A p-adic analogue of Siegel's Theorem on sums of squares

Dittmann, Philip and Anscombe, Sylvy

Received: 15 April 2019 | Revised: 27 July 2019 | Accepted: 15 August 2019
DOI: 10.1002/mana.201900173

ORIGINAL PAPER

MATHEMATISCHE NACHRICHTEN

A p-adic analogue of Siegel's theorem on sums of squares

Sylvy Anscombe[1] | **Philip Dittmann**[2,3] | **Arno Fehm**[3]

[1]Jeremiah Horrocks Institute, University of Central Lancashire, Preston, PR1 2HE, United Kingdom
[2]Afdeling Algebra, KU Leuven, Celestijnenlaan 200b, Leuven, 3001, Belgium
[3]Institut für Algebra, Fakultät Mathematik und Naturwissenschaft – Fachrichtung Mathematik, Technische Universität Dresden, 01062 Dresden, Germany

Correspondence
Sylvy Anscombe, Jeremiah Horrocks Institute, University of Central Lancashire, Preston PR1 2HE, United Kingdom.
Email: sanscombe@uclan.ac.uk

Funding information
University of Oxford Clarendon Fund; Merton College, Oxford; Deutsche Forschungsgemeinschaft, Grant/Award Number: 404427454; The Leverhulme Trust, Grant/Award Number: RPG-2017-179; KU Leuven, Grant/Award Number: IF C14/17/083

Abstract
Siegel proved that every totally positive element of a number field K is the sum of four squares, so in particular the Pythagoras number is uniformly bounded across number fields. The p-adic Kochen operator provides a p-adic analogue of squaring, and a certain localisation of the ring generated by this operator consists of precisely the totally p-integral elements of K. We use this to formulate and prove a p-adic analogue of Siegel's theorem, by introducing the p-Pythagoras number of a general field, and showing that this number is uniformly bounded across number fields. We also generally study fields with finite p-Pythagoras number and show that the growth of the p-Pythagoras number in finite extensions is bounded.

KEYWORDS
Kochen operator, number fields, p-valuations

MSC (2010)
11E25, 11S99, 11U09, 12D15

1 | INTRODUCTION

The study of sums of squares has a long history. In the context of the integers, Fermat, Euler, Lagrange and many others studied which integers are a sum of a certain number of square integers. The possibly most famous result in this direction is Lagrange's Four Squares Theorem [13, Thm. 369] that every nonnegative integer is the sum of four squares. In fact, earlier Euler had proved a version of this theorem for $\mathbb{Q}$: every nonnegative rational number is the sum of four square rational numbers. A comprehensive history of these theorems may be found in [6, Chapter VIII]. In the other direction, for both $\mathbb{Z}$ and $\mathbb{Q}$ there exist nonnegative numbers that cannot be written as a sum of three squares. The *Pythagoras number* $\pi(F)$ of a field F is the smallest n such that

$$\{x_1^2 + \cdots + x_m^2 \mid x_1, \ldots, x_m \in F, m \in \mathbb{N}\} = \{x_1^2 + \cdots + x_n^2 \mid x_1, \ldots, x_n \in F\}.$$

Using this terminology, Euler's theorem becomes the statement that $\pi(\mathbb{Q}) = 4$. The following generalization of Euler's theorem was conjectured by Hilbert and proven by Siegel in [25], cf. [20, Ch. 7, §1, 1.4]:

Theorem 1.1 (Siegel). *For all number fields F, $\pi(F) \leq 4$.*

The study of the Pythagoras number of a field is intimately related to the study of the orderings on that field, since by a theorem of Artin and Schreier the sums of squares are precisely the totally positive elements. In a number field F, these can be described simply as those elements that are mapped to $\mathbb{R}_{\geq 0}$ by every embedding of F into $\mathbb{R}$, cf. [20, Ch. 3 and 7].

We define and study a p-adic version of the Pythagoras number, namely the *p-Pythagoras number* $\pi_p(F)$ of a field F, or more generally the $(\mathfrak{p}, \tau)$-Pythagoras number, see Section 2.2 for the definition. Just like the Pythagoras number gives information on the set of totally positive elements, the p-Pythagoras number relates to the set of totally p-integral elements, which in a number field F can be described simply as those elements that are mapped to $\mathbb{Z}_p$ by every embedding of F into $\mathbb{Q}_p$. Our main result is an inexplicit analogue of Siegel's theorem:

Theorem 1.2. *Let p be a prime number. There exists $N_p \in \mathbb{N}$ such that $\pi_p(F) \le N_p$ for every number field F.*

This result will be deduced from the more general Theorem 4.9. We also give some general results on fields F with finite $(\mathfrak{p}, \tau)$-Pythagoras number and prove in Theorem 5.9 that the growth of the $(\mathfrak{p}, \tau)$-Pythagoras number is bounded in finite extensions. As an application, we show in Corollary 6.5 that for every open-closed subset of the p-adic spectrum of F, the associated holomorphy ring is diophantine. A further application can be found in the forthcoming work [2], in which we use the results of this paper to show that rings of formal power series over number fields are $\mathbb{Z}$-diophantine in their quotient fields.

2 | THE $(\mathfrak{p}, \tau)$-PYTHAGORAS NUMBER

2.1 | p-valuations

A (Krull) valuation v on a field F is a *p-valuation* if it has a finite residue field $\bar{F}_v$ of characteristic p and value group $v(F^\times)$ such that the interval $(0, v(p)]$ is finite. A (finite) *prime* $\mathfrak{P}$ of a field F is an equivalence class of p-valuations on F (for the usual notion of equivalence of valuations), for some prime number p. We write $v_\mathfrak{P}$ for a representative of $\mathfrak{P}$ which has $\mathbb{Z}$ as smallest non-trivial convex subgroup of the value group. See [22] for basics regarding p-valuations, and [10] for details on this notion of prime and some of the following definitions.

Example 2.1. The primes of a number field K correspond precisely to the finite places in the usual sense and we will identify them. If $K = \mathbb{Q}$ and p is a prime number then v_p denotes the usual p-adic valuation, and we denote the corresponding prime also by p.

For the rest of this work we fix a triple $(K, \mathfrak{p}, \tau)$, where K is a number field, $\mathfrak{p}$ is a finite prime of K, and τ is a pair of natural numbers $(e, f) \in \mathbb{N}^2$. We denote by $t_\mathfrak{p}$ a uniformizer of $v_\mathfrak{p}$, i.e. an element with $v_\mathfrak{p}\left(t_\mathfrak{p}\right) = 1$, we let q denote the size of the residue field $\bar{K}_{v_\mathfrak{p}}$.

For a field extension F/K with $\mathfrak{P}$ a prime of F lying above $\mathfrak{p}$, the *relative initial ramification* is $e(\mathfrak{P}|\mathfrak{p}) := v_\mathfrak{P}\left(t_\mathfrak{p}\right)$, the *relative residue degree* is $f(\mathfrak{P}|\mathfrak{p}) := \left[\bar{F}_{v_\mathfrak{P}} : \bar{K}_{v_\mathfrak{p}}\right]$, and the pair $(e(\mathfrak{P}|\mathfrak{p}), f(\mathfrak{P}|\mathfrak{p}))$ is the *relative type* of $\mathfrak{P}$ over $\mathfrak{p}$. We say $\mathfrak{P}$ is of relative type *at most* τ if $e(\mathfrak{P}|\mathfrak{p})$ is no greater than e, and $f(\mathfrak{P}|\mathfrak{p})$ divides f. Likewise, for $\tau' = (e', f')$ we write $\tau \le \tau'$ if $e \le e'$ and $f \mid f'$. We denote by $\mathcal{S}(F)$ the set of primes of F, by $\mathcal{S}^*_\mathfrak{p}(F) \subseteq \mathcal{S}(F)$ the set of those primes $\mathfrak{P}$ of F lying above $\mathfrak{p}$, and by $\mathcal{S}^\tau_\mathfrak{p}(F) \subseteq \mathcal{S}^*_\mathfrak{p}(F)$ the subset of those primes $\mathfrak{P}$ of F which are of relative type at most τ over $\mathfrak{p}$. The corresponding *holomorphy ring* is

$$R^\tau_\mathfrak{p}(F) := \bigcap_{\mathfrak{P} \in \mathcal{S}^\tau_\mathfrak{p}(F)} \mathcal{O}_\mathfrak{P},$$

where $\mathcal{O}_\mathfrak{P}$ is the valuation ring of $\mathfrak{P}$, and

$$\Gamma^\tau_\mathfrak{p}(F) := \left\{ \frac{a}{1 + t_\mathfrak{p} b} \;\middle|\; a, b \in \mathcal{O}_\mathfrak{p}\left[\gamma^\tau_{\mathfrak{p}, t_\mathfrak{p}}(F)\right], 1 + t_\mathfrak{p} b \neq 0 \right\}$$

is the corresponding *Kochen ring*, where

$$\gamma^\tau_{\mathfrak{p}, t_\mathfrak{p}}(X) := \frac{1}{t_\mathfrak{p}} \cdot \left(\frac{X^{q^f} - X}{\left(X^{q^f} - X\right)^2 - 1} \right)^e$$

is the *Kochen operator*. Here and in what follows, if $\gamma \in F(X)$ is a rational function, we mean by $\gamma(F)$ the image of γ on $F \setminus \{\text{poles of } \gamma\}$. Note that $\Gamma^\tau_\mathfrak{p}(F)$ does not depend on the choice of $t_\mathfrak{p}$, since the quotient of two uniformizers of $v_\mathfrak{p}$ is an element of $\mathcal{O}^\times_\mathfrak{p}$. Recall that $R^\tau_\mathfrak{p}(F)$ is the integral closure of $\Gamma^\tau_\mathfrak{p}(F)$, with equality in the case $e = 1$, see [22, Cor. 6.9] and the subsequent discussion for more details.

Example 2.2. If $\mathfrak{p}$ is any place of the number field K, we denote by $K_{\mathfrak{p}}$ the completion of K with respect to $\mathfrak{p}$. If $\mathfrak{p}$ is a finite place, then $K_{\mathfrak{p}}$ is a non-archimedean local field and $\mathfrak{p}$ extends to a unique prime $\mathfrak{P}$ of $K_{\mathfrak{p}}$ of the same type, so $R^{\tau}_{\mathfrak{p}}(K_{\mathfrak{p}}) = R^{(1,1)}_{\mathfrak{p}}(K_{\mathfrak{p}}) = \mathcal{O}_{\mathfrak{P}}$. In fact, any non-archimedean local field E of characteristic zero carries a unique prime, whose valuation ring we denote by $\mathcal{O}_E$, cf. [22, Thm. 6.15]. We say that an extension of non-archimedean local fields is of relative type at most τ if this is true for the respective primes.

The real holomorphy ring of F is the intersection of the positive cones of the orderings on F, i.e. the set of elements that are nonnegative under every ordering on F. By the theorem of Artin and Schreier it can alternatively be described as the set of sums of squares, and the classical Pythagoras number may be seen as a measure of the complexity of this description in terms of squares. The holomorphy ring $R^{\tau}_{\mathfrak{p}}(F)$ is defined above as an intersection of the valuation rings of certain p-valuations, and it also equals the integral closure of $\Gamma^{\tau}_{\mathfrak{p}}(F)$. Thus a p-adic analogue of the Pythagoras number should somehow measure the complexity of the description of $R^{\tau}_{\mathfrak{p}}(F)$ in terms of the rational function $\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}$. We now define such a p-adic analogue.

