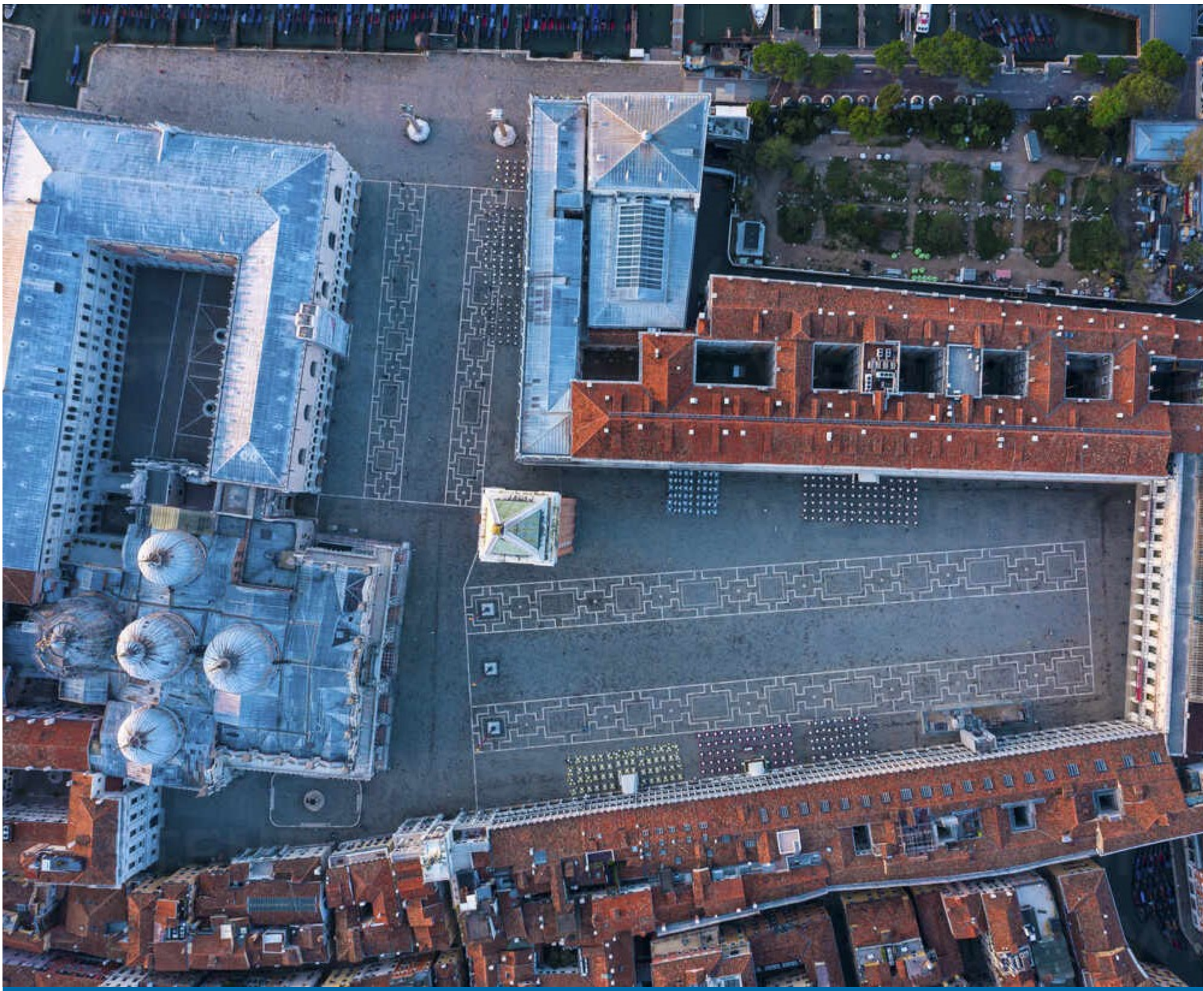
Methods for sums of squares in fields

Marco Zaninelli



Supervisor **Karim Johannes Becher**

Thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy
Faculty of Science — Antwerpen, 24/08/2023

University of Antwerp

University of Antwerp

Faculty of Science
Doctor of Philosophy

Methods for sums of squares in fields

Thesis submitted in fulfilment of the requirements for the degree of
Doctor of Philosophy
at the University of Antwerp

Marco Zaninelli

Antwerpen, 24/08/2023

Supervisor
Karim Johannes Becher

Jury
Chair
Wendy Lowen, University of Antwerp

Supervisor
Karim Johannes Becher, University of Antwerp

Members
David Grimm, University of Santiago de Chile
Yong Hu, Southern University of Science and Technology
Lieven Le Bruyn, University of Antwerp
David B. Leep, University of Kentucky

Contact
Marco Zaninelli

University of Antwerp
zaninelli.marco@uantwerpen.be

Contents

Acknowledgements

I thank Karim Johannes Becher for mentoring my PhD studies and for all he did for me during my time in Antwerp, which can not be summarised in few lines.

I further thank Wendy Lowen for being the chair of my doctoral jury, and David Grimm, Yong Hu, Lieven Le Bruyn and David Leep for being members of it.

Special thanks go to my friends and colleagues who proofread parts of the first draft of this manuscript and gave valuable input. Among them are David Grimm, Nicolas Daans, Shira Gilat, Parul Gupta, Kader Bingöl, Sten Veraa and Arne Mertens.

I thank all the mathematicians who contributed to the research that led to this thesis, and in particular to Parul Gupta for her help with local-global principles, Eberhard Becker for introducing me to real holomorphy rings, David Grimm and Yong Hu for their precious contributions in the context of Chapter 7, David Leep for directing me towards [MSV93]. I further thank Nicolas Daans, Gonzalo Manzano Flores, Shira Gilat and Kader Bingöl for helping me overtaking countless mathematical obstacles which I encountered during my research activity.

I am in debt to Remi Rasson for his help with bureaucracy regarding the thesis; to Sten Veraa who selflessly watched my back from all sorts of bureaucratic dangers since my first day in Antwerp to the last; to with Nicolas Daans for a wide range of Flemish-speaking issues.

Credit for the realisation of this thesis also goes to Julia Ramos Gonzalez and Dries Hautekiet, who kindly hosted me many times in the unforeseen months between the end of my stay in Antwerp and the public defense of this dissertation. I also thank all the people that made my stay in Antwerp so nice, which include most of the names mentioned above, together with my fellow expats Piergiorgio Panero, Serena Santi, Bernardo Ercoli, and many others.

Finally, I am grateful to a bunch of people who did not directly contribute to this dissertation or to my stay in Antwerp, but who are ultimately the ones to whom all my work is dedicated to, who believed in me at any moment without ever needing evidence of my qualities. Among these are my parents Cinzia Bentivoglio and Maurizio Zaninelli, my sisters Martina and Michela, my brother in law and nephew Matteo and Diego Libanti, and all the rest of my family. This includes Shira Gilat, whom I also and especially thank for being the dundika she is, and all my friends in Italy and around the world.

Front cover: aerial view of San Marco Square, Venice, from https://www.westend61.de/. Fun fact: San Marco Square is the only square (*piazza*) in Venice; all the others are called fields (*campo*).

Introduction

In this thesis we develop techniques to study sums of squares in fields. We produce methods to write sums of squares in fields using few squares, and we establish lower bounds for the number of squares that are necessary to represent sums of squares.

The earliest known human investigations about squares and sums of squares date back to no less than three and a half millennia ago, with ancient tablets from around 1800 b.C. witnessing the interest of the Old Babylonians in finding pythagorean triples, (that is, integers x, y, z such that $x^2 + y^2 = z^2$); see [Neug57, Sections 2.19, 2.20]. Since then, issues about sums of squares were frequently raised and solved in the four corners of the world, but it is mostly in the last three centuries that such a subject assumed its current shape. Two turning points in particular can be easily identified in this period. The first one is Euler's and Lagrange's seminal works on sums of squares in $\mathbb{Q}$ and in $\mathbb{Z}$ during the eighteenth century, which culminated into Lagrange's renowned four-square theorem stating that every positive integer is a sum of four squares, and which laid the foundations of modern number theory. The second one is Hilbert's works on sums of squares in number fields and in real polynomials at the turn of the nineteenth century. Hilbert postulated that any sum of squares in a number field is a sum of four squares (which was later proved by C. Siegel in [Si21]), and investigated positive definite forms over the real numbers. The latter enquiry led him to ask, in the seventeenth of the 23 problems of his influential list [Hi02], "whether every (ed: real positive) definite form may not be expressed as a quotient of sums of squares of forms." E. Artin [Ar27] gave a positive answer to Hilbert's question, showing that real positive definite forms are exactly the quotients of sums of squares of forms, but did not provide any bound on the number of squares appearing in such sums. This led other mathematicians to investigate systematically the following questions.

Question 1. *Given a commutative ring R, does there exist $n \in \mathbb{N}$ such that any sum of squares in R is a sum of n squares in R? If so, what is the smallest such number?*

Such a minimum number was later called *the Pythagoras number of R* and denoted by $p(R)$; in case the answer to the first question is negative, one sets $p(R) = \infty$. We adopt the notation ΣR^2 for the sums of squares in R and $\Sigma_n R^2$ for the sums of n squares in R, for any positive integer n. In view of this notation, $p(R) = \mathsf{inf}\{n \in \mathbb{N}^+ \mid \Sigma R^2 = \Sigma_n R^2\}$, and Question 1 amounts to the computation of the Pythagoras number of a ring. In case R is a field, a specific range of techniques that may be applied to tackle this issue is available in the literature. In this thesis we focus mainly on the study of sums of squares in fields of characteristic different from 2 (any sum of squares in a field of characteristic 2 is a square). Our principal objective is to develop methods to compute upper bounds on the Pythagoras number of fields.

The investigation of sums of squares is inseparably connected with the study of quadratic forms. Indeed, let K be a field and $n \in \mathbb{N}$. Then sums of n squares in K are exactly the elements of K that are represented by the quadratic form $X_1^2 + \ldots + X_n^2$ over K. In view of this, we begin the first chapter of this document by introducing the reader to the basics of the theory of quadratic forms over fields of characteristic different from 2, and only in Section 1.2 we focus our attention to sums of squares in fields. A crucial property of the quadratic form $X_1^2 + \ldots + X_n^2$ discovered by A. Pfister [Pfi65b] is that it is multiplicative whenever n is a power of 2. In terms of sums of squares, this entails for any $m \in \mathbb{N}$ that the product of two sums of 2^m squares in a field is again a sum of 2^m squares, that is, $(\Sigma_{2^m} K^2)^\times = \Sigma_{2^m} K^2 \smallsetminus \{0\}$ is a multiplicative subgroup of $K^\times$ for any field K. In the perspective of computing upper bounds for the Pythagoras number of fields, this is a very useful property, since it is often possible to write sums of squares as products of sums of squares with certain properties, and thus reduce the problem to bound the number of squares necessary to represent sums of squares with such properties. In Chapter 1, we focus on products of quadratic forms.

Set $m = \lceil \log_2 n \rceil$. From the multiplicativity of $(\Sigma_{2^m} K^2)^\times$ for a rational function field in n variables, we obtain that the product of two positive definite quadratic forms in $\mathbb{R}[X_1, \ldots, X_n]$ is a sum of 2^m squares in $\mathbb{R}(X_1, \ldots, X_n)$. It is straightforward that $X_1^2 \cdot (X_1^2 + \ldots + X_n^2)$ is not a sum of $n-1$ squares in $\mathbb{R}(X_1, \ldots, X_n)$, hence this bound is optimal when n is a power of 2. When n is not a power of 2, it is not clear in general whether the bound 2^m is optimal. Nevertheless, it was already known to Hilbert [Hi88] that this bound is not optimal when $n = 3$; in this case any product of two positive definite quadratic forms is a sum of three squares of fractions of real forms in three variables. A modern proof of this due to C. Scheiderer [Sche10, §9] inspired us the work in Section 1.4, where we show that this bound is in fact not optimal for all integers of the form $n = 2^{k+1} + 1$ where $k \in \mathbb{N}$. More precisely, we show the following.

Theorem 1 (Theorem 1.4.10). *Let $k \in \mathbb{N}$, let $n = 2^{k+1}+1$ and let $\phi_1, \phi_2 \in \mathbb{R}[X_1, \ldots, X_n]$ be positive definite quadratic forms. Then $\phi_1 \cdot \phi_2$ can be written as a sum of $(3n-1)/2$ rational functions in $\mathbb{R}(X_1, \ldots, X_n)$.*

Note that for large k, the bound $(3n-1)/2 = 2^{k+2} - 2^k + 1$ provided by Theorem 1 is significantly smaller than the bound 2^{k+2} discussed above. Nevertheless, we do not know whether the new bound is actually optimal for arbitrary k. In fact, we show that the bound is not yet optimal for $k = 1$, that is, for $n = 5$. In this situation, Theorem 1 implies that the product of two positive definite quadratic forms in $\mathbb{R}[X_1, \ldots, X_5]$ is a sum of 7 squares in $\mathbb{R}(X_1, \ldots, X_5)$; we prove that it is actually a sum of 6 squares. Furthermore, we show that it is possible to obtain an explicit formula to write the former product as a sum of 6 squares, provided that one is able to compute an explicit simultaneous diagonalisation of the two quadratic forms in question. However, this is made by means of the so-called Degen-Cayley's identity for products of the sums of 8 squares. In view of A. Hurwitz' work [Hur98], the existence of an analogous formula for products of sums of a higher number of squares can be excluded. Hence we cannot obtain any further improvement to the bound in Theorem 1 for higher k by reproducing this method. Furthermore, it remains open whether the bound 6 is optimal.

Question 2. *Is the product of two positive definite quadratic forms in $\mathbb{R}[X_1, \ldots, X_5]$ a sum of five squares in $\mathbb{R}(X_1, \ldots, X_5)$?*

The behaviour of quadratic forms is heavily depending on the underlying base field. Luckily, in certain situations it is possible to infer information about quadratic forms over a field, and more specifically about the elements that they represent, from the understanding of quadratic forms over more familiar fields. This is the case for henselian valued fields, where it is often possible to obtain information on quadratic forms from the study of the quadratic forms over the residue field. Valued field, valuations and valuation rings will be thoroughly discussed in Chapter 2, since their use in the following chapters will be pervasive. In Section 2.4, we focus on their applications to the study of sums of squares. We also discuss the connections between valuations and absolute values; see Section 2.3. Absolute values will be involved in the other key tool to move the study of quadratic forms to familiar fields, that is, the so-called local-global principles. The most famous local-global principle is undoubtedly the one due to H. Hasse and H. Minkowski, which can be stated as follows.

Theorem A (Hasse-Minkowski). *Let K be a number field, let $x \in K$ and let ϕ be a quadratic form over K. Then x is represented by ϕ over K if and only if it is represented by ϕ over the completion of K with respect to any absolute value on K.*

The usefulness of Theorem A lies in the fact that studying quadratic forms in a number field is more difficult than doing so in its completions, which are indeed henselian valued fields with a finite residue field.

Another local-global principle that will play a crucial role in this dissertation is due to K. Kato. Boiled down to the quadratic forms in which we are interested, it may be stated as follows.

Theorem B (Kato). *Let F be a finite field extension of $\mathbb{Q}(X)$ and let $f \in \Sigma F^2$. Then $f \in \Sigma_4 F^2$ if and only if $f \in \Sigma_4 (F \otimes_{\mathbb{Q}} \mathbb{Q}_2)^2$, where $\mathbb{Q}_2$ is the field of the dyadic numbers.*

In Chapter 3, we examine holomorphy rings, that is, intersections of valuation rings of a field. Our attention for such objects is explained by the fact that in presence of an adequate local-global principle they may contain, roughly speaking, all the information about sums of squares that one can extract from the completions. Another advantage of holomorphy rings is that they have very nice algebraic properties, under mild assumptions. In full generality, they are integrally closed domains. When the intersection is finite, they are semilocal Bézout domains. In Chapter 7 we will exploit this property extensively.

Another type of holomorphy ring carrying good algebraic properties -and which will play an important role in this thesis- is given by the intersection of all real valuations on a field. Let K be a field. We say that K is *real* if $-1 \notin \Sigma K^2$, and *nonreal* otherwise. Given a valuation ring $\mathcal{O}$ of K, we say that $\mathcal{O}$ is *real* if the residue field of $\mathcal{O}$ is real, and *nonreal* otherwise. The intersection of all real valuation rings of K is denoted by $\mathcal{H}(K)$ and is called *the real holomorphy ring of K*; if no real valuation ring of K exists, we set $\mathcal{H}(K) = K$. It is known that $\mathcal{H}(K)$ is a Prüfer domain, that its fraction field is K, and that $(x_1\mathcal{H}(K)+\ldots+x_n\mathcal{H}(K))^{*2} = (x_1^2+\ldots+x_n^2)\mathcal{H}(K)$ for any $n \in \mathbb{N}$, $x_1, \ldots, x_1 \in \mathcal{H}(K)$; see e.g. [Bec82]. It is also known that $\mathcal{H}(F)$ is a Dedekind domain for any finite field extension $F/\mathbb{Q}(X)$; see e.g. [FJ08, Proposition 3.3.2].

In Section 3.2, we will show for a real field K that $\mathcal{H}(K)$ can be obtained as the intersection of certain valuation rings, which are associated to the orderings on K. After that, in Section 4.1, the most relevant results in the literature around Pythagoras number of function fields in one variable will be presented to the reader. This integrates the introduction to the Pythagoras number of a field given in Section 1.2, where ample attention is dedicated to the connection between the Pythagoras number of a nonreal field and its level.

Let K be a field. The *level* of K, which we denote by $s(K)$, is defined as the minimal $n \in \mathbb{N}$ such that $-1 \in \Sigma_n K^2$ if such an n exists (that is, if K is nonreal), and as ∞ otherwise. A fascinating property of the level of a field is that it is always ∞ or a power of 2; this was proven by Pfister [Pfi65a] as a consequence of the multiplicativity of

$(\Sigma_{2^k}K^2)^\times$ for $k \in \mathbb{N}$. Furthermore, the identity

$$x = \frac{(x+1)}{2}^2 - \frac{(x-1)}{2}^2$$

allows us to establish elementarily the relation $s(K) \leqslant p(K) \leqslant s(K) + 1$ and the identity $\Sigma K^2 = K$ for every nonreal field K of characteristic different from 2. As a consequence, the Pythagoras number of a nonreal field is always equal to 2^k or $2^k + 1$ for some $k \in \mathbb{N}$. Moreover, any pair of the form $(2^k, 2^k)$ or $(2^k, 2^k+1)$ with $k \in \mathbb{N}$ is realised as $(s(K), p(K))$ for some field K; see e.g. [Pfi95, Example 3.1.2 (9) and Proposition 7.1.5].

The situation of real fields is not quite the same. Though for a while only real fields of Pythagoras number ∞, 2^k or 2^k+1 for $k \in \mathbb{N}$ were known, eventually D. Hoffman [Ho99] showed that there exist real fields of arbitrary Pythagoras number. Nevertheless, to this date the only known examples of real fields with finite Pythagoras number not contained in $\{2^k, 2^k + 1 \mid k \in \mathbb{N}\}$ are constructed by infinite iterations of function field extensions. This comes from the fact that it is not yet understood how the Pythagoras number of a field behaves under finitely generated extensions. Even finite extensions produce big problems. A. Prestel [Pre78] found real fields K with prescribed Pythagoras number in $\{2^k, 2^k + 1 \mid k \in \mathbb{N}^+\} \cup \{\infty\}$ admitting a real quadratic field extension F/K such that $p(F) = 2$; this implies that the Pythagoras number can drop drastically when extending a field. On the other hand, for any real field K and any finite field extension F/K it is known [Pfi95, Proposition 7.1.13] that $p(F) \leqslant [F : K] \cdot p(K)$, but this upper bound does not seem very satisfactory, since no example is known where $p(F) \geqslant p(K)+2$. For finite field extensions of $\mathbb{Q}$, the situation became completely clear after the publication of Theorem A in [Ha23]. Let K be a number field. If K is nonreal, then $p(K) = \mathsf{min}\{s(K) + 1, 4\}$. If K is real and there exists a dyadic absolute value of K having odd degree, then $p(K) = 4$, otherwise $p(K) = 3$; see [Pfi95, Examples 7.1.4 (2), (3)]. Note that $s(K)$ can also be computed explicitly using Theorem A; see [Pfi95, Examples 3.1.2 (6)].

When we turn our attention to transcendental field extensions, the behaviour of the Pythagoras number is even more obscure. A fundamental discovery by J.W.S. Cassels [Cas64, Theorem 2] was that $p(K(X)) \geqslant p(K) + 1$ for any real field K. Since $p(\mathbb{R}) = 1$ and $p(\mathbb{R}(X)) = 2$, it is elementary that such a bound is optimal. On the other hand, examples of fields K such that $p(K(X)) \geqslant p(K) + 2$ are known [Pfi95, Example 7.1.11], therefore the converse inequality fails to hold generally. As a matter of fact, it is not even known whether $p(K) < \infty$ implies $p(K(X)) < \infty$ for any real field K.

Nevertheless, classic fields seem to behave quite well under rational function field extensions. For instance, it was shown by Y. Pourchet [Pou71] that $p(K(X)) \leqslant 5$ for any number field K; soon after [HJ74], J.S. Hsia and R.P. Johnson concluded the following.

Theorem C (Pourchet, Hsia, Johnson). *Let K be a real number field. Then*

$$p(K(X)) = p(K) + 1.$$

The lion's share in the proof of this statement lies in Pourchet's paper, which is very technical, and relies on four main ingredients. The first one is a local-global principle for quadratic forms over $K(X)$, where K is a number field. This may be seen as a special case of Theorem B when $K = \mathbb{Q}$, and more generally as a special case of Kato's local-global principle from [Kat86], though the statement for rational function fields was known much earlier. In Chapter 5 we give a new argument for this local-global principle, which only makes use of classical instruments of quadratic forms. As a matter of fact, its only ingredients are Springer's theorem for non-dyadic completely valued fields and the Hasse-Minkowski Local-Global Principle. Furthermore, our argument also holds slightly more generally, allowing us to prove the following theoretical statement.

Theorem 2 (Theorem 5.2.2)**.** *Let $m \in \mathbb{N}^+$ and let $\mathcal{E}$ be a set of field extensions of K. Assume that for every $l \in \{m-1, m\}$, $p \in \mathcal{P}_K$, $f_1, \dots, f_l \in K[X] \smallsetminus pK[X]$ such that $\langle\langle \overline{f}_1^{v_p}, \dots, \overline{f}_l^{v_p} \rangle\rangle_{K(X)_{v_p}}$ is anisotropic, there exist $L \in \mathcal{E}$ and $\alpha \in L$ such that $p(\alpha) = 0$ and $\langle\langle f_1(\alpha), \dots, f_l(\alpha) \rangle\rangle_L$ is anisotropic. Then every anisotropic m-fold Pfister form over $K(X)$ is anisotropic over $L(X)$ for some $L \in \mathcal{E}$.*

From Theorem 2 we recover Theorem B for the case $F = \mathbb{Q}(X)$, but also an analogous statement for $\mathbb{Q}(\!(t_1)\!) \cdots (\!(t_n)\!)(X)$; see Corollary 5.3.12.

The other main ingredients of the proof of Theorem C are a classical approximation theorem and the so called root-continuity. The first one is standard and will not require much attention. The second one will be discussed thoroughly in sections 6.2 and 6.4; the central idea is to exploit Krasner's lemma [EP05, Theorem 4.1.7] to show that for polynomials with coefficients in a henselian valued field, being represented by a given quadratic form -and thus, in particular, being a sum of n squares, for $n \in \mathbb{N}^+$- is an open property. Roughly speaking, this amounts to saying that the property of being represented by a given quadratic form is preserved modulo small movements in the topology induced by the Gauss extensions of the valuation over the base field; see Corollary 6.4.1 for a more precise statement. Our result is valid over arbitrary non-dyadic henselian valued fields, thus in a much broader environment than the one -completions of a number field- adopted by Pourchet.

The last crucial ingredient in Pourchet's proof is the identity

$$4gh = (\lambda g + \lambda^{-1} h)^2 - (\lambda g - \lambda^{-1} h)^2,$$

which holds over a field K for any $f, g \in K[X]$ and $\lambda \in K^\times$. Such an elementary identity and its clever use are arguably Pourchet's most groundbreaking contribution in his proof. This inspires Section 6.1, which is quite technical, but is developed as arbitrarily as possible, generalising remarkably the original proof, which was only working in p-adic fields; we state the main result in Corollary 6.1.8. Finally, in Section 6.3 we put together all the ingredients and recover that $p(K(X)) \leqslant 5$ for every number field K.

In the light of what was explained above, it should not surprise that very little is known for transcendental field extensions that are not purely transcendental, even when the transcendence degree is low and even over very well known base fields. In Chapter 4 we focus on bounding from above the Pythagoras number of field extensions of $\mathbb{Q}$ of transcendence degree 1, that is, of algebraic field extensions of $\mathbb{Q}(X)$. This can easily be reduced to the finitely generated case, that is, to bounding Pythagoras number of finite field extensions of $\mathbb{Q}(X)$. This issue is particularly interesting and has already been studied by F. Pop, who showed in an unpublished note [Pop90] the following upper bound.

Theorem D (Pop)**.** *Let K be a finite field extension of $\mathbb{Q}(X)$. Then $p(K) \leqslant 6$.*

In Section 4.2, we provide an argument for Theorem D which is inspired by Pop's work, but which differs in the techniques involved: Pop's argument is based on standard geometrical techniques, whereas ours is inherently algebraic. We observe for a finite field extension $K/\mathbb{Q}(X)$ that the real holomorphy ring of K contains much of the information about $\Sigma_5 K^2$; more precisely, we show that $\mathcal{H}(K)^\times \cap \Sigma K^2 \subseteq \Sigma_5 K^2$, and we recover Theorem D from the properties of $\mathcal{H}(K)$, and in particular from the fact that it is a

Dedekind domain. Our argument also recovers for a rational function field over a number field that a large class of sums of squares -morally half of them- are indeed sums of five squares; see Corollary 4.2.8. As opposed to Pourchet's argument, we obtain this through an elementary and elegant argument. Unfortunately, it remains open whether the bound 6 in Theorem D is optimal, or can be lowered down to 5.

In Chapter 7 we provide for a field K and for $n \in \mathbb{N}^+$ a sufficient condition to satisfy $p(K) \leqslant 2^n+1$, namely the presence of a Bézout subring of K possessing certain properties. We name such subrings *square-effective.* Given a field K and a subring $\mathcal{H} \subseteq K$, we set $p^*(\mathcal{H}) = \inf\{k \in \mathbb{N} \mid \mathcal{H}^\times \cap \Sigma K^2 \subseteq \Sigma_k K^2\} \in \mathbb{N} \cup \{\infty\}$. By using only elementary algebra, we show the following result.

