algebraic theory of real varieties, I, in Studies and Essays presented to Yu-Why Chen on his 60th Birthday, Taiwan University 1970, 107—135.

[DE_2] *D. Dubois* and *G. Efroymson*, A dimension theorem for real primes, Canad. J. Math. **26** (1974), 108—114.

[DLP] *Z. D. Dai, T. Y. Lam* and *C. K. Peng*, Levels in algebra and topology, Bull. Amer. Math. Soc. (new series) **3** (1980), 845—848.

[EL] *R. Elman* and *T. Y. Lam*, Quadratic forms under algebraic extensions, Math. Ann. **219** (1976), 21—42.

[F] *L. Fejér*, Über trigonometrische Polynome, J. reine angew. Math. **146** (1916), 53—82.

[G] *M. Greenberg*, Lectures on Forms in Many Variables, Lecture Notes in Mathematics, W. A. Benjamin, Reading, Mass., 1969.

[H] *D. Hilbert*, Über ternäre definite Formen. Acta Math. **17** (1893), 169—197.

[Hs] *J. Hsia*, Two theorems on integral matrices, Linear and Multilinear Algebra **5** (1978), 257—264.

[HJ] *J. Hsia* and *R. Johnson*, On the representation in sums of squares for definite functions in one variable over an algebraic number field. Amer. J. Math. **96** (1974), 448—453.

[HKK] *J. Hsia*, *Y. Kitaoka* and *M. Kneser*, Representations of positive definite quadratic forms. J. reine angew. Math. **301** (1978), 132—141.

[J] *V. A. Jakubović*, Factorization of symmetric matrix polynomials, Dokl. Akad. Nauk SSSR **194** (1970), 532—535.

[Jo] *J.-R. Joly*, Sommes de carrés dans certains anneaux principaux, Bull. Sc. Math. **94** (1970), 85—95.

[L] *T. Y. Lam*, The Algebraic Theory of Quadratic Forms, Lecture Notes in Mathematics, W. A. Benjamin, Reading, Mass. (2nd Printing), 1980.

[Ld] *H. Lindel*, Projektive Moduln über Polynomringen $A[T_1, \ldots, T_m]$ mit einem regulären Grundring A, Manuscripta Math. **23** (1978), 143—154.

[Li] *H. Liese*. Quadratsummen in $\mathbb{Z}$ und $\mathbb{Z}[[x]]$, Staatsexamens-Arbeit, Münster 1975 (unpublished).

[Lg] *S. Lang*, Introduction to Algebraic Geometry, New York 1958.

[M_1] *L. Mordell*, A new Waring problem with squares of linear forms, Quart. J. Math. (Oxford) **4** (1930), 276—288.

[M_2] *L. Mordell*, On the representation of a binary quadratic form as a sum of squares of linear forms. Math. Zeit. **35** (1932), 1—15.

[MH] *J. Milnor* and *D. Husemoller*, Symmetric Bilinear Forms, Berlin-Heidelberg-New York 1973.

[N] *M. Nagata*, A remark on the unique factorization theorem. J. Math. Soc. Japan **9** (1957), 143—145.

[P_1] *A. Pfister*, Darstellung von -1 als Summe von Quadraten in einem Körper, London J. Math. **40** (1965), 159—165.

[P_2] *A. Pfister*, Zur Darstellung definiter Funktionen als Summe von Quadraten. Invent. Math. **4** (1967), 229—237.

[P_3] *A. Pfister*, Systems of quadratic forms, Bull. Soc. Math. France Mém. **59** (1979), 115—123.

[P] *Y. Pourchet*, Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques, Acta Arithm. **19** (1971), 89—104.

[Pe_1] *M. Peters*, Die Stufe von Ordnungen ganzer Zahlen in algebraischen Zahlkörpern, Math. Ann. **195** (1972), 309—314.

[Pe_2] *M. Peters*, Summen von Quadraten in Zahlringen, J. reine angew. Math. **268/269** (1974), 318—323.

[Po] *V. M. Popov*, Hyperstability of Control Systems, Berlin-Heidelberg-New York 1973.

[Pr] *A. Prestel*, Remarks on the pythagoras and Hasse number of real fields, J. reine angew. Math. **303/304** (1978), 284—294.

[PS] *G. Pólya* and *G. Szegö*, Problems and Theorems in Analysis. 2, Berlin-Heidelberg-New York 1976.

[R] *P. Ribenboim*, Pfister's dimension and the level of fields, Math. Scand. **35** (1974), 301—308.

[RR] *M. Rosenblum* and *J. Rovnyak*, The factorization problem for nonnegative operator valued functions, Bull. Amer. Math. Soc. **77** (1971), 287—318.

[S] *P. Samuel*, Anneaux Factoriels, Soc. de Mat. de São Paulo 1963.

[St] *G. Stengle*, Integral solution of Hilbert's Seventeenth Problem. Math. Ann. **246** (1979), 33—39.

[Sw] *R. Swan*, Vector bundles and projective modules. Trans. Amer. Math. Soc. **105** (1962), 264—277.

[W] *E. Witt*, Zerlegung reeller algebraischer Funktionen in Quadrate, Schiefkörper über reellem Funktionenkörper, J. reine angew. Math. **171** (1934), 4—11.

[ZS] *O. Zariski* and *P. Samuel*, Commutative Algebra. 2, Princeton 1962.

University of Toronto, Toronto, Canada M5S 1A1
Institute of Mathematics, Academia Sinica, Peking, China
University of California, Berkeley, California 94720, U.S.A.
University of Illinois, Urbana, Illinois 61801, U.S.A.

Eingegangen 3. November 1981