2.2 | The $(\mathfrak{p},\tau)$-Pythagoras number

Let F/K be an extension. For $g \in \mathcal{O}_{\mathfrak{p}}[X_1,\dots,X_n]$, we write

$$R^{\tau}_{\mathfrak{p},g,t_{\mathfrak{p}}}(F) := \left\{ \frac{a}{1+t_{\mathfrak{p}}b} \;\middle|\; a,b \in g\left(\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(F),\dots,\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(F)\right), 1+t_{\mathfrak{p}}b \neq 0 \right\},$$

and for $n \geq 1$

$$R^{\tau}_{\mathfrak{p},g,t_{\mathfrak{p}},n}(F) := \left\{ x \in F \;\middle|\; x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0 \text{ with } 1 \leq m \leq n, a_0,\dots,a_{m-1} \in R^{\tau}_{\mathfrak{p},g,t_{\mathfrak{p}}}(F) \right\}.$$

We denote by $\mathcal{P}_{\mathfrak{p},n}$ the finite set of those $g \in \mathcal{O}_{\mathfrak{p}}[X_1,\dots,X_n]$ of degree and height at most n (cf. [4, Def. 1.6.1]). We write

$$R^{\tau}_{\mathfrak{p},n}(F) := \bigcup_{t_{\mathfrak{p}}} \bigcup_{g \in \mathcal{P}_{\mathfrak{p},n}} R^{\tau}_{\mathfrak{p},g,t_{\mathfrak{p}},n}(F),$$

where $t_{\mathfrak{p}}$ varies over those (finitely many) elements of the ring of integers $\mathcal{O}_K$ which are uniformizers for $\mathfrak{p}$ of minimal height. Then $\left(R^{\tau}_{\mathfrak{p},n}(F)\right)_{n\in\mathbb{N}}$ is an increasing chain of subsets of F and

$$R^{\tau}_{\mathfrak{p}}(F) = \bigcup_{n\in\mathbb{N}} R^{\tau}_{\mathfrak{p},n}(F).$$

The $(\mathfrak{p},\tau)$-*Pythagoras number* $\pi^{\tau}_{\mathfrak{p}}(F)$ of F is the smallest n such that

$$R^{\tau}_{\mathfrak{p}}(F) = R^{\tau}_{\mathfrak{p},n}(F),$$

and we write $\pi^{\tau}_{\mathfrak{p}}(F) = \infty$ if there is no such n. In other words,

$$\pi^{\tau}_{\mathfrak{p}}(F) := \inf\left\{ n \in \mathbb{N} \;\middle|\; R^{\tau}_{\mathfrak{p}}(F) = R^{\tau}_{\mathfrak{p},n}(F) \right\} \in \mathbb{N} \cup \{\infty\}.$$

In the case $K = \mathbb{Q}$, $\mathfrak{p} = p$ and $\tau = (1,1)$, we write $R_p(F)$ and $\pi_p(F)$, omitting the relative type (1,1), and we speak of the p-Pythagoras number. We also write $\gamma_p := \gamma^{(1,1)}_{p,p}$, and note that the only two uniformizers (of the prime p) in $\mathbb{Z}$ of minimal height are p and $-p$, with $\gamma^{(1,1)}_{p,-p} = -\gamma_p$. We discuss some possible variations of our definition of the $(\mathfrak{p},\tau)$-Pythagoras number in Remarks 3.11 and 3.12.

Example 2.3. Since $\mathbb{C}$ is algebraically closed and carries no p-valuation, we have

$$R_p(\mathbb{C}) = \mathbb{C} = \gamma_p(\mathbb{C}),$$

in particular $\pi_p(\mathbb{C}) = 1$.

Example 2.4. It follows easily from Hensel's lemma that

$$R_p(\mathbb{Q}_p) = \mathbb{Z}_p = \gamma_p(\mathbb{Q}_p),$$

in particular $\pi_p(\mathbb{Q}_p) = 1$, see [22, Thm. 6.15].

Example 2.5. In [11, Lem. 3.02] it is shown that every so-called pseudo p-adically closed field F (where pseudo p-adically closed means that a certain geometric local-global principle holds for varieties over F) satisfies

$$R_p(F) = \gamma_p(F) + \gamma_p(F) + \gamma_p(F),$$

hence $\pi_p(F) \leq 3$. This applies for example to the field $\mathbb{Q}^{\mathrm{t}p}$ of totally p-adic algebraic numbers by a result of Moret–Bailly [17], where the local-global principle takes the following simple form: If V is a geometrically irreducible smooth variety over $\mathbb{Q}^{\mathrm{t}p}$ which has a $\mathbb{Q}_p$-rational point for every embedding of $\mathbb{Q}^{\mathrm{t}p}$ into $\mathbb{Q}_p$, then it has a $\mathbb{Q}^{\mathrm{t}p}$-rational point.

It is known that there are fields F with $\pi(F) = \infty$, for example $F = \mathbb{R}(x_1, x_2, \dots)$, see [15, Ch. XI, Example 5.9(5)]. On the other hand, we do not know if $\pi_p(F) = \infty$ for any field:

Question 2.6. Is $\pi_p(\mathbb{Q}(X_1, X_2, \dots)) = \infty$?

2.3 | Explicit bounds and uniformity in p

We now prove a few rather elementary statements about $\pi_p(\mathbb{Q})$. We will drop the relative type $\tau = (1, 1)$ from all notation. Let ℓ be a prime number distinct from p.

Lemma 2.7. *We have $\gamma_p(\mathbb{Q}) \subseteq \mathbb{Z}_{(\ell)}$ if and only if neither $X^p - X + 1$ nor $X^p - X - 1$ has a zero in $\mathbb{F}_\ell$.*

Proof. Let $x \in \mathbb{Q}$, recall that $\gamma_p(x) = \frac{1}{p}\left((x^p - x) - (x^p - x)^{-1}\right)^{-1}$ and denote by v_ℓ the ℓ-adic valuation. If $v_\ell(x^p - x) < 0$ or $v_\ell(x^p - x) > 0$, then $v_\ell(\gamma_p(x)) > 0$. If $v_\ell(x^p - x) = 0$, then $x \in \mathbb{Z}_{(\ell)}$, and $v_\ell(\gamma_p(x)) < 0$ if and only if $(x^p - x) - (x^p - x)^{-1} \equiv 0 \mod \ell$, which means that $x^p - x \equiv \pm 1 \mod \ell$. □

Proposition 2.8. $\mathbb{Z}[\gamma_p(\mathbb{Q})] \subsetneq \mathbb{Z}_{(p)}$.

Proof. There exists a prime number $\ell \neq p$ such that $\mathbb{Z}[\gamma_p(\mathbb{Q})]$ is contained in $\mathbb{Z}_{(l)}$ by Lemma 2.7: specifically, the criterion given there is satisfied by $\ell = 2$ if p is odd and by $\ell = 17$ for $p = 2$. □

Lemma 2.9. *If $\ell - 1 \mid p - 1$ then $\gamma_p(\mathbb{Q}) \subseteq \ell\mathbb{Z}_{(\ell)}$.*

Proof. If $\ell - 1 | p - 1$, then $x^p - x = 0$ for all $x \in \mathbb{F}_\ell$. Thus $v_\ell(\gamma_p(x)) > 0$ for all $x \in \mathbb{Q}$, where v_ℓ is the ℓ-adic valuation. □

Proposition 2.10. *For every finite set $\mathcal{P} \subseteq \mathbb{Q}[X_1, X_2, \dots]$, there exist some p and $\ell \neq p$ with*

$$\bigcup_{g \in \mathcal{P}} R_{p,g,p}(\mathbb{Q}) \subseteq \mathbb{Z}_{(\ell)}.$$

In particular, $\sup_p \pi_p(\mathbb{Q}) = \infty$.

Proof. Choose $\ell > |\mathcal{P}| + 1$ such that $\mathcal{P} \subseteq \mathbb{Z}_{(\ell)}[X_1, X_2, \dots]$. There exists $a \in \mathbb{Z}$ such that $a \not\equiv 0 \pmod{\ell}$ and $a \not\equiv g(0, \dots, 0) \pmod{\ell}$ for every $g \in \mathcal{P}$. By Dirichlet's theorem on primes in arithmetic progressions (see [18, VII, (13.2)]), there exist infinitely many primes $p > \ell$ with $p \equiv 1 \pmod{\ell - 1}$ and $p \equiv -a^{-1} \pmod{\ell}$. Then

$$g(\gamma_p(\mathbb{Q}), \dots, \gamma_p(\mathbb{Q})) \subseteq g(0, \dots, 0) + \ell\mathbb{Z}_{(\ell)}$$

by Lemma 2.9, hence $1 + pg(\gamma_p(\mathbb{Q}), \dots, \gamma_p(\mathbb{Q})) \subseteq \mathbb{Z}_{(\ell)}^\times$ by the choice of a and p. Thus $R_{p,g,p}(\mathbb{Q}) \subseteq \mathbb{Z}_{(\ell)}$ for every $g \in \mathcal{P}$.

By the integral closedness of $\mathbb{Z}_{(\ell)}$ this implies $R_{p,g,p,n}(\mathbb{Q}) \subseteq \mathbb{Z}_{(\ell)}$ for every n. Note that $R_{p,g,-p,n}(F) = -R_{p,g^*,p,n}(F)$, where $g^*(X_1, \dots, X_n) = -g(-X_1, \dots, -X_n)$ has the same height as g. Therefore, applying the above to the set $\mathcal{P}$ of all $f \in \mathbb{Q}[X_1, \dots, X_n]$ of degree and height at most n, we obtain ℓ and $p > \ell$ with

$$\bigcup_{g \in \mathcal{P}_{p,n}} \left(R_{p,g,p,n}(F) \cup R_{p,g,-p,n}(F)\right) \subseteq \bigcup_{p \in \mathcal{P}} R_{p,g,p,n}(F) \subseteq \mathbb{Z}_{(\ell)},$$

and therefore $\pi_p(\mathbb{Q}) > n$. □

2.4 | The Kochen operator

For later use, we explore several simple properties of the Kochen operator. Let F/K be any extension.

Lemma 2.11. *Let $\mathfrak{P} \in \mathcal{S}^*_{\mathfrak{p}}(F)$ and suppose that $x \in F$ is not a pole of $\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}$. Then*

$$v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(x)\right) = \begin{cases} -eq^f v_\mathfrak{P}(x) - v_\mathfrak{P}(t_\mathfrak{p}) & \text{if } v_\mathfrak{P}(x) < 0, \\ ev_\mathfrak{P}(x) - v_\mathfrak{P}(t_\mathfrak{p}) & \text{if } v_\mathfrak{P}(x) > 0, \\ ev_\mathfrak{P}\left(x^{q^f} - x\right) - v_\mathfrak{P}(t_\mathfrak{p}) & \text{if } v_\mathfrak{P}(x) = 0 \text{ and } v_\mathfrak{P}\left(x^{q^f} - x\right) > 0, \\ -ev_\mathfrak{P}\left(\left(x^{q^f} - x\right)^2 - 1\right) - v_\mathfrak{P}(t_\mathfrak{p}) & \text{if } v_\mathfrak{P}(x) = 0 \text{ and } v_\mathfrak{P}\left(x^{q^f} - x\right) = 0. \end{cases}$$

Proof. This is a matter of calculating valuations. □

Lemma 2.12. *Let $\mathfrak{P} \in \mathcal{S}^*_{\mathfrak{p}}(F)$. Suppose that $x \in F$ is not a pole of $\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}$ and satisfies either*

(i) $0 < (e+1)v_\mathfrak{P}(x) \le v_\mathfrak{P}(t_\mathfrak{p})$, *or*
(ii) $v_\mathfrak{P}(x) = 0$ *and* $\left[\mathbb{F}_q\left(\operatorname{res}_\mathfrak{P}(x)\right) : \mathbb{F}_q\right] \nmid f$, *where* $\operatorname{res}_\mathfrak{P}(x)$ *is the residue of* x.

Then

$$v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(x)\right) \le -\frac{1}{e+1} v_\mathfrak{P}(t_\mathfrak{p}) < 0.$$

Proof. In case (i), Lemma 2.11 gives that

$$v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(x)\right) = ev_\mathfrak{P}(x) - v_\mathfrak{P}(t_\mathfrak{p}) \le -\frac{1}{e+1} v_\mathfrak{P}(t_\mathfrak{p}).$$

In case (ii), the residue of x is not a root of $X^{q^f} - X$, and so

$$v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(x)\right) = -ev_\mathfrak{P}\left(\left(x^{q^f} - x\right)^2 - 1\right) - v_\mathfrak{P}(t_\mathfrak{p}) \le -v_\mathfrak{P}(t_\mathfrak{p}) \le -\frac{1}{e+1} v_\mathfrak{P}(t_\mathfrak{p}),$$

also by Lemma 2.11. □

Lemma 2.13. *Let $\mathfrak{P} \in \mathcal{S}^*_{\mathfrak{p}}(F)$, let and $x, y \in F$, and suppose that x is not a pole of $\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}$, and $v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(x)\right) < 0$. If $v_\mathfrak{P}(x-y) \ge v_\mathfrak{P}(t_\mathfrak{p})$, then also y is not a pole of $\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}$, and $v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(y)\right) < 0$.*

Proof. If $v_\mathfrak{P}(x) \le 0$, then in particular $v_\mathfrak{P}(x) < v_\mathfrak{P}(t_\mathfrak{p})$, while if $v_\mathfrak{p}(x) > 0$, then $v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(x)\right) = ev_\mathfrak{P}(x) - v_\mathfrak{P}(t_\mathfrak{p})$ by Lemma 2.11, hence $v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(x)\right) < 0$ implies that $v_\mathfrak{P}(x) < v_\mathfrak{P}(t_\mathfrak{p})$ also in this case. Therefore, in either case we conclude from $v_\mathfrak{P}(x-y) \ge v_\mathfrak{P}(t_\mathfrak{p})$ that $v_\mathfrak{P}(x) = v_\mathfrak{P}(y)$. We make a case distinction:

Suppose first that $v_\mathfrak{P}(x) \ne 0$. By Lemma 2.11, in this case, $v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(x)\right)$ depends only on $v_\mathfrak{P}(x)$. Therefore $v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(y)\right) = v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(x)\right) < 0$.