Theorem 3 (Theorem 7.1.3)**.** *Let K be a field and $\mathcal{H}$ a square-effective subring of K having fraction field K. Let J be the Jacobson radical of $\mathcal{H}$. If $(1 + \Sigma K^2) \cap \mathsf{J} \neq \emptyset$, then*

$$p(K) \leqslant p^*(\mathcal{H}) + 1.$$

In Section 7.1 and Section 7.2, we examine square-effective domains, in order to identify situations in which Theorem 3 may be applied. This happens for example when a field K contains a semilocal-Bézout subring $\mathcal{H}$ such that $\mathsf{Frac}(\mathcal{H}) = K$ and $1 + \mathcal{H}^2 \subseteq \mathcal{H}^\times$. This sends us back to the holomorphy rings given by a finite intersection of valuation rings, and therefore to local-global principles involving valuations. Indeed, in certain fields K the presence of such a local-global principle is sufficient to produce a subring $\mathcal{H} \subseteq K$ satisfying at the same time the hypotheses of Theorem 3, and an upper bound for $p^*(\mathcal{H})$ of the form 2^k for some $k \in \mathbb{N}$.

In Section 7.3, we apply Theorem 3 in the context of field extensions of transcendence degree 1, retrieving the following statement contained in [BGVG14, Theorem 6.13].

Theorem E (Becher, Grimm, Van Geel)**.** *Let $n, r \in \mathbb{N}$. Let K be a field such that $p(E) \leqslant 2^{n+1}$ for every finite field extension $E/K(X)$. Let $F/K(\!(t_1)\!)\cdots(\!(t_r)\!)(X)$ be a finite field extension. Then $p(F) \leqslant 2^{n+1} + 1$.*

This applies in particular to $K = \mathbb{R}$, for $n = 0$. The proof given in [BGVG14] is based on [CTPS12, Theorem 3.1], which is a sophisticated local-global principle involving the most modern techniques of field patching, and which is exploited for $2^n + 1$ and $2^n + 2$-dimensional quadratic forms over F. Our argument only exploits the local-global principle for 2^n+1-dimensional quadratic forms that are Pfister neighbours, which makes the proof simpler and easier to reproduce in other situations. As an example of this phenomenon, we show the following.

Theorem 4 (Example 7.3.4)**.** *Set $M(X,Y) = X^2Y^4 + X^4Y^2 - 3X^2Y^2 + 1 \in \mathbb{R}[X,Y]$, $K = \mathbb{R}(Y)(\!(t)\!)$ and $F = K(X)\left(\sqrt{(tX-1)M(X,Y)}\right)$. Then $p(F) = 5$.*

The polynomial $X^2Y^4 + X^4Y^2 - 3X^2Y^2 + 1$ from Theorem 4 is known as *Motzkin polynomial* and is known to be a sum of 4 but not of 3 squares in $\mathbb{R}(X,Y)$; see [CEP71]. Theorem 4 could be obtained from [CTPS12, Theorem 3.1], but using our method (which is inspired by Becher and Van Geel in [BVG09, Lemma 3.8 - Theorem 3.10]) we only involve Milnor's exact sequence as a local-global principle ingredient.

In Section 7.4, we apply Theorem 3 to the fraction fields of a complete local domain of Krull dimension 2. We retrieve the upper bound $p(F) \leqslant 3$ for every finite field extension $F/\mathbb{R}(\!(t_2,t_1)\!)$, which is contained in [Hu15]. In order to do so, we use a local-global principle from [HHK15, Corollary 4.7] and techniques from algebraic geometry. Roughly speaking, for a finite field extension $F/\mathbb{R}(\!(t_0,t_1)\!)$ we identify finitely many valuation rings of F, whose intersection produces the desired square-effective ring, as the valuation rings corresponding to the (finitely many) irreducible components of a regular model of the affine scheme associated to the integral closure of $\mathbb{R}[\![t_0,t_1]\!]$ in F. We also obtain the following.

Theorem 5 (Corollary 7.4.11)**.** *Let K be a field and let $n \in \mathbb{N}$ be such that $p(E) \leqslant 2^{n+1}$ for any finite field extension $E/K(X)$. Let $r \in \mathbb{N}$ and let $F/K(\!(t_1)\!)\cdots(\!(t_r)\!)(\!(t_{r+1},t_{r+2})\!)$ be a finite field extension. Then $p(F) \leqslant 2^{n+1}+1$.*

The hypothesis of Theorem 5 applies in particular when K is a field extension of transcendence degree n of $\mathbb{R}$ (or of transcendence degree $n-1 \geqslant 1$ of $\mathbb{Q}$); in this case, we obtain that $p(F) \leqslant 2^{n+1}+1$ for any field F as in the statement. When $n \geqslant 2$, this is a significant improvement compared to the bound $p(F) < 2^{n+2}$, which one could derive from [Hu17, Corollary 4.7] by using [BVG09, Theorem 3.5].

Notations

We fix some general terminology that will be used throughout this thesis. We denote by

- $\mathbb{N}$ the set of natural numbers, including 0;
- $\mathbb{N}^+$ the set $\mathbb{N} \smallsetminus \{0\}$;
- $\mathbb{Z}$ the ring of integers;
- $\mathbb{Q}$ the field of rational numbers;
- $\mathbb{R}$ the field of real numbers;
- $\mathbb{C}$ the field of complex numbers.

Given a matrix A, we denote by A^t the transpose matrix of A. For a set S, we set:

- $S^{(1)} = S$;
- $S^{(n)} = S \times S^{(n-1)}$ for $n \in \mathbb{N}^+$.

In this thesis we will only make use of rings with unit, so by a *commutative ring* we will mean a commutative ring with unit. For a commutative ring R, we denote by

- $\mathsf{char}(R)$ the characteristic of R;
- $\mathbf{0}_R$ the zero ideal of R;
- R^n the set $\{x^n \mid x \in R\}$, for $n \in \mathbb{N}$;
- $\Sigma_n R^2$ the set $\{\Sigma_{i=1}^n x_i^2 \mid x_1, \dots, x_n \in R\}$ for $n \in \mathbb{N}$;
- ΣR^2 the set $\{\Sigma_{i=1}^n x_i^2 \mid n \in \mathbb{N}, x_1, \dots, x_n \in R\}$;
- $\mathsf{Spec}(R)$ the set of prime ideals of R, with its affine scheme structure when considered as a scheme;
- $\mathsf{Max}(R)$ the set of maximal ideals of R;
- $S^\times$ the set $\{x \in S \mid \text{there exists } y \in S \text{ such that } xy = 1\}$, for any $S \subseteq R$;
- $\mathsf{Jac}(R)$ the Jacobson radical ideal of R, that is, $\mathsf{Jac}(R) = \{x \in R \mid 1 - Rx \subseteq R^\times\}$;
- $(x)_R$ or simply xR the principal ideal of R generated by $x \in R$;
- $R_\mathfrak{p}$ the localisation of R at $\mathfrak{p} \in \mathsf{Spec}(R)$.

For a function f, we denote by $\mathsf{Im}(f)$ the image of f.

Nederlandse samenvatting

In deze thesis worden er methoden ontwikkeld om sommen van kwadraten in lichamen te bestuderen. In het bijzonder zoeken we het minimal aantal kwadraten dat nodig is om sommen van kwadraten in een lichaam te representeren.

In het eerste hoofdstuk van deze thesis, bestuderen we producten van twee kwadratische vormen over $\mathbb{R}$. Zij $n \in \mathbb{N}^+$ en $\phi, \psi \in \mathbb{R}[X_1, \ldots, X_n]$ positief definiete kwadratische vormen. Stel $m = \lceil \log_2 n \rceil$. Het is bekend dat $\phi \cdot \psi$ een som van 2^m kwadraten is in $\mathbb{R}(X_1, \ldots, X_n)$. In het geval dat $n = 2^{k+1} + 1$ voor $k \in \mathbb{N}$, tonen we dat $\phi \cdot \psi$ een som van $(3n-1)/2$ kwadraten in $\mathbb{R}(X_1, \ldots, X_n)$ is. Deze bovengrens is lager dan 2^m als $n \geqslant 5$. In het algemeen weten we niet of $(3n-1)/2$ een optimale grens is voor de lengte van $\phi \cdot \psi$; we tonen toch dat het niet optimaal is voor $n = 5$, wanneer $\phi \cdot \psi$ een som van zes kwadraten in $\mathbb{R}[X_1, \ldots, X_n]$ is.

Voor een lichaam K heet het minimale aantal kwadraten dat nodig is om al de sommen van kwadraten in K te schrijven *het Pythagorasgetal van* K, en we noteren het als $p(K)$. F. Pop toonde dat $p(F) \leqslant 6$ voor elk functielichaam $F/\mathbb{Q}$ in één variabele. Pop's bewijs volgt uit een lokaal-globaal principe door K. Kato en standaard technieken van algebraïsche meetkunde. Pop's werk geeft inspiratie voor een alternatief argument dat volgt uit hetzelfde lokaal-globaal principe door middel van algebraische technieken. Specifieker, stel een functielichaam $F/\mathbb{Q}$ in één variabele. De doorsnede van de discrete valuatieringen van F met een reëel residulichaam heet *de reële holomorfie ring van* F, en wordt aangeduid met $\mathcal{H}(F)$. Men kan bewijzen dat $\mathcal{H}(F)$ een Dedekinddomein is en dat het andere nuttige algebraïsche eigenschappen heeft. Dankzij deze eigenschappen, kunnen we tonen dat elke som van kwadraten in F die invertebaar is in $\mathcal{H}(F)$, een som van 5 kwadraten is; we vinden ook de grens $p(K) \leqslant 6$ met elementaire berekeningen terug.

Eerder had Y. Pourchet getoond dat $p(F) \leqslant 5$, als $F = K(X)$ voor een getallenlichaam K. Pourchet's bewijs maakt sterk gebruik van het feit dat K een getallenlichaam is, maar het maakt niet duidelijk welke van zijn eigenschappen noodzakelijk zijn. We ontleden het in verschillende stukken en we bewijzen dat elk van deze stukken onder zwakkere voorwaarden geldt. We geven ook een nieuw bewijs van het lokaal-globaal principe dat in Pourchet's bewijs gebruikt wordt. Ons argument werkt in een meer algemene setting en levert ook een lokaal-globaal principe voor de lichamen $K(\!(t_1)\!) \ldots (\!(t_r)\!)(X)$ waar $r \in \mathbb{N}$.

Zij K nu een lichaam. In het laatste hoofdstuk wordt er een methode ontwikkeld om bovengrenzen voor het Pythagorasgetal van K van de vorm $2^n + 1$ met $n \in \mathbb{N}$ te bewijzen. Onze methode steunt op de aanwezigheid van een deelring van K met bepaalde algebraische eigenschappen. In enkele situaties kan de aanwezigheid van zo'n ring worden getoond door een lokaal-global principe voor 2^n+1-dimensionale kwadratische vormen. Buiten het gebruik van lokaal-globaal principes, is onze methode elementair. We gebruiken deze techniek om de grens $p(F) \leqslant 2^{n+1} + 1$ te tonen voor elke eindige lichaamsuitbreiding $F/K(\!(t_1)\!) \ldots (\!(t_r)\!)(\!(t_{r+1}, t_{r+2})\!)$ waar $r, n \in \mathbb{N}$ en K een lichaam is zodat $p(E) \leqslant 2^{n+1}$ voor elke eindige lichaamsuitbreiding $E/K(X)$. Hieruit halen we terug dat $p(E) \leqslant 3$ voor elke eindige lichaamsuitbreiding $E/\mathbb{R}(\!(t_1, t_2)\!)$, wat eerder door Y. Hu was bewezen. We halen ook terug uit onze methode dat $p(F) \leqslant 3$ voor elk functielichaam F in één variabele over $\mathbb{R}(\!(t_1)\!) \ldots (\!(t_r)\!)$ waar $r \in \mathbb{N}$; dit werd eerder door

K. Becher, D. Grimm en J. Van Geel bewezen.

Chapter 1
Quadratic forms

Given a field K, sums of squares in K are the elements that are represented by the quadratic form $X_1^2 + \ldots + X_n^2$ over K for some $n \in \mathbb{N}^+$. Classical methods from quadratic form theory appear thus naturally in the context of sums of squares. In Section 1.1 we provide the basics of the theory of quadratic forms, which will then be used in Section 1.4 and in the following chapters, especially in Chapter 5 and Chapter 6. We will mostly focus on fields of characteristic different from 2. In Section 1.2 we introduce the reader to quadratic forms over real fields and to the Pythagoras number of a field. In Section 1.3 we outline the current knowledge about simultaneous diagonalisations of quadratic forms over fields. In Section 1.4 we study products of two quadratic forms over a field; we present an upper bound for the number of squares that are necessary to represent as a sum of squares a product of two positive definite quadratic forms over a real closed field.

1.1 Basic concepts

This section is a partial introduction to the theory of quadratic forms over fields. A reader who is already familiar with the theory of quadratic forms might want to skip Section 1.1. In the following overview we largely rely on [Pfi95] and [Lam05].

In some situations, we will make use of quadratic forms over commutative rings that are not fields, and in particular over polynomial rings. In view of this, the most basic definitions in this section will be given in the context of arbitrary commutative rings. For details about the theory of quadratic forms over arbitrary commutative rings, we refer an interested reader to [Ba78]. We fix, for the rest of Section 1.1, a commutative ring R.

Given $n \in \mathbb{N}^+$, we call *n-ary quadratic form over R* any homogeneous polynomial of degree 2 in n variables with coefficients in R; by convention, we also consider the zero polynomial as an n-ary quadratic form over R. A 2-ary quadratic form is also called *binary*. We call *quadratic form over R* any n-ary quadratic form over R for any $n \in \mathbb{N}^+$.

Let $n \in \mathbb{N}^+$. We adopt the notations $R^n = \{x^n \mid x \in \mathbb{N}\}$ and

$$R^{(n)} = \underbrace{R \times \cdots \times R}_{n}.$$

By interpreting polynomials as R-valued functions via evaluation, an n-ary quadratic form over R can be viewed as a polynomial function $R^{(n)} \to R$. In most situations we only care about the polynomial functions induced by quadratic forms.

Let S/R be an extension of commutative rings and let $\phi \in R[X_1, \ldots, X_n]$ be a quadratic form. Of course ϕ can also be seen as a quadratic form in $S[X_1, \ldots, X_n]$, that is, as a function $S^n \to S$, in which case we denote it by ϕ_S. Given $s \in S$, we say that *s is represented by ϕ over S* if there exist $s_1, \ldots, s_n \in S$ such that $\phi_S(s_1, \ldots, s_n) = s$. We denote by $D_S(\phi)$ the set of all nonzero elements of S that are represented by ϕ over S, and we say that ϕ is *universal over S* if $D_S(\phi) = S \setminus \{0\}$. Furthermore, we say that ϕ is *isotropic over S* if there exists a vector $\mathbf{s} \in S^{(n)} \setminus \{0\}$ such that $\phi_S(\mathbf{s}) = 0$; otherwise we say that ϕ is *anisotropic over S*. A vector $\mathbf{s} \in S^{(n)}$ such that $\phi(\mathbf{s}) = 0$ is called *isotropic with respect to ϕ*. When there is no possibility of misunderstanding, we adopt simplified notations and write for $r \in R$ that *r is represented by ϕ* if r represented by ϕ over R, that *ϕ is universal* if ϕ is universal over R and that ϕ is *isotropic* (respectively, *anisotropic*) if ϕ is isotropic (respectively, anisotropic) over R.

1.1.1 Examples. (a) The 1-ary quadratic form $X^2 \in R[X]$ is anisotropic if and only if R is reduced.

(b) Set $\phi = X_1^2 - X_2^2 \in R[X_1, X_2]$. Clearly ϕ is isotropic whenever $R \neq \{0\}$. If $2 = 0$ in R, then $D_R(X_1^2 - X_2^2) = R^{\times 2}$, trivially. If $2 \in R^\times$, then ϕ is called *hyperbolic plane over R*; furthermore ϕ is universal, since for any $x \in R$ we have the identity

$$x = \left(\frac{(x+1)}{2}\right)^2 - \left(\frac{(x-1)}{2}\right)^2.$$

1.1.2 Proposition. *Let ϕ be a quadratic form over R. Then*

$$R^{\times 2} D_R(\phi) = D_R(\phi).$$

Proof. The statement follows trivially from the identity $r^{-1} = r \cdot r^{-2}$ for $r \in R^\times$. □

Let $n \in \mathbb{N}^+$. Given two n-ary quadratic forms ϕ_1, ϕ_2 over R, we say that ϕ_1 and ϕ_2 are *isometric* if there exists an invertible matrix $A \in (\mathsf{M}_n(R))^\times$ such that $\phi_1(\mathbf{x}) = \phi_2(A \cdot \mathbf{x}^t)$ for every $\mathbf{x} \in R^{(n)}$. It is clear from the definition that isometry is an equivalence relation on the quadratic forms over R. In the sequel, we will often abuse of notation and denote the class modulo isometry of a quadratic form by the quadratic form itself.

Let K be a field of characteristic different from 2 and let ϕ be an n-ary quadratic form over K. We say that ϕ is *regular* if for any $\mathbf{x} \in K^{(n)}$ we have that $\mathbf{x} = 0$ whenever $\phi(\mathbf{x}+\mathbf{y}) - \phi(\mathbf{x}) - \phi(\mathbf{y}) = 0$ for all $\mathbf{y} \in K^{(n)}$. A regular quadratic form is a regular n-ary quadratic form for a unique $n \in \mathbb{N}$; in view of this, n will at times be omitted in the sequel.

1.1.3 Examples. (a) Let ϕ be a regular quadratic form over $\mathbb{R}$. By Sylvester's law of inertia [Lam05, Proposition II.3.2 (3)], there exist unique $m, n \in \mathbb{N}$ such that

$$\phi \simeq_{\mathbb{R}} X_1^2 + \ldots + X_m^2 - X_{m+1}^2 - \ldots - X_{m+n}^2.$$

(b) Any regular quadratic form over $\mathbb{C}$ is isometric to $X_1^2 + \ldots + X_n^2$ for a unique $n \in \mathbb{N}$.

Given $n \in \mathbb{N}^+$ and $a_1, \ldots, a_n \in R$, we denote by $\langle a_1, \ldots, a_n \rangle_R$ the n-ary quadratic form $a_1 X_1^2 + \ldots + a_n X_n^2 \in R[X_1, \ldots, X_n]$; when the base ring R is clear from the context, we may omit it and write just $\langle a_1, \ldots, a_n \rangle$. A quadratic form of the form $\langle a_1, \ldots, a_n \rangle_R$ for some $n \in \mathbb{N}^+$ and $a_1, \ldots, a_n \in R$ is called *diagonal*. Given a quadratic form ϕ over R, we call *a diagonalisation of ϕ* any diagonal quadratic form over R that is isometric to ϕ. Any quadratic form over a field of characteristic different from 2 has a diagonalisation; see [Lam05, Corollary 1.2.4].

Quadratic forms can be added and multiplied in the following way. Let $m, n \in \mathbb{N}^+$ and let ϕ, ψ be respectively an m-ary and an n-ary quadratic form over R. We denote by $\phi \perp \psi$ the *orthogonal sum of ϕ and ψ*, that is, the $(m+n)$-ary quadratic form over R

$$\phi(X_1, \ldots, X_m) \perp \psi(X_{m+1}, \ldots, X_{m+n}) \in R[X_1, \ldots, X_{m+n}].$$

We also denote

$$n \times \phi = \underbrace{\phi \perp \cdots \perp \phi}_{n \text{ times}}$$

and, by convention, we set $0 \times \phi = 0$.

Given $c \in R$, $m, n \in \mathbb{N}^+$ and $a_1, \ldots, a_m, b_1, \ldots, b_n \in R \smallsetminus \{0\}$, we denote

$$c\langle a_1, \ldots, a_m\rangle_R = \langle ca_1, \ldots, ca_m\rangle_R \quad \text{and}$$

$$\langle a_1, \ldots, a_m\rangle_R \otimes \langle b_1, \ldots, b_n\rangle_R = a_1\langle b_1, \ldots, b_n\rangle_R \perp \cdots \perp a_m\langle b_1, \ldots, b_n\rangle_R.$$

Let K be a field of characteristic different from 2 and ϕ, ψ regular quadratic forms over K. Consider $m, n \in \mathbb{N}^+$ and $a_1, \ldots, a_m, b_1, \ldots, b_n \in K^\times$ such that $\phi \simeq \langle a_1, \ldots, a_m\rangle_K$ and $\psi \simeq \langle b_1, \ldots, b_n\rangle_K$. We define $\phi \otimes \psi = \langle a_1, \ldots, a_m\rangle_K \otimes \langle b_1, \ldots, b_n\rangle_K$. It is straightforward that $\phi \otimes \psi$ is well-defined up to isometry.

1.1.4 Example. Let $n \in \mathbb{N}^+$. Then $D_R(n \times \langle 1\rangle_R)$ is the set of the nonzero sums of n squares in R, that is,

$$D_R(n \times \langle 1\rangle_R) = \{\Sigma_{i=1}^n x_i^2 \mid x_i \in R \text{ for every } i \in \mathbb{N} \text{ with } 1 \leqslant i \leqslant n\} \smallsetminus \{0\}.$$

In order to facilitate readability, we introduce the notation $D_R(n) = D_R(n \times \langle 1\rangle_R)$, and we denote by $\Sigma_n R^2$ the set of the sums of n squares in R, that is, $\Sigma_n R^2 = D_R(n) \cup \{0\}$. We also denote by ΣR^2 the set of all the sums of squares in R, that is, $\Sigma R^2 = \bigcup_{n \in \mathbb{N}} \Sigma_n R^2$.

We are now able to state the following characterisations of isotropy for quadratic forms over a field.

1.1.5 Proposition (First Representation Theorem)**.** *Let K be a field of characteristic different from 2, $a \in K^\times$ and ϕ a regular quadratic form over K. Then $a \in D_K(\phi)$ if and only if $\phi \perp \langle -a\rangle_K$ is isotropic.*

Proof. See [Lam05, Corollary I.3.5 (First Representation Theorem)]. □

Let ϕ, ψ be quadratic forms over R. We say that ψ is a *subform of* ϕ if there exists a quadratic form ψ' over R such that $\phi \simeq \psi \perp \psi'$; in this case we write $\psi \subseteq \phi$. Evidently, if ψ is a subform of ϕ, then $D_R(\psi) \subseteq D_R(\phi)$ and ϕ is isotropic whenever ψ is so.

1.1.6 Proposition. *Let K be a field of characteristic different from 2.*

(a) *A regular binary isotropic quadratic form over K is isometric to the hyperbolic plane.*

(b) *Let ϕ be a regular quadratic form over K. Then ϕ is isotropic if and only if the hyperbolic plane is a subform of ϕ.*

Proof. See [Lam05, Theorem I.3.4]. □

1.1.7 Corollary. *Any regular isotropic quadratic form over a field of characteristic different from 2 is universal.*

Proof. The statement follows trivially from Proposition 1.1.6, together with the fact from Example 1.1.1 (b) that the hyperbolic plane over a field of characteristic different from 2 is universal. □

The next example witnesses that the assumption on the characteristic of the base field in Corollary 1.1.7 is necessary.

1.1.8 Example. Let $\phi = X_1^2 + X_2^2 \in \mathbb{F}_2(t)[X_1, X_2]$. Then $\phi(1,1) = 0$, whereby ϕ is isotropic, but $t \notin D_{\mathbb{F}_2(t)}(\phi)$, whereby ϕ is not universal.

A field extension F/K is called *quadratic* if $[F : K] = 2$. The following two statements are classical results about the behaviour of isotropy of quadratic forms under finite field extensions, and more precisely under odd degree extensions and quadratic extensions.

1.1.9 Theorem (Springer). *Let F/K be a finite field extension of odd degree and let ϕ be a quadratic form over K. If ϕ is anisotropic, then ϕ_F is anisotropic.*

Proof. See [Sp52] or [Lam05, Theorem VII.2.7]. □

1.1.10 Theorem. *Let K be a field of characteristic different from 2, let $d \in K^\times \smallsetminus K^{\times 2}$ and let $F = K(\sqrt{d})$. Let ϕ be an anisotropic quadratic form over K. Then ϕ_F is isotropic if and only if there exists $a \in K^\times$ such that $\langle a, -da\rangle_K$ is a subform of ϕ.*

Proof. See e.g. [Lam05, Theorem VII.3.1]. □

Given four quadratic forms ϕ, ϕ', ψ, ψ' over R, we have that $\phi \perp \psi \simeq \phi' \perp \psi'$ whenever $\phi \simeq \phi'$ and $\psi \simeq \psi'$. In fields of characteristic different from 2 we have also an opposite phenomenon, which is summarised in the following statements due to E. Witt [Wi37].

1.1.11 Theorem (Witt's Cancellation Theorem). *Let K be a field of characteristic different from 2 and let ϕ, ϕ_1, ϕ_2 be regular quadratic forms over K. If $\phi \perp \phi_1 \simeq \phi \perp \phi_2$, then $\phi_1 \simeq \phi_2$.*

Proof. See e.g. [Pfi95, Theorem 2.1.1]. □

1.1.12 Corollary (Witt's Decomposition). *Let K be a field of characteristic different from 2 and ϕ a regular quadratic form over K. Then there exist a unique $i \in \mathbb{N}$ and, up to isometry, a unique anisotropic quadratic form ϕ_0 over K such that $\phi \simeq i \times \langle 1, -1\rangle_K \perp \phi_0$.*

Proof. The existence of such i and ϕ_0 follows from Proposition 1.1.6, and the uniqueness from Theorem 1.1.11. □

Let K be a field of characteristic different from 2. Given two regular quadratic forms ϕ, ψ over K, we say that *ϕ and ψ are Witt equivalent* if there exist an anisotropic quadratic form ϕ_0 over K and $i, j \in \mathbb{N}$ such that $\phi \simeq i \times \langle 1, -1\rangle_K \perp \phi_0$ and $\psi \simeq j \times \langle 1, -1\rangle_K \perp \phi_0$. This defines an equivalence relation on the quadratic forms over K. Denote by WK the set of equivalence classes of regular quadratic forms over K modulo Witt equivalence. The operation $\perp$ induces a group structure on WK having the class of 0 as neutral element, and the operation $\otimes$ turns WK into a commutative ring whose unit element is the class of $\langle 1\rangle_K$; see [Pfi95, Theorem 1.9] for more details. We call *WK the Witt ring of K.*

Assume that $2 \in R^\times$ and let $k \in \mathbb{N}^+$. Given $a_1, \ldots, a_k \in R \smallsetminus \{0\}$, we set

$$\langle\langle a_1, \ldots, a_k\rangle\rangle_R = \langle 1, -a_1\rangle_R \otimes \cdots \otimes \langle 1, -a_k\rangle_R.$$

1.1.13 Remark. Observe that [Pfi95] and [Lam05] use this notation with a different sign convention. Nevertheless, the quadratic forms that can be presented in this way are the same.