Suppose now that $v_\mathfrak{P}(x) = 0$. As $x - y$ divides $x^{q^f} - y^{q^f}$ in $\mathcal{O}_\mathfrak{P}$, we have that $v_\mathfrak{P}\left(y^{q^f} - y - x^{q^f} + x\right) \ge v_\mathfrak{P}(x-y) \ge v_\mathfrak{P}(t_\mathfrak{p})$. If $v_\mathfrak{P}\left(x^{q^f} - x\right) = 0$, then in particular $v_\mathfrak{P}\left(x^{q^f} - x\right) < v_\mathfrak{P}(t_\mathfrak{p})$, while if $v_\mathfrak{P}\left(x^{q^f} - x\right) > 0$, then $v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(x)\right) < 0$ implies that $v_\mathfrak{P}\left(x^{q^f} - x\right) < \frac{1}{e} v_\mathfrak{P}(t_\mathfrak{p}) \le v_\mathfrak{P}(t_\mathfrak{p})$ by Lemma 2.11. Thus $v_\mathfrak{P}\left(y^{q^f} - y\right) = v_\mathfrak{P}\left(x^{q^f} - x\right)$ in both cases. If $v_\mathfrak{P}\left(x^{q^f} - x\right) = 0$, then Lemma 2.11 gives immediately that $v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(y)\right) < 0$, while if $v_\mathfrak{P}\left(x^{q^f} - x\right) > 0$, then Lemma 2.11 shows that $v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(x)\right)$ depends only on $v_\mathfrak{P}\left(x^{q^f} - x\right)$, hence $v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(y)\right) = v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(x)\right) < 0$. □

3 | DIOPHANTINE FAMILIES

A *diophantine* subset of a field F is the image of the F-rational points of some F-variety V under a morphism $V \to \mathbb{A}^1_F$. As we want to discuss questions of uniformity we use the following slightly more sophisticated notion: An *n-dimensional diophantine* *family over* K is a map D from the class of field extensions F of K to sets which is given by finitely many polynomials $f_1, \dots, f_r \in K[X_1, \dots, X_n, Y_1, \dots, Y_m]$, for some m, in the sense that

$$D(F) = \{x \in F^n \mid \exists y \in F^m : f_1(x, y) = 0, \dots, f_r(x, y) = 0\}$$

for every extension F/K. In this case, we say that the polynomials $f_1, \dots, f_r$ *define* D. Note that if E/F is an extension, then $D(F) \subseteq D(E)$.

Remark 3.1. From the point of view of algebraic geometry, an n-dimensional diophantine family D over K is given by a morphism of (not necessarily irreducible) K-varieties $\varphi : V \to \mathbb{A}^n_K$ in the sense that $D(F) = \varphi(V(F))$ for every extension F/K.

Remark 3.2. From the point of view of model theory, an n-dimensional diophantine family D over K is given by an existential formula $\varphi(x_1, \dots, x_n)$ in the language of rings with free variables among $x_1, \dots, x_n$ and parameters from K, in the sense that for every extension F/K, $D(F)$ is the set defined by φ in F, i.e. the set of $a \in F^m$ such that $F \vDash \varphi(a)$. Such a formula is equivalent (modulo the theory of fields) to a formula of the form

$$\exists y_1 \dots y_m : \bigwedge_{i=1}^{r} f_i(x_1, \dots, x_n, y_1, \dots, y_m) = 0$$

with $f_1, \dots, f_r \in K[X_1, \dots, X_n, Y_1, \dots, Y_m]$.

Most of the usual constructions for diophantine sets (see e.g. [24]) go through for diophantine families:

Lemma 3.3. *If D_1, D_2 are n-dimensional diophantine families over K, then there are n-dimensional diophantine families $D_1 \cup D_2$ and $D_1 \cap D_2$ over K such that $(D_1 \cup D_2)(F) = D_1(F) \cup D_2(F)$ and $(D_1 \cap D_2)(F) = D_1(F) \cap D_2(F)$ for every F/K.*

Proof. Suppose that the polynomials $f_1, \dots, f_r \in K[X_1, \dots, X_n, Y_1, \dots, Y_m]$ define D_1 and that the polynomials $g_1, \dots, g_s \in K[X_1, \dots, X_n, Z_1, \dots, Z_l]$ define D_2. We may assume that the variables Y_i and Z_j are distinct. We observe that $f_1, \dots, f_r, g_1, \dots, g_s$ define $D_1 \cap D_2$. Slightly less trivially, we have that $f_1 g_1, \dots, f_i g_j, \dots, f_r g_s$ define $D_1 \cup D_2$. □

Lemma 3.4. *Suppose that D_1 and D_2 are n_1- respectively n_2-dimensional diophantine families over K. Then there is an $(n_1 + n_2)$-dimensional diophantine family $D_1 \times D_2$ over K such that $(D_1 \times D_2)(F) = D_1(F) \times D_2(F)$ for every F/K.*

Proof. Suppose that the polynomials $f_1, \dots, f_r \in K[X_1, \dots, X_{n_1}, Y_1, \dots, Y_m]$ define D_1 and that the polynomials $g_1, \dots, g_s \in K\left[X'_1, \dots, X'_{n_2}, Z_1, \dots, Z_l\right]$ define D_2. This time, we suppose that all the variables X_i, X'_i, Y_i, Z_i are distinct. Then the polynomials $f_1, \dots, f_r, g_1, \dots, g_s$ define $D_1 \times D_2$. □

Lemma 3.5. *Let D be an n-dimensional diophantine family over K and let $f = \left(\frac{g_1}{h_1}, \dots, \frac{g_k}{h_k}\right)$ be a tuple of rational functions with $g_i, h_i \in K[X_1, \dots, X_n]$ such that for every i the polynomials g_i and h_i are coprime. Then there is an k-dimensional diophantine family fD with*

$$(fD)(F) = \left\{ \left(\frac{g_1(x)}{h_1(x)}, \dots, \frac{g_k(x)}{h_k(x)} \right) \,\middle|\, x \in D(F), h_i(x) \neq 0 \ \textit{for all } i \right\}$$

for every F/K.

Proof. Let $f_1, \dots, f_r \in K[X_1, \dots, X_n, Y_1, \dots, Y_m]$ define D. Then a tuple $(z_1, \dots, z_k) \in F^k$ is an element of the right hand side if and only if there exists $(x_1, \dots, x_n, y_1, \dots, y_m, w_1, \dots, w_k) \in F^{n+m+k}$ such that

1. $g_i(x_1, \dots, x_n) - z_i h_i(x_1, \dots, x_n) = 0$ for all $i = 1, \dots, k$,
2. $w_i h_i(x_1, \dots, x_n) = 1$ for all $i = 1, \dots, k$, and
3. $f_j(x_1, \dots, x_n, y_1, \dots, y_m) = 0$ for all $j = 1, \dots, r$.

Each of these conditions is the vanishing of a polynomial in the variables $W_1, \dots, W_k$, $X_1, \dots, X_k$, $Y_1, \dots, Y_r$ and $Z_1, \dots, Z_k$ over K. □

Remark 3.6. Perhaps the most trivial 1-dimensional diophantine family over K is the one assigning the set F to every field F/K. As described above in Section 2.1, given a rational function $\gamma \in K(X)$ and a field F/K, we write $\gamma(F)$ to mean the image under

γ of $F \setminus \{\text{poles of } \gamma\}$. By this small abuse of notation, γ may be identified with the map which sends a field F/K to its image $\gamma(F)$ under γ. Then by Lemma 3.5, γ is a 1-dimensional diophantine family over K. This applies in particular to the Kochen operator $\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}$.

Lemma 3.7. *If D is an n-dimensional diophantine family over K and $a = (a_1, \dots, a_r) \in K^r$, $r < n$, then there is an $(n-r)$-dimensional family D_a over K with*

$$D_a(F) = \left\{x \in F^{n-r} \mid (x, a) \in D(F)\right\}$$

for every F/K.

Proof. Again, let $f_1, \dots, f_r \in K[X_1, \dots, X_n, Y_1, \dots Y_m]$ define D. We write

$$g_i(X_1, \dots, X_{n-r}, Y_1, \dots, Y_m) := f_i(X_1, \dots, X_{n-r}, a_1, \dots, a_r, Y_1, \dots, Y_m).$$

Then the polynomials $g_1, \dots, g_r \in K[X_1, \dots, X_{n-r}, Y_1, \dots, Y_m]$ define the $(n-r)$-dimensional diophantine family D_a over K. □

Example 3.8. Each of the $R^{\tau}_{\mathfrak{p},n}$ is a 1-dimensional diophantine family over K.

Proposition 3.9. *Let $D, D_1, D_2, \dots$ be n-dimensional diophantine families over K. If $D(F) \subseteq \bigcup_{i\in\mathbb{N}} D_i(F)$ for every extension F/K, then there exists N such that $D(F) \subseteq \bigcup_{i=1}^{N} D_i(F)$ for every extension F/K.*

Proof. In light of Remark 3.2, this is a direct consequence of the compactness theorem of model theory, see for example [16, Thm. 2.1.4]. □

Proposition 3.10. *Let D be a 1-dimensional diophantine family over K and let $\mathcal{K}$ be a class of extensions of K. If*

(i) $D(L) = R^{\tau}_{\mathfrak{p}}(L)$ for every $L \in \mathcal{K}$, and
(ii) $D(E) \subseteq \mathcal{O}_E$ for every finite extension $E/K_{\mathfrak{p}}$ of relative type at most τ,

then there exists N such that $\pi^{\tau}_{\mathfrak{p}}(L) \leq N$ for every $L \in \mathcal{K}$.

Proof. Let F be any extension of K. For $\mathfrak{P} \in S^{\tau}_{\mathfrak{p}}(F)$ let $(F', \mathfrak{P}')$ denote a p-adic closure of $(F, \mathfrak{P})$ (see [22, §3]). By the p-adic Lefschetz principle, the assumption (ii) implies that $D(F') \subseteq \mathcal{O}_{\mathfrak{P}'}$, in particular $D(F) \subseteq \mathcal{O}_{\mathfrak{P}'} \cap F = \mathcal{O}_{\mathfrak{P}}$. (In model-theoretic terms, F' is elementarily equivalent, in the language of valued fields, to a finite extension E of $K_{\mathfrak{p}}$ of relative type at most τ. More precisely, if F_0 denotes the algebraic part of F', then both $F_0K_{\mathfrak{p}}$ and F' are elementary extensions of F_0 by [22, Thm. 5.1].) In particular, $D(F) \subseteq \bigcap_{\mathfrak{P}\in S^{\tau}_{\mathfrak{p}}(F)} \mathcal{O}_{\mathfrak{P}} = R^{\tau}_{\mathfrak{p}}(F)$. So since $R^{\tau}_{\mathfrak{p}}(F) = \bigcup_{n=1}^{\infty} R^{\tau}_{\mathfrak{p},n}(F)$, by Proposition 3.9 there exists N such that $D(F) \subseteq \bigcup_{n=1}^{N} R^{\tau}_{\mathfrak{p},n}(F)$ for every F/K. In fact $\left(R^{\tau}_{\mathfrak{p},n}(F)\right)_{n\in\mathbb{N}}$ is an increasing chain, so $D(F) \subseteq R^{\tau}_{\mathfrak{p},N}(F)$. Thus for $L \in \mathcal{K}$, (i) implies that $R^{\tau}_{\mathfrak{p}}(L) = D(L) \subseteq R^{\tau}_{\mathfrak{p},N}(L)$, which shows that $\pi^{\tau}_{\mathfrak{p}}(L) \leq N$. □

Remark 3.11. We also have the following converse: If $\pi^{\tau}_{\mathfrak{p}}(L) \leq N$ for all $L \in \mathcal{K}$, then $D = R^{\tau}_{\mathfrak{p},N}$ is a diophantine family satisfying both conditions. This indicates that while our definition of $\pi^{\tau}_{\mathfrak{p}}$ depends on the construction of the height function on polynomials over $\mathcal{O}_{\mathfrak{p}}$, the property of a class $\mathcal{K}$ to have bounded $(\mathfrak{p}, \tau)$-Pythagoras number is a very robust notion and does not depend on the details of the height function.