Let ϕ be a quadratic form over R and $k \in \mathbb{N}^+$. We say that ϕ is a *k-fold Pfister form over R* if there exist $a_1, \ldots, a_k \in R \smallsetminus \{0\}$ such that $\phi \simeq \langle\langle a_1, \ldots, a_k\rangle\rangle_R$. By convention, we say that ϕ is a *0-fold Pfister form over R* if $\phi \simeq \langle 1\rangle_R$.

1.1.14 Examples. Assume that $2 \in R^\times$. Then we have the following.

(a) The hyperbolic plane $X_1^2 - X_2^2 \in R[X_1, X_2]$ coincides with the quadratic form $\langle 1, -1\rangle_R$, and thus with the Pfister form $\langle\langle 1\rangle\rangle_R$.

(b) Let $k \in \mathbb{N}^+$. In this thesis a fundamental role will be played by the k-fold-Pfister form over R corresponding to the sum of 2^k squares, that is, by

$$2^k \times \langle 1\rangle_R = \langle\langle \underbrace{-1, \dots, -1}_{k \text{ times}} \rangle\rangle_R.$$

The elements that are represented by a Pfister form can be characterised as follows.

1.1.15 Theorem. *Let K be a field of characteristic different from 2 and let ϕ be a Pfister form over K. Then*

$$D_K(\phi) = \{a \in K^\times \mid a\phi \simeq \phi\}.$$

In particular, $D_K(\phi)$ is a subgroup of $K^\times$.

Proof. See e.g. [Lam05, Theorem X.1.8]. □

The following fact is known.

1.1.16 Theorem. *Let K be a field of characteristic different from 2 and $k \in \mathbb{N}$. Then $\Sigma_{2^k} K^2 \smallsetminus \{0\}$ is a subgroup of $K^\times$.*

Proof. Observe that $\Sigma_{2^k} K^2 \smallsetminus \{0\} = D_K(2^k)$. By Theorem 1.1.15 and Example 1.1.14 (b), we have that $D_K(2^k)$ is a subgroup of $K^\times$, whereby the statement. □

Let S/R be a ring extension and let ϕ be a quadratic form over R. We say that ϕ is *hyperbolic over S* if it is isometric to $n \times \langle 1, -1\rangle_S$ over S for some $n \in \mathbb{N}$. Again we adopt a simpler notation when there is no possibility of misunderstanding and write that ϕ is *hyperbolic* if it is hyperbolic over R. It is clear that a hyperbolic form is isotropic. For Pfister forms over a field, the converse also holds.

1.1.17 Theorem. *A Pfister form over a field is hyperbolic if and only if it is isotropic.*

Proof. See [Lam05, Theorem X.1.7] for the non-trivial implication. □

In the sequel, we will use the following known statements about isotropy of Pfister forms.

1.1.18 Theorem. *Let K be a field of characteristic different from 2, let $n \in \mathbb{N}^+$ and let $a, a_1, \dots, a_n \in K^\times$. Then $\langle\langle a_1, \dots, a_n, a\rangle\rangle_K$ is isotropic if and only if a is represented by $\langle\langle a_1, \dots, a_n\rangle\rangle_K$.*

Proof. We set $\phi = \langle\langle a_1, \dots, a_n\rangle\rangle_K$. If $a \in D_K(\phi)$, then it is clear that $\phi \perp \langle -a\rangle_K$ is isotropic; see also Proposition 1.1.5. Since $\phi \perp \langle -a\rangle_K$ is a subform of $\langle\langle a_1, \dots, a_n, a\rangle\rangle_K$, we conclude that the latter is isotropic as well. Vice versa, assume that $\langle\langle a_1, \dots, a_n, a\rangle\rangle_K$ is isotropic. If ϕ is isotropic, then ϕ is universal, by Corollary 1.1.7, and thus there is nothing to show. Assume now that ϕ is anisotropic. Since $\langle\langle a_1, \dots, a_n, a\rangle\rangle_K \simeq \phi \perp -a\phi$, there exist $x, y \in D_K(\phi)$ such that $0 = x - ay$, that is, $a = x/y$. By Theorem 1.1.15, we have that $D_K(\phi)$ is a multiplicative subgroup of $K^\times$. Therefore $a \in D_K(\phi)$. □

1.1.19 Theorem. *Let K be a field of characteristic different from 2, let $d \in K \smallsetminus K^2$ and let $L = K(\sqrt{d})$. Let ϕ be an anisotropic Pfister form over K and let ψ be such that $\phi \simeq \langle 1 \rangle \perp \psi$. Then ϕ_L isotropic if and only if $-d \in D_K(\psi)$.*

Proof. Observe that ψ is unique up to isometry, by Theorem 1.1.11, thus $D_K(\psi)$ does not depend on the choice of ψ. Assume first that ϕ_L is isotropic. Then by Theorem 1.1.10 there exists $a \in K$ such that $\langle a, -da \rangle_K$ is a subform of ϕ. It follows that $a \in D_K(\phi)$ and $a\langle a, -da \rangle_K \simeq \langle 1, -d \rangle_K$ is a subform of $a\phi$. By Theorem 1.1.15, we have that $a\phi \simeq \phi$, thus $\langle 1, -d \rangle_K$ is a subform of $\phi \simeq \langle 1 \rangle_K \perp \psi$. Then $\langle -d \rangle_K$ is a subform of ψ by Theorem 1.1.11, that is, $-d \in D_K(\psi)$. Assume now that $-d \in D_K(\psi)$. Since $d \in L^{\times 2} = D_L(1)$, we obtain that 0 is nontrivially represented by $\langle 1 \rangle_L \perp \psi_L \simeq \phi_L$. □

1.1.20 Corollary. *Let ϕ be a Pfister form over K such that ϕ_L is isotropic for every quadratic field extension L/K. Let ψ be such that $\phi \simeq \langle 1 \rangle \perp \psi$. Then $K \smallsetminus -K^2 \subseteq D_K(\psi)$.*

Proof. Consider $x \in K \smallsetminus -K^2$. Then $-x \notin K^2$, thus $K(\sqrt{-x})/K$ is a quadratic extension. By the hypothesis, it follows that $\phi_{K(\sqrt{-x})}$ is isotropic. Hence $x \in D_K(\psi)$, by Theorem 1.1.19. □

We conclude this section by recalling several classic results of the theory of quadratic forms over polynomial rings. The following statement is known as Cassels-Pfister Theorem. It was proven by Cassels [Cas64] for the quadratic forms corresponding to sums of squares and later generalised by Pfister [Pfi65b] to arbitrary quadratic forms.

1.1.21 Theorem (Cassels-Pfister)**.** *Let K be a field, let $f \in K[X]$ and let ϕ be a regular quadratic form over K. If ϕ represents f over $K(X)$, then ϕ represents f over $K[X]$.*

Proof. See [Lam05, Cassels-Pfister Theorem IX.1.3]. □

1.1.22 Remark. Theorem 1.1.21 does not hold for rings of multivariate polynomials. For instance, the polynomial

$$M(X_1, X_2) = X_1^2 X_2^4 + X_1^4 X_2^2 - 3X_1^2 X_2^2 + 1$$

is represented by the quadratic form $4 \times \langle 1 \rangle$ over the field $\mathbb{R}(X_1, X_2)$, but not over the polynomial ring $\mathbb{R}[X_1, X_2]$. The polynomial M is known as the *Motzkin polynomial*, after T.S. Motzkin, who came up with it in [Mo67].

The following statement shows that any isotropic quadratic form over a given field of characteristic different from 2 remains universal when extended to polynomial rings.

1.1.23 Proposition. *Let K be a field of characteristic different from 2 and let ϕ be a regular isotropic quadratic form over K. Then ϕ_S is universal for any extension S/K of commutative rings.*

Proof. Since ϕ is isotropic over K, it follows by Proposition 1.1.6 that we may choose a quadratic form ψ over K such that $\phi \simeq \langle 1, -1 \rangle_K \perp \psi$. Then

$$f = \left(\frac{f+1}{2} \right)^2 - \left(\frac{f-1}{2} \right)^2 + \psi(0, \ldots, 0) \in D_S(\phi)$$

for every extension S/K and $f \in S \smallsetminus \{0\}$. Therefore ϕ_S is universal. □

Given a nonzero polynomial $f \in R[X]$, we denote by $\mathtt{lc}(f)$ its leading coefficient, that is, $\mathtt{lc}(f) \in R$ such that $f = \mathtt{lc}(f) X^{\deg(f)} + g$, for some $g \in R[X]$ with $\deg(g) < \deg(f)$.

1.1.24 Theorem. *Let K be a field of characteristic different from 2, ϕ a Pfister form over K and $f \in K[X] \smallsetminus \{0\}$. Then $f \in D_{K[X]}(\phi)$ if and only if $\mathtt{lc}(f) \in D_K(\phi)$ and $\phi_{K[X]/(p)}$ is isotropic for every irreducible factor p of f with odd multiplicity.*

Proof. The statement follows from Theorem 1.1.17 and Theorem 1.1.21, together with [Lam05, Theorem X.2.13]. □

1.2 Sums of squares and real fields

In this section, we introduce the reader to the basics of sums of squares in fields. We explore their connections with real fields, and thus to orderings on fields. In this section we largely rely on [Lam05], [Pfi95] and [Pre84].

Let R be a commutative ring. In the context of the study of sums of squares in R, one may wonder how many squares are necessary to represent an arbitrary sum of squares in R, and if there exists $m \in \mathbb{N}$ such that all sums of squares in R can be represented as sums of m squares in R. In order to investigate these questions, we introduce the following (standard) notations.

We say that R is *pythagorean* if $\Sigma R^2 = R^2$. This is equivalent to having $\Sigma_2 R^2 = R^2$, that is, every couple of elements in R can be extended to a pythagorean triple.

Given $x \in R$, we denote by $\ell_R(x)$ *the length of x in R*, which we define as

$$\ell_R(x) = \mathsf{inf}\{k \in \mathbb{N} \mid x \in \Sigma_k R^2\} \in \mathbb{N} \cup \{\infty\}.$$

Here we are only interested in distinguishing elements of finite length from elements of infinite length, hence ∞ is simply a symbol denoting infinity. The same convention is used in the following definitions. We set

$$\begin{aligned} p(R) &= \mathsf{sup}\{\ell_R(x) \mid x \in \Sigma R^2\} \ \in \mathbb{N} \cup \{\infty\} \text{ and} \\ s(R) &= \ell_R(-1) \quad \in \mathbb{N} \cup \{\infty\}. \end{aligned}$$

We call $p(R)$ the *Pythagoras number of R*. The name Pythagoras number is motivated by the fact that R is pythagorean if and only if $p(R) = 1$. We also call $s(R)$ the *level of R* (the notation $s(R)$ for the level of R comes indeed from the German word *Stufe*, from which the English term was inspired). Observe that

$$\begin{aligned} p(R) &= \mathsf{inf}\{k \in \mathbb{N} \mid \Sigma R^2 = \Sigma_k R^2\} \text{ and} \\ s(R) &= \mathsf{inf}\{k \in \mathbb{N} \mid -1 \in \Sigma_k R^2\}, \end{aligned}$$

whereby $s(R) = \infty$ if and only if $-1 \notin \Sigma R^2$. If R is a field, we call R *real* if $-1 \notin \Sigma R^2$, and *nonreal* otherwise.

1.2.1 Remarks. (*a*) In any nontrivial ring R we have $\ell_R(1) = 1$, and thus $p(R) \geqslant 1$.

(*b*) For an extension of commutative rings S/R we have $s(S) \leqslant s(R)$, by definition.

(*c*) For every field K of characteristic 2 we have $p(K) = s(K) = 1$. In view of this, in the sequel we will focus on fields of characteristic different from 2.

1.2.2 Examples. (*a*) $p(\mathbb{R}) = p(\mathbb{C}) = s(\mathbb{C}) = 1$, $s(\mathbb{R}) = \infty$.

(*b*) Let K be a finite field of odd cardinality. Then $s(K) = 1$ if $|K| \equiv 1 \bmod 4$, and $s(K) = 2$ otherwise. Furthermore, $p(K) = 2$. See [Pfi95, Examples 3.1.2 and 7.1.2].

The Pythagoras number of $\mathbb{Q}$ was computed in [Eu51, 98. Theorem 20, Coroll. 1] by Euler. Note that this was shown before Lagrange's Four Squares Theorem from [Lag70] stating that $p(\mathbb{Z}) = 4$, for which one needs a more refined argument.

1.2.3 Theorem (Euler)**.** *$p(\mathbb{Q}) = 4$.*

Proof. See e.g. [Lam05, Theorem XI.1.4]. □

It is natural to introduce the Pythagoras number and the level in the context of arbitrary commutative rings. Nevertheless, their behaviour in the setting of fields is significantly different from the general one, and the techniques that are used in their analysis are also somewhat different. In this dissertation we focus on the Pythagoras number (and incidentally the level) of fields. More details about the level and the Pythagoras number of a commutative ring that is not a field can be found e.g. in [CDLR82] or [Pfi95, §3.2 and 7.2].

As witnessed by the following known statement, the level and the Pythagoras number of nonreal fields are tightly related.

1.2.4 Proposition. *Let K be a nonreal field. Then we have $s(K) \leqslant p(K) \leqslant s(K) + 1$. If, furthermore, $\mathsf{char}(K) \neq 2$, then $K = \Sigma K^2 = \Sigma_{s(K)+1} K^2$.*

Proof. If $\mathsf{char}(K) = 2$, then $s(K) = p(K) = 1$, trivially. Otherwise, the statement follows directly from the identity

$$x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2,$$

which holds for every $x \in K$. □

1.2.5 Corollary. *Let K be a field with $\mathsf{char}(K) \neq 0$. Then $s(K) \leqslant 2$ and $K = \Sigma_3 K^2$.*

Proof. Set $p = \mathsf{char}(K)$. Recall from Example 1.2.2 (b) that $s(\mathbb{F}_p) \leqslant 2$. Since $\mathbb{F}_p \subseteq K$, we have $s(K) \leqslant s(\mathbb{F}_p) \leqslant 2$. Hence $K = \Sigma_3 K^2$, by Proposition 1.2.4. □

In view of Proposition 1.2.4, it is natural to wonder which pairs $(n, n), (n, n+1)$ for $n \in \mathbb{N}$ can be obtained as $(s(K), p(K))$ for a field K. The following statement shows that $s(K)$ can only assume certain values.

1.2.6 Theorem (Pfister)**.** *Let K be a nonreal field. Then there exists $n \in \mathbb{N}$ such that*

$$s(K) = 2^n.$$

Proof. See [Pfi95, Theorem 3.1.3]. □

As a consequence of Proposition 1.2.4 and Theorem 1.2.6, the Pythagoras number of a nonreal field is always a power of 2 or a power of 2 plus one. The following statement shows that any power of 2 is the level of a field.

1.2.7 Theorem. *Let $n \in \mathbb{N}^+$ and let K be a real field. Set $d = X_1^2 + \ldots + X_{2^n}^2$ and $F = K(X_1, \ldots, X_{2^n})(\sqrt{-d})$. Then*

$$s(F) = 2^n.$$

Proof. See e.g. [Pfi95, Theorem 3.1.4]. □

1.2.8 Proposition. *Let K be a field. Then $s(K) = s(K(X))$. Furthermore, if K is nonreal and $\mathsf{char}(K) \neq 2$, then we have that $p(K(X)) = s(K) + 1$, and there exists an algebraic field extension L/K such that $p(L) = s(L) = s(K)$.*

Proof. See [Pfi95, Example 3.1.2 (9) and Proposition 7.1.5]. □

It follows by Theorem 1.2.7 and Proposition 1.2.8 that for $n \in \mathbb{N}$ there exist fields K, L such that $(s(K), p(K)) = (2^n, 2^n)$ and $(s(L), p(L)) = (2^n, 2^n + 1)$. This concludes the study of the Pythagoras number of nonreal fields. In the following two statements, which will be used in Section 6.2, we briefly study the level of products of fields. These results should be know to experts of the subject.

1.2.9 Lemma. *Let $n \in \mathbb{N}^+$ and let $K_1, \dots, K_n$ be fields. Then*

$$s(K_1 \times \cdots \times K_n) = \mathsf{max}\{s(K_1), \dots, s(K_n)\} \in \{\infty\} \cup \{2^n \mid n \in \mathbb{N}\}.$$

Proof. Set $s = s(K_1 \times \cdots \times K_n)$ and $m = \mathsf{max}\{s(K_1), \dots, s(K_n)\}$. We show first that $s \geqslant m$. If $s = \infty$, this is trivial. Assume that $s < \infty$ and let $\mathbf{x}_1, \dots, \mathbf{x}_s \in K_1 \times \cdots \times K_n$ be such that $\mathbf{x}_1^2 + \ldots + \mathbf{x}_s^2 = -1$ in $K_1 \times \cdots \times K_n$. Consider now $1 \leqslant i \leqslant n$ and let $\pi_i : K_1 \times \cdots \times K_n \to K_i$ be the i-th projection. For $1 \leqslant j \leqslant s$, set $y_j = \pi_i(\mathbf{x}_j) \in K_i$. Since $\mathbf{x}_1^2 + \ldots + \mathbf{x}_s^2 = -1$ in $K_1 \times \cdots \times K_n$, we have that $y_1^2 + \ldots + y_s^2 = -1$ in K_i, whereby $s(K_i) \leqslant s$. Since this holds for $1 \leqslant i \leqslant n$, we conclude that $s \geqslant m$.

We show now that $m \geqslant s$. If $m = \infty$, this is trivial, thus we may assume that $s < \infty$. For any $1 \leqslant i \leqslant n$, let $x_{i1}, \dots, x_{im}$ be such that $x_{i1}^2 + \ldots + x_{im}^2 = -1$. For $1 \leqslant j \leqslant m$, we set $x_j = (x_{1j}, \dots, x_{nj})$. Then $x_1^2 + \ldots + x_m^2 = -1$ in $K_1 \times \cdots \times K_n$, whereby $m \geqslant s$. □

We say that a polynomial is *square-free* if it is not divisible by the square of any nonconstant polynomial.

1.2.10 Proposition. *Let K be a field, $k \in \mathbb{N}$ and $F, G \in K[X]$ square-free such that $\mathtt{lc}(G) \in \Sigma_{2^k} K^2$. Assume that $F \in \Sigma_{2^k} K[X]^2$ and $K[X]/(F) \simeq K[X]/(G)$ as K-algebras. Then $G \in \Sigma_{2^k} K[X]^2$.*

Proof. If $k = 0$, then $F, G \in K^\times$, and the statement is trivial. Assume now $k \geqslant 1$. Since $F \in \Sigma_{2^k} K[X]^2$, we have $s(K[X]/(F)) < 2^k$. Thus $s(K[X]/(F)) \leqslant 2^{k-1}$, by Theorem 1.2.6. Consider an irreducible factor H of G. By Lemma 1.2.9, we have that $s(K[X]/(H)) \leqslant s(K[X]/(G)) \leqslant 2^{k-1}$. Denoting by ϕ the k-fold Pfister form $\langle\langle -1, \dots, -1 \rangle\rangle_{K[X]/(F)}$, this implies that ϕ is isotropic over $K[X]/(H)$. Since this holds for any monic irreducible factor of G and since $\mathtt{lc}(G) \in (\Sigma_{2^k} K^2)^\times = D_K(\phi)$, we conclude by Theorem 1.1.24 that $G \in D_{K(X)}(\phi)$. Hence $G \in D_{K[X]}(\phi)$, by Theorem 1.1.21. □

In the rest of this thesis we will focus on the study of sums of squares in real fields. It is known that real fields are the ones that can be endowed with an ordering.

Let K be a field. By a *preordering on K* we mean a subset $P \subseteq K$ such that $K^2 \subseteq P$, $P + P \subseteq P$, $P \cdot P \subseteq P$ and $-1 \notin P$. In certain sources, including [Pre84], preorderings are called *prepositive cones.*

1.2.11 Proposition. *Let K be a field. Then K is real if and only if ΣK^2 is a preordering on K.*

Proof. It is straightforward that $K^2 \subseteq \Sigma K^2$, $\Sigma K^2 + \Sigma K^2 \subseteq \Sigma K^2$ and $\Sigma K^2 \cdot \Sigma K^2 \subseteq \Sigma K^2$. Furthermore, K is real if and only if $-1 \notin \Sigma K^2$, whereby the statement. □

1.2.12 Remark. Let K be a field. If K is real, it follows by Proposition 1.2.11 that ΣK^2 is the minimal preordering on K with respect to inclusion. In other words, any preordering on K contains ΣK^2, and there exists a preordering on K if and only if K is real. In particular, only fields of characteristic 0 may admit a preordering; all other fields are nonreal.

Let K be a field and let P be a preordering on K. Given $a, b \in K$, we write $a \leqslant_P b$ whenever $b - a \in P$. Then $\leqslant_P$ constitutes a binary relation on K.

1.2.13 Proposition. *Let K be a field and let P be a preordering on K. Then $\leqslant_P$ is a partial order on K. Furthermore, for every $a, b, c \in K$ such that $a \leqslant_P b$, we have that $a + c \leqslant_P b + c$ and, if $0 \leqslant_P c$, we have that $ac \leqslant_P bc$.*

Proof. The binary relation $\leqslant_P$ is reflexive because $0 \in P$. Assume now that $b \leqslant_P a$. Then $-(a-b)^2 = (a-b)(b-a) \in P$. If $a - b \neq 0$, then $-(a-b)^2/(a-b)^2 \in P$, which contradicts the assumption that $-1 \notin P$. Therefore $a - b \notin K^\times$, that is, $a = b$. Thus $\leqslant_P$ is antisymmetric. If $b \leqslant_P c$, then $c - a = (c - b) + (b - a) \in P$, hence $\leqslant_P$ is transitive. Therefore $\leqslant_P$ is a partial order on K. Finally, we have that $a + c \leqslant_P b + c$ because $P + P \subseteq P$ and, if $c \geqslant_P 0$, we have that $ac \leqslant_P bc$ because $P \cdot P \subseteq P$. □

Let K be a field. An *ordering on K* (also a *positive cone of K*) is a preordering on K that is maximal with respect to inclusion. Given a preordering P on K, it is elementary to show that P is an ordering if and only if $P \cup -P = K$ [Lam05, Corollary VIII.9.4 (1)], or equivalently, if and only if $\leqslant_P$ is a total order on K.

1.2.14 Examples. (*a*) $\mathbb{R}^2$ is an ordering on $\mathbb{R}$. The total order $\leqslant_{\mathbb{R}^2}$ is the natural order relation on $\mathbb{R}$, and is the unique ordering on $\mathbb{R}$.

(*b*) $\Sigma\mathbb{Q}^2$ is an ordering on $\mathbb{Q}$. The total order $\leqslant_{\Sigma\mathbb{Q}^2}$ is the natural order relation on $\mathbb{Q}$.

(*c*) Let $K = \mathbb{Q}(\sqrt{2})$ and set $P = \Sigma K^2$. Then P is a preordering on K, but not an ordering. One can show that $0 \not\leqslant_P \sqrt{2} \not\leqslant_P 0$.

A standard application of Zorn's Lemma shows that any preordering on K is contained in an ordering on K. Together with Proposition 1.2.11, this can be seen as part of the following statement from [AS27], known as Artin-Schreier's Criterion.

1.2.15 Theorem (Artin-Schreier)**.** *For a field K, the following are equivalent:*

(*i*) *K is real.*

(*ii*) *ΣK^2 is a preordering on K.*

(*iii*) *There exists an ordering on K.*

Proof. The equivalence between (*i*) and (*ii*) has already been given in Proposition 1.2.11. See [Lam05, Theorem VIII.1.10] for the equivalence between (*i*) and (*iii*). □

Furthermore, the following statement shows that we can recover preorderings on a field from its orderings.

1.2.16 Theorem (Artin)**.** *Let K be a field and let P be a preordering on K. Then*

$$P = \bigcap \{Q \subseteq K \mid Q \text{ ordering on } K \text{ and } P \subseteq Q\}.$$

In particular, ΣK^2 is the intersection of all orderings on K.

Proof. See [Lam05, Theorem VIII.9.6]. □

Let K be a real field, let $n \in \mathbb{N}^+$ and let ϕ be an n-ary quadratic form over K. We say that ϕ is *positive definite* if $\phi(\mathbf{x}) >_P 0$ for every ordering P on K and for every nonzero vector $\mathbf{x} \in K^{(n)}$. In view of Theorem 1.2.16, this amounts to having $\phi(\mathbf{x}) \in (\Sigma K^2)^\times$ for every nonzero vector $\mathbf{x} \in K^{(n)}$.

Let K be a field. We say that K is *real closed* if K is real and if every proper finite field extension of K is nonreal. The following statement lists some of the most common characterisations of real closed fields.

1.2.17 Theorem. *Let K be a field. Then the following are equivalent:*

(*i*) *K is real closed.*

(*ii*) *K is real, $|K^\times/K^{\times 2}| = 2$ and any odd degree polynomial in $K[X]$ has a root in K.*

(*iii*) *$K(\sqrt{-1})$ is algebraically closed, but K is not.*

Proof. See [Lam05, Theorem VIII.2.5]. □

1.2.18 Corollary. *Let K be a real closed field. Then K^2 is an ordering on K.*

Proof. By Theorem 1.2.17, we have $K^\times = K^{\times 2} \cup -K^{\times 2}$ and $K^{\times 2} \cap -K^{\times 2} = \emptyset$, whereby we obtain the statement. □

Let K be a real closed field. It follows by Corollary 1.2.18 that $\leqslant_{K^2}$ is a total order relation on K; we denote it by $\leqslant_K$ and we call it *the order on K*.

Let ϕ be a quadratic form over K. By Sylvester's law [Lam05, Proposition II.3.2 (3)], there exist unique $n_+, n_- \in \mathbb{N}$ such that $\phi \simeq n_+ \times \langle 1 \rangle \perp n_- \times \langle -1 \rangle$; we call $n_+ \times \langle 1 \rangle$ *the positive definite part of ϕ* and $n_- \times \langle -1 \rangle$ *the negative definite part of ϕ*. Note that n_+, n_- depend on ϕ, and that $n_+ \times \langle 1 \rangle$ of a quadratic form is indeed positive definite when nonzero.

1.2.19 Example. The field $\mathbb{R}$ is real closed. The field $\mathbb{Q}$ is not real closed. One can show that the real algebraic numbers are the smallest real closed field containing $\mathbb{Q}$; see e.g. [Pfi95, Example 6.1.18].

1.3 The Principal Axis Theorem

Let $n \in \mathbb{N}^+$ and let K be a field of characteristic different from 2. Recall from Section 1.1 that any regular quadratic form in $K[X_1, \ldots, X_n]$ may be diagonalised by applying a K-linear automorphism of the underlying K-vector space $K^{(n)}$, that is, up to a change of basis of $K^{(n)}$. It is known that two positive definite quadratic forms over a real closed field can be simultaneously diagonalised -actually it is enough that one of the two is positive definite; see the Principal Axis Theorem (Theorem 1.3.2)-. This will help our work with products of positive definite quadratic forms in Section 1.4. In this section, we discuss over which fields a simultaneous diagonalisation of two quadratic forms one of which is positive definite can be obtained.

Let $n \in \mathbb{N}^+$ and let ϕ be an n-ary quadratic form over K. We may associate to ϕ the symmetric bilinear form $b_\phi : K^{(n)} \times K^{(n)} \to K$ defined by setting

$$b_\phi(\mathbf{x}, \mathbf{y}) = (\phi(\mathbf{x} + \mathbf{y}) - \phi(\mathbf{x}) - \phi(\mathbf{y}))/2$$

for any $\mathbf{x}, \mathbf{y} \in K^{(n)}$. We call b_ϕ *the symmetric bilinear form associated to* ϕ. Conversely, to any symmetric bilinear form $b : K^{(n)} \times K^{(n)} \to K$, we may associate the quadratic form $\phi_b : K^{(n)} \to K$ defined by $\phi_b(\mathbf{x}) = b(\mathbf{x}, \mathbf{x})$ for every $\mathbf{x} \in K^{(n)}$. These two procedures are the inverse to one another. We may thus inspect quadratic forms over K by studying the corresponding symmetric bilinear forms. We may also translate quadratic forms into matrices as follows. For $i, j \in \{1, \dots, n\}$, let $a_{ij} \in K$ be such that $\phi = \sum_{1 \leqslant i,j \leqslant n} a_{ij} X_i X_j$. Let further $A_\phi \in \mathsf{M}_n(K)$ be the $n \times n$ symmetric matrix

$$A_\phi = ((a_{ij} + a_{ji})/2)_{1 \leqslant i,j \leqslant n},$$

which we call *the symmetric matrix associated to* ϕ. Vice versa, given a symmetric matrix $A = (a_{ij})_{1 \leqslant i,j \leqslant n} \in \mathsf{M}_n(K)$, we define the *quadratic form associated to* A as $\phi_A(X_1, \dots, X_n) = \sum_{i,j=1}^n a_{ij} X_i X_j$. Then $\phi_A(\mathbf{x}) = \mathbf{x}^t A_\phi \mathbf{x}$ for every $\mathbf{x} \in K^{(n)}$.

Let $\mathfrak{B}$ be a K-basis of $K^{(n)}$. We say that $\mathfrak{B}$ *is orthogonal with respect to* ϕ, or that $\mathfrak{B}$ *is an orthogonal basis for* ϕ, if $M^t A_\phi M$ is diagonal, where M is the matrix associated to the base change from the canonical basis of $K^{(n)}$ to $\mathfrak{B}$. Given another n-ary quadratic form ψ over K, we say that the pair (ϕ, ψ) *can be simultaneously diagonalised* if there exists a K-basis of $K^{(n)}$ that is orthogonal with respect to both ϕ and ψ.

1.3.1 Example. Let $(\mathbf{e}_1, \mathbf{e}_2)$ be the canonical $\mathbb{R}$-basis of $\mathbb{R}^{(2)}$, that is, $\mathbf{e}_1 = (1, 0)$ and $\mathbf{e}_2 = (0, 1)$. Set

$$\phi = \tfrac{3}{4} X_1^2 + \tfrac{1}{2} X_1 X_2 + \tfrac{3}{4} X_2^2 \in \mathbb{R}[X_1, X_2] \text{ and } \psi = 4 X_1 X_2 \in \mathbb{R}[X_1, X_2].$$

Then we have

$$A_\phi = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 3/4 \end{pmatrix} \text{ and } A_\psi = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}.$$

Set $\mathfrak{b}_1 = (1, 1)$, $\mathfrak{b}_2 = (1, -1)$ and let $\mathfrak{B} = (\mathfrak{b}_1, \mathfrak{b}_2)$. Let $M \in \mathsf{M}_2(\mathbb{R})$ be the matrix associated to the base change from $(\mathbf{e}_1, \mathbf{e}_2)$ to $\mathfrak{B}$. A simple computation shows that

$$M^t A_\phi M = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } M^t A_\psi M = \begin{pmatrix} 4 & 0 \\ 0 & -4 \end{pmatrix},$$

whereby $\mathfrak{B}$ is orthogonal with respect to both ϕ and ψ. As a matter of fact, under the basis $\mathfrak{B}$ (that is, after the substitution $Y_1 = X_1 + X_2$ and $Y_2 = X_1 - X_2$), we may write $\phi(Y_1, Y_2) = 2Y_1^2 + Y_2^2$ and $\psi(Y_1, Y_2) = 4Y_1^2 - 4Y_2^2$.

The fact that ϕ and ψ from Example 1.3.1 can be simultaneously diagonalised is a special case of the following more general phenomenon, known as *Principal Axis Theorem.*

1.3.2 Theorem (Principal Axis Theorem)**.** *Let K be a real closed field, let $n \in \mathbb{N}^+$ and let $\phi, \psi \in K[X_1, \dots, X_n]$ be quadratic forms. Suppose that ϕ is positive definite. Then there exists a basis of $K^{(n)}$ that is orthogonal with respect to both ϕ and ψ.*

Proof. See [Lan02, Corollary XV.7.3] for the case $K = \mathbb{R}$; the very same argument carries through whenever K is real closed. □

1.3.3 Remark. Let K be a real closed field, $n \in \mathbb{N}^+$ and $\phi, \psi \in K[X_1, \dots, X_n]$ quadratic forms with ϕ positive definite. By Theorem 1.3.2 we may assume, after a change of basis, that $\phi = X_1^2 + \ldots + X_n^2$ and $\psi = a_1 X_1^2 + \ldots + a_n X_n^2$ for some $a_1, \dots, a_n \in K$.

The Principal Axis Theorem can actually be proven under milder assumptions. In particular, the hypothesis that K is real closed can be weakened. In order to do this, we introduce PAP-fields. Given a field K, we say that K *has the Principal Axis Property* or, in short, that K *is a PAP-field*, if for every $n \in \mathbb{N}^+$ and every symmetric $A \in \mathsf{M}_n(K)$ there exist $B, M \in \mathsf{M}_n(K)$ such that B is diagonal, M is orthogonal and $A = M^t \cdot B \cdot M$.

PAP-fields are exactly the fields to which the Principal Axis Theorem can be extended. This was shown by W. C. Waterhouse in [Wa76] for fields of characteristic different from 2 and by A. Charnow and E. Charnow in [CC86] in arbitrary characteristic. Nevertheless, in view of the following statement, only real fields can be PAP-fields.

1.3.4 Proposition. *A PAP-field is real and pythagorean.*

Proof. This follows for example from [MSV93, Lemma 1]. □

1.3.5 Theorem. *Let K be a real field. Then the following are equivalent:*

(*i*) *K is a PAP-field.*

(*ii*) *K is the intersection of its real closed field extensions.*

(*iii*) *Every symmetric matrix over K has an eigenvalue over K.*

(*iv*) *For every $n \in \mathbb{N}^+$, every pair of n-ary quadratic forms over K with one of the two positive definite can be simultaneously diagonalised.*

Proof. See [Wa76, Theorem 2]. □

1.3.6 Corollary. *Let K be a PAP-field, let $n \in \mathbb{N}^+$ and let $\phi, \psi \in K[X_1, \ldots, X_n]$ be quadratic forms such that ϕ is positive definite. Set $\mathbf{X} = (X_1, \ldots, X_n)^t$. Then there exists an invertible matrix $M \in \mathsf{M}_n(K)$ such that $\phi(M \cdot \mathbf{X}) = X_1^2 + \ldots + X_n^2$ and $\psi(M \cdot \mathbf{X})$ is diagonal.*

Proof. Consider the symmetric matrices A_ϕ, A_ψ associated to ϕ, ψ respectively. By Theorem 1.3.5, there exists a K-basis $\mathfrak{B}$ of $K^{(n)}$ which is orthogonal with respect to both ϕ and ψ, and thus an invertible matrix $A \in \mathsf{M}_n(K)$ such that $A^t A_\phi A$ and $A^t A_\psi A$ are diagonal. Let T_A be the endomorphism of $K^{(n)}$ defined by setting $T_A(\mathbf{x}) = A\mathbf{x}$ for every $\mathbf{x} \in K^{(n)}$, and set $\phi' = \phi \circ T_A$. Consider $1 \leqslant i \leqslant n$ and set $a_i = (A^t A_\phi A)_{ii}$. Observe that $a_i = \phi'(\mathbf{e}_i)$ where $\mathbf{e}_i$ is the i-th vector of the canonical basis of $K^{(n)}$. Hence $a_i \in D_K(\phi') = D_K(\phi)$. Since K is real and ϕ is positive definite, we obtain $a_i \in (\Sigma K^2)^\times$. Therefore $a_i \in K^{\times 2}$, by Proposition 1.3.4. Let $b_i \in K^\times$ be such that $a_i = b_i^2$. Let B be the diagonal matrix such that $B_{ii} = b_i^{-1}$ for any $1 \leqslant i \leqslant n$ and set $M = BA$. Since B is diagonal, we have that $\phi(M \cdot \mathbf{X}) = X_1^2 + \ldots + X_n^2$ and that $\psi(M \cdot \mathbf{X})$ is diagonal. □

1.3.7 Corollary. *Let K be a PAP-field and $n \in \mathbb{N}^+$. Let further $\phi, \psi \in K[X_1, \ldots, X_n]$ be quadratic forms such that ϕ is positive definite and let $\leqslant$ be an ordering on K. Set $\mathbf{X} = (X_1, \ldots, X_n)^t$. Then there exists $M \in \mathsf{M}_n(K)$ invertible and $a_1, \ldots, a_n \in K$ such that $\phi(M \cdot \mathbf{X}) = X_1^2 + \ldots + X_n^2$, $\psi(M \cdot \mathbf{X}) = a_1 X_1^2 + \ldots + a_n X_n^2$ and $a_{i+1} \leqslant a_i$ for every $1 \leqslant i \leqslant n - 1$.*

Proof. In view of Corollary 1.3.6, there exist an orthogonal matrix $M \in \mathsf{M}_n(K)$ and $a_1, \ldots, a_n \in K$ such that $\phi(M \cdot \mathbf{X}) = X_1^2 + \ldots + X_n^2$ and $\psi(M \cdot \mathbf{X}) = a_1 X_1^2 + \ldots + a_n X_n^2$. Since $\leqslant$ is a total order on K, we may simply permute the variables in order to obtain that $a_{i+1} \leqslant a_i$ for every $1 \leqslant i \leqslant n - 1$. □

1.3.8 Example. Let $\phi, \psi \in \mathbb{R}[X_1, X_2]$ be as in Example 1.3.1; we have seen there that $\phi = 2Y_1^2 + Y_2^2$ and $\psi = 4Y_1^2 - 4Y_2^2$, up to a change of basis. In particular, it is clear that ϕ is positive definite. In view of Corollary 1.3.7, it is possible to orthonormalize ϕ via a change of basis that keeps ψ diagonal. More precisely, the substitution $Z_1 = Y_1/\sqrt{2}$ and $Z_2 = Y_2$ allows us to write $\phi(Z_1, Z_2) = Z_1^2 + Z_2^2$ and $\psi(Z_1, Z_2) = 2Z_1^2 - 4Z_2^2$.

1.3.9 Remark. Let K be a PAP-field that is not real closed. Then K has multiple orderings, and it is in general not possible to order elements simultaneously with respect to all of its orderings; this prevents us to order the a_i's in Corollary 1.3.7 simultaneously with respect to multiple orderings. This is the only obstruction that prevents us from formulating all of our results in the following section for a PAP-field instead of real closed field; cf. Question 1.4.17.

1.3.10 Example. As an example of the phenomenon described in Remark 1.3.9, let K be the intersection of two minimal real closed field extensions of $\mathbb{Q}(\sqrt{2})$ and let $a_1 = \sqrt{2}$, $a_2 = -\sqrt{2}$. Then K has precisely two orderings $\leqslant_1, \leqslant_2$ such that $0 <_1 a_1$, $0 <_2 a_2$; see [Lam05, p. 243,244]. Then $a_2 <_1 a_1$, but $a_1 <_2 a_2$.

1.4 Products of two quadratic forms

Products of sums of squares have been studied for a long time, with the first results dating back to the 3rd century a.D., when Diophantus of Alexandria wrote his treatise Arithmetica; in the 19th problem of its third book (see [He81] for an English translation of the original problem), Diophantus showed the following identity:

$$(x_1^2 + x_2^2) \cdot (y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2. \tag{1.4.1}$$

Diophantus' formula is also referred to as Brahmagupta–Fibonacci identity, from the names of the mathematicians who respectively re-discovered it and re-introduced it to Europe centuries later, and can be easily verified to hold in any commutative ring.

In 1748 [Eu48] Euler found an analogous formula for products of sums of 4 squares, which now carries his name, and around 1818, F. Degen [De22] detected an analogous identity for products of sums of 8 squares. A couple of decades later, the latter was rediscovered independently by J.T. Graves and by A. Cayley, and is nowadays usually referred to as Degen or Degen-Cayley identity.

It is natural to look for generalisations of such identities; this is known as Hurwitz' problem, from the mathematician A. Hurwitz, who showed in 1898 [Hur98] that an identity for products of sums of n squares analougous to Equation (1.4.1) can only exist for sums of $1, 2, 4$, or 8 squares. More precisely, Hurwitz showed that, given a field K of characteristic different from 2 and $n \in \mathbb{N}^+$, if there exist n quadratic forms $f_1, \dots, f_n \in K[X_1, \dots, X_n, Y_1, \dots, Y_n]$ that are linear in the X_i's and in the Y_i's and such that

$$(X_1^2 + \ldots + X_n^2)(Y_1^2 + \ldots + Y_n^2) = f_1^2 + \ldots + f_n^2, \tag{1.4.2}$$

then $n \in \{1, 2, 4, 8\}$.

A few years later, Hurwitz himself [Hur22] and (independently) J. Radon [Ra22] showed that similar formulas can be obtained in a slightly different situation, namely when sums of squares of different lengths are multipied.

Given $n \in \mathbb{N}$, we let $a, b, c \in \mathbb{N}$ be the unique numbers such that c is odd, $n = 2^{(4a+b)}c$ and $0 \leqslant b \leqslant 3$; we also set $\rho(n) = 8a + 2^b$. This association defines a function $\rho : \mathbb{N} \to \mathbb{N}$, called the *Hurwitz-Radon function.*

1.4.3 Theorem (Hurwitz-Radon)**.** *Let K be a field of characteristic different from 2 and let $r, n \in \mathbb{N}^+$. Then there exist n quadratic forms $f_1, \ldots, f_n \in K[X_1, \ldots, X_r, Y_1, \ldots, Y_n]$ that are linear in the X_i's and in the Y_j's and such that*

$$(X_1^2 + \ldots + X_r^2)(Y_1^2 + \ldots + Y_n^2) = f_1^2 + \ldots + f_n^2$$

if and only if $r \leqslant \rho(n)$.

Proof. See [Lam05, Theorem V.5.11]. □

Even when explicit identities for products of sums of squares are not available, it is still possible, at least in certain situations, to find upper bounds for the number of squares necessary to write the product of two sums of squares as a sum of squares. An example of this phenomenon can be obtained from Hilbert's famous theorem stating that all positive definite ternary forms of degree 4 with real coefficients are sums of 3 squares; see [Hi88]. This implies that for every $l_1, l_2, l_3 \in \mathbb{R}[X_1, X_2, X_3]$ that are linear in the X_i's, there exist quadratic forms $f_1, f_2, f_3 \in \mathbb{R}[X_1, X_2, X_3]$ such that

$$(X_1^2 + X_2^2 + X_3^2)(l_1^2 + l_2^2 + l_3^2) = f_1^2 + f_2^2 + f_3^2, \tag{1.4.4}$$

though the corresponding identity of the form 1.4.2 does not exist, by Hurwitz's theorem.

An elementary proof of the existance of the identities (1.4.4) due to C. Scheiderer [Sche10, §9] inspired our results on products of positive definite quadratic forms over real closed fields, which take the remainder of this section.

Let $n \in \mathbb{N}^+$, let K be a real closed field, and let $\phi_1, \phi_2 \in K[X_1, \ldots, X_n]$ be positive definite quadratic forms. Since $\phi_1, \phi_2 \in \Sigma_n K[X_1, \ldots, X_n]^2$, it follows by Theorem 1.1.16 that $\phi_1 \cdot \phi_2 \in \Sigma_{2^k} K(X_1, \ldots, X_n)^2$, where $k \in \mathbb{N}$ is the minimal integer such that $2^k \geqslant n$. In the following, we improve this bound and show that $\phi_1 \cdot \phi_2 \in \Sigma_m K(X_1, \ldots, X_n)^2$ for $m < 2^k$, under certain conditions on n.

Let K be a field of characteristic different from 2, let $n \in \mathbb{N}^+$ and let ϕ be an n-ary quadratic form over K. Recall that b_ϕ denotes the symmetric bilinear form corresponding to ϕ. Given $m \in \mathbb{N}$ and $\mathbf{u}_1, \ldots, \mathbf{u}_m \in K^{(n)}$, we say that $\mathbf{u}_1, \ldots, \mathbf{u}_m$ are *orthogonal with respect to ϕ* if $b_\phi(\mathbf{u}_i, \mathbf{u}_j) = 0$ for every $i, j \in \{1, \ldots, m\}$ with $i \neq j$. Note that of a K-basis of $K^{(n)}$ that is orthogonal with respect to ϕ is precisely an orthogonal K-basis for ϕ as defined in Section 1.3. As a consequence, the existence of such a basis is equivalent to the existence of a diagonalisation of A_ϕ.

1.4.5 Theorem. *Let K be a real closed field, $n \in \mathbb{N}^+$ and $\phi_1, \phi_2 \in K[X_1, \ldots, X_n]$ two quadratic forms such that ϕ_1 is positive definite. Let $\lambda \in K^\times$ and set $\phi = \phi_2 - \lambda\phi_1$. Let further $s, t \in \mathbb{N}$ be such that $\phi \simeq s \times \langle 1 \rangle \perp t \times \langle -1 \rangle$ and denote $N = n - \mathsf{max}\{s, t\}$. Then there exists N nonzero vectors in $K^{(n)}$ that are orthogonal with respect to ϕ_1, ϕ_2 and isotropic with respect to ϕ.*

Proof. Let T be a K-automorphism of $K^{(n)}$, let $k \in \mathbb{N}^+$ and $\mathbf{v}_1, \ldots, \mathbf{v}_k \in K^{(n)}$. For $i \in \{1, 2\}$, it is clear from the definitions that $\mathbf{v}_1, \ldots, \mathbf{v}_k$ are orthogonal with respect to $\phi_i \circ T$ if and only if $T^{-1}(\mathbf{v}_1), \ldots, T^{-1}(\mathbf{v}_k)$ are orthogonal with respect to ϕ_i. Similarly, $\mathbf{v}_1, \ldots, \mathbf{v}_k$ are isotropic with respect to ϕ if and only if $T^{-1}(\mathbf{v}_1), \ldots, T^{-1}(\mathbf{v}_k)$ are isotropic with respect to $\phi \circ T$. Therefore we may prove the statement up to a change of basis of $K^{(n)}$. By Corollary 1.3.7, up to such a change of basis we may assume that

$$\phi_1 = X_1^2 + \ldots + X_n^2 \quad \text{and} \quad \phi_2 = a_1 X_1^2 + \ldots + a_n X_n^2,$$

for certain $a_1, \ldots, a_n \in K$ such that $a_{i+1} \leqslant_K a_i$ for every $1 \leqslant i \leqslant n-1$. Therefore $a_{i+1} - \lambda \leqslant_K a_i - \lambda$ for every $1 \leqslant i \leqslant n-1$.

Consider the canonical K-basis $\mathfrak{C} = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$ of $K^{(n)}$. Evidently $\mathfrak{C}$ is orthogonal with respect to ϕ_1, ϕ_2 and ϕ. We denote $m = \mathsf{min}\{s,t\}$ and $M = \mathsf{max}\{s,t\}$. Since $\Sigma_{i=1}^n (a_i - \lambda) X_i^2 = \phi \simeq s \times \langle 1 \rangle \perp t \times \langle -1 \rangle$ and $a_{i+1} - \lambda \geqslant_K a_i - \lambda$ for every $1 \leqslant i \leqslant n-1$, we conclude that $a_i - \lambda >_K 0$ for every $1 \leqslant i \leqslant s$, $a_i = \lambda$ for every $s < i \leqslant n-t$ and $a_i - \lambda <_K 0$ for every $n-t < i \leqslant n$. By the definition of $\leqslant_K$, there exist $\alpha_1, \ldots \alpha_s, \alpha_{n-t}, \ldots, \alpha_n \in K^\times$ such that

$$\phi = \Sigma_{i=1}^s \alpha_i^2 X_i^2 - \Sigma_{i=n-t+1}^n \alpha_i^2 X_i^2.$$

Consider $1 \leqslant i \leqslant m$. Let V_i denote the 2-dimensional K-subspace of $K^{(n)}$ generated by $\{\mathbf{e}_i, \mathbf{e}_{n-i}\}$. Since $\phi|_{V_i} = \alpha_i^2 X_i^2 - \alpha_{n-i}^2 X_{n-i}^2 \simeq \langle 1, -1 \rangle_K$, there exists a nonzero vector $\mathbf{u}_i \in V_i$ that is isotropic with respect to ϕ. We observe that for every $\mathbf{v} \in K^{(n)}$ having null i-th and $(n-i)$-th coordinates, $\mathbf{u}_i$ and $\mathbf{v}$ are orthogonal with respect to ϕ_1 and ϕ_2.

For every $s < i \leqslant n-t$, we denote $\mathbf{u}_i = \mathbf{e}_i$. Then $\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{u}_{s+1}, \ldots, \mathbf{u}_{n-t}$ are $m + (n-s-t) = n - M = N$ nonzero vectors that are isotropic with respect to ϕ and are orthogonal with respect to both ϕ_1 and ϕ_2. □

1.4.6 Corollary. *Let K be a real closed field, let $n \in \mathbb{N}^+$ and let $\phi_1, \phi_2 \in K[X_1, \ldots, X_n]$ be positive definite quadratic forms. Set $N = \lceil \frac{n}{2} \rceil$. Then there exist $\mathbf{u}_1, \ldots, \mathbf{u}_N \in K^{(n)}$ nonzero and $\lambda \in K^\times$ such that $\mathbf{u}_1, \ldots, \mathbf{u}_N$ are orthogonal with respect to ϕ_1 and ϕ_2, and are isotropic with respect to the quadratic form $\phi_2 - \lambda\phi_1$.*

Proof. As for Theorem 1.4.5, it is enough to prove the statement up to a change of basis. Hence we may assume, by Corollary 1.3.7 that

$$\phi_1 = X_1^2 + \ldots + X_n^2 \quad \text{and} \quad \phi_2 = a_1 X_1^2 + \ldots + a_n X_n^2,$$

for $a_1, \ldots, a_n \in K$ such that $a_{i+1} \leqslant_K a_i$ for every $1 \leqslant i \leqslant n-1$. Let $\lambda = a_N$. Set $s = |\{N < i \leqslant n \mid a_i \neq a_N\}|$ and $t = |\{1 \leqslant i < N \mid a_i \neq a_N\}|$. Then

$$\phi_2 - \lambda\phi_1 = \Sigma_{i=1}^n (a_i - \lambda) X_i^2 \simeq s \times \langle 1 \rangle \perp t \times \langle -1 \rangle.$$

By Theorem 1.4.5, there exist $n - \mathsf{max}\{s,t\}$ vectors as in the statement. Since $a_N - \lambda = 0$, we have $s, t \leqslant N-1$. Thus $n - \mathsf{max}\{s,t\} \geqslant n - (N-1) \geqslant N$, whereby the statement. □

Let K be a field of characteristic different from 2, let $n \in \mathbb{N}^+$ and let ϕ be an n-ary quadratic form. Given $m \in \mathbb{N}^+$ and $\mathbf{u}_1, \ldots, \mathbf{u}_m \in K^{(n)}$, we say that $\mathbf{u}_1, \ldots, \mathbf{u}_m$ are *orthonormal with respect to ϕ* if they are orthogonal with respect to ϕ and if $\phi(\mathbf{u}_i) = 1$ for every $1 \leqslant i \leqslant m$.

1.4.7 Remark. Let K be a real closed field and let ϕ be a positive definite quadratic form. We retrieve from Corollary 1.3.6 the existence of a K-basis of $K^{(n)}$ that is orthonormal with respect to ϕ. As a matter of fact, any set of vectors of $K^{(n)}$ that are orthonormal with respect to ϕ can be extended to a K-basis of $K^{(n)}$ that is orthonormal with respect to ϕ. This will be exploited in the next statement.

The following statement, together with Theorem 1.4.5 and Corollary 1.4.6, allows us to write two positive definite quadratic forms over a real closed field with a "common" part, and thus to express their product in a convenient way.

1.4.8 Lemma. *Let $N, n \in \mathbb{N}^+$, let K be a real closed field and let $\phi_1, \phi_2 \in K[X_1, \ldots, X_n]$ be two positive definite quadratic forms. Assume that there exist $\mathbf{u}_1, \ldots, \mathbf{u}_N \in K^{(n)} \smallsetminus \{\mathbf{0}\}$*

and $\lambda \in K^{\times}$ such that $\mathbf{u}_1, \ldots, \mathbf{u}_N$ are orthogonal with respect to ϕ_1 and to ϕ_2, and are isotropic with respect to $\phi_2 - \lambda\phi_1$. Set $\mathbf{X} = (X_1, \ldots, X_n)^t$. Then there exists $M \in \mathsf{M}_n(K)$ and $h_{N+1}, \ldots, h_n \in K[X_1, \ldots, X_n]$ linear such that

$$\phi_1(M \cdot \mathbf{X}) = X_1^2 + \ldots + X_N^2 + X_{N+1}^2 + \ldots + X_n^2 \text{ and}$$

$$\phi_2(M \cdot \mathbf{X}) = \lambda(X_1^2 + \ldots + X_N^2) + h_{N+1}^2 + \ldots + h_n^2.$$

Proof. Set $\phi = \phi_2 - \lambda\phi_1$ and let U be the K-subspace of $K^{(n)}$ generated by $\{\mathbf{u}_1, \ldots, \mathbf{u}_N\}$. Choose a K-basis $(\mathbf{v}_1, \ldots, \mathbf{v}_N)$ of U that is orthonormal with respect to ϕ_1, and extend it to a K-basis $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ of $K^{(n)}$ that is orthonormal with respect to ϕ_1. Let M be the change-of-basis matrix from the canonical basis to $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$. Since $\phi|_U = 0$, we have $\phi_2|_U = \lambda\phi_1|_U$. Furthermore, $\mathbf{v}_1, \ldots, \mathbf{v}_N$ are orthonormal with respect to ϕ_1, thus $(\phi_1(M \cdot \mathbf{X}))|_U = X_1^2 + \ldots + X_N^2$ and $(\phi_2(M \cdot \mathbf{X}))|_U = \lambda(X_1^2 + \ldots + X_N^2)$. Therefore $\phi_1(M \cdot \mathbf{X}) = X_1^2 + \ldots + X_n^2$ and $\phi_2(M \cdot \mathbf{X}) = \lambda(X_1^2 + \ldots + X_N^2) + h(X_1, \ldots, X_n)$, for some quadratic form $h \in K[X_1, \ldots, X_n]$.