Remark 3.12. The notion that a class $\mathcal{K}$ has bounded $(\mathfrak{p}, \tau)$-Pythagoras number is robust in a further sense: under taking a suitable alternative for the Kochen operator. Consider a rational function $\delta \in K(X)$ and suppose that $R^{\tau}_{\mathfrak{p}}(F)$ is the integral closure in F of the ring

$$R'(F) := \left\{ \frac{a}{1 + t_{\mathfrak{p}}b} \;\middle|\; a, b \in \mathcal{O}_{\mathfrak{p}}[\delta(F)],\ 1 + t_{\mathfrak{p}}b \neq 0 \right\},$$

for every extension F/K. We introduce a new 1-dimensional diophantine family R'_n over K, by defining $R'_n(F)$ in terms of δ exactly as $R_{\mathfrak{p},n}(F)$ is defined in terms of $\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}$. Then

$$R^{\tau}_{\mathfrak{p}}(F) = \bigcup_{n=1}^{\infty} R'_n(F),$$

for all F/K. Simply adapting the proof of Proposition 3.10, a class $\mathcal{K}$ of extensions of K has bounded $(\mathfrak{p}, \tau)$-Pythagoras number if and only if there is $M \in \mathbb{N}$ such that $R'_M(L) = R^\tau_\mathfrak{p}(L)$, for all $L \in \mathcal{K}$. Also note that at least in the case $\tau = (1,1)$, the Kochen operator $\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}$ is universal in the sense that every such δ is in fact a rational function in $\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}$, see [22, Cor. 7.12].

4 | THE $(\mathfrak{p}, \tau)$-PYTHAGORAS NUMBER OF NUMBER FIELDS

Introduced by Poonen ([21]), and subsequently used and developed by others including Koenigsmann ([14]) and the second author ([7]), the following diophantine predicates behave well in local fields, and satisfy a strong local-global principle. They are defined from central simple algebras. For further details about central simple algebras, the Brauer group, and associated local-global principles, see [19, Sect. 6.3].

Let A be a central simple algebra of prime degree ℓ over a field F. Following [7, Sect. 2], we let

$$S_A(F) := \left\{ \mathrm{Trd}(x) \;\middle|\; x \in A,\ \mathrm{Nrd}(x) = 1 \right\} \subseteq F,$$

where Trd and Nrd are the reduced norm and reduced trace, see [12, Construction 2.6.1] for details. We also define

$$T_A(F) := \begin{cases} S_A(F) & \text{if } \ell > 2, \\ S_A(F) - S_A(F) & \text{if } \ell = 2. \end{cases}$$

If A is a central simple algebra over F and E/F is any extension, we view $A_E := A \otimes_F E$ as a central simple algebra over E and write $S_A(E) := S_{A_E}(E)$ and $T_A(E) := T_{A_E}(E)$.

Lemma 4.1. *Both S_A and T_A are 1-dimensional diophatine families over F.*

Proof. This is shown in [7, Lem. 2.12] and the subsequent discussion. □

Recall that A is *split* if it is isomorphic to a matrix algebra over F, and A splits over E if A_E is split. The behaviour of S_A and T_A in a completion F of a number field L is determined by whether or not A splits over F, and the behaviour of S_A and T_A in L is controlled by a local-global principle, which leads to the following:

Proposition 4.2 ([7, Prop. 2.9])**.** *Let L be a number field and A a central simple algebra over L of prime degree ℓ which splits over all real completions of L. Then*

$$T_A(L) = \bigcap_{\mathfrak{p}} \mathcal{O}_\mathfrak{p},$$

where the intersection is over the finitely many finite primes $\mathfrak{p}$ of L such that A does not split over $L_\mathfrak{p}$.

Proposition 4.3 (see [7, Prop. 2.6])**.** *Let F be a non-archimedean local field of characteristic zero and let A be a central simple algebra over F of prime degree ℓ. If A is non-split then $T_A(F) = \mathcal{O}_F$.*

Note that [7, Prop. 2.6] is stated for central division algebras of prime degree, but a non-split central simple algebra of prime degree is a division algebra.

Recall that above we fixed a number field K, a finite place $\mathfrak{p}$ of K, and a pair $\tau = (e, f) \in \mathbb{N}^2$. Given this data $(K, \mathfrak{p}, \tau)$, we now describe a choice of algebras A, B over K.

Proposition 4.4. *For every prime number ℓ there exist central simple algebras A, B of degree ℓ over K such that*

1. *neither of them splits over $K_\mathfrak{p}$,*
2. *for every finite place $\mathfrak{q} \neq \mathfrak{p}$ of K, at least one of them splits over $K_\mathfrak{q}$,*
3. *for every infinite place $\mathfrak{q}$ of K, both of them split over $K_\mathfrak{q}$.*

Proof. The Brauer equivalence classes $[A]$ of central simple algebras A over a field F form the Brauer group $\mathrm{Br}(F)$ of F, see [19, (6.3.2) Def.]. For an extension F/K, there is a group homomorphism $\mathrm{Br}(K) \longrightarrow \mathrm{Br}(F)$ given by $[A] \mapsto [A_F]$. Moreover, the local Hasse invariant is an isomorphism

$$\mathrm{inv}_{K_{\mathfrak{q}}} : \mathrm{Br}\big(K_{\mathfrak{q}}\big) \to \begin{cases} \mathbb{Q}/\mathbb{Z} & \text{if } \mathfrak{q} \text{ is finite,} \\ \frac{1}{2}\mathbb{Z}/\mathbb{Z} & \text{if } \mathfrak{q} \text{ is infinite and } K_{\mathfrak{q}} \cong \mathbb{R}, \\ 0 & \text{if } \mathfrak{q} \text{ is infinite and } K_{\mathfrak{q}} \cong \mathbb{C}, \end{cases} \tag{4.1}$$

and so A splits over $K_{\mathfrak{q}}$ if and only if $\mathrm{inv}_{K_{\mathfrak{q}}}([A]) = 0$. There will be no ambiguity if we write $\mathrm{inv}_{K_{\mathfrak{q}}}([A]) = \mathrm{inv}_{K_{\mathfrak{q}}}\big(\big[A_{K_{\mathfrak{q}}}\big]\big)$. Note that each of the local Hasse invariants $\mathrm{inv}_{K_{\mathfrak{q}}}$ takes its values in $\mathbb{Q}/\mathbb{Z}$.

The Albert–Brauer–Hasse–Noether Theorem ([19, (8.1.17) Thm.]) gives the exact sequence

$$0 \to \mathrm{Br}(K) \longrightarrow \bigoplus_{\mathfrak{q}\in\mathbb{S}(K)} \mathrm{Br}\big(K_{\mathfrak{q}}\big) \xrightarrow{\mathrm{inv}_K} \mathbb{Q}/\mathbb{Z} \to 0, \tag{4.2}$$

where $\mathbb{S}(K)$ is the set of (finite and infinite) places of K, and inv_K is the sum of the local invariant maps $\mathrm{inv}_{K_{\mathfrak{q}}}$.

Fix two distinct finite places $\mathfrak{q}_1, \mathfrak{q}_2 \neq \mathfrak{p}$ of K. We define two sequences $\big(a_{\mathfrak{q}}\big)_{\mathfrak{q}\in\mathbb{S}(K)}$ and $\big(b_{\mathfrak{q}}\big)_{\mathfrak{q}\in\mathbb{S}(K)}$ of rational numbers, indexed by the places of K, by

- $a_{\mathfrak{p}} = b_{\mathfrak{p}} = \ell^{-1}$,
- $a_{\mathfrak{q}_1} = (\ell - 1)\ell^{-1}$ and $b_{\mathfrak{q}_1} = 0$,
- $a_{\mathfrak{q}_2} = 0$ and $b_{\mathfrak{q}_2} = (\ell - 1)\ell^{-1}$,
- $a_{\mathfrak{q}} = b_{\mathfrak{q}} = 0$, for every other place $\mathfrak{q}$.

Note that only finitely many of the elements of these sequences are nonzero. Thus, by applying the inverses of the local Hasse invariants from (a), the sequences $\big(a_{\mathfrak{q}}\big)_{\mathfrak{q}}$ and $\big(b_{\mathfrak{q}}\big)_{\mathfrak{q}}$ correspond to elements of the direct sum $\bigoplus_{\mathfrak{q}} \mathrm{Br}\big(K_{\mathfrak{q}}\big)$. We also note the sums

$$\sum_{\mathfrak{q}\in\mathbb{S}(K)} a_{\mathfrak{q}} = \sum_{\mathfrak{q}\in\mathbb{S}(K)} b_{\mathfrak{q}} = 0 \quad \text{in } \mathbb{Q}/\mathbb{Z}.$$

By the exactness of the short exact sequence (4.2), we get (unique) equivalence classes $[A]$ and $[B]$ in $\mathrm{Br}(K)$ such that $\mathrm{inv}_{K_{\mathfrak{q}}}([A]) = a_{\mathfrak{q}} + \mathbb{Z}$ and $\mathrm{inv}_{K_{\mathfrak{q}}}([B]) = b_{\mathfrak{q}} + \mathbb{Z}$, for all $\mathfrak{q} \in \mathbb{S}(K)$. Thus both $[A]$ and $[B]$ are of period ℓ. As K is a number field, this implies that they are also of index ℓ ([23, 32.19]), which means that if A and B denote the unique division algebras in $[A]$ respectively $[B]$, then these are of degree ℓ. □

Proposition 4.5. *Let ℓ be a prime number with $\ell > ef$. If A and B are algebras as in Proposition 4.4, then*

(i) for all finite extensions $E/K_{\mathfrak{p}}$ of relative type at most τ,

$$T_A(E) + T_B(E) = \mathcal{O}_E;$$

(ii) and for all number fields L/K,

$$T_A(L) + T_B(L) \supseteq \bigcap_{\mathfrak{P}\in S_{\mathfrak{p}}^*(L)} \mathcal{O}_{\mathfrak{P}}.$$

Proof. First, suppose that $E/K_{\mathfrak{p}}$ is a finite extension of relative type at most τ. Thus $\big[E : K_{\mathfrak{p}}\big] \leq ef < \ell$, so since A and B do not split over $K_{\mathfrak{p}}$, they also do not split over E by [12, Cor. 4.5.9]. Therefore we may apply Proposition 4.3 to obtain

$$T_A(E) + T_B(E) = \mathcal{O}_E + \mathcal{O}_E = \mathcal{O}_E.$$

Next, let L/K be any number field and let $\mathfrak{Q}$ be a prime of L which lies over a prime $\mathfrak{q}$ of K. If $\mathfrak{q} \neq \mathfrak{p}$, then at least one of A and B splits over $K_{\mathfrak{q}}$ and therefore also over the completion $L_{\mathfrak{Q}}$ by construction. Hence

$$T_A(L) + T_B(L) = \bigcap_{\substack{\mathfrak{Q}\in S(L) \\ A_{L_{\mathfrak{Q}}} \text{ not split}}} \mathcal{O}_{\mathfrak{Q}} + \bigcap_{\substack{\mathfrak{Q}\in S(L) \\ B_{L_{\mathfrak{Q}}} \text{ not split}}} \mathcal{O}_{\mathfrak{Q}} = \bigcap_{\substack{\mathfrak{Q}\in S(L) \\ A_{L_{\mathfrak{Q}}} \text{ and } B_{L_{\mathfrak{Q}}} \text{ not split}}} \mathcal{O}_{\mathfrak{Q}} \supseteq \bigcap_{\mathfrak{P}\in S_{\mathfrak{p}}^*(L)} \mathcal{O}_{\mathfrak{P}},$$

where the first equality is Proposition 4.2 and the second equality follows from weak approximation (see e.g. [9, 1.1.3]). □

As before, fix a uniformizer $t_{\mathfrak{p}} \in K$ of $\mathfrak{p}$. For central simple algebras A, B over K and an extension F/K we define $D^{\tau}_{\mathfrak{p},t_{\mathfrak{p}},A,B}(F)$ as

$$\left\{ \frac{x}{1+t_{\mathfrak{p}}w^{e+1}y} \;\middle|\; x, y \in T_A(F)+T_B(F), w \in \gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(F),\ 1+t_{\mathfrak{p}}w^{e+1}y \neq 0 \right\}.$$

Lemma 4.6. *$D^{\tau}_{\mathfrak{p},t_{\mathfrak{p}},A,B}$ is a 1-dimensional diophantine family over K.*

Proof. We have seen in Lemma 4.1 that T_A and T_B are 1-dimensional diophantine families over K. The claim follows by applying Lemma 3.5 to the 5-dimensional diophantine family $T_A \times T_B \times T_A \times T_B \times \gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}$ over K (Lemma 3.4) and the rational function $(X_1+X_2)\left(1+t_{\mathfrak{p}}X_5^{e+1}(X_3+X_4)\right)^{-1}$. □

Proposition 4.7. *If A, B are K-algebras as in Proposition 4.4, then*

$$D^{\tau}_{\mathfrak{p},t_{\mathfrak{p}},A,B}(E) \subseteq \mathcal{O}_E$$

for every finite extension $E/K_{\mathfrak{p}}$ of relative type at most τ.

Proof. By Proposition 4.5(i), we have $T_A(E)+T_B(E) = \mathcal{O}_E$. Since also $\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(E) \subseteq \mathcal{O}_E$ and $1+t_{\mathfrak{p}}\mathcal{O}_E \subseteq \mathcal{O}_E^{\times}$, we have $D^{\tau}_{\mathfrak{p},t_{\mathfrak{p}},A,B}(E) \subseteq \mathcal{O}_E$, as required. □

Proposition 4.8. *If A, B are K-algebras as in Proposition 4.4, then*

$$D^{\tau}_{\mathfrak{p},t_{\mathfrak{p}},A,B}(L) = R^{\tau}_{\mathfrak{p}}(L)$$

for every number field L containing K.

Proof. By Proposition 4.7, $D^{\tau}_{\mathfrak{p},t_{\mathfrak{p}},A,B}(L_{\mathfrak{P}}) \subseteq \mathcal{O}_{L_{\mathfrak{P}}}$ for every $\mathfrak{P} \in \mathcal{S}^{\tau}_{\mathfrak{p}}(L)$, hence

$$D^{\tau}_{\mathfrak{p},t_{\mathfrak{p}},A,B}(L) \subseteq \bigcap_{\mathfrak{P}\in\mathcal{S}^{\tau}_{\mathfrak{p}}(L)} \mathcal{O}_{L_{\mathfrak{P}}} \cap L = \bigcap_{\mathfrak{P}\in\mathcal{S}^{\tau}_{\mathfrak{p}}(L)} \mathcal{O}_{\mathfrak{P}} = R^{\tau}_{\mathfrak{p}}(L).$$

To show the other inclusion, let $r \in R^{\tau}_{\mathfrak{p}}(L)$. Since L/K is finite, the set $\mathcal{S}^{*}_{\mathfrak{p}}(L)$ of primes of L over $\mathfrak{p}$ is finite. Write $\mathfrak{P}_1, \dots, \mathfrak{P}_k \in \mathcal{S}^{\tau}_{\mathfrak{p}}(L)$ for the primes over $\mathfrak{p}$ of relative type $\leq \tau$, and $\mathfrak{Q}_1, \dots, \mathfrak{Q}_l$ for the primes over $\mathfrak{p}$ not of relative type $\leq \tau$. For each $i \in \{1, \dots, l\}$, by Lemma 2.12 there exists z_i such that

$$v_{\mathfrak{Q}_i}\left(\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(z_i)\right) \leq -\frac{1}{e+1} v_{\mathfrak{Q}_i}(t_{\mathfrak{p}}),$$

i.e. $v_{\mathfrak{Q}_i}\left(\left(t_{\mathfrak{p}}\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(z_i)^{e+1}\right)^{-1}\right) \geq 0$. By weak approximation and continuity of rational functions, there exists $z \in L$ such that $v_{\mathfrak{Q}_i}\left(\left(t_{\mathfrak{p}}\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(z)^{e+1}\right)^{-1}\right) \geq 0$ for each $i \in \{1, \dots, l\}$. By another application of weak approximation there exists $y \in L$ such that

$$v_{\mathfrak{Q}_i}\left(\left(t_{\mathfrak{p}}\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(z)^{e+1}\right)^{-1} + y\right) \geq \max\left\{0, -v_{\mathfrak{Q}_i}\left(rt_{\mathfrak{p}}\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(z)^{e+1}\right)\right\}, \quad i = 1, \dots, l,$$

$$v_{\mathfrak{P}_i}(y) \geq 0, \quad i = 1, \dots, k.$$

In particular, $y \in \bigcap_{\mathfrak{P}\in\mathcal{S}^{*}_{\mathfrak{p}}(L)} \mathcal{O}_{\mathfrak{P}}$ and $x := r\left(1+t_{\mathfrak{p}}\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(z)^{e+1}y\right)$ satisfies $v_{\mathfrak{Q}_i}(x) \geq 0$ for each $i \in \{1, \dots, l\}$. As $\mathfrak{P}_i \in \mathcal{S}^{\tau}_{\mathfrak{p}}(L)$, we have $r, t_{\mathfrak{p}}, \gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(z), y \in \mathcal{O}_{\mathfrak{P}_i}$, hence $v_{\mathfrak{P}_i}(x) \geq 0$ for all $i \in \{1, \dots, k\}$. Thus $x \in \bigcap_{\mathfrak{P}\in\mathcal{S}^{*}_{\mathfrak{p}}(L)} \mathcal{O}_{\mathfrak{P}}$. As

$$\bigcap_{\mathfrak{P}\in\mathcal{S}^{*}_{\mathfrak{p}}(L)} \mathcal{O}_{\mathfrak{P}} \subseteq T_A(L)+T_B(L)$$

by Proposition 4.5(ii), we get that

$$r = x\left(1 + t_{\mathfrak{p}}\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(z)^{e+1}y\right)^{-1} \in D^{\tau}_{\mathfrak{p},t_{\mathfrak{p}},A,B}(L),$$

as required. □

Theorem 4.9. *For every finite place $\mathfrak{p}$ of a number field K and every $\tau \in \mathbb{N}^2$, there exists $N \in \mathbb{N}$ such that $\pi^{\tau}_{\mathfrak{p}}(L) \leq N$ for every number field L containing K.*

Proof. We choose algebras A and B over K according to Proposition 4.4, and we apply Proposition 3.10 to the class $\mathcal{K}$ of finite extensions L/K and the diophantine family $D = D^{\tau}_{\mathfrak{p},t_{\mathfrak{p}},A,B}$, where the two assumptions of Proposition 3.10 are verified in Proposition 4.8 and Proposition 4.7, respectively. □

Remark 4.10. Given an arbitrary field $F \supseteq K$ there is no obvious relation between $\pi^{\tau}_{\mathfrak{p}}(F)$ and $\pi^{\tau'}_{\mathfrak{p}}(F)$ for $\tau \neq \tau'$. For example if $\tau \leq \tau'$ then we have $R^{\tau}_{\mathfrak{p}}(F) \supseteq R^{\tau'}_{\mathfrak{p}}(F)$, but also $\gamma^{\tau}_{\mathfrak{p}} \neq \gamma^{\tau'}_{\mathfrak{p}}$. Likewise, there is no reason to suspect that the bounds N in Theorem 4.9 should be related for different choices of τ.

5 | THE $(\mathfrak{p}, \tau)$-PYTHAGORAS NUMBER IN FINITE EXTENSIONS

The growth of the classical Pythagoras number is bounded in finite extensions E/F by

$$\pi(E) \leq [E : F] \cdot \pi(F),$$

see [20, Ch. 7, Prop. 1.13]. We now combine ideas from the proof of Theorem 4.9 with techniques for p-valuations on general fields to prove an (inexplicit) analogue of this for the $(\mathfrak{p}, \tau)$-Pythagoras number.

As before fix K, $\mathfrak{p}$ and $\tau = (e, f)$ and let F/K be an extension. We equip $\mathcal{S}^{\tau}_{\mathfrak{p}}(F)$ with the *constructible topology*, which by definition has a basis consisting of the sets

$$\mathcal{S}^{\tau}_{\mathfrak{p}}(F; a) := \left\{\mathfrak{P} \in \mathcal{S}^{\tau}_{\mathfrak{p}}(F) \;\middle|\; v_{\mathfrak{P}}(a) \geq 0\right\}, \quad a \in F,$$

and their complements. In [1], we studied approximation theorems for spaces of localities, i.e. valuations, orderings, and absolute values, on a given field. We now deduce an approximation theorem in the setting of the space $\mathcal{S}^{\tau}_{\mathfrak{p}}(F)$.

Theorem 5.1. *Let $S_1, \dots, S_n \subseteq \mathcal{S}^{\tau}_{\mathfrak{p}}(F)$ be disjoint and closed, let $x_1, \dots, x_n \in F$, and let $z_1, \dots, z_n \in F^{\times}$. Assume that, for any $\mathfrak{P}_i \in S_i$ and $\mathfrak{P}_j \in S_j$, if the valuation w is the finest common coarsening of $v_{\mathfrak{P}_i}$ and $v_{\mathfrak{P}_j}$, then $w(x_i - x_j) \geq w(z_i) = w(z_j)$. Then there exists $x \in F$ with*

$$v_{\mathfrak{Q}}(x - x_i) > v_{\mathfrak{Q}}(z_i) \text{ for all } \mathfrak{Q} \in S_i, \text{ for } i = 1, \dots, n.$$

Proof. Corollary 5.5 of [1] is a similar statement in which $\mathcal{S}^{\tau}_{\mathfrak{p}}(F)$ is replaced by a space $\mathrm{S}^{e}_{\pi}(F)$, for $\pi \in F^{\times}$ and $e \in \mathbb{N}$, By definition (see [1, Example 2.4]), $\mathrm{S}^{e}_{\pi}(F)$ is the space of equivalence classes of valuations v on F with value group Γ_v, which has $\mathbb{Z}$ as a convex subgroup and $0 < v(\pi) \leq e$. We note that $\mathcal{S}^{\tau}_{\mathfrak{p}}(F) \subseteq \mathrm{S}^{e}_{t_{\mathfrak{p}}}(F)$, and if we equip $\mathrm{S}^{e}_{t_{\mathfrak{p}}}(F)$ with its own constructible topology (see [1, Sect. 2]) then $\mathcal{S}^{\tau}_{\mathfrak{p}}(F)$ is a closed subspace: By [22, Lem. 6.2], $\mathcal{S}^{\tau}_{\mathfrak{p}}(F)$ is the intersection over all sets $\left\{v \in \mathrm{S}^{e}_{t_{\mathfrak{p}}}(F) : v(a) \geq 0\right\}$ for $a \in \mathcal{O}_{\mathfrak{p}} \cup \gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(F)$. Therefore, each S_i is also a closed subset of $\mathrm{S}^{e}_{t_{\mathfrak{p}}}(F)$ and so we may obtain the required element $x \in F$ by an application of [1, Cor. 5.5]. □

Lemma 5.2. *Let $\tau \leq \tau' \in \mathbb{N}^2$. There is a rational function $\omega_{\tau,\tau'} \in \mathbb{Q}(t_{\mathfrak{p}})(X)$ such that $v_{\mathfrak{P}}(\omega_{\tau,\tau'}(x)) > 0$ for all $x \in F$ and $\mathfrak{P} \in \mathcal{S}^{\tau'}_{\mathfrak{p}}(F)$, and moreover $v_{\mathfrak{P}}\left(\omega_{\tau,\tau'}(x)\right) = 1$ if $v_{\mathfrak{P}}(x) = 1$ and $\mathfrak{P}$ is of exact relative type τ over $\mathfrak{p}$.*

Proof. Write $\tau' = (e', f')$. By Dirichlet's theorem on primes in arithmetic progressions there exists $k \in \mathbb{N}$ such that $\ell := 1 + ke$ is a prime number and $\ell > e'$. Let $\beta(X) = t_{\mathfrak{p}}^{-k}X^{\ell}$. For every $\mathfrak{P} \in \mathcal{S}^{\tau'}_{\mathfrak{p}}(F)$ and $x \in F$ we have $v_{\mathfrak{P}}(\beta(x)) = \ell v_{\mathfrak{P}}(x) - kv_{\mathfrak{P}}(t_{\mathfrak{p}})$, which is non-zero (since $\ell > k$ and $\ell > e' \geq v_{\mathfrak{P}}(t_{\mathfrak{p}})$ imply $\ell \nmid kv_{\mathfrak{P}}(t_{\mathfrak{p}})$), and equals 1 if $v_{\mathfrak{P}}(x) = 1$ and $v_{\mathfrak{P}}(t_{\mathfrak{p}}) = e$. Thus $\omega_{\tau,\tau'}(X) = \left(\beta(X) + \beta(X)^{-1}\right)^{-1}$ satisfies the claim. □

Lemma 5.3. *There is a rational function $\rho_\tau \in \mathbb{Q}(X)$ such that for all $\mathfrak{P} \in S^\tau_\mathfrak{p}(F)$ and all $x \in F$ we have*

$$v_\mathfrak{P}(\rho_\tau(x)) \begin{cases} = 0, & \text{if } v_\mathfrak{P}(x) = 0, \\ > 0, & \text{if } v_\mathfrak{P}(x) \neq 0, \end{cases}$$

and if $v_\mathfrak{P}(x) = 0$ then $\mathrm{res}_\mathfrak{P}(\rho_\tau(x)) = \mathrm{res}_\mathfrak{P}(x)$.