On the other hand, the K-basis $(\mathbf{v}_1, \ldots, \mathbf{v}_N)$ of U can also be extended to a K-basis of $K^{(n)}$ that is orthogonal with respect to ϕ_2. Since ϕ_2 is positive definite, under such a basis ϕ_2 can be written as $\phi_2 = \lambda(X_1^2 + \ldots + X_N^2) + h_{N+1}^2 + \ldots + h_n^2$ for some $h_{N+1}, \ldots, h_n \in K[X_1, \ldots, X_n]$ linear. □

1.4.9 Lemma. *Let $k, m, N \in \mathbb{N}$ be such that $N \leqslant 2^{k+1}$ and $m \leqslant \min\{2^{k+1} - 1, N - 2^k\}$. Set $n = 2^{k+1} + m$. Let K be a real closed field, let $h_{N+1}, \ldots, h_n \in K[X_1, \ldots, X_n]$ be linear and let $\lambda \in K^{\times 2}$. Set $\phi_1 = X_1^2 + \ldots + X_n^2$ and $\phi_2 = \lambda(X_1^2 + \ldots + X_N^2) + h_{N+1}^2 + \ldots + h_n^2$. Then $\phi_1 \cdot \phi_2$ can be written as a sum of $(3n-1)/2$ rational functions in $K(X_1, \ldots, X_n)$.*

Proof. If $m = 0$, then $n = 2^{k+1}$, thus $\phi_1 \cdot \phi_2 \in \Sigma_n F^2 \cdot \Sigma_n F^2 \subseteq \Sigma_n F^2$, by Theorem 1.1.16; furthermore, we have $n = 2^{k+1} \leqslant (2^{k+2} + 2^{k+1} - 1)/2 = (3n-1)/2$, whereby the statement.

Assume now $m > 0$. Let $\mu \in K$ be such that $\mu^2 = \lambda$. We set $F = K(X_1, \ldots, X_n)$, $f = X_1^2 + \ldots + X_N^2$, $g = X_{N+1}^2 + \ldots + X_n^2$, and $h = h_{N+1}^2 + \ldots + h_n^2$. Then $\phi_1 = f + g$ and $\phi_2 = \mu^2 f + h$, whereby $\phi_1 \in D_F(\langle f, g\rangle_F)$ and $\phi_2 \in D_F(\langle f, h\rangle_F)$. Observe that $f \in \Sigma_N F^2 \subseteq \Sigma_{2^{k+1}} F^2$, and $g, h \in \Sigma_{n-N} F^2 \subseteq \Sigma_{2^k} F^2$, because $n - N \leqslant 2^{k+1} + m - N \leqslant 2^k$. Set $\pi = \langle 1, fg, fh, gh\rangle_F$. Then

$$\phi_1 \cdot \phi_2 \in D_F(\langle f, g\rangle_F) \cdot D_F(\langle f, h\rangle_F) = f D_F(\langle 1, fg\rangle_F) \cdot f D_F(\langle 1, fh\rangle_F) \subseteq D_F(\pi).$$

Since $g, h \in \Sigma_{2^k} F^2$, we have $gh \in \Sigma_{2^k} F^2$, by Theorem 1.1.16. Hence $gh \in D_F(2^k)$, and we obtain $gh(2^k \times \langle 1\rangle_F) \simeq 2^k \times \langle 1\rangle_F$, by Theorem 1.1.15. Thus $2^k \times \langle gh\rangle_F \simeq 2^k \times \langle 1\rangle_F$.

Analogously, since $f, g \in \Sigma_{2^{k+1}} F^2$, we have $gh \in \Sigma_{2^{k+1}} F^2$, by Theorem 1.1.16, whereby $2^{k+1} \times \langle fg\rangle_F \simeq 2^{k+1} \times \langle 1\rangle_F$. As $2^k \times \langle 1, gh\rangle_F = 2^k \times \langle 1\rangle_F$, we obtain that

$$2^k \times \pi = 2^k \times (\langle 1, fg\rangle_F \otimes \langle 1, gh\rangle_F) = 2^{k+1} \times (\langle 1, fg\rangle_F) = 2^{k+2} \times \langle 1\rangle_F.$$

Since $(2^k - 1) \times \langle 1\rangle_F \perp \pi \subseteq 2^k \times \pi$, it follows by Witt's Cancellation (Theorem 1.1.11) that $\pi \subseteq (2^{k+2} - 2^k + 1) \times \langle 1\rangle_F$. Hence $\phi_1 \cdot \phi_2$ can be written as a sum of $2^{k+2} - 2^k + 1$ squares in F. Observe now that

$$2^{k+2} - 2^k + 1 = 3 \cdot 2^k + 1 = (3 \cdot 2^{k+1} + 3 - 1)/2 = (3(2^{k+1} + 1) - 1)/2.$$

Since $m > 0$, we have that $2^{k+1} + 1 \leqslant n$, that is, $3(2^{k+1} + 1) \leqslant 3n$. We obtain that $2^{k+2} - 2^k + 1 \leqslant (3n-1)/2$, which concludes the proof. □

1.4.10 Theorem. *Let $k \in \mathbb{N}$, let $n = 2^{k+1} + 1$. Let K be a real closed field and let $\phi_1, \phi_2 \in K[X_1, \ldots, X_n]$ be positive definite quadratic forms. Then $\phi_1 \cdot \phi_2$ can be written as a sum of $(3n-1)/2$ squares of rational functions in $K(X_1, \ldots, X_n)$.*

Proof. Set $N = \lceil \frac{n}{2} \rceil$ and $m = 1$. Then $N = 2^k + m \leqslant 2^{k+1}$ and $2^{k+1} + m - N = 2^k$. Up to a change of basis, we may choose $\lambda \in K^{\times 2}$, $h_{N+1}, \ldots, h_n \in K[X_1, \ldots, X_n]$ such that $\phi_1 = X_1^2 + \ldots + X_n^2$ and $\phi_2 = \lambda(X_1^2 + \ldots + X_N^2) + h_{N+1}^2 + \ldots + h_n^2$, by Corollary 1.4.6 and Lemma 1.4.8. Then the statement follows from Lemma 1.4.9. □

1.4.11 Remark. Let $k \in \mathbb{N}^+$ and $n = 2^{k+1} + 1$. Then $2^k - 1 > 0$, hence

$$\frac{3n-1}{2} = 2^{k+2} - 2^k + 1 < 2^{k+2} = 2n - 2.$$

Hence Theorem 1.4.10 improves significantly the upper bound $2n-2 = 2^{k+2}$, which can be obtained from Theorem 1.1.16. Furthermore, recalling that ρ denotes the Hurwitz-Radon function, we have $\rho(n) = 1 < n$. Therefore Theorem 1.4.3 does not help producing upper bounds for the squares necessary to represent the product $\phi_1 \cdot \phi_2$ from Theorem 1.4.10 as a sum of squares. Nevertheless, we do not know whether the upper bound from Theorem 1.4.10 is optimal.

1.4.12 Question. *For which $k \in \mathbb{N}^+$ is the bound $(3n-1)/2$ from Theorem 1.4.10 optimal?*

The following examples show that the bound $(3n-1)/2$ is not optimal for $n = 3, 5$ (that is, for $k = 0, 1$). We also show for $k \leqslant 1$ that an explicit identity of the type of (1.4.2) can be constructed, after simultaneously diagonalising two quadratic forms.

1.4.13 Example. Let K a real closed field and let $\phi_1, \phi_2 \in K[X_1, X_2, X_3]$ be positive definite quadratic forms. Theorem 1.4.10 applied with $k = 0$ only shows that

$$\phi_1 \cdot \phi_2 \in \Sigma_4 K(X_1, X_2, X_3)^2,$$

producing thus no improvement to Pfister's bound from Theorem 1.1.16.

However, by Corollary 1.4.6 and Lemma 1.4.8 we may assume, up to a change of basis, that $\phi_1 = X_1^2 + X_2^2 + X_3^2$ and $\phi_2 = \lambda(X_1^2 + X_2^2 + Y_3^2)$ for some $\lambda \in K^{\times 2}$ and $Y_3 \in K[X_1, X_2, X_3]$ linear. Then $\phi_1 \cdot \phi_2/\lambda = (X_1^2 + X_2^2 + X_3Y_3)^2 + (X_1^2 + X_2^2)(X_3 - Y_3)^2$ Since $\lambda \in K^{\times 2}$, we conclude that $\phi_1 \cdot \phi_2 \in \Sigma_3 K[X_1, X_2, X_3]^2$.

1.4.14 Example. Let K a real closed field and let $\phi_1, \phi_2 \in K[X_1, \ldots, X_5]$ be positive definite quadratic forms. In view of Theorem 1.4.10, we have that

$$\phi_1 \cdot \phi_2 \in \Sigma_7 K(X_1, \ldots, X_5)^2.$$

However, by Corollary 1.4.6 and Lemma 1.4.8 we may assume, up to a change of basis, that $\phi_1 = X_1^2 + \ldots + X_5^2$ and $\phi_2 = \lambda(X_1^2 + X_2^2 + X_3^2 + Y_4^2 + Y_5^2)$ for some $\lambda \in K^{\times 2}$ and $Y_4, Y_5 \in K[X_1, \ldots, X_5]$ linear. We may then apply Degen's 8-square identity to compute $\phi_1 \cdot \phi_2/\lambda$. We obtain

$$\begin{aligned}\phi_1 \cdot \phi_2/\lambda = {} & (X_1^2 + X_2^2 + X_3^2 + X_4Y_4 + X_5Y_5)^2 \\ & + (X_4Y_5 - X_5Y_4)^2 \\ & + (X_1Y_5 - X_5Y_1)^2 \\ & + (X_1Y_4 - X_4Y_1)^2 \\ & + (X_2Y_4 - X_3Y_5 - X_4Y_2 + X_5Y_3)^2 \\ & + (X_2Y_5 + X_3Y_4 - X_4Y_3 - X_5Y_2)^2.\end{aligned}$$

Since $\lambda \in K^{\times 2}$, we conclude that $\phi_1 \cdot \phi_2 \in \Sigma_6 K[X_1, \dots, X_5]^2$.

1.4.15 Remarks. (*a*) Example 1.4.13 can be found in [Sche10, §9], and the upper bound 3 on the number of squares that are needed to represent $\phi_1 \cdot \phi_2$ is trivially optimal.

(*b*) In the context of Example 1.4.14, one may wonder whether a permutation of the variables in Degen's identity produces a formula that allows us to write $\phi_1 \cdot \phi_2$ as a sum of 5 squares of polynomials (which would then be evidently an optimal upper bound). In order to check this, we have run a simple magma program on a computer, and it turned out that this does not happen.

1.4.16 Question. *Can the product of any two positive definite* 5*-ary quadratic forms over a real closed field be written as a sum of* 5 *squares of fractions of polynomials? If so, can we represent it as the sum of* 5 *squares of polynomials?*

Finally, observe that most of this section would also hold for a field K that has the Principal Axis Property, but that is not real closed, that is, an intersection of multiple real closed fields. As a matter of fact, the only exception to this is Theorem 1.4.5, in which proof we ordered some elements with respect to the ordering on K, by means of Corollary 1.3.7. We could not have done the same if K possessed multiple orderings; cf. Remark 1.3.9. This is the only obstacle that prevents us from substituting the real closed field K with a PAP-field in Theorem 1.4.5-Theorem 1.4.10 and Examples 1.4.13, 1.4.14.

1.4.17 Question. *Does Theorem 1.4.10 still hold if we replace the assumption that K is real-closed with the one that K is a PAP-field?*

Chapter 2
Valuation theory

In this chapter we introduce the reader to valuation theory. In doing so, we largely rely on [EP05]. The tools given here will be extensively exploited in the upcoming chapters.

2.1 Basic concepts

An *ordered abelian group* (or, more concisely, an *ordered group*) is an abelian group $(\Gamma, +, 0)$ with a total order relation $\leqslant$ on Γ such that, for every $x, y \in \Gamma$, we have that $x \leqslant y$ if and only $x - y \leqslant 0$. Let $(\Gamma, +, 0, \leqslant)$ be an ordered abelian group. When there is no possibility of confusion, we will denote $(\Gamma, +, 0, \leqslant)$ simply by $(\Gamma, \leqslant)$ or Γ. Furthermore, given $\gamma, \delta \in \Gamma$, we adopt the standard notations $\gamma \geqslant \delta$ to indicate $\delta \leqslant \gamma$, and $\gamma < \delta$ (respectively, $\gamma > \delta$) to denote $\gamma \neq \delta$ and $\gamma \leqslant \delta$ (respectively, $\gamma \neq \delta$ and $\gamma \geqslant \delta$).

2.1.1 Example. The group $\mathbb{Z}$ can be turned into an ordered group in two ways. The natural way is to define an order on $\mathbb{Z}$, which we call *natural*, by setting $1 > 0$, the other one by setting $0 > 1$. In the sequel, when talking about the ordered group $\mathbb{Z}$, we always use the natural order.

Let $(\Gamma, \leqslant_\Gamma)$, $(\Delta, \leqslant_\Delta)$ be two ordered groups. A *morphism of ordered groups from* $(\Gamma, \leqslant_\Gamma)$ *to* $(\Delta, \leqslant_\Delta)$ is a morphism of groups $\phi : \Gamma \to \Delta$ that preserves the orders, that is, such that $\phi(x) \leqslant_\Delta \phi(y)$ for every $x, y \in \Gamma$ such that $x \leqslant_\Gamma y$. We say that two ordered groups are *ordered-isomorphic* if they are isomorphic as ordered groups.

Let Γ be an ordered group. We say that Γ is *discrete* if the set $\{\gamma \in \Gamma \mid \gamma > 0\}$ has a minimal element. A subgroup Δ of Γ is a *convex ordered group* if for every $\gamma \in \Gamma$ and $\delta \in \Delta$ such that $0 \leqslant \gamma \leqslant \delta$, we have that $\gamma \in \Delta$. If Γ has only finitely many convex subgroups, then we define the *rank of* Γ as the number of proper convex subgroups of Γ, otherwise we define it to be ∞. We denote the rank of Γ by $\mathbf{rk}(\Gamma)$. Note that in [EP05] a finer notion of rank is introduced, which distinguishes between different order types, and carries therefore more information than the concept we introduced.

2.1.2 Examples. (*a*) Let $\leqslant$ be the natural order on $\mathbb{R}$. Then $(\mathbb{R}, \leqslant)$ is an ordered group of rank 1, and it is not discrete.

(*b*) Any non-trivial subgroup of $\mathbb{R}$, together with the order induced by the natural order on $\mathbb{R}$, is an ordered group of rank 1. It is well known that the converse is also true, that is, any ordered group of rank 1 is order-isomorphic to a non-trivial subgroup of $\mathbb{R}$ with the order induced by the natural order on $\mathbb{R}$; see [EP05, Proposition 2.1.1].

(*c*) In this dissertation, we will mostly exploit ordered groups of rank 1. Nevertheless, it is easy to build ordered groups of arbitrary rank as follows. Let $n \in \mathbb{N}$ and let

$(\Gamma_1, \leqslant_1), \dots (\Gamma_n, \leqslant_n)$ be ordered groups. Set

$$\Gamma = \prod_{i=1}^{n} \Gamma_i.$$

We define an order on Γ as follows: for every $1 \leqslant i \leqslant n$ and $\gamma_i, \delta_i \in \Gamma_i$, we set $(\gamma_1, \dots, \gamma_n) \leqslant (\delta_1, \dots, \delta_n)$ if $\gamma_j = \delta_j$ for $1 \leqslant j \leqslant n$ or if there exists $1 \leqslant k \leqslant n$ such that $\gamma_k <_k \delta_k$ and $\gamma_j = \delta_j$ for every $1 \leqslant j \leqslant k-1$. Then the relation $\leqslant$ is an order on Γ, called *the lexicographical order on* Γ. Furthermore, any proper convex subgroup of $(\Gamma, \leqslant)$ is of the form

$$\prod_{i=1}^{k-1} \{0\} \times \Delta \times \prod_{i=k+1}^{n} \Gamma_i$$

for some $1 \leqslant k \leqslant n$ and some convex subgroup Δ of $(\Gamma_k, \leqslant_{\Gamma_k})$. It follows in particular that $\mathbf{rk}(\Gamma) = \Sigma_{i=1}^{n} \mathbf{rk}(\Gamma_i)$.

(*d*) Let $n \in \mathbb{N}$ and let $\leqslant$ be the lexicographical order on $\mathbb{Z}^{(n)}$ induced by the natural order on $\mathbb{Z}$. Then $(\mathbb{Z}^{(n)}, \leqslant)$ is a discrete ordered group of rank n.

(*e*) The rank of an ordered group is not independent of the order considered. For example, let $G_1 = \mathbb{Z} \times \mathbb{Z}$ and let $\leqslant_1$ be the lexicographical order on G_1 introduced above. Let $G_2 = \mathbb{Z} + \pi\mathbb{Z} \subseteq \mathbb{R}$ and let $\leqslant_2$ be the order on G_2 induced by the natural order on $\mathbb{R}$. Then G_1 and G_2 are isomorphic as groups, but not as ordered groups; in fact, $\mathbf{rk}(G_1) = 2$, whereas $\mathbf{rk}(G_2) = 1$.

Given an ordered abelian group $(\Gamma, +, 0, \leqslant)$, we extend the semi-group structure $(\Gamma, +, 0)$ by introducing a symbol ∞ that does not belong to Γ and by setting $x + \infty = \infty$ for every $x \in \Gamma$; we also extend the order relation $\leqslant$ to $\Gamma \cup \{\infty\}$ by setting $x \leqslant \infty$ for every $x \in \Gamma$.

Let K be a field. A *valuation on* K is a map $v : K \to \Gamma \cup \{\infty\}$ such that Γ is an ordered abelian group and such that the following conditions hold for every $x, y \in K$:

(*i*) $v(x) = \infty$ if and only if $x = 0$,

(*ii*) $v(xy) = v(x) + v(y)$,

(*iii*) $v(x + y) \geqslant \mathsf{min}\{v(x), v(y)\}$.

A pair (K, v) where K is a field and v is a valuation on K is called *valued field.*

Remark. In several of the sources used in this thesis, among which [OM73] and [Neuk99], the term *valuation* is attached to a different concept, namely to what is called *absolute value* in [EP05], which are essentially the same thing as valuations of rank 1; see Section 2.3.

Let K be a field and let v be a valuation on K. Simple computations show that $v(1) = v(-1) = 0$ and that $v(x + y) = \mathsf{min}\{v(x), v(y)\}$ for every $x, y \in K$ such that $v(x) \neq v(y)$. Furthermore, we denote $\mathcal{O}_v = \{x \in K \mid v(x) \geqslant 0\}$. It is easy to see that $\mathcal{O}_v$ is a local ring, whose unique maximal ideal is given by $\{x \in K \mid v(x) > 0\}$. We denote this maximal ideal by $\mathfrak{m}_v$, we denote the quotient field $\mathcal{O}_v/\mathfrak{m}_v$ by Kv, we denote by vK the ordered group $v(K^\times)$, and we set $\mathbf{rk}(v) = \mathbf{rk}(vK)$. For any $x \in \mathcal{O}_v$, we denote by $\overline{x}^v$ the class of x in Kv. Note that $\mathcal{O}_v^\times = \mathcal{O}_v \smallsetminus \mathfrak{m}_v = \{x \in K \mid v(x) = 0\}$. We call Kv the *residue field of* v, we call vK the *value group of* v, and we call $\mathbf{rk}(v)$ the *rank of* v. We say that v *is discrete* if vK is discrete.

We say that v is *dyadic* if $\mathsf{char}(Kv) = 2$, and that v is *non-dyadic* otherwise. This distinction is often relevant when studying quadratic forms over (K, v).

Let $S \subseteq K$. We say that v is *trivial on* S if $v(S) \subseteq \{0, \infty\}$, that is, if $S \subseteq \mathcal{O}_v^\times \cup \{0\}$. This is especially relevant when S is a subfield of K, in which case v is trivial on S if and only if $S \subseteq \mathcal{O}_v$. We say that v *is trivial* if v is trivial on K, that is, $\mathcal{O}_v = K$.

Let v, w be valuations on K. We say that v *and* w *are equivalent* if there exists an isomorphism of ordered groups $\phi : vK \to wK$ such that $w = \phi \circ v$, and that they are *inequivalent* otherwise. If v and w are equivalent, we write $v \sim w$. In other words, $v \sim w$ if and only if $\mathcal{O}_v = \mathcal{O}_w$. Clearly, $\sim$ is an equivalence relation on the valuations on K.

Given two valued fields (K, v), (L, w) and a field isomorphism $\phi : K \to L$, we say that ϕ is an *isomorphism between the valued fields* (K, v) *and* (L, w) if $v \circ \phi = v$; if (K, v), (L, w) are isomorphic valued fields, we denote it by $(K, v) \simeq (L, w)$.

2.1.3 Examples. (a) Let $p \in \mathbb{N}$ be a prime number. For every $x \in \mathbb{Q}^\times$, let $v_p(x) \in \mathbb{Z}$ be the unique integer $n \in \mathbb{Z}$ such that $x = p^n a/b$ for some $a, b \in \mathbb{Z} \smallsetminus p\mathbb{Z}$. Then the map $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ sending 0 to ∞ and $x \in \mathbb{Q}^\times$ to $v_p(x)$ is a valuation on $\mathbb{Q}$ with value group $\mathbb{Z}$, which is called *the* p*-adic valuation on* $\mathbb{Q}$. The residue field of v is naturally isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Furthermore, any non-trivial valuation on $\mathbb{Q}$ is equivalent to the p-adic valuation for a unique prime $p \in \mathbb{N}$; see [EP05, Theorem 2.1.4 (a)].

(b) Let K be a field and $p \in K[X]$ irreducible. Mimicking Example 2.1.3 (a), we build a valuation on $K(X)$ as follows. For any $f \in K(X)^\times$, let $v_p(f) \in \mathbb{Z}$ be the unique integer $n \in \mathbb{Z}$ such that $f = p^n g/h$ for some $g, h \in K[X] \smallsetminus pK[X]$. Then the map $v_p : K(X) \to \mathbb{Z} \cup \{\infty\}$ sending 0 to ∞ and $x \in K(X)^\times$ to $v_p(x)$ is a valuation on $K(X)$ with value group $\mathbb{Z}$, which is called *the* p*-adic valuation on* $K(X)$, and which is trivial on K. The residue field of v_p is naturally isomorphic to $K[X]/pK[X]$.

(c) An analogous, more general construction can be made in order to build *the* p*-adic valuation on* K whenever K is the fraction field of a unique factorization domain R and $p \in R$ is a prime element; the value group is again $\mathbb{Z}$, and the residue field of the p-adic valuation on K is naturally isomorphic to $\mathsf{Frac}(R/pR)$.

(d) Let K be a field. There exists a valuation on $K(X)$ that is not the p-adic valuation for any $p \in K[X]$ prime. For any $f \in K(X)^\times$, set $v_\infty(f) = \deg(h) - \deg(g)$, where $g, h \in K[X]$ are such that $f = g/h$. Setting $v_\infty(0) = \infty$, we obtain a valuation v_∞ on $K(X)$ with value group $\mathbb{Z}$, which is trivial on K, and whose residue field is canonically isomorphic to K. The valuation v_∞ is called *the degree valuation on* $K(X)$. One can show that any non-trivial valuation on $K(X)$ that is trivial on K is equivalent to the degree valuation on $K(X)$ or to the p-adic valuation v_p for a (unique) monic irreducible polynomial $p \in K[X]$; see [EP05, Theorem 2.1.4 (b)]. Furthermore, v_∞ is not the p-adic valuation for any $p \in K[X]$ prime, but is the $1/X$-adic valuation obtained by viewing $K(X)$ as the fraction field of the principal ideal domain $K[1/X]$.

All valuations in Examples 2.1.3 are discrete valuations of rank 1. These are frequently involved in algebraic geometry, and are the only valuations necessary in the upcoming chapters of this thesis. Nevertheless, there exist valuations with arbitrary value groups.

2.1.4 Examples. (a) Let $p \in \mathbb{Z}$ be prime. Consider the p-adic valuation v_p on $\mathbb{Q}$ described in Example 2.1.3 (a) and the X-adic valuation v_X on $\mathbb{Q}(X)$ described in Example 2.1.3 (b). For every $f \in \mathbb{Q}(X)^\times$, let $g, h \in \mathbb{Q}[X] \smallsetminus X\mathbb{Q}[X]$ be such that $f = X^{v_X(f)} g/h$ and let $f_0 = g(0)/h(0) \in \mathbb{Q}$. Then the map $v : \mathbb{Q}(X) \to (\mathbb{Z} \times \mathbb{Z}) \cup \{\infty\}$ sending 0 to ∞ and $f \in \mathbb{Q}(X)^\times$ to $(v_X(f), v_p(f_0))$ is a discrete valuation of rank 2 on $\mathbb{Q}(X)$.

(b) Let K be a field and let Γ be an ordered abelian group. Let $K[\![t^\Gamma]\!]$ be the ring of *Hahn series in the variable t over K*; see [EP05] for the definition of $K[\![t^\Gamma]\!]$. We denote by $K(\!(t^\Gamma)\!)$ the field of fractions of $K[\![t^\Gamma]\!]$. For every $\{a_\gamma\}_{\gamma\in\Gamma} \subseteq K$ having well-ordered support, we set $v(\Sigma_{\gamma\in\Gamma} a_\gamma t^\gamma) = \mathsf{min}\{\gamma \in \Gamma \mid a_\gamma \neq 0\}$. For every $g, h \in K[\![t^\Gamma]\!] \smallsetminus \{0\}$, we set $v(g/h) = v(g) - v(h)$. Then the map $v : K(\!(t^\Gamma)\!) \to \Gamma \cup \{\infty\}$ sending 0 to ∞ and $f \in K(\!(t^\Gamma)\!)^\times$ to $v(f) \in \Gamma$ is a valuation on $K(\!(t^\Gamma)\!)$. Furthermore, the residue field of v is naturally isomorphic to K, and $vK(\!(t^\Gamma)\!) = \Gamma$.

When $\Gamma = \mathbb{Z}$, the ring $K[\![t^\Gamma]\!]$ is called *ring of formal power series in the variable t over K* and is denoted by $K[\![t]\!]$; similarly, the fraction field of $K[\![t]\!]$ is called *field of formal power series in the variable t over K* and is denoted by $K(\!(t)\!)$. In this case, the valuation v is called the t-adic valuation on $K(\!(t)\!)$ and is denoted by v_t. When $\Gamma = \mathbb{Q}$, the valuation v on L has rank 1, but it is not discrete.