Proof. Write $\rho_\tau(X) = X\left(X^{q^f} - X + 1\right)^{-1}$. Let $\mathfrak{P} \in S^\tau_\mathfrak{p}(F)$ and let $x \in F$. If $v_\mathfrak{P}(x) < 0$ then $v_\mathfrak{P}\left(x^{q^f} - x + 1\right) = q^f v_\mathfrak{P}(x) < 0$, and so $v_\mathfrak{P}(\rho_\tau(x)) = \left(1 - q^f\right) v_\mathfrak{P}(x) > 0$. On the other hand, if $v_\mathfrak{P}(x) > 0$ then $v_\mathfrak{P}\left(x^{q^f} - x + 1\right) = 0$, so $v_\mathfrak{P}(\rho_\tau(x)) = v_\mathfrak{P}(x) > 0$. Finally, if $v_\mathfrak{P}(x) = 0$ then

$$\mathrm{res}_\mathfrak{P}\left(x^{q^f} - x + 1\right) = \mathrm{res}_\mathfrak{P}(x)^{q^f} - \mathrm{res}_\mathfrak{P}(x) + 1 = 1 \neq 0,$$

and in particular $v_\mathfrak{P}\left(x^{q^f} - x + 1\right) = 0$. Therefore $v_\mathfrak{P}(\rho_\tau(x)) = 0$ and $\mathrm{res}_\mathfrak{P}(\rho_\tau(x)) = \mathrm{res}_\mathfrak{P}(x)$. □

Proposition 5.4. *Let $\tau \leq \tau' = (e', f')$ and let S_0 denote an open-closed subset of $S^{\tau'}_\mathfrak{p}(F)$ such that $S^\tau_\mathfrak{p}(F) \subseteq S_0$. There exists $y \in F$ such that*

$$v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(y)\right) \begin{cases} \in \left[0, e'eq^f\right], & \text{if } \mathfrak{P} \in S_0, \\ < 0, & \text{if } \mathfrak{P} \in S^{\tau'}_\mathfrak{p}(F) \setminus S_0. \end{cases}$$

Proof. For each $\mathfrak{P} \in S^{\tau'}_\mathfrak{p}(F) \setminus S_0$, we choose $y_\mathfrak{P} \in F$ as follows. First, if the relative type of $\mathfrak{P}$ is exactly $\tau'' = (e'', f'')$ with $e'' > e$, then let $t_\mathfrak{P}$ be a uniformizer of $v_\mathfrak{P}$ and set $y_\mathfrak{P} = \omega_{\tau'',\tau'}\left(t_\mathfrak{P}\right)$. By Lemma 5.2, $v_\mathfrak{P}(y_\mathfrak{P}) = 1$; and by Lemma 2.12, $v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}\left(y_\mathfrak{P}\right)\right) < 0$. Also, for all $\mathfrak{Q} \in S^{\tau'}_\mathfrak{p}(F)$ we have $v_\mathfrak{Q}\left(y_\mathfrak{P}\right) > 0$. In particular, $y_\mathfrak{P} \in R^{\tau'}_\mathfrak{p}(F)$.

On the other hand, if the relative type of $\mathfrak{P}$ is exactly $\tau'' = (e'', f'')$ with $f'' \nmid f$, then let $a_\mathfrak{P}$ with $v_\mathfrak{P}\left(a_\mathfrak{P}\right) = 0$ and $\mathrm{res}_\mathfrak{P}\left(a_\mathfrak{P}\right)$ a generator of $Fv_\mathfrak{P}$, and set $y_\mathfrak{P} = \rho_{\tau'}\left(a_\mathfrak{P}\right)$. By Lemma 5.3, $v_\mathfrak{P}\left(y_\mathfrak{P}\right) = 0$ and $\mathrm{res}_\mathfrak{P}\left(y_\mathfrak{P}\right)$ is a generator of $Fv_\mathfrak{P}$. By Lemma 2.12, we have $v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}\left(y_\mathfrak{P}\right)\right) < 0$. Also, for all $\mathfrak{Q} \in S^{\tau'}_\mathfrak{p}(F)$ we have $v_\mathfrak{Q}\left(y_\mathfrak{P}\right) \geq 0$, i.e. $y_\mathfrak{P} \in R^{\tau'}_\mathfrak{p}(F)$.

In either case, we have chosen $y_\mathfrak{P} \in R^{\tau'}_\mathfrak{p}(F)$ such that $v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}\left(y_\mathfrak{P}\right)\right) < 0$. Next we make use of the compactness of $S^{\tau'}_\mathfrak{p}(F)$. For $y \in F$, we let

$$S_y = \left\{\mathfrak{P} \in S^{\tau'}_\mathfrak{p}(F) \,\middle|\, v_\mathfrak{P}\left(\gamma^\tau_{\mathfrak{p},t_\mathfrak{p}}(y)\right) < 0\right\}.$$

Each S_y is an open-closed subset of $S^{\tau'}_\mathfrak{p}(F)$. By our choice of the elements $y_\mathfrak{P}$, the family

$$\left\{S_{y_\mathfrak{P}} \setminus S_0 \;:\; \mathfrak{P} \in S^{\tau'}_\mathfrak{p}(F) \setminus S_0\right\}$$

is an open covering of $S^{\tau'}_\mathfrak{p}(F) \setminus S_0$. So by compactness there exist $\mathfrak{P}_1, \dots, \mathfrak{P}_n \in S^{\tau'}_\mathfrak{p}(F) \setminus S_0$ such that with $S'_i := S_{y_{\mathfrak{P}_i}}$, we have

$$S^{\tau'}_\mathfrak{p}(F) = S_0 \cup S'_1 \cup \dots \cup S'_n.$$

Choose open-closed sets $S_1 \subseteq S'_1, \dots, S_n \subseteq S'_n$ such that

$$S^{\tau'}_\mathfrak{p}(F) = S_0 \sqcup S_1 \sqcup \dots \sqcup S_n$$

is a partition. We seek to apply Theorem 5.1 to the sets $S_0, S_1, \dots, S_n$, the elements $x_0 = t_\mathfrak{p}^{-1}$, $x_1 = y_{\mathfrak{P}_1}, \dots, x_n = y_{\mathfrak{P}_n}$ and $z_0 = t_\mathfrak{p}, \dots, z_n = t_\mathfrak{p}$. To verify that the hypothesis of the theorem holds, we argue as follows: let w be any valuation on F that is a common coarsening of valuations $v_\mathfrak{P}$ and $v_\mathfrak{Q}$ corresponding to primes $\mathfrak{P} \in S_i$ and $\mathfrak{Q} \in S_j$, for $i \neq j$. Note that w is a proper coarsening of these valuations since S_i and S_j are disjoint and $v_\mathfrak{P}$, $v_\mathfrak{Q}$ are incomparable. Then $w(z_i) = w\left(z_j\right) = 0$ and $w\left(x_i - x_j\right) \geq 0$. Therefore, by Theorem 5.1, there exists $y \in F$ such that

$$v_\mathfrak{P}(y - x_i) > v_\mathfrak{P}\left(t_\mathfrak{p}\right),$$

for each $\mathfrak{P} \in S_i$ and each i. In particular, for $\mathfrak{P} \in S_0$ we have that $v_{\mathfrak{P}}(y) = -v_{\mathfrak{P}}(t_{\mathfrak{p}}) < 0$, hence

$$v_{\mathfrak{P}}\left(\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(y)\right) = eq^f v_{\mathfrak{P}}(t_{\mathfrak{p}}) - v_{\mathfrak{P}}(t_{\mathfrak{p}}) = \left(eq^f - 1\right)v_{\mathfrak{P}}(t_{\mathfrak{p}}) \in \{0, \dots, e'eq^f\},$$

cf. Lemma 2.11. On the other hand, for $\mathfrak{Q} \in S_i$, with $i > 0$, we get that $v_{\mathfrak{Q}}(y - y_{\mathfrak{P}_i}) > v_{\mathfrak{Q}}(t_{\mathfrak{p}})$. Since we have $v_{\mathfrak{Q}}\left(\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(y_{\mathfrak{P}_i})\right) < 0$, then $v_{\mathfrak{Q}}\left(\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(y)\right) < 0$ by Lemma 2.13. □

Fix $n, m \in \mathbb{N}$ and let $\tau' = (e', f')$, where $e' = me$ and $f' = m!f$. Let $\mathcal{E}$ be the class of fields E which contain some F/K with $[E : F] = m$ and $\pi^{\tau}_{\mathfrak{p}}(F) = n$. We adapt the arguments of Section 4 in order to show that $\pi^{\tau}_{\mathfrak{p}}(E)$ is bounded by a function of m, n. We let

$$D^{\tau,(1)}_{\mathfrak{p},m,n}(F) := \left\{x \in F \mid \exists a_0, \dots, a_{m-1} \in R^{\tau}_{\mathfrak{p},n}(F) \ : \ x^m + a_{m-1}x^{m-1} + \dots + a_0 = 0\right\},$$

and

$$D^{\tau,(2)}_{\mathfrak{p},m,n}(F) := \left\{ \frac{a}{1 + t_{\mathfrak{p}}\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(y)^{e'}b} \;\middle|\; a, b \in D^{\tau,(1)}_{\mathfrak{p},m,n}(F),\ y \in F,\ \gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(y) \neq \infty,\ 1 + t_{\mathfrak{p}}\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(y)^{e'}b \neq 0 \right\}.$$

Lemma 5.5. *Both $D^{\tau,(1)}_{\mathfrak{p},m,n}$ and $D^{\tau,(2)}_{\mathfrak{p},m,n}$ are 1-dimensional diophantine families over K.*

Proof. This is very similar to Lemma 4.6. This time we use the fact that $R^{\tau}_{\mathfrak{p},n}$ is a 1-dimensional diophantine family over K, as seen in Example 3.8. From this is immediately follows that $D^{\tau,(1)}_{\mathfrak{p},m,n}$ is a 1-dimensional diophantine family over K. To see that $D^{\tau,(2)}_{\mathfrak{p},m,n}$ is a 1-dimensional diophantine family over K we now apply Lemma 3.5 to the 3-dimensional diophantine family $D^{\tau,(1)}_{\mathfrak{p},m,n} \times D^{\tau,(1)}_{\mathfrak{p},m,n} \times \gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}$ and the rational function $X_1\left(1 + t_{\mathfrak{p}}X_3^{e'}X_2\right)^{-1}$. □

Proposition 5.6. *For every $E \supseteq K$ we have $D^{\tau,(2)}_{\mathfrak{p},m,n}(E) \subseteq R^{\tau}_{\mathfrak{p}}(E)$.*

Proof. Since $R^{\tau}_{\mathfrak{p}}(E)$ is integrally closed in E and $R^{\tau}_{\mathfrak{p},n}(E) \subseteq R^{\tau}_{\mathfrak{p}}(E)$, we have $D^{\tau,(1)}_{\mathfrak{p},m,n}(E) \subseteq R^{\tau}_{\mathfrak{p}}(E)$. Let $\mathfrak{P} \in S^{\tau}_{\mathfrak{p}}(E)$. Then $v_{\mathfrak{P}}(t_{\mathfrak{p}}) > 0$. Furthermore, for $y \in E$ and $b \in R^{\tau}_{\mathfrak{p}}(E)$, we have $v_{\mathfrak{P}}\left(\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(y)^{e'}b\right) \geq 0$, hence $v_{\mathfrak{P}}\left(1 + t_{\mathfrak{p}}\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(y)^{e'}b\right) = 0$. Therefore elements of the form $a\left(1 + t_{\mathfrak{p}}\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(y)^{e'}b\right)^{-1}$ are contained in $R^{\tau}_{\mathfrak{p}}(E)$, where $a, b \in D^{\tau,(1)}_{\mathfrak{p},m,n}(E)$ and $y \in E$. This establishes $D^{\tau,(2)}_{\mathfrak{p},m,n}(E) \subseteq R^{\tau}_{\mathfrak{p}}(E)$. □

Lemma 5.7. *For every $E \in \mathcal{E}$ we have $R^{\tau'}_{\mathfrak{p}}(E) \subseteq D^{\tau,(1)}_{\mathfrak{p},m,n}(E)$.*

Proof. Choose F such that $[E : F] = m$ and $\pi^{\tau}_{\mathfrak{p}}(F) = n$, although the choice of F will not matter. Let S be the set of primes of E (of arbitrary type) lying over elements of $S^{\tau}_{\mathfrak{p}}(F)$. By our choice of τ', we have $S \subseteq S^{\tau'}_{\mathfrak{p}}(E)$. If we denote by A the integral closure of $R^{\tau}_{\mathfrak{p}}(F)$ in E, then A is the holomorphy ring corresponding to S and we have

$$R^{\tau'}_{\mathfrak{p}}(E) \subseteq A \subseteq R^{\tau}_{\mathfrak{p}}(E).$$