Let $\mathcal{O}$ be a domain. We denote the fraction field of $\mathcal{O}$ by $\mathsf{Frac}(\mathcal{O})$. We call any intermediate ring extension of $\mathsf{Frac}(\mathcal{O})/\mathcal{O}$ an *overring of $\mathcal{O}$*. We call $\mathcal{O}$ a *valuation ring* if for every $x \in \mathsf{Frac}(\mathcal{O})^\times$ we have that $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$. Clearly, any overring of a valuation ring is again a valuation ring. Given a valuation v on K, it is straightforward that $\mathcal{O}_v$ is a valuation ring.

Let K be a field. A *valuation ring of K* is a valuation ring having fraction field K. Let $\mathcal{O}$ be a valuation ring of K. We use $\mathcal{O}$ to build a valuation on K as follows. For $x, y \in K^\times$, we set $x\mathcal{O}^\times \leqslant y\mathcal{O}^\times$ if $y\mathcal{O} \subseteq x\mathcal{O}$. Then $(K^\times/\mathcal{O}^\times, \cdot, \mathcal{O}^\times, \leqslant)$ is an ordered abelian group and is the value group of a valuation v on K, which we define by setting $v(0) = \infty$ and $v(x) = x\mathcal{O}^\times$ for any $x \in K^\times$. Then $\mathcal{O} = \mathcal{O}_v$. We call v *the natural valuation corresponding to $\mathcal{O}$*. We define *the rank of $\mathcal{O}$* as the rank of v. Note that $\mathbf{rk}(\mathcal{O})$ coincides with the Krull dimension of $\mathcal{O}$; see [EP05, Lemma 2.3.1].

2.1.5 Examples. (a) Let $p \in \mathbb{N}$ be prime. Let $\mathbb{Z}_{(p)}$ be the localisation of $\mathbb{Z}$ at p, that is,

$$\mathbb{Z}_{(p)} = \{m/n \mid m \in \mathbb{Z},\, n \in \mathbb{Z} \smallsetminus p\mathbb{Z}\}.$$

Then $\mathbb{Z}_{(p)}$ is a valuation ring of $\mathbb{Q}$ of rank 1. As a matter of fact, $\mathbb{Z}_{(p)} = \mathcal{O}_{v_p}$ where v_p is the p-adic valuation on $\mathbb{Q}$ described in Example 2.1.3 (a).

(b) Let K be a field and let $p \in K[X]$ be an irreducible polynomial. Let $K[X]_{(p)}$ be the localisation of $K[X]$ at p, that is,

$$K[X]_{(p)} = \{f/g \mid f \in K[X],\, g \in K[X] \smallsetminus pK[X]\}.$$

Then $K[X]_{(p)}$ is a valuation ring of $K(X)$ of rank 1. Indeed, $K[X]_{(p)} = \mathcal{O}_{v_p}$ where v_p is the p-adic valuation on $K(X)$ from Example 2.1.3 (b).

(c) Let K be a field and let

$$\mathcal{O} = \{f/g \mid f, g \in K[X],\, g \neq 0 \text{ and } \deg g \geqslant \deg f\}.$$

Then $\mathcal{O}$ is a valuation ring of $K(X)$ of rank 1. Indeed, $\mathcal{O} = \mathcal{O}_{v_\infty}$ where v_∞ is the degree valuation on $K(X)$ from Example 2.1.3 (d).

Given a field K, a valuation ring $\mathcal{O}$ of K and a valuation v on K such that $\mathcal{O} = \mathcal{O}_v$, there exist 1-1 correspondences between prime ideals of $\mathcal{O}$, convex subgroups of vK and valuation rings of K lying over $\mathcal{O}$. The next lemma gives an explicit description of such correspondences.

Given a ring R, we denote by $\mathsf{Spec}(R)$ the set of prime ideals of R.

2.1.6 Lemma. *Let K be a field, let $\mathcal{O}$ be a valuation ring and let v be a valuation on K such that $\mathcal{O} = \mathcal{O}_v$. Let $S_1 = \mathsf{Spec}(\mathcal{O})$, let S_2 be the set of the convex subgroups of vK and let S_3 be the set of overrings of $\mathcal{O}$. Consider $\mathfrak{p} \in S_1$, $\Delta \in S_2$ and $\mathcal{O}' \in S_3$. Let $\mathfrak{m}'$ be the maximal ideal of $\mathcal{O}'$. We set the following:*

$$\begin{aligned}
&\phi_{12}(\mathfrak{p}) = \{\gamma \in vK \mid \gamma, -\gamma < v(x) \textit{ for every } x \in \mathfrak{p}\}\\
&\phi_{13}(\mathfrak{p}) = \mathcal{O}_{\mathfrak{p}}\\
&\phi_{21}(\Delta) = \{x \in K \mid v(x) > \delta \textit{ for every } \delta \in \Delta\}\\
&\phi_{23}(\Delta) = \{x \in K \mid v(x) \geqslant \delta \textit{ for some } \delta \in \Delta\}\\
&\phi_{31}(\mathcal{O}') = \mathfrak{m}' \cap \mathcal{O}\\
&\phi_{32}(\mathcal{O}') = \{\gamma \in vK \mid \gamma, -\gamma < v(x) \textit{ for every } x \in \mathfrak{m}' \cap \mathcal{O}\}.
\end{aligned}$$

Then for every $1 \leqslant i, j \leqslant 3$ such that $i \neq j$, we have that ϕ_{ij} is a bijection between S_i and S_j, whose inverse map is ϕ_{ji}. Furthermore, the rank of $\mathcal{O}$ coincides with the Krull-dimension of $\mathcal{O}$.

Proof. The statement summarises [EP05, Lemma 2.3.1] and the discussion immediately before, at page 43. □

2.1.7 Corollary. *Let K be a field and let $\mathcal{O}$ be a valuation ring of K. Then $\mathbf{rk}(\mathcal{O}) = 1$ if and only if $\mathcal{O}$ is a proper maximal subring of K.*

Proof. Let v be a valuation on K such that $\mathcal{O} = \mathcal{O}_v$. Then the statement follows from Lemma 2.1.6, in view of the correspondence between convex subgroups of Kv and valuation rings of K containing $\mathcal{O}$. □

2.1.8 Example. Let $K = \mathbb{Q}(X)$. Let v_X be the X-adic valuation on $K(X)$ described in Example 2.1.3 (b) and let v be the valuation on K described in Example 2.1.4 (a). Set $\mathcal{O} = \mathcal{O}_v$ and $\mathcal{O}' = \mathcal{O}_{v_X}$. Then $\mathcal{O} \subseteq \mathcal{O}'$. By Lemma 2.1.6, there exist bijections between prime ideals of $\mathcal{O}$, convex subgroups of vK and overrings of $\mathcal{O}$. More precisely, $X\mathcal{O} \in \mathsf{Spec}(\mathcal{O})$ is the prime ideal of $\mathcal{O}$ and $\{0\} \times \mathbb{Z}$ is the convex subgroup of $vK = \mathbb{Z} \times \mathbb{Z}$ corresponding to $\mathcal{O}'$.

Let K be a field. Given subrings $\mathcal{O}, \mathcal{O}'$ of K, we denote by $\mathcal{O}\mathcal{O}'$ the smallest subring of K containing both $\mathcal{O}$ and $\mathcal{O}'$. Let $\mathcal{O}, \mathcal{O}'$ be valuation rings of K. Then $\mathcal{O}\mathcal{O}'$ is an overring of $\mathcal{O}$ (and of $\mathcal{O}'$), and thus it is also a valuation ring of K. We say that *$\mathcal{O}$ and $\mathcal{O}'$ are dependent* if $\mathcal{O}\mathcal{O}' \subsetneq K$, and that they are *independent* otherwise. Let v, w be valuations on K. We say that *v, w are dependent* if $\mathcal{O}_v$ and $\mathcal{O}_w$ are dependent, and that they are *independent* otherwise.

2.1.9 Theorem (Weak Approximation Theorem)**.** *Let K be a field, $n \in \mathbb{N}$ and let $v_1, \ldots, v_n$ be pairwise independent valuations on K. Then for every $x_1, \ldots, x_n \in K$ and $(\gamma_1, \ldots, \gamma_n) \in \prod_{i=1}^{n} v_iK$, there exists $x \in K$ such that $v_i(x - x_i) > \gamma_i$ for all $1 \leqslant i \leqslant n$.*

Proof. See e.g. [EP05, Theorem 2.4.1]. □

It follows by Corollary 2.1.7 that any set of inequivalent valuations of rank 1 on a field is independent, therefore we may apply Theorem 2.1.9 to it.

An important class of valuations of rank 1 is the one of $\mathbb{Z}$-valuations. Let K be a field and let v be a valuation on K. Then v is discrete and of rank-1 if and only if vK is order-isomorphic to $\mathbb{Z}$. We call v a *$\mathbb{Z}$-valuation on K* if $vK = \mathbb{Z}$.

A *discrete valuation ring* is a local principal ideal domain that is not a field. Given a discrete valuation ring $\mathcal{O}$, a generator of the maximal ideal of $\mathcal{O}$ is called *a uniformizer of* $\mathcal{O}$. A number of characterisations for discrete valuation rings are known in the literature. In the following statement we list some of those, which will be used later in this thesis.

2.1.10 Proposition. *Let $\mathcal{O}$ be a domain. Then the following are equivalent:*

(i) $\mathcal{O}$ is a discrete valuation ring.

(ii) $\mathcal{O}$ is a noetherian valuation ring that is not a field.

(iii) $\mathcal{O} = \mathcal{O}_v$ for a $\mathbb{Z}$-valuation v on $\mathsf{Frac}(\mathcal{O})$.

(iv) $\mathcal{O}$ is local, noetherian, integrally closed and has a unique nonzero prime ideal.

(v) $\mathcal{O}$ is a regular local ring of Krull-dimension 1.

Proof. The statement follows from [Mat86, Theorems 11.1 and 11.2]. □

2.2 Extensions of valuation rings and Hensel's Lemma

Let K be a field and let v be a valuation on K.

Let K_0 be a subfield of K. Let v_0 be the restriction of v to K_0, that is, $v_0 = v|_{K_0}$. Then v_0 is a valuation on K_0 whose value group is a subgroup of vK and whose residue field embeds canonically into Kv. Furthermore $\mathcal{O}_v \cap K_0 = \mathcal{O}_{v_0}$. We denote $vK_0 = v_0K_0$ and $K_0v = K_0v_0$.

Let now L/K be a field extension and let w be a valuation on L. We say that w *is an extension of v to L* if $w|_K = v$. We say that w *is an unramified extension of v* if $vK = wL$, and that it is a *ramified extension of v* otherwise. If w is an unramified extension of v and $Lw = Kv$, we say that w *is an immediate extension of v*.

2.2.1 Example. Let (K, v) be a valued field. For $k \in \mathbb{N}$ and $a_0, \ldots, a_k \in K$, we set

$$w(\Sigma_{i=0}^{k} a_i X^i) = \mathsf{min}\{v(a_i) \mid 1 \leqslant i \leqslant k\} \in vK \cup \{\infty\}.$$

For $g, h \in K[X] \smallsetminus \{0\}$ we set $w(g/h) = w(g) - w(h)$. Set $L = K(X)$. Then w is a valuation on L, which is called *Gauss extension of v to L with respect to X*. Note that $w(X) = 0$. Let $\overline{X}$ be the class of X in Lw. Then $\overline{X} \in Lw$ is transcendental over Kv, $Lw = Kv(\overline{X})$ and $wL = vK$. Furthermore, w is the unique extension of v to L such that $w(X) = 0$ and $\overline{X} \in Lw$ is transcendental over Kv; see e.g. [EP05, Corollary 2.2.2]. As a consequence, w is an unramified but not immediate extension of v.

2.2.2 Theorem (Chevalley)**.** *Given a field extension L/K, any valuation on K admits an extension to L.*

Proof. See e.g. [EP05, Theorem 3.1.1]. □

2.2.3 Remark. The proof of Theorem 2.2.2 given in [EP05, Theorem 3.1.1] is based on Zorn's Lemma, and relies thus on the axiom of choice. By using the Gauss extension, it is possible to give an alternative, constructive argument of Theorem 2.2.2 for rational function fields and for finite field extensions.

In view of its crucial role in the study of extensions of valuations, the equations in the following statement are known as *Fundamental Inequality* and *Fundamental Equality.*

2.2.4 Theorem (Fundamental Inequality and Fundamental Equality)**.** *Let L/K be a finite field extension and let v be a valuation on K. Then there exist only finitely many extensions of v to L. Furthermore, let $n \in \mathbb{N}^+$ be the number of extensions of v to L and let $v_1, \ldots, v_n$ be these extensions. Then we have that*

$$\Sigma_{i=1}^{n}[v_iL : vK] \cdot [Lv_i : Kv] \leqslant [L : K].$$

Finally, if $vK = \mathbb{Z}$ and L/K is separable, then

$$\Sigma_{i=1}^{n}[v_iL : vK] \cdot [Lv_i : Kv] = [L : K].$$

Proof. See [EP05, Theorems 3.3.4 and 3.3.5]. □

2.2.5 Corollary. *Let L/K be a finite field extension, let v be the trivial valuation on K and let w be an extension of v to L. Then w is trivial.*

Proof. By Lagrange's theorem we have $|wL| = |vK| \cdot [wL : vK]$. Since v is trivial, we have $|vK| = 1$. By the Fundamental Inequality in Theorem 2.2.4, we have that $[wL : vK] \leqslant [L : K]$, hence $[wL : vK]$ is finite. Thus $|wL|$ is finite. Since wL is torsion-free, by [Ef06, Lemma 2.1.1], we conclude that $wL = \{0\}$. □

2.2.6 Corollary. *Let L/K be a finite field extension, v a valuation on K and w an extension of v to L. Then $\mathbf{rk}(w) = \mathbf{rk}(v)$. If, moreover, w is discrete, then v is discrete.*

Proof. This follows directly from Theorem 2.2.4. □

In the sequel, we will often use the Fundamental Inequality for quadratic extensions. In this setting, we have the following statement.

2.2.7 Corollary. *Let K be a field, let $a \in K^\times \smallsetminus K^{\times 2}$ and set $L = K(\sqrt{a})$. Let v be a non-dyadic valuation on K and let w be an extension of v to L. Then the following hold:*

(1) *Assume that $v(a) \notin 2vK$. Then w is the unique extension of v to L. Furthermore, we have that $[wL : vK] = 2$ and $[Lw : Kv] = 1$.*

(2) *Assume that $v(a) \in 2vK$. Then we have that $wL = vK$, that $aK^{\times 2} \cap \mathcal{O}_v^\times \neq \emptyset$, and that $Lw \simeq Kv(\sqrt{\overline{x}^v})$ for every $x \in aK^{\times 2} \cap \mathcal{O}_v^\times$. Furthermore, if $[Lw : Kv] = 2$, then w is the unique extension of v to L, otherwise there exist exactly two different extensions of v to L.*

Proof. Let $\alpha \in L$ be such that $\alpha^2 = a$. In L we have that $w(a) = w(\alpha^2) = 2w(\alpha)$, hence $w(a) \in 2wL$. If $v(a) \notin 2vK$, we obtain that $[wL : vK] = 2$, otherwise $wL = vK$. Then the statement follows trivially from the Fundamental Equality in Theorem 2.2.4. □

2.2.8 Example. Let $K = \mathbb{R}(\!(t)\!)(X)$ and let v be the Gauss extension to K with respect to X of the t-adic valuation on $\mathbb{R}(\!(t)\!)$. Set $a = X^2 + 1$ and $L = K(\sqrt{a})$, and let w be an extension of v to L. Since $v(a) = 0$, it follows by Corollary 2.2.7 that $wL = vK = \mathbb{Z}$ and

$$Lw \simeq Kv\left(\sqrt{\overline{a}^v}\right).$$

Thus $Lw \simeq \mathbb{R}(X)(\sqrt{a})$, and w is the unique extension of v to L, since $[Lw : Kv] = 2$.

Let K be a field and let v be a valuation on K. We say that v is *henselian* if for every algebraic field extension L/K, v has a unique extension to L. Of course this is equivalent to v having a unique extension to every finite field extension of K. Furthermore, the definition implies directly that any extension of a henselian valuation to an algebraic field extension is again henselian.

The name henselian is motivated by the fact that v is henselian if and only if an analogous statement to Hensel's Lemma holds with respect to v. Let R be a local ring, let $\mathfrak{m}$ be its maximal ideal and let $\kappa = R/\mathfrak{m}$. Given $a \in R$, we denote $\overline{a} = a + \mathfrak{m}$. Given $f \in R[X]$ and $n \in \mathbb{N}$, $a_1, \ldots, a_n \in R$ such that $f = a_0 + a_1X + \ldots + a_nX^n$, we denote by ∂f the formal derivative of f with respect to X, and we set $\overline{f} = \overline{a}_0 + \overline{a}_1X + \ldots + \overline{a}_nX^n \in \kappa[X]$. We say that R *is henselian* if for every $f \in R[X]$ monic and $\alpha \in \kappa$ such that $\overline{f}(\alpha) = 0$ and $\overline{\partial f}(\alpha) \neq 0$, there exists $a \in R$ such that $f(a) = 0$ and $\overline{a} = \alpha$. We have the following:

2.2.9 Theorem. *For a valued field (K, v), the following are equivalent:*

(i) v is henselian.

(ii) $\mathcal{O}_v$ is henselian.

Proof. See [EP05, Theorem 4.1.3]. □

Let R be a local ring and let I be its maximal ideal. Let $\mathfrak{B} = \{x + I^nR \mid x \in R, n \in \mathbb{N}\}$. Then $\mathfrak{B}$ is the basis of a topology on R, which we call *the I-adic topology on R*. The I-adic topology on R makes the operations of R continuous. The set of quotient R-modules $\{R/I^nR\}_{n\in\mathbb{N}}$ and the set of the natural maps $\{R/I^nR \to R/I^mR \mid n, m \in \mathbb{N}, n \geqslant m\}$ form an inverse system. Hence we may construct its inverse limit, which we denote by $\widehat{R}$ and call *the completion of R*. Then $\widehat{R}$ is a local ring, and in fact an R-algebra via the natural ring homomorphism $R \to \widehat{R}$. Its maximal ideal is $I\widehat{R}$. We say that R is *complete* if $R \to \widehat{R}$ is a ring isomorphism.

The most important class of henselian valuations is given by complete $\mathbb{Z}$-valuations. This can be obtained as an example of the following general statement.

2.2.10 Theorem. *A complete local ring is henselian.*

Proof. This follows from [Mat86, Theorem 8.3] and [EP05, Theorem 4.1.3]. □

Given a $\mathbb{Z}$-valuation v, we say that v is *complete* if $\mathcal{O}_v$ is a complete local ring.

2.2.11 Corollary. *A complete $\mathbb{Z}$-valuation is henselian.*

Proof. Since v is complete, we have that $\mathcal{O}_v$ is complete. Hence the statement follows from Theorem 2.2.9 and Theorem 2.2.10. □

2.2.12 Examples. (a) Let K be a field and $n \in \mathbb{N}$. Set $K[\![t_1, \ldots, t_n]\!] = K[\![t_1]\!] \ldots [\![t_n]\!]$. Then $K[\![t_1, \ldots, t_n]\!]$ is a henselian local ring, by Theorem 2.2.10. In particular, $K[\![t]\!]$ is a henselian discrete valuation ring.

(b) For $p \in \mathbb{N}$ prime, the ring of p-adic numbers is a henselian discrete valuation ring.

The implication $(i) \implies (ii)$ of the following statement is commonly known as *Krasner's Lemma*, or as *Krasner-Ostrowski's Lemma.*

2.2.13 Lemma. *Let (K, v) be a valued field, let K^{alg} be an algebraic closure of K and let w be an extension of v to K^{alg}. Then the following are equivalent:*

(*i*) *v is henselian.*

(*ii*) *For every $\alpha, \beta \in K^{alg}$ such that $w(\alpha - \sigma(\alpha)) < w(\alpha - \beta)$ for every K-automorphism σ of K^{alg} with $\sigma(\alpha) \neq \alpha$, we have that $K(\alpha, \beta)/K(\beta)$ is purely inseparable.*

Proof. The statement can be obtained for example from [Ef06, Lemma 18.5.1], by using the characterisation of relative henselian valuations given in [Ef06, Lemma 18.1.2]. □

Krasner's Lemma is also known in the following form. Let K be a field, K^{alg} an algebraic closure of K and $m \in \mathbb{N}$. Given $F \in K^{alg}[X] \smallsetminus \{0\}$ having precisely m roots of F in K^{alg}, we set $C_v(F) = -\infty$ if $m \leqslant 1$, and we set

$$C_v(F) = \mathsf{sup}\{v(\alpha_i - \alpha_j) \mid 1 \leqslant i < j \leqslant m\}$$

where $\alpha_1, \dots, \alpha_m$ are the distinct roots of F in K^{alg} otherwise. Furthermore, given $\alpha \in K^{alg}$, we set $C_v(\alpha/K) = C_v(F)$ where F is the minimal poynomial of α over K.

2.2.14 Theorem (Krasner)**.** *Let $\alpha, \beta \in K^{alg}$ be such that $v(\alpha - \beta) > C_v(\alpha/K)$. Then the extension $K(\alpha, \beta)/K(\beta)$ is purely inseparable. In particular, if α is separable, we have $K(\alpha) \subseteq K(\beta)$.*

Proof. See for example [EP05, Theorem 4.1.7]. □

2.3 Absolute values

Let K be a field. An *absolute value* on K is a map $|\ | : K \to \mathbb{R}$ such that the following hold for every $x, y \in K$:

(*i*) $|0| = 0$ and $|x| > 0$ whenever $x \neq 0$;

(*ii*) $|x \cdot y| = |x| \cdot |y|$;

(*iii*) $|x + y| \leqslant |x| + |y|$.

Given an absolute value $|\ |$ on K, we say that $|\ |$ is *non-archimedean* if we have $|x + y| \leqslant \mathsf{max}\{|x|, |y|\}$ for every $x, y \in K$, and we say that $|\ |$ is *archimedean* otherwise. Non-archimedean absolute values are characterised in the following way:

2.3.1 Proposition. *Let K be a field and let $|\ |$ be an absolute value on K. Then $|\ |$ is non-archimedean if and only if there exists $c \in \mathbb{R}$ such that $|n \cdot 1| \leqslant c$ for every $n \in \mathbb{Z}$.*

Proof. See [EP05, Proposition 1.1.1]. □

2.3.2 Examples. (*a*) The map sending 0 to 0 and every $x \in K^\times$ to 1 is an absolute value, called *the trivial absolute value on K*.

(*b*) The euclidean absolute value $|\ |$ on $\mathbb{C}$, given by $|a + bi| = \sqrt{a^2 + b^2}$ for every $a, b \in \mathbb{R}$, is an archimedean absolute value.

(*c*) Given a subfield K of $\mathbb{C}$, it follows by Proposition 2.3.1 that the absolute value on K induced by the euclidean absolute value on $\mathbb{C}$ is an archimedean absolute value on K.

(d) Let $p \in \mathbb{N}$ be prime. We define an absolute value $| \ |_p$ on $\mathbb{Q}$ as follows. Given $q \in \mathbb{Q}^\times$, let $r, n, m \in \mathbb{Z}$ be such that $m, n \notin p\mathbb{Z}$ and $q = p^r m/n$, and set $|q|_p = e^{-r}$. Set further $|0|_p = 0$. Then $| \ |_p$ is a non-archimedean absolute value on $\mathbb{Q}$, called *p-adic absolute value on $\mathbb{Q}$*.

(e) The construction in (d) can be generalised as follows. Let $v : K \to \mathbb{R} \cup \{\infty\}$ be a valuation and let $x \in K^\times$. Set $|x|_v = e^{-v(x)}$. Then $| \ |_v$ is a non-archimedean absolute value on K, which we call *the absolute value induced by v on K*.

The procedure of Example 2.3.2 (e) can be reversed as follows. Let K be a field and let $| \ |$ be a non-archimedean absolute value. We define a valuation on K, which we call *the valuation induced by* $| \ |$, by setting $v(0) = \infty$ and $v(x) = \log |x| \in \mathbb{R}$ for every $x \in K^\times$. Recall from Examples 2.1.2 that ordered groups of rank 1 are essentially the nontrivial ordered subgroups of $\mathbb{R}$. Hence v has rank 1.

We can also extend the construction from Example 2.3.2 (e) to valuations of rank 1, up to a choice of an embedding of ordered groups $vK \to \mathbb{R}$. We may thus see non-archimedean absolute values as valuations of rank 1, and arbitrary absolute values as a generalisation of the latter; alternatively, we may see valuations as a generalisation of non-archimedean absolute values towards arbitrary ranks. In order to avoid the embarrassment of the choice of the aforementioned embedding, we define an equivalence relation on the absolute values of K in the following way. Let $| \ |_1$ and $| \ |_2$ be two absolute values on K. We say that $| \ |_1$ and $| \ |_2$ are *equivalent* if there exists $c \in \mathbb{R}^{\times 2}$ such that $|x|_1 = |x|_2^c$ for any $x \in K$. When $| \ |_1$ and $| \ |_2$ are non-archimedean, we see that $| \ |_1$ and $| \ |_2$ are equivalent if and only if the corresponding induced valuations are equivalent. As for valuations, it will often be convenient to work with absolute values up to equivalence.

2.3.3 Example. Let K be a number field and $| \ |$ a non-archimedean absolute value on K. Then there exists, up to equivalence, a unique $p \in \mathbb{N}$ prime such that $| \ |$ restricts to $| \ |_p$ on $\mathbb{Q}$.

We discuss now completions of fields. Let K be a field and let $| \ |$ be an absolute value on K. Since the euclidean topology on $\mathbb{R}$ is a metric, $| \ |$ induces a metric on K. We say that *K is complete with respect to* $| \ |$ if every Cauchy sequence in K with respect to the metric on K induced by $| \ |$ converges in K; see [EP05, page 9] for more details. The following statement shows that K possesses a field extension that is complete with respect to an absolute value that restricts to $| \ |$ on K.

2.3.4 Theorem. *For a field K and an absolute value $| \ |$ on K, we have the following:*

(1) *There exists a field $\widehat{K}$, an absolute value $| \ |_{\widehat{K}}$ on $\widehat{K}$ and an embedding $\iota : K \to \widehat{K}$ such that $\widehat{K}$ is complete with respect to $| \ |_{\widehat{K}}$, $\mathsf{Im}(\iota)$ is dense in $\widehat{K}$ with respect to the metric induced by $| \ |_{\widehat{K}}$, and $|x| = |\iota(x)|_{\widehat{K}}$ for every $x \in K$.*

(2) *Let L be a field, let $| \ |_L$ be an absolute value on L such that L is complete with respect to $| \ |_L$ and let $\theta : K \to L$ be an embedding such that $|x| = |\theta(x)|_L$ for every $x \in K$. Then there exists a unique continuous embedding $\eta : \widehat{K} \to L$ such that $\eta|_K = \theta$ and $|\eta(x)|_L = |x|_{\widehat{K}}$ for every $x \in \widehat{K}$. If, moreover, $\mathsf{Im}(\theta)$ is dense in L with respect to the metric induced by $| \ |_L$, then η is an isomorphism.*

Proof. (1) is contained in [EP05, Theorem 1.1.4] literally. The argument for (2) is also contained in [EP05, Theorem 1.1.4], but the statement is formulated in a slightly different way, since it is assumed from the beginning that $\mathsf{Im}(\theta)$ is dense in L with respect to the metric induced by $|\ |_L$. Nonetheless, this assumption is only needed to obtain that η is surjective; see the proof of [EP05, Theorem 1.1.4] at page 12. □

Under the notation of Theorem 2.3.4, the pair $(\widehat{K}, |\ |_{\widehat{K}})$ is called the *completion of K with respect to $|\ |$*. Theorem 2.3.4 (2) ensures that the completion of K with respect to $|\ |$ is unique, up to isomorphism.

2.3.5 Example. The only fields that are complete with respect to an archimedean absolute value are, up to isomorphism, $\mathbb{R}$ and $\mathbb{C}$, which are complete with respect to the ordinary absolute value; see [EP05, Theorem 1.2.3] for an argument.

Let L/K be a field extension and let $|\ |$ be an absolute value on L. It is straightforward that the restriction of $|\ |$ to K is an absolute value on K.

2.3.6 Corollary. *Let L/K be a field extension. Let $|\ |$ be an absolute value on L and let $\widehat{L}$ be the completion of L with respect to $|\ |$. Let $|\ |_K$ be the restriction of $|\ |$ to K and let $\widehat{K}$ be the completion of K with respect to $|\ |_K$. Then there exists a unique continuous K-embedding $\eta : \widehat{K} \to \widehat{L}$ such that $|\eta(x)|_{\widehat{L}} = |x|_{\widehat{K}}$ for every $x \in \widehat{K}$.*

Proof. The statement follows directly from Theorem 2.3.4 (2). □

2.3.7 Corollary. *Let L/K be a field extension and w a $\mathbb{Z}$-valuation on L. Assume that there exists a $\mathbb{Z}$-valuation v on K that is equivalent to $w|_K$. Then there exists a unique continuous K-embedding of valued fields $\eta : K^v \to L^w$ such that $\widehat{w} \circ \eta$ is equivalent to $\widehat{v}$. Furthermore, if L/K is finite, then L^w/K^v is finite as well.*

Proof. The first statement follows from Corollary 2.3.6. See e.g. [Neuk99, p. 161] for the finiteness of L^w/K^v when L/K is finite. □

2.3.8 Examples. Let K be a number field.

(*a*) Let $|\ |$ be an archimedean absolute value on K. In view of Example 2.3.5 and Corollary 2.3.7, the completion of K with respect to $|\ |$ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$.

(*b*) Let $|\ |$ be a non-archimedean absolute value on K. In view of Example 2.3.3 and Corollary 2.3.7, the completion of K with respect to $|\ |$ is isomorphic to a finite extension of $\mathbb{Q}_p$ for a unique $p \in \mathbb{N}$ prime. See also [Neuk99, Proposition II.5.2].

Let K be a field. When working with different absolute values on K, we might want to attach to the completion of K with respect to an absolute value a name that depends explicitly on the absolute value generating the completion, in order to avoid possible misunderstandings. For this reason, and in view of the correspondence between non-archimedean absolute values and valuations of rank 1, we take inspiration from the notation of valuations. We denote by $\mathcal{W}_K$ the set of absolute values on K and, given $w \in \mathcal{W}_K$, we denote by $(K^w, \widehat{w})$ the completion of K with respect to w.

2.3.9 Example. Let $w \in \mathcal{W}_{\mathbb{Q}}$. Then $\mathbb{Q}^w \simeq \mathbb{C}$, $\mathbb{Q}^w \simeq \mathbb{R}$ or $\mathbb{Q}^w \simeq \mathbb{Q}_p$ for $p \in \mathbb{N}$ prime; see e.g. [EP05, Appendix A].

Let K be a field and let v be a $\mathbb{Z}$-valuation on K. Denote by $|\ |$ the absolute value on K induced by v and by $(\widehat{K}, |\ |_{\widehat{K}})$ the completion of K with respect to $|\ |$. Set $K^v = \widehat{K}$, and denote by $\widehat{v}$ the $\mathbb{Z}$-valuation on $\widehat{K}$ associated to $|\ |_{\widehat{K}}$. We call the valued field $(K^v, \widehat{v})$ the *completion of* (K, v), and we call K^v *the completion of K with respect to v*. We say that the valued field (K, v) is *complete* if $(K, v) \simeq (K^v, \widehat{v})$. This is equivalent to having that v is complete; furthermore, $K^v \simeq \mathsf{Frac}(\widehat{\mathcal{O}_v})$ and $Kv \simeq K^v\widehat{v}$ in a canonical way; see [EP05, Theorem 2.4.3 and Proposition 2.4.4].

2.3.10 Examples. (*a*) Let $p \in \mathbb{N}$ be prime, and let v_p be the p-adic valuation on $\mathbb{Q}$. Then $\mathbb{Q}^{v_p} = \mathbb{Q}_p$ and $\mathcal{O}_{\widehat{v}_p} = \mathbb{Z}_p$, which is a complete discrete valuation ring of $\mathbb{Q}_p$; see e.g. [Ef06, Example 9.2.1]. Equivalently, the valued field $(\mathbb{Q}_p, \widehat{v}_p)$ is complete.

(*b*) Let K be a field and let v_X be the X-adic valuation on $K(X)$. Set $\mathcal{O} = K[X]_{(X)}$. Then $\mathcal{O}$ is a discrete valuation ring, but it is not complete. As a matter of fact, the completion of $\mathcal{O}$ is the ring of formal power series in one variable $K[\![X]\!]$; see for example [Ef06, Example 9.2.2]. In other words, $(K(X), v_X)$ is not complete, and its completion is $(K(\!(X)\!), \widehat{v}_X)$, where $\widehat{v}_X$ is the X-adic valuation on $K(\!(X)\!)$.

We end this chapter by stating a celebrated local-global principle by H. Hasse and H. Minkowski. A *global field* is a finite extension of $\mathbb{Q}$ or of $F(X)$ for some finite field F.

2.3.11 Theorem (Hasse-Minkowski)**.** *Let K be a global field and let ϕ be an anisotropic quadratic form over K. Then there exists $w \in \mathcal{W}_K$ such that ϕ_{K^w} is anisotropic.*

Proof. See [OM73, Theorem 66:1] for the case $\mathsf{char}(K) \neq 2$, and [Pol70, Theorem 3.2] for the case $\mathsf{char}(K) = 2$. □

2.4 Valuations and sums of squares

In this section, we present standard tools on valuations and sums of squares in arbitrary fields, which will be useful in the sequel. We also state several classic results about the level and the Pythagoras number of familiar fields from number theory.

We begin with a preliminary result, which we state for an arbitrary domain. Let R be a commutative ring. We denote by $\mathsf{Max}(R)$ the set of maximal ideals of R and by $\mathsf{Jac}(R)$ the *Jacobson radical of* R, which is the ideal of R defined by

$$\mathsf{Jac}(R) = \{x \in R \mid 1 - Rx \subseteq R^\times\}\,.$$

We recall that $\mathsf{Jac}(R) = \bigcap \mathsf{Max}(R)$; see [AMD69, Proposition 1.1.9]. We say that R is *semilocal* if $\mathsf{Max}(R)$ is finite, that is, if R has only finitely many maximal ideals.

2.4.1 Lemma. *Let R be a domain and $k \in \mathbb{N}^+$. Then the following hold:*

(1) $1 + \Sigma_{k-1}R^2 \subseteq R^\times$ *if and only if* $s(R/\mathfrak{m}) \geqslant k$ *for every* $\mathfrak{m} \in \mathsf{Max}(R)$.

(2) *If* $(1 + \Sigma_k R^2) \cap \mathsf{Jac}(R) \neq \emptyset$, *then* $s(R/\mathfrak{m}) \leqslant k$ *for every* $\mathfrak{m} \in \mathsf{Max}(R)$.

(3) *If R is semilocal and such that* $s(R/\mathfrak{m}) \leqslant k$ *for every* $\mathfrak{m} \in \mathsf{Max}(R)$, *then we have* $(1 + \Sigma_k R^2) \cap \mathsf{Jac}(R) \neq \emptyset$.

Proof. Parts (1) and (2) follow immediately from the definition of the level and from the fact that $R^\times = R \smallsetminus \bigcup \mathsf{Max}(R)$ and $\mathsf{Jac}(R) = \bigcap \mathsf{Max}(R)$.

(3) Assume that R is semilocal and $s(R/\mathfrak{m}) \leqslant k$ for every $\mathfrak{m} \in \mathsf{Max}(R)$. For every $\mathfrak{m} \in \mathsf{Max}(R)$, choose $f_{\mathfrak{m},1}, \ldots, f_{\mathfrak{m},k} \in R$ with $1 + f_{\mathfrak{m},1}^2 + \ldots + f_{\mathfrak{m},k}^2 \in \mathfrak{m}$. By the Chinese Remainder Theorem, for $1 \leqslant i \leqslant k$ we find $f_i \in R$ such that $f_i \equiv f_{\mathfrak{m},i} \bmod \mathfrak{m}$ for all $\mathfrak{m} \in \mathsf{Max}(R)$. Then $1 + f_1^2 + \ldots + f_k^2 \in \bigcap \mathsf{Max}(R) = \mathsf{Jac}(R)$. This shows that $(1 + \Sigma_k R^2) \cap \mathsf{Jac}(R) \neq \emptyset$. □

For the remainder of this section, we fix a field K. We call a valuation ring $\mathcal{O}$ of K *real* if its residue field is real, and *nonreal* otherwise; similarly, we call a valuation v on K *real* if $\mathcal{O}_v$ is real, and *nonreal* otherwise. In the sequel, we often use the following result from [BGVG14]. Because of its direct link with Lemma 2.4.1, we include the proof.

2.4.2 Proposition. *Let v be a valuation on K and $n \in \mathbb{N}$. Then the following hold:*

(1) *$s(Kv) \geqslant n$ if and only if, for every $x_1, \ldots, x_n \in K$, we have*

$$v(x_1^2 + \ldots + x_n^2) = 2\mathsf{min}\{v(x_i) \mid 1 \leqslant i \leqslant n\}.$$

(2) *v is real if and only if, for every $n \in \mathbb{N}$ and $x_1, \ldots, x_n \in K$, we have*

$$v(x_1^2 + \ldots + x_n^2) = 2\mathsf{min}\{v(x_i) \mid 1 \leqslant i \leqslant n\}.$$

Proof. (1) By Lemma 2.4.1 (1), we have that $s(Kv) \geqslant n$ if and only if $1+\Sigma_{n-1}{\mathcal{O}_v}^2 \subseteq \mathcal{O}_v^\times$, that is, $v(1 + \Sigma_{n-1}{\mathcal{O}_v}^2) = \{0\}$. For all $x_1, \ldots, x_n \in K$ such that $v(x_1) \leqslant \ldots \leqslant v(x_n)$, we have that $x_1^2 + \ldots + x_n^2 \in x_1^2(1 + \Sigma_{n-1}{\mathcal{O}_v}^2)$. Therefore $s(Kv) \geqslant n$ if and only if $v(x_1^2 + \ldots + x_n^2) = 2\mathsf{min}\{v(x_i) \mid 1 \leqslant i \leqslant n\}$ for all $x_1, \ldots, x_n \in K$.

(2) This follows from (1), since v is real if and only if $s(Kv) \geqslant n$ for every $n \in \mathbb{N}$. □

2.4.3 Lemma. *Let v be a non-dyadic valuation on K, $x \in \mathcal{O}_v^\times$. Then $\ell_K(x) \geqslant \ell_{Kv}(\overline{x}^v)$. Furthermore, if $1 + \mathfrak{m}_v \subseteq K^{\times 2}$, then $\ell_K(x) = \ell_{Kv}(\overline{x}^v)$.*

Proof. Set $l = \ell_K(x)$ and $m = \ell_{Kv}(\overline{x}^v)$. If $l = \infty$, then $l \geqslant m$, trivially. Assume $l < \infty$. If $s(Kv) < l$, then $\overline{x}^v \in \Sigma_l(Kv)^2$, by Proposition 1.2.4. Assume that $s(Kv) \geqslant l$. Consider $x_1, \ldots, x_n \in K$ such that $x_1^2 + \ldots + x_l^2 = x$. Since $x \in \mathcal{O}_v$, it follows by Proposition 2.4.2 that $x_1, \ldots, x_l \in \mathcal{O}_v$. Hence $\overline{x}^v = (\overline{x}_1^v)^2 + \ldots + (\overline{x}_l^v)^2$. This shows that $l \geqslant m$.

Assume now that $1 + \mathfrak{m}_v \subseteq K^{\times 2}$. If $m = \infty$, then $l \leqslant m$, trivially. Assume $m < \infty$. By the definition of m, there exist $x_1, \ldots, x_m \in \mathcal{O}_v$ such that $x_1^2+\ldots+x_m^2-x \in \mathfrak{m}_v$. Since $x \in \mathcal{O}_v^\times$, we may assume $x_1 \in \mathcal{O}_v^\times$. Set $z = x-x_1^2-\ldots-x_m^2$ and $f = (x-x_2^2-\ldots-x_m^2)/x_1^2$. Since $z \in \mathfrak{m}_v$, we have $z/x_1^2 \in \mathfrak{m}_v$. Furthermore, we have $f = 1+(z/x_1)^2 \in 1+\mathfrak{m}_v \subseteq K^{\times 2}$, whereby $f \in K^{\times 2}$. Let $y \in K^\times$ be such that $f = y^2$. Then $x = (x_1y)^2 + x_2^2 + \ldots + x_m^2$, whereby $l \leqslant m$. Therefore $l = m$. □

2.4.4 Remark. The assumption $\mathsf{char}(Kv) \neq 2$ in Lemma 2.4.3 is necessary. As an example, consider $K = \mathbb{Q}_2(X)$, and let v be the Gauss extension to K with respect to X of the dyadic valuation on $\mathbb{Q}_2$. Then $s(K) \leqslant s(\mathbb{Q}_2)$, and thus $\ell_K(X) \leqslant 5$, by Proposition 1.2.4 and [Pfi95, Example 3.1.2 (6)]. Furthermore, $Kv \simeq \mathbb{Z}/2\mathbb{Z}(\overline{X}^v)$, and $\ell_{Kv}(\overline{X}^v) = \infty$.

2.4.5 Corollary. *Let v be a valuation on K. Then $s(K) \geqslant s(Kv)$. Furthermore, if v is nondyadic and $1 + \mathfrak{m}_v \subseteq K^{\times 2}$, then $s(K) = s(Kv)$.*

Proof. If v is dyadic, then $s(Kv) = 1$, and thus $s(K) \geqslant s(Kv)$, trivially. If v is non-dyadic, then the statement follows directly from Lemma 2.4.3, since $s(K) = \ell_K(-1)$. □

Remark. It is easy to see that the assumption $1 + \mathfrak{m}_v \subseteq K^{\times 2}$ in Corollary 2.4.5 cannot be dropped. For instance, the $(X^2 + 1)$-adic valuation on $\mathbb{R}(X)$ has residue field of level 1, whereas $\mathbb{R}(X)$ has infinite level.

2.4.6 Proposition. *Let v be a non-dyadic henselian valuation on K. Then $1+\mathfrak{m}_v \subseteq K^{\times 2}$. In particular, $s(K) = s(Kv)$.*

Proof. Consider $x \in \mathfrak{m}_v$ and set $f = X^2 - 1 - x \in \mathcal{O}_v[X]$. Observe that $f(1) \in \mathfrak{m}_v$, and $\partial f(1) = 2 \notin \mathfrak{m}_v$, since v is non-dyadic. Since v is henselian, there exists $y \in \mathcal{O}_v$ such that $f(y) = 0$, whereby $1+x = y^2 \in F^{\times 2}$. Then the statement follows from Corollary 2.4.5. □

2.4.7 Example. If $\mathsf{char}(K) = 2$, then $s(K) = s(K(\!(t)\!)) = 1$, trivially. Otherwise, since the t-adic valuation on $K(\!(t)\!)$ is henselian and has residue field K, it follows by Proposition 2.4.6 that $s(K(\!(t)\!)) = s(K)$.

For a valuation v on K, we have the following inequality of Pythagoras numbers, which is analogous to the inequality $s(K) \geqslant s(Kv)$ from Corollary 2.4.5.

2.4.8 Proposition. *Let v be a valuation on K. Then $p(K) \geqslant p(Kv)$.*

Proof. If v is dyadic, then $p(Kv) = 1$, and the statement is trivial. Assume that v is non-dyadic. Consider $x \in \mathcal{O}_v$ such that $\overline{x}^v \in \Sigma Kv^2$. Let $n \in \mathbb{N}$, $x_1, \dots, x_n \in \mathcal{O}_v$ be such that $\overline{x}^v = (\overline{x}_1^v)^2 + \dots + (\overline{x}_n^v)^2$. Then $\ell_K(x_1^2 + \dots + x_n^2) \geqslant \ell_{Kv}(\overline{x}^v)$, by Lemma 2.4.3. Thus

$$\mathsf{sup}\{\ell_{Kv}(\overline{x}^v) \mid x \in \mathcal{O}_v \text{ such that } \overline{x}^v \in \Sigma(Kv)^2\} \leqslant \mathsf{sup}\{\ell_K(x) \mid x \in \Sigma(Kv)^2\},$$

that is, $p(Kv) \leqslant p(K)$. □

Even for a henselian valuation v on K, we do not have the equality $p(K) = p(Kv)$. As an example, consider $K = \mathbb{C}(\!(t)\!)$, and let v be the t-adic valuation on K. Then $Kv \simeq \mathbb{C}$, whereby $p(Kv) = 1$. But since $v(t) = 1$, we have that $t \notin K^2$, whereby $p(\mathbb{C}(\!(t)\!)) \geqslant 2$. Nevertheless, we are often interested in bounding $p(K)$ from above in terms of $p(Kv)$. The issue was examined in [BGVG14], where the following notation was introduced:

$$p'(K) = \begin{cases} p(K) & \text{if } K \text{ is real,} \\ s(K) + 1 & \text{if } K \text{ is nonreal.} \end{cases}$$

By Proposition 1.2.4, we obtain that $p(K) \leqslant p'(K) \leqslant p(K) + 1$. The advantage of the invariant p' compared to p is its better behaviour with respect to henselian valuations, which is expressed in the following statement, which extends [BGVG14, Proposition 4.3].

2.4.9 Theorem. *Let v be a non-dyadic henselian valuation on K with $1 + \mathfrak{m}_v \subseteq K^{\times 2}$. Then*

$$p'(K) = p'(Kv)\,.$$

Proof. By Corollary 2.4.5, we have $s(K) = s(Kv)$. Hence K and Kv are either both real, or both nonreal. In the latter case, $p'(K) = s(K)+1 = s(Kv)+1 = p'(Kv)$. Assume that K and Kv are real. Then $p(K) \geqslant p(Kv)$, by Proposition 2.4.8, thus $p'(K) \geqslant p'(Kv)$. If $p(Kv) = \infty$, then $p'(K) = p'(Kv) = p(Kv) = \infty$. Assume $p(Kv) < \infty$. In order to show $p(K) \leqslant p(Kv)$, consider $x \in (\Sigma K^2)^\times$. Then $v(x) \in 2vK$, by Proposition 2.4.2. Hence there exists $t \in K^\times$ such that $t^2 x \in \mathcal{O}_v^\times$. Set $y = t^2 x$. Clearly $\ell_K(x) = \ell_K(y)$. Since $1 + \mathfrak{m}_v \subseteq K^2$, it follows by Lemma 2.4.3 that $\ell_K(y) = \ell_{Kv}(\overline{y}^v)$. As $\ell_{Kv}(\overline{y}^v) \leqslant p(Kv)$, we obtain that $\ell_K(x) \leqslant p(Kv)$. Therefore $p(K) \leqslant p(Kv)$. Thus $p'(K) = p'(Kv)$. □

2.4.10 Example. By Theorem 2.4.9, we have that $p(K(\!(t)\!)) = p(K)$ if K is real, and $p(K(\!(t)\!)) = s(K)+1$ otherwise. By Proposition 1.2.4 we have that $p(K) \in \{s(K), s(K)+1\}$ if K is nonreal, and both cases are actually possible [Lam05, Theorem XI.5.7].

The techniques developed above can be used to compute the Pythagoras number and the level of global and local fields, to which we dedicate the remainder of this section. We call K *local* if it is the completion of a global field with respect to an absolute value (see Section 2.3).

2.4.11 Proposition. *A field is local if and only if it is isomorphic to $\mathbb{R}$, $\mathbb{C}$ or a finite field extension of $\mathbb{Q}_p$ or $\mathbb{F}_p(\!(t)\!)$ for $p \in \mathbb{N}$ prime.*

Proof. This follows from the characterisation of absolute values over number fields; see e.g. [EP05, Appendix B]. □

We say that a local field is *archimedean* if it is isomorphic to $\mathbb{R}$ or to $\mathbb{C}$, and *non-archimedean* otherwise.

2.4.12 Proposition. *Non-archimedean local fields are precisely the fields that are complete with respect to a $\mathbb{Z}$-valuation having finite residue field; furthermore, such a $\mathbb{Z}$-valuation is uniquely determined by the field.*

Proof. See e.g. [Jac89, Section 9.12]. □

We say that a local field is *dyadic* if it is complete with respect to a dyadic $\mathbb{Z}$-valuation, and non-dyadic otherwise.

2.4.13 Proposition. *Let K be a nonreal, non-dyadic local field and v the $\mathbb{Z}$-valuation with respect to which K is complete. Then $s(K) = 1$, $p(K) \leqslant 2$ if $|Kv| \equiv 1 \bmod 4$, and $s(K) = 2$, $p(K) \leqslant 3$ otherwise.*

Proof. If $K \simeq \mathbb{C}$, then $s(K) = 1$. Assume now $K \not\simeq \mathbb{C}$. Then $K \simeq K_0^w$ for a global field K_0 and an absolute value w on K_0, by Proposition 2.4.11. Since K is nonreal, we have that w is non-archimedean. Therefore $\widehat{w}$ is a complete non-dyadic $\mathbb{Z}$-valuation on K such that $K\widehat{w}$ is finite. Hence $s(K) = s(K\widehat{w})$, by Proposition 2.4.6. In view of Example 1.2.2, we have that $s(K) = 1$ if $|Kv| \equiv 1 \bmod 4$, and $s(K) = 2$ otherwise. By Proposition 1.2.4, we conclude that $p(K) \leqslant 2$ if $|Kv| \equiv 1 \bmod 4$, and $p(K) \leqslant 3$ otherwise. □

2.4.14 Proposition. *Let $K/\mathbb{Q}_2$ be a finite field extension. Then $s(K) \leqslant 2$ if $[K : \mathbb{Q}_2]$ is even, and $s(K) = 4$ otherwise.*

Proof. See [Pfi95, Example 3.1.2 (6)]. □

The Hasse-Minkowski Local-Global Principle allows us to express the level of a global field in terms of the level of certain local fields. Recall from Section 2.3 that $\mathcal{W}_K$ denotes the set of absolute values on K.

2.4.15 Theorem. *Let K be a global field. Then we have*

$$s(K) = \max\{s(K^w) \mid w \in \mathcal{W}_K\}.$$

Proof. Set $m = \max\{s(K^w) \mid w \in \mathcal{W}_K\}$. Since $s(K^w) \leqslant s(K)$ for every $w \in \mathcal{W}_K$, it is clear that $m \leqslant s(K)$. Set now $\phi = (m+1) \times \langle 1 \rangle_K$. Then ϕ_{K^w} is isotropic for every $w \in \mathcal{W}_K$, by the definition of m. It follows by the Hasse-Minkowski Local-Global Principle (Theorem 2.3.11) that ϕ is isotropic. Therefore $s(K) \leqslant m$, by Proposition 1.1.5. □

2.4.16 Corollary. *For a nonreal global field K, we have $s(K) \leqslant 4$.*

Proof. This follows from Theorem 2.4.15, Proposition 2.4.13 and Proposition 2.4.14. □

It follows from Corollary 2.4.16 that a nonreal local field has Pythagoras number at most 5. As a matter of fact, any local or global field has Pythagoras number at most 4. More precisely, we have the following statements.

2.4.17 Theorem. *For a local field K, we have $p(K) = \min\{s(K) + 1, 4\}$.*

Proof. See [Pfi95, Example 7.1.4 (a)]. □

2.4.18 Theorem. *Let K be a number field. Then we have the following:*

(1) *If K is nonreal, then $p(K) = \mathsf{min}\{s(K) + 1, 4\}$.*

(2) *Assume that K is real. If there exists a dyadic $\mathbb{Z}$-valuation v on K such that $[K^v : \mathbb{Q}_2]$ is odd, then $p(K) = 4$, otherwise $p(K) = 3$.*

Proof. See [Pfi95, Examples 7.1.4 (2), (3)]. □

2.4.19 Example. $p(\mathbb{Q}(\sqrt{5})) = 3$.

Theorem 2.4.18 and the previous results cover the following classic statement.

2.4.20 Theorem (Euler, Hilbert, Siegel)**.** *If K is a number field, then $p(K) \leqslant 4$.*

Theorem 2.4.20 was originally announced by Hilbert, according to C.L. Siegel [Si21], but only proven by Siegel himself [Si21, Hauptsatz (Satz 1)]. Theorem 2.4.20 implies that $p(K) \leqslant 4$ for every algebraic field extension $K/\mathbb{Q}$. This is part of a more general fact, which allows one to extend a bound on the Pythagoras number of finitely generated field extensions to arbitrary field extensions. More precisely, we have the following statement.

2.4.21 Proposition. *Let K/K_0 be a field extension. Then*

$$p(K) \leqslant \mathsf{sup}\{p(F) \mid F/K_0 \textit{ is a finitely generated field extension contained in } K/K_0\}.$$

Proof. Set $S = \{p(F) \mid F/K_0$ is a finitely generated field extension contained in $K/K_0\}$ and $p = \mathsf{sup}\, S$. If $p = \infty$, then there is nothing to show. Assume that $p < \infty$. In order to show that $p(K) \leqslant p$, consider $x \in \Sigma K^2$. Let $n \in \mathbb{N}$, $x_1, \ldots, x_n \in K$ be such that $x = \Sigma_{i=1}^n x_i^2$ and let $F = K_0(x_1, \ldots, x_n) \subseteq K$. Since $F \in S$, we have $p(F) \leqslant p$, whereby $x \in \Sigma_p F^2 \subseteq \Sigma_p K^2$. Therefore $p(K) \leqslant p$. □

Chapter 3
The Real Holomorphy Ring

This chapter is dedicated to the study of the real holomorphy ring of a field, that is, the intersection of all its real valuation rings. We are especially interested in the real holomorphy ring of a function field in one variable $F/\mathbb{Q}$, whose algebraic properties will be exploited in the following chapters to obtain information about sums of squares in F. Before introducing real holomorphy rings, we study arbitrary intersections of valuation rings of a field.