Since $\pi^{\tau}_{\mathfrak{p}}(F) = n$, we have $R^{\tau}_{\mathfrak{p}}(F) = R^{\tau}_{\mathfrak{p},n}(F)$; and trivially $R^{\tau}_{\mathfrak{p},n}(F) \subseteq R^{\tau}_{\mathfrak{p},n}(E)$. As the degree of the extension E/F is m, $D^{\tau,(1)}_{\mathfrak{p},m,n}(E)$ contains the integral closure of $R^{\tau}_{\mathfrak{p}}(F)$ in E, which is A. In particular $R^{\tau'}_{\mathfrak{p}}(E) \subseteq D^{\tau,(1)}_{\mathfrak{p},m,n}(E)$. □

Proposition 5.8. *For every $E \in \mathcal{E}$ we have $D^{\tau,(2)}_{\mathfrak{p},m,n}(E) = R^{\tau}_{\mathfrak{p}}(E)$.*

Proof. In view of Proposition 5.6, it only remains to show that $R^{\tau}_{\mathfrak{p}}(E) \subseteq D^{\tau,(2)}_{\mathfrak{p},m,n}(E)$. Let $x \in R^{\tau}_{\mathfrak{p}}(E)$. In fact, we aim to find $b \in R^{\tau'}_{\mathfrak{p}}(E)$ and $y \in E$ with

$$x\left(1 + t_{\mathfrak{p}}\gamma^{\tau}_{\mathfrak{p},t_{\mathfrak{p}}}(y)^{e'}b\right) \in R^{\tau'}_{\mathfrak{p}}(E),$$

which we will do by applying Theorem 5.1. As $R_{\mathfrak{p}}^{\tau'}(E) \subseteq D_{\mathfrak{p},m,n}^{\tau,(1)}$ by Lemma 5.7, this will show that $x \in D_{\mathfrak{p},m,n}^{\tau,(2)}(E)$. We define the sets

$$S_0 := \{\mathfrak{P} \in S_{\mathfrak{p}}^{\tau'}(E) \mid v_{\mathfrak{P}}(x) \geq 0\}$$

and

$$S_1 := S_{\mathfrak{p}}^{\tau'}(E) \setminus S_0.$$

Note that S_0 and S_1 are open-closed in $S_{\mathfrak{p}}^{\tau'}(E)$ and $S_1 \cap S_{\mathfrak{p}}^{\tau}(E) = \emptyset$. We find a suitable element $y \in E$ by a direct application of Proposition 5.4: we obtain $y \in E$ such that

$$v_{\mathfrak{P}}\left(\gamma_{\mathfrak{p},t_{\mathfrak{p}}}^{\tau}(y)\right) \begin{cases} \in \left[0, e'eq^f\right], & \text{if } \mathfrak{P} \in S_0, \\ < 0, & \text{if } \mathfrak{P} \in S_1. \end{cases}$$

We obtain a suitable $b \in E$ by solving a more straightforward approximation problem: By Theorem 5.1, there exists $b \in R_{\mathfrak{p}}^{\tau'}(E)$ such that

$$v_{\mathfrak{P}}(b) \geq 0, \qquad \text{if } \mathfrak{P} \in S_0,$$

$$\text{and} \qquad v_{\mathfrak{P}}\left(b + t_{\mathfrak{p}}^{-1}\gamma_{\mathfrak{p},t_{\mathfrak{p}}}^{\tau}(y)^{-e'}\right) \geq v_{\mathfrak{P}}\left(x^{-1}t_{\mathfrak{p}}^{-1}\gamma_{\mathfrak{p},t_{\mathfrak{p}}}^{\tau}(y)^{-e'}\right), \qquad \text{if } \mathfrak{P} \in S_1.$$

Indeed, if a valuation w on E coarsens $v_{\mathfrak{P}}$ and $v_{\mathfrak{Q}}$ for $\mathfrak{P} \in S_0$ and $\mathfrak{Q} \in S_1$, $v_{\mathfrak{P}}(x) \geq 0$ and $v_{\mathfrak{Q}}(x) < 0$ imply that $w(x) = 0$, and $v_{\mathfrak{P}}\left(\gamma_{\mathfrak{p},t_{\mathfrak{p}}}^{\tau}(y)\right) \in \left[0, e'eq^f\right]$ implies that $w\left(\gamma_{\mathfrak{p},t_{\mathfrak{p}}}^{\tau}(y)\right) = 0$. Therefore also $w\left(t_{\mathfrak{p}}\gamma_{\mathfrak{p},t_{\mathfrak{p}}}^{\tau}(y)^{e'}\right) = 0$ and $w\left(xt_{\mathfrak{p}}\gamma_{\mathfrak{p},t_{\mathfrak{p}}}^{\tau}(y)^{e'}\right) = 0$. In particular, the hypothesis of the theorem is satisfied, and the $b \in E$ so obtained lies in $R_{\mathfrak{p}}^{\tau'}(E)$.

For $\mathfrak{P} \in S_0$, we have $v_{\mathfrak{P}}\left(t_{\mathfrak{p}}^{-1}\gamma_{\mathfrak{p},t_{\mathfrak{p}}}^{\tau}(y)^{-e'}\right) < 0$, hence

$$v_{\mathfrak{P}}\left(b + t_{\mathfrak{p}}^{-1}\gamma_{\mathfrak{p},t_{\mathfrak{p}}}^{\tau}(y)^{-e'}\right) \begin{cases} = v_{\mathfrak{P}}\left(t_{\mathfrak{p}}^{-1}\gamma_{\mathfrak{p},t_{\mathfrak{p}}}^{\tau}(y)^{-e'}\right), & \text{if } \mathfrak{P} \in S_0, \\ \geq v_{\mathfrak{P}}\left(x^{-1}t_{\mathfrak{p}}^{-1}\gamma_{\mathfrak{p},t_{\mathfrak{p}}}^{\tau}(y)^{-e'}\right), & \text{if } \mathfrak{P} \in S_1, \end{cases}$$

i.e.

$$v_{\mathfrak{P}}\left(1 + t_{\mathfrak{p}}\gamma_{\mathfrak{p},t_{\mathfrak{p}}}^{\tau}(y)^{e'}b\right) = 0, \quad \text{if } \mathfrak{P} \in S_0,$$
$$v_{\mathfrak{P}}\left(x\left(1 + t_{\mathfrak{p}}\gamma_{\mathfrak{p},t_{\mathfrak{p}}}^{\tau}(y)^{e'}b\right)\right) \geq 0, \quad \text{if } \mathfrak{P} \in S_1.$$

Since $v_{\mathfrak{P}}(x) \geq 0$ for $\mathfrak{P} \in S_0$, we obtain that $x\left(1 + t_{\mathfrak{p}}\gamma_{\mathfrak{p},t_{\mathfrak{p}}}^{\tau}(y)^{e'}b\right) \in R_{\mathfrak{p}}^{\tau'}(E)$. □

Theorem 5.9. *There is a function $\alpha_{\mathfrak{p}}^{\tau} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that*

$$\pi_{\mathfrak{p}}^{\tau}(E) \leq \alpha_{\mathfrak{p}}^{\tau}\left(\pi_{\mathfrak{p}}^{\tau}(F), [E : F]\right),$$

for every field extension E/F with $\pi_{\mathfrak{p}}^{\tau}(F) < \infty$.

Proof. Let $m, n \in \mathbb{N}$. We apply Proposition 3.10 to the class $\mathcal{E}$ and the diophantine family $D_{\mathfrak{p},m,n,}^{\tau,(2)}$, where the two assumptions of Proposition 3.10 are verified in Proposition 5.8 and Proposition 5.6, respectively. Thus there exists N such that $\pi_{\mathfrak{p}}^{\tau}(E) \leq N$ for every $E \in \mathcal{E}$, so we can choose $\alpha_{\mathfrak{p}}^{\tau}(n, m) = N$. □

Remark 5.10. Beyond the statement of the theorem, we are unable to say much about the behaviour of the $(\mathfrak{p}, \tau)$-Pythagoras number in finite extensions:

For example, it is known that the classical Pythagoras does not increase in finite extensions of number fields, cf. [20, Ch. 7, Example 1.4 (2) and (3)], but we don't expect this to happen for the $(\mathfrak{p}, \tau)$-Pythagoras number.

In fact, it is known that there are finite extensions of infinite algebraic extensions of $\mathbb{Q}$ in which the classical Pythagoras number increases, see for instance [5, Example on p. 432], and one may expect that similar examples exist for the $(\mathfrak{p}, \tau)$-Pythagoras number. For example, if F is the closure of $\mathbb{Q}$ under adjoining preimages of γ_p, one trivially has $R_p(F) = F = \gamma_p(F)$, hence

$\pi_p(F) = 1$. One can then deduce from a theorem of Weissauer [26, Satz 9.7] that in any proper finite extension E of F one has $R_p(E) \neq \gamma_p(E)$, and one might suspect that in fact $\pi_p(E) > 1$, although this seems not easy to prove.

6 | DIOPHANTINE HOLOMORPHY RINGS OF p-VALUATIONS

By definition, in any field F with finite $(\mathfrak{p}, \tau)$-Pythagoras number the holomorphy ring $R^\tau_\mathfrak{p}(F)$ is a diophantine subset. In this section we generalize this observation, by showing in Corollary 6.5 that the same applies to the holomorphy rings associated to arbitrary open-closed subsets of $\mathcal{S}^\tau_\mathfrak{p}(F)$. Theorem 6.4 is a uniform version of this fact.

As a technical tool, it turns out to be useful to extend some of the ideas from diophantine families over fields to commutative algebras which are finite-dimensional vector spaces over fields. To this end, we introduce a small piece of notation. Write $X = (X_1, \dots, X_n)$ and $Y = (Y_1, \dots, Y_m)$. For $f_1, .., f_r \in K[X, Y]$ and for any commutative (unital, associative) F-algebra B, we write

$$P_{f_1,\dots,f_r}(B) := \left\{x \in B^n \mid \exists y \in B^m : f_1(x, y) = \dots = f_r(x, y) = 0\right\}.$$

The following lemma is straightforward, but we include it for lack of a suitable reference.

Lemma 6.1. *Let $f_1, \dots, f_r \in K[X, Y]$ and let $l \in \mathbb{N}$. Then*

$$F^n \cap P_{f_1^l,\dots,f_r^l}(B) = \bigcap_{\mathfrak{m}\in \mathrm{MaxSpec}(B)} \left(F^n \cap P_{f_1,\dots,f_r}(B/\mathfrak{m})\right),$$

for all extensions F/K, and all commutative F-algebras B of dimension at most l. Here F is identified with its image in B and $B/\mathfrak{m}$.

Proof. Let B be a commutative F-algebra which has dimension at most l as an F-vector space. As B is finite dimensional, it is Artinian, hence the Jacobson radical $\mathfrak{j}$ of B is nilpotent ([3, Prop. 8.4]), and therefore more precisely $\mathfrak{j}^l = 0$. Then for all $s \in \{1, \dots, r\}$, all extensions F/K, all $a \in F$, $x \in F^n$, and $y \in B^m$, we have

$$\begin{aligned} f_s(x, y)^l = 0 &\iff f_s(x, y + \mathfrak{j}) = 0 \\ &\iff f_s(x, y + \mathfrak{m}) = 0, \text{ for all } \mathfrak{m} \in \mathrm{MaxSpec}(B). \end{aligned}$$

The result now follows from the Chinese Remainder Theorem. □

Lemma 6.2. *Let $f_1, \dots, f_r \in K[X, Y]$ and let $k \in \mathbb{N}$. There exists an $(n + k)$-dimensional diophantine family D over K such that*

$$D(F) = \left\{(x, z) \in F^n \times F^k \;\middle|\; x \in P_{f_1,\dots,f_r}(B_z)\right\},$$

for all extensions F/K, and where B_z denotes the commutative F-algebra

$$F[T] \Big/ \left(T^k + \sum_{i=0}^{k-1} z_i T^i\right).$$

Proof. In a more advanced way, this construction can be described through the Weil restriction of the affine variety cut out by the polynomials $f_1, \dots, f_r$, along the family of schemes described by the B_z, fibred over the parameter space $\mathbb{A}^k$. Alternatively, from a model-theoretic standpoint, one can prove the statement by a quantifier-free interpretation of B_z in F, uniformly in the parameter tuple z. We give an elementary description instead.

We introduce two new tuples of variables $Z = (Z_i)_{0\leq i<k}$ and $U = (U_{i,j})_{0\leq i<k, 1\leq j\leq m}$. We write

$$g(Z, T) := T^k + \sum_{i=0}^{k-1} Z_i T^i \in K[Z, T]$$

and, for each $s \in \{1, \dots, r\}$, we let

$$\hat{f}_s(X, U, T) := f_s\left(X, \sum_{i=0}^{k-1} U_{i,1} T^i, \dots, \sum_{i=0}^{k-1} U_{i,m} T^i\right).$$

Choose $d \in \mathbb{N}$ to be the maximum of the degrees of the polynomials $\hat{f}_s$ in the variable T, and introduce a new tuple of variables $W = \left(W_l\right)_{0 \leq l \leq d}$. Then, for each s, we consider the polynomial

$$\tilde{f}_s(X, Z, U, W, T) := \hat{f}_s(X, U, T) - g(Z, T) \sum_{l=0}^{d} W_l T^l.$$

Note that $\tilde{f}_s(x, z, u, w, T) = 0$ for some w if and only if $g(z, T)$ divides $\hat{f}_s(x, u, T)$ in $F[T]$. By taking coefficients with respect to the variable T, we obtain a family of polynomials $h_{s,l} \in K[X, Z, U, W]$, for $1 \leq s \leq r$ and $0 \leq l \leq d + k$, such that

$$\tilde{f}_s(X, Z, U, W, T) = \sum_{l=0}^{d+k} h_{s,l}(X, Z, U, W) T^l.$$

We may define the required $(n + k)$-dimensional diophantine family D over K by writing

$$D(F) = \left\{(x, z) \in F^n \times F^k \;\middle|\; \exists u \in F^{km},\ w \in F^{d+1} \,:\, h_{s,l}(x, z, u, w) = 0 \text{ for all } s, l\right\},$$

for F/K. □

Lemma 6.3. *For every field extension F/K and every $a \in F$, we have*

$$\mathcal{S}^\tau_{\mathfrak{p}}(F; a) = \bigcup_{\mathfrak{m} \in \mathrm{MaxSpec}(B_a)} \mathrm{res}_{(B_a/\mathfrak{m})/F}\left(\mathcal{S}^\tau_{\mathfrak{p}}(B_a/\mathfrak{m})\right),$$

where $\mathrm{res}_{E/F}$ denotes restriction of primes from E to F, and B_a is the commutative F-algebra

$$F[T] \Big/ \left(t_{\mathfrak{p}} a^e \left(\left(T^{q^f} - T\right)^2 - 1\right) - \left(T^{q^f} - T\right)\right).$$

Proof. Denote $\mathrm{MaxSpec}(B_a) = \left\{\mathfrak{m}_1, \dots, \mathfrak{m}_r\right\}$ and $E_i = B_a/\mathfrak{m}_i$. Let

$$g_a = t_{\mathfrak{p}} a^e \left(\left(T^{q^f} - T\right)^2 - 1\right) - \left(T^{q^f} - T\right) \in F[T]$$

and note that g_a is closely related to $\gamma^\tau_{\mathfrak{p}, t_{\mathfrak{p}}}$.

First let $\mathfrak{P} \in \mathcal{S}^\tau_{\mathfrak{p}}(E_i)$ for some i. If θ denotes the residue of T in E_i, we have $\gamma^\tau_{\mathfrak{p}, t_{\mathfrak{p}}}(\theta) \in \mathcal{O}_{\mathfrak{P}}$ and therefore $v_{\mathfrak{P}}\left(\theta^{q^f} - \theta\right) > v_{\mathfrak{P}}\left(\left(\theta^{q^f} - \theta\right)^2 - 1\right)$, so since $g_a(\theta) = 0$ we necessarily have $v_{\mathfrak{P}}\left(t_{\mathfrak{p}} a^e\right) > 0$ and therefore $v_{\mathfrak{P}}(a) \geq 0$.

Conversely, let $\mathfrak{P} \in \mathcal{S}^\tau_{\mathfrak{p}}(F; a)$. Then $g_a \in \mathcal{O}_{\mathfrak{P}}[T]$ has a simple zero $T = 0$ modulo the maximal ideal of $\mathcal{O}_{\mathfrak{P}}$, which implies that there exists some i and $\mathfrak{Q} \in \mathcal{S}^\tau_{\mathfrak{p}}\left(E_i\right)$ with $\mathfrak{P} = \mathrm{res}_{E_i/F}(\mathfrak{Q})$: Indeed, if (F', v') is a henselization of $\left(F, v_{\mathfrak{P}}\right)$, then $v' = v_{\mathfrak{P}'}$ for a prime $\mathfrak{P}'$ of F', and Hensel's lemma in the form [9, Thm. 4.1.3(4)] shows that g_a has a zero in F', which induces an F-embedding $E_i \to F'$, and one can take $\mathfrak{Q} = \mathrm{res}_{F'/E_i}(\mathfrak{P}')$. □

Theorem 6.4. *For every $N \in \mathbb{N}$ there exists a 2-dimensional diophantine family $D^\tau_{\mathfrak{p},N}$ over K such that*

$$D^\tau_{\mathfrak{p},N}(F) = \left\{(x, a) \in F^2 \;\middle|\; v_{\mathfrak{P}}(x) \geq 0 \textit{ for every } \mathfrak{P} \in \mathcal{S}^\tau_{\mathfrak{p}}(F; a)\right\}$$

for every extension F/K with $\pi^\tau_{\mathfrak{p}}(F) \leq N$.

Proof. Let $l = 2q^f$. By Theorem 5.9 there exists N' such that for all $E/F/K$ with $[E : F] \le l$ and $\pi^\tau_\mathfrak{p}(F) \le N$, we have $\pi^\tau_\mathfrak{p}(E) \le N'$, and so

$$R^\tau_\mathfrak{p}(E) = R^\tau_{\mathfrak{p},N'}(E). \tag{6.1}$$

By Example 3.8, $R^\tau_{\mathfrak{p},N'}$ is a 1-dimensional diophantine family over K, and so we may choose polynomials $f_1, \dots, f_r \in K[X, Y_1, \dots, Y_m]$ such that

$$R^\tau_{\mathfrak{p},N'}(F) = \{x \in F \mid \exists y \in F^m : f_1(x, y) = \cdots = f_r(x, y) = 0\} \tag{6.2}$$

for all F/K. For each F/K with $\pi^\tau_\mathfrak{p}(F) \le N$, and each $a \in F$, we have

$$\begin{aligned} F \cap P_{f_1^l,\dots,f_r^l}(B_a) &= \bigcap_{\mathfrak{m}\in\mathrm{MaxSpec}(B_a)} \left(F \cap P_{f_1,\dots,f_r}(B_a/\mathfrak{m})\right) && \text{by Lemma 6.1,} \\ &= \bigcap_{\mathfrak{m}\in\mathrm{MaxSpec}(B_a)} \left(F \cap R^\tau_\mathfrak{p}(B_a/\mathfrak{m})\right) && \text{by (6.1) and (6.2),} \\ &= \bigcap_{\mathfrak{P}\in S^\tau_\mathfrak{p}(F;a)} \mathcal{O}_\mathfrak{P} && \text{by Lemma 6.3,} \end{aligned} \tag{6.3}$$

where B_a is the l-dimensional algebra from Lemma 6.3.

By Lemma 6.2, we may define a 2-dimensional diophantine family D over K satisfying

$$D(F) = \left\{(x, a) \in F^2 \;\middle|\; x \in P_{f_1^l,\dots,f_r^l}(B_a)\right\}$$

for every extension F/K. By (6.3), for every F/K with $\pi^\tau_\mathfrak{p}(F) \le N$ we in fact have

$$D(F) = \left\{(x, a) \in F^2 \;\middle|\; x \in \bigcap_{\mathfrak{P}\in S^\tau_\mathfrak{p}(F;a)} \mathcal{O}_\mathfrak{P}\right\},$$

proving the claim. □

Corollary 6.5. *If $\pi^\tau_\mathfrak{p}(F) < \infty$, then for every open-closed set $S \subseteq S^\tau_\mathfrak{p}(F)$, the holomorphy ring $\bigcap_{\mathfrak{P}\in S} \mathcal{O}_\mathfrak{P}$ is diophantine in F.*

Proof. As S is open-closed, it is of the form $S^\tau_\mathfrak{p}(F; a)$ for some $a \in F$, see [10, Lem. 10.4, 10.5]. Hence the claim follows from Theorem 6.4 and Lemma 3.7. □

By Example 2.5 this applies in particular to pseudo p-adically closed fields like $\mathbb{Q}^{tp}$, although for such fields there are in fact simpler ways of establishing Theorem 5.9.

ACKNOWLEDGEMENTS

Some of this work was completed while the authors were participating in the *Model Theory, Combinatorics and Valued Fields* trimester at the Institut Henri Poincaré, and they would like to extend their thanks to the organisers and the IHP for funding and hospitality. They would like to thank Florian Pop for discussions on the p-Pythagoras number. The results of Section 4 were in this generality first obtained, in a different formulation, in P. D.'s doctoral thesis [8], during the research for which he was supported by Merton College Oxford and the University of Oxford Clarendon Fund. S. A. was supported by The Leverhulme Trust under grant RPG-2017-179. P. D. was supported by KU Leuven IF C14/17/083. A. F. was funded by the Deutsche Forschungsgemeinschaft (DFG) - 404427454.

ORCID

Sylvy Anscombe https://orcid.org/0000-0002-9930-2804

REFERENCES

[1] S. Anscombe, P. Dittmann, and A. Fehm, *Approximation theorems for spaces of localities*, arXiv:1901.02632 [math.AC].

[2] S. Anscombe, P. Dittmann, and A. Fehm, *Denseness results in the theory of algebraic fields*, Manuscript (2019).
[3] M. F. Atiyah and I. G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.
[4] E. Bombieri and W. Gubler, *Heights in diophantine geometry*, Cambridge University Press, 2006.
[5] Th. C. Craven, *Intersections of real closed fields*, Canad. J. Math. **32** (1980), no. 2, 431–440.
[6] L. E. Dickson, *History of the theory of numbers. Volume II. Diophantine analysis*, Carnegie Institute of Washington, 1920.
[7] P. Dittmann, *Irreducibility of polynomials over global fields is Diophantine*, Compos. Math. **154** (2018), no. 4, 761–772.
[8] P. S. Dittmann, A model-theoretic approach to the arithmetic of global fields, Doctoral thesis, University of Oxford, 2018.
[9] A. J. Engler and A. Prestel, *Valued fields*, Springer Monogr. Math., Springer, 2005.
[10] A. Fehm, *Elementary local-global principles for fields*, Ann. Pure Appl. Logic **164** (2013), 989–1008.
[11] C. Grob, Die Entscheidbarkeit der Theorie der maximalen pseudo p-adisch abgeschlossenen Körper, Dissertation, Universität Konstanz, 1987 (German).
[12] P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Stud. Adv. Math., vol. 101, 2006.
[13] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Fifth Edition, Oxford Science Publications, 1979.
[14] J. Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, Ann. of Math. (2) **183** (2016), 73–93.
[15] T.-Y. Lam, *Introduction to quadratic forms over fields*, Amer. Math. Soc., Providence, R.I., 2005.
[16] D. Marker, *Model theory: an introduction*, Springer, New York, 2002.
[17] L. Moret-Bailly, *Groupes de Picard et problèmes de Skolem. II*, Annales scientifiques de l'E.N.S. **22** (1989), no. 2, 181–194 (French).
[18] J. Neukirch, *Algebraic number theory*, Springer, 1999.
[19] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, 2nd edition, Springer, 2007.
[20] A. Pfister, *Quadratic forms with applications to algebraic geometry and topology*, Cambridge University Press, 1995.
[21] B. Poonen, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131** (2009), no. 3, 675–682.
[22] A. Prestel and P. Roquette, *Formally p-adic fields*, Springer, 1984.
[23] I. Reiner, *Maximal orders*, Clarendon Press, Oxford, 2003.
[24] A. Shlapentokh, *Hilbert's tenth problem: diophantine classes and other extensions to global fields*, Cambridge University Press, 2006.
[25] C. Siegel, *Darstellung total positiver Zahlen durch Quadrate*, Math. Z. **11** (1921), no. 3–4, 246–275 (German).
[26] R. Weissauer, *Der Hilbertsche Irreduzibilitätssatz*, J. Reine Angew. Math. **334** (1982), 203–220 (German).

How to cite this article: Anscombe S, Dittmann P, Fehm A. A p-adic analogue of Siegel's theorem on sums of squares. *Mathematische Nachrichten*. 2020;1–18. https://doi.org/10.1002/mana.201900173