3.1 Intersections of valuation rings

In this section we summarise several known properties of intersections of valuation rings of a field that will be used in the sequel.

3.1.1 Proposition. *The following statements hold:*

(1) *The intersection of integrally closed subrings of a field is integrally closed.*

(2) *Every valuation ring is integrally closed.*

Proof. See e.g. [Kap74, Theorem 52] for (1), and [EP05, Theorem 3.1.3] for (2). □

3.1.2 Theorem. *Let K be a field and let R be a subring of K. Then the integral closure of R in K is given by the intersection of all valuation rings of K containing R. In particular, if K is the fraction field of R, then R is integrally closed if and only if it is the intersection of all the valuation rings of K containing R.*

Proof. The statement follows from [EP05, Theorem 3.1.3] and Proposition 3.1.1. □

Valuation rings are especially related to *Prüfer domains*, which are a specific type of integrally closed domains. Let R be a domain. For two R-submodules I, J of $\mathsf{Frac}(R)$, set

$$I * J = \{\textstyle\sum_{k=1}^{n} x_k y_k \mid n \in \mathbb{N} \text{ and } x_k \in I, y_k \in J \text{ for } 1 \leqslant k \leqslant n\} \subseteq \mathsf{Frac}(R),$$

and observe that $I * J$ is an R-submodule of $\mathsf{Frac}(R)$. A *fractional ideal of R* is an R-submodule I of $\mathsf{Frac}(R)$ such that there exists $r \in R \smallsetminus \{0\}$ such that $rI \subseteq R$. Given a fractional ideal I of R, we set $I^{*0} = R$ and $I^{*n} = I^{*(n-1)} * I$ for any $n \in \mathbb{N}^+$; furthermore, we say that I is *invertible* if there exists a fractional ideal J of R such that $I * J = R$. A *Prüfer domain* is a domain in which any nonzero finitely generated ideal is invertible.

3.1.3 Theorem. *Let R be a domain. Then the following are equivalent:*

(*i*) *R is a Prüfer domain.*

(*ii*) *For every* $a, b \in R$ *not both zero, the ideal* $aR + bR$ *is invertible.*

(*iii*) $R_{\mathfrak{p}}$ *is a valuation ring for every* $\mathfrak{p} \in \mathsf{Spec}(R)$.

(*iv*) $R_{\mathfrak{m}}$ *is a valuation ring for every* $\mathfrak{m} \in \mathsf{Max}(R)$.

Proof. See [Gi92, Theorem 22.1]. □

3.1.4 Corollary. *Every Prüfer domain is integrally closed.*

Proof. For any domain R we have, by [Kap74, Theorem 53], that

$$R = \bigcap_{\mathfrak{m} \in \mathsf{Max}(R)} R_{\mathfrak{m}}.$$

Then the statement follows by Proposition 3.1.1 and Theorem 3.1.3. □

The concept of Prüfer domain generalises the one of Dedekind domain. A *Dedekind domain* is a domain whose nonzero fractional ideals are invertible.

3.1.5 Proposition. *For a domain* R *that is not a field, the following are equivalent:*

(*i*) R *is a Dedekind domain.*

(*ii*) R *is integrally closed, noetherian and of Krull dimension* 1.

(*iii*) R *is noetherian and its localisations at its maximal ideals are discrete valuation rings.*

Proof. See e.g. [Bo98, Theorem VII.2.1]. □

3.1.6 Corollary. *Let* R *be a domain. Then* R *is a Dedekind domain if and only if* R *is a noetherian Prüfer domain.*

Proof. Recall that a noetherian valuation ring that is not a field is a discrete valuation ring, by Proposition 2.1.10. Since the localisation of a noetherian ring is noetherian, the statement follows from Proposition 3.1.5 and Theorem 3.1.3. □

A *Bézout domain* is a domain whose finitely generated ideals are principal.

3.1.7 Proposition. *Bézout domains are Prüfer domains and, in particular, integrally closed.*

Proof. The statement follows from Corollary 3.1.6 and Corollary 3.1.4. □

Let K be a field. By a *Bézout ring of* K we mean a subring R of K which is a Bézout domain and such that $\mathsf{Frac}(R) = K$.

3.1.8 Proposition. *Let* R *be a domain and let* $K = \mathsf{Frac}(R)$. *Then the following are equivalent:*

(*i*) R *is a semilocal Bézout ring of* K.

(*ii*) R *is a finite intersection of valuation rings of* K.

Proof. ($i \Rightarrow ii$) Assume that R is a Bézout ring of K. Then for each $\mathfrak{m} \in \mathsf{Max}(R)$, $R_{\mathfrak{m}}$ is a valuation ring of K, by [Kap74, Theorem 64]. Furthermore $R = \bigcap_{\mathfrak{m} \in \mathsf{Max}(R)} R_{\mathfrak{m}}$, by [Kap74, Theorem 53], and if R is semilocal, then this is a finite intersection.

($ii \Rightarrow i$) See [Kap74, Theorem 107]. □

An analogous relation to the one described in Corollary 3.1.6 connects Bézout domains with principal ideal domains.

3.1.9 Proposition. *A ring is a noetherian Bézout domain if and only if it is a principal ideal domain.*

Proof. The statement follows directly from the definitions. □

In order to study intersections of valuation rings, we introduce the following notations. Let F be a field. We denote by $\Omega(F)$ the set of valuation rings of F. Given $T \subseteq F$, we denote by $\Omega(F/T)$ the set of valuation rings of F containing T.

Let now $S \subseteq \Omega(F)$. We set $\mathcal{H}_S = \{x \in F \mid x \in \mathcal{O} \text{ for every } \mathcal{O} \in S\}$, that is,

$$\mathcal{H}_S = \bigcap S = \bigcap_{\mathcal{O} \in S} \mathcal{O},$$

if $S \neq \emptyset$, and $\mathcal{H}_S = F$ otherwise. We call $\mathcal{H}_S$ the *holomorphy ring of F associated to S.*

Observe that $\mathcal{H}_S$ is integrally closed, by Proposition 3.1.1. Furthermore, let $\mathcal{O} \in S$ and let $\mathfrak{m}$ be the maximal ideal of $\mathcal{O}$. Then we have that $\mathfrak{m} \cap \mathcal{H}_S \in \mathsf{Spec}(\mathcal{H}_S)$.

3.1.10 Proposition. *Let $\emptyset \subsetneq S \subseteq \Omega(F)$. Then we have*

$$\mathcal{H}_S^\times = \bigcap_{\mathcal{O} \in S} \mathcal{O}^\times.$$

Proof. Let $x \in F^\times$ and let x^{-1} be its inverse in F. For every $\mathcal{O} \in S$, we have that $x \in \mathcal{O}^\times$ if and only if $x, x^{-1} \in \mathcal{O}$. Then $x \in \bigcap_{\mathcal{O} \in S} \mathcal{O}^\times$ if and only if $x, x^{-1} \in \bigcap_{\mathcal{O} \in S} \mathcal{O} = \mathcal{H}_S$, that is, if and only if $x \in \mathcal{H}_S^\times$, whereby the statement. □

It is particularly interesting to study intersections of valuation rings of a function field in one variable. By a *function field in one variable* we mean a finitely generated field extension of transcendence degree 1. Given a function field in one variable F/K, there exists $x \in F$ such that $F/K(x)$ is a finite extension; clearly such elements x exist and are exactly the elements of F that are transcendental over K.

3.1.11 Proposition. *Let F/K be a function field in one variable and let $\mathcal{O} \in \Omega(F/K)$. If $\mathcal{O} \neq F$, then $\mathcal{O}$ is a discrete valuation ring of F.*

Proof. Assume that $\mathcal{O}$ is nontrivial. Let $x \in F$ be such that $F/K(x)$ is finite. Then x is transcendental over K and $\mathcal{O} \cap K(x)$ is a valuation ring of $K(x)$, which is a rational function field in one variable over K. It follows by [EP05, Theorem 2.1.4 (b)] that $\mathcal{O} \cap K(x)$ is a discrete valuation ring. Then $\mathcal{O}$ is also a discrete valuation ring, by Corollary 2.2.6. □

3.1.12 Theorem. *Let F/K be a function field in one variable and let $S \subsetneq \Omega(F/K)$. Then $\mathcal{H}_S$ is a Dedekind domain and* $\mathsf{Frac}(\mathcal{H}_S) = F$.

Proof. See [FJ08, Proposition 3.3.2]. □

3.2 The real holomorphy ring of a field

In this section, we describe what is known in the literature about the real holomorphy ring of a field; in doing so, we largely rely on [Lam81], [Lam05] and [Pre84].

Given a field F, we denote by $\mathcal{R}(F)$ the set of real valuation rings of F. Let F be a real field. We define *the real holomorphy ring of* F as $\mathcal{H}(F) = \bigcap \mathcal{R}(F)$, i.e.,

$$\mathcal{H}(F) = \{x \in K \mid x \in \mathcal{O} \text{ for every } \mathcal{O} \in \mathcal{R}(F)\}.$$

3.2.1 Lemma. *Let F be a real field and $x \in F^\times$ such that $x^2 \neq -1$. Then*

$$x/(1+x^2), x^2/(1+x^2) \in \mathcal{H}(F).$$

Proof. For every real valuation v on F we have that $v(1+x^2) = 2\mathsf{min}\{0, v(x)\}$, by Proposition 2.4.2; thus

$$v(1+x^2) = \mathsf{min}\{0, v(x^2)\} \geqslant \mathsf{min}\{0, v(x)\}.$$

Hence $x/(1+x^2), x^2/(1+x^2) \in \mathcal{H}(F)$. □

In certain situations we are interested in a specific overring of the real holomorphy ring. Let F be a real field and $S \subseteq F$. We set $\mathcal{R}(F/S) = \{\mathcal{O} \in \mathcal{R}(F) \mid S \subseteq \mathcal{O}\}$, and we define the *real holomorphy ring of F relative to S* as $\mathcal{H}(F/S) = \bigcap \mathcal{R}(F/S)$, that is,

$$\mathcal{H}(F/S) = \{x \in F \mid x \in \mathcal{O} \text{ for every } \mathcal{O} \in \mathcal{R}(F/S)\}.$$

In this thesis, we will mostly encounter real holomorphy rings relative to a subfield.

3.2.2 Corollary. *Let F be a real field and $S \subseteq F$. Then $\mathsf{Frac}(\mathcal{H}(F/S)) = F$.*

Proof. As $\mathsf{Frac}(\mathcal{H}(F/S)) \subseteq F$ by construction, it is enough to show the opposite inclusion. Let $x \in K$. By Lemma 3.2.1, we have $x/(1+x^2), x^2/(1+x^2) \in \mathcal{H}(F) \subseteq \mathcal{H}(F/S)$. Since

$$x = x^2/(1+x^2) \cdot \left(x/(1+x^2)\right)^{-1},$$

we obtain that $x \in \mathsf{Frac}(\mathcal{H}(F/S))$. Hence $F \subseteq \mathsf{Frac}(\mathcal{H}(F/S))$. □

3.2.3 Theorem. *Let F be a real field, let $S \subseteq K$ and set $\mathcal{H} = \mathcal{H}(F/S)$. Let $n \in \mathbb{N}$ and $x_1, \ldots, x_n \in \mathcal{H}$. Then we have*

$$(x_1\mathcal{H} + \ldots + x_n\mathcal{H})^{*2} = (x_1^2 + \ldots + x_n^2)\mathcal{H}.$$

Proof. Set $x = x_1^2 + \ldots + x_n^2$. It is straightforward that $x \in (x_1\mathcal{H} + \ldots + x_n\mathcal{H})^{*2}$, whereby $x\mathcal{H} \subseteq (x_1\mathcal{H} + \ldots + x_n\mathcal{H})^{*2}$. In order to prove the opposite inclusion, consider a real valuation v on K. By Proposition 2.4.2, we have $v(x) = 2\mathsf{min}\{v(x_i) \mid 1 \leqslant i \leqslant n\}$. Consider $1 \leqslant i, j \leqslant n$. We have $v(x_ix_j) \geqslant v(x)$, that is, $x_ix_j/x \in \mathcal{O}_v$. We obtain that $x_ix_j/x \in \bigcap \mathcal{R}(F/S) = \mathcal{H}$, that is, $x_ix_j \in x\mathcal{H}$, whereby $(x_1\mathcal{H} + \ldots + x_n\mathcal{H})^{*2} \subseteq x\mathcal{H}$. □

3.2.4 Corollary. *Let F be a real field and $S \subseteq F$. Then $\mathcal{H}(F/S)$ is a Prüfer domain.*

Proof. By Theorem 3.2.3, any nonzero finitely generated ideal of $\mathcal{H}(F/S)$ is invertible. Hence $\mathcal{H}(F/S)$ is a Prüfer domain. □

3.2.5 Proposition. *Let F/K be a real field extension and let $S \subseteq K$. Then we have $\mathcal{H}(K/S) \subseteq \mathcal{H}(F/S)$.*

Proof. Let $\mathcal{O} \in \mathcal{R}(F/S)$. Recall from Section 2.2 that $\mathcal{O} \cap K$ is a valuation ring of K containing S and that its residue field embeds canonically into the residue field of $\mathcal{O}$. The latter is real by assumption, therefore $\mathcal{O} \cap K \in \mathcal{R}(K/S)$. We conclude that

$$\mathcal{H}(K/S) \subseteq \bigcap \{x \in K \mid x \in \mathcal{O} \text{ for every } \mathcal{O} \in \mathcal{R}(F/S)\} \subseteq \mathcal{H}(F/S).$$

□

3.2.6 Proposition. *Let F/K be a real function field in one variable. Then $\mathcal{H}(F/K)$ is a Dedekind domain.*

Proof. Let $x \in F$ be transcendental over K and denote by v the (x^2+1)-adic valuation on $K(x)$. By Theorem 2.2.2, there exists an extension of v to F, which we denote by w. Note that $K(x)v \simeq K(\sqrt{-1})$, whereby v is nonreal. Since $K(x)v$ embeds into Fw, the latter is nonreal as well. Since w is trivial on K, we obtain that $\mathcal{O}_w \in \Omega(F/K) \smallsetminus \mathcal{R}(F/K)$. We conclude that $\mathcal{R}(F/K) \subsetneq \Omega(F/K)$. Hence the statement follows from Theorem 3.1.12. □

3.2.7 Lemma. *Let F/K be a real function field in one variable and let I be an ideal of $\mathcal{H}(F/K)$. Then the following are equivalent:*

(i) *There exists $f \in \Sigma\mathcal{H}(F/K)^2$ such that $I = f\mathcal{H}(F/K)$.*

(ii) *There exists an ideal J of $\mathcal{H}(F/K)$ such that $I = J^{*2}$.*

(iii) *There exist $a, b \in \mathcal{H}(F)$ such that $I = (a^2+b^2)\mathcal{H}(F/K)$.*

Proof. ($i \Rightarrow ii$) Let $f \in \Sigma\mathcal{H}(F/K)^2$ be such that $I = f\mathcal{H}(F/K)$ and consider $n \in \mathbb{N}$, $f_1, \dots, f_n \in \mathcal{H}(F/K)$ such that $f = \Sigma_{i=1}^n f_i^2$. Set $J = f_1\mathcal{H}(F/K) + \ldots + f_n\mathcal{H}(F/K)$. Then $I = J^{*2}$, by Theorem 3.2.3.

($ii \Rightarrow iii$) Note that $\mathcal{H}(F/K)$ is a Dedekind domain, by Proposition 3.2.6. Hence there exist $a, b \in \mathcal{H}(F/K)$ such that $J = a\mathcal{H}(F/K) + b\mathcal{H}(F/K)$. It follows by Theorem 3.2.3 that $I = (a^2+b^2)\mathcal{H}(F/K)$.

($iii \Rightarrow i$) This implication is trivial. □

We focus now on function fields in one variable over number fields.

3.2.8 Proposition. *Let K be a real number field and $S \subseteq K$. Then $\mathcal{R}(K/S) \subseteq \{K\}$, and $\mathcal{H}(K/S) = K$.*

Proof. Recall from Example 2.1.3 (a) that any nontrivial valuation on $\mathbb{Q}$ is equivalent to the p-adic valuation for some $p \in \mathbb{N}$ prime, and is thus nonreal. Then $\mathcal{R}(\mathbb{Q}/S) \subseteq \{\mathbb{Q}\}$, whereby $\mathcal{H}(\mathbb{Q}/S) = \mathbb{Q}$. Hence $\mathcal{R}(K/S) \subseteq \{K\}$ and $\mathcal{H}(K/S) = K$ for any number field K, by Corollary 2.2.5. □

3.2.9 Corollary. *Let $F/\mathbb{Q}$ be a real function field in one variable and I an ideal of $\mathcal{H}(F)$. Then $\mathcal{H}(F)$ is a Dedekind domain, and the following are equivalent:*

(i) *There exists $f \in \Sigma\mathcal{H}(F)^2$ such that $I = f\mathcal{H}(F)$.*

(ii) *There exist $a, b \in \mathcal{H}(F)$ such that $I = (a^2+b^2)\mathcal{H}(F)$.*

Proof. By Proposition 3.2.8, we have that $\mathcal{H}(\mathbb{Q}) = \mathcal{H}(\mathbb{Q}/\emptyset) = \mathbb{Q}$. Then $\mathbb{Q} \subseteq \mathcal{H}(F)$, by Proposition 3.2.5. Therefore $\mathcal{H}(F) = \mathcal{H}(F/\mathbb{Q})$. Then the statement follows form Proposition 3.2.6 and Lemma 3.2.7. □

Let F be a field and let P be a preordering on F. Since $\mathsf{char}(F) = 0$, we have that $\mathbb{Z} \subseteq F$. We may thus set

$$\mathcal{O}(P) = \{x \in F \mid \exists\, n \in \mathbb{N} \text{ such that } -n \leqslant_P x \leqslant_P n\}.$$

3.2.10 Theorem. *Let F be a field and let P be an ordering on F. Then $\mathcal{O}(P)$ is a valuation ring of F.*

Proof. See [Lam81, Theorem 2.6]. □

Let F be a field and let P be an ordering on F. We denote by $\mathfrak{m}(P)$ the maximal ideal of $\mathcal{O}(P)$ and we set $\kappa(P) = \mathcal{O}(P)/\mathfrak{m}(P)$, $\overline{P} = (P \cap \mathcal{O}(P) + \mathfrak{m}(P))/\mathfrak{m}(P) \subseteq \kappa(P)$.

We say that P is *archimedean* if for every $x \in F$ there exists $n \in \mathbb{N}$ such that $x \leqslant_P n$. Clearly, this is equivalent to having $\mathcal{O}(P) = F$.

3.2.11 Theorem. *Let F be a field and let P be an ordering on F. Then $\overline{P}$ is an archimedean ordering on $\kappa(P)$. In particular, we have that $\mathcal{O}(P) \in \mathcal{R}(F)$.*

Proof. By [Lam81, Theorem 2.6, Proposition 2.9] we have that $\bar{P}$ is an ordering on $\kappa(P)$. Moreover, $\overline{P}$ is also archimedean; see [Lam81, p. 19]. □

Given a field F, we denote by $\mathfrak{X}_F$ the set of orderings on F.

3.2.12 Corollary. *Let F be a real field. Then we have*

$$\mathcal{H}(F) = \bigcap_{P \in \mathfrak{X}_F} \mathcal{O}(P).$$

Proof. Set

$$\mathcal{H} = \bigcap_{P \in \mathfrak{X}_F} \mathcal{O}(P).$$

Then $\mathcal{H}(F) \subseteq \mathcal{H}$, by Theorem 3.2.11. Conversely, we obtain by [Lam81, Proposition 3.8], that for any $\mathcal{O} \in \mathcal{H}(F)$ there exists an ordering $P_{\mathcal{O}}$ on F such that $\mathcal{O}(P_{\mathcal{O}}) \subseteq \mathcal{O}$. Hence we also have that $\mathcal{H} \subseteq \mathcal{H}(F)$. □

3.2.13 Proposition. *Let F be a field, let $P \in \mathfrak{X}_F$ and let $\kappa(P)$ be the residue field of $\mathcal{O}(P)$. Then there exists a unique embedding $i_P : \kappa(P) \to \mathbb{R}$ such that for every $x \in \mathcal{O}(P)^\times$ we have that $x \in P$ if and only if $i_P(x + \mathfrak{m}(P)) > 0$.*

Proof. Set $\overline{P} = P \cap \mathcal{O}(P) + \mathfrak{m}(P)$. In view of Theorem 3.2.11, we know that $\overline{P}$ is an archimedean ordering on the residue field $\kappa(P)$. We conclude by [PD01, Theorem 1.1.5] that there exists a unique embedding of ordered fields from $(\kappa(P), \overline{P})$ into $(\mathbb{R}, \mathbb{R}^2)$. Hence the statement is proven. □

Let F be a real field and let $P \in \mathfrak{X}_F$. We denote by i_P the embedding of ordered fields $\kappa(P) \to \mathbb{R}$ described in Proposition 3.2.13. Fix $x \in \mathcal{H}(F)$. Note that $x \in \mathcal{O}(P)$, by Theorem 3.2.11. Thus we may define a map $\tilde{x} : \mathfrak{X}_F \to \mathbb{R}$ by setting $\tilde{x}(P) = i_P(x + \mathfrak{m}(P))$ for any $P \in \mathfrak{X}_F$.

3.2.14 Remark. Let F be a real field, $x, y \in \mathcal{H}(F)$ and $a, b \in \mathbb{Q}$, and set $z = ax + by \in F$. Then we have that $\tilde{z} = a\tilde{x} + b\tilde{y}$. In particular, the association $x \mapsto \tilde{x}$ is an embedding of $\mathbb{Q}$-vector spaces $\mathcal{H}(F) \to \mathbb{R}^{\mathfrak{X}_F}$.

Let F be a field. For every $x \in F$, let $H_x = \{P \in \mathfrak{X}_F \mid x \in P\}$; let τ_F be the topology on $\mathfrak{X}_F$ having $\{H_x \mid x \in F\}$ as a subbasis. The topology τ_F is called *the Harrison topology on $\mathfrak{X}_F$*. The Harrison topology satisfies the following properties.

3.2.15 Theorem. *For a field F, the topological space $(\mathfrak{X}_F, \tau_F)$ is compact and Hausdorff.*

Proof. See [Lam05, Theorem VIII.6.3]. □

3.2.16 Lemma. *Let F be a real field and let $x \in \mathcal{H}(F)$. Then the following hold:*

(1) *Let τ_e denote the euclidean topology on $\mathbb{R}$. Then $\tilde{x}$ is a continuous map from the topological space $(\mathfrak{X}_F, \tau_F)$ to the topological space $(\mathbb{R}, \tau_e)$.*

(2) *There exist $a, b \in \mathbb{Q}$ such that $\mathsf{Im}(\tilde{x}) \subseteq [a, b]$.*

(3) *$x \in \Sigma F^2$ if and only if $\mathsf{Im}(\tilde{x}) \subseteq [0, \infty)$.*

(4) *$x \in \mathcal{H}(F)^\times$ if and only if $0 \notin \mathsf{Im}(\tilde{x})$.*

Proof. (1) The statement follows from [Lam81, Theorem 9.7].

(2) By Theorem 3.2.15, we have that $(\mathfrak{X}_F, \tau_F)$ is compact. Since the continuous image of a compact set is compact, we obtain that $\mathsf{Im}(\tilde{x})$ is a compact subspace of $(\mathbb{R}, \tau_e)$. Hence $\mathsf{Im}(\tilde{x})$ is bounded, whereby the statement.

(3) By construction of the map $\tilde{x}$, we have that $\mathsf{Im}(\tilde{x}) \subseteq \mathbb{R}^2$ if and only if $x \in P$ for every $P \in \mathfrak{X}_F$, that is, if and only if $x \in \bigcap \mathfrak{X}_F$. By Theorem 1.2.15, we have that $\bigcap \mathfrak{X}_F = \Sigma F^2$, whereby the statement is proved.

(4) Recall that $\mathcal{H}(F)^\times = \bigcap_{P \in \mathfrak{X}_F} \mathcal{O}(P)^\times$, by Proposition 3.1.10. Hence $x \in \mathcal{H}(F)^\times$ if and only if $x \notin \mathfrak{m}(P)$ for every $P \in \mathfrak{X}_F$. By construction of the map $\tilde{x}$, for every $P \in \mathfrak{X}_F$ we have that $x \notin \mathfrak{m}(P)$ if and only if $\tilde{x}(P) \neq 0$, whereby the statement. □

We conclude this section with the following characterisation of the real holomorphy ring, which will prove useful in Chapter 6.

3.2.17 Lemma. *For a field F and a preordering P on F, we have that*

$$\mathcal{O}(P) = \{x \in F \mid \exists\, n \in \mathbb{N} \textit{ such that } n - x^2 \in P\}.$$

Proof. Set $\mathcal{O} = \{x \in F \mid \exists\, n \in \mathbb{N}$ such that $n - x^2 \in P\}$. Let $x \in \mathcal{O}(P)$ and let $n \in \mathbb{N}$ be such that $-n \leqslant_P x \leqslant_P n$. Since $P \cdot P \subseteq P$, we have that $n^2 - x^2 \in P$. Hence $\mathcal{O}(P) \subseteq \mathcal{O}$. Vice versa, let $x \in \mathcal{O}$ and let $n \in \mathbb{N}$ be such that $n - x^2 \in P$. If $1 \leqslant_P x$, then we have $-n \leqslant 0 \leqslant_P x \leqslant_P x^2 \leqslant_P n$. If $x \leqslant_P -1$, then we have $-n \leqslant_P -x^2 \leqslant_P x \leqslant_P -1 \leqslant_P n$. Otherwise, we have $-1 \leqslant_P x \leqslant_P 1$. In any case $x \in \mathcal{O}(P)$. Thus $\mathcal{O} \subseteq \mathcal{O}(P)$. □

3.2.18 Theorem. *Let F be a real field. Then we have*

$$\mathcal{H}(F) = \{x \in F \mid \exists n \in \mathbb{N} \textit{ such that } n - x^2 \in \Sigma F^2\}.$$

Proof. Set $\mathcal{H} = \{x \in F \mid \exists n \in \mathbb{N}$ such that $n - x^2 \in \Sigma F^2\}$. In view of Corollary 3.2.12, it is enough to show that $\mathcal{H} = \bigcap_{P \in \mathfrak{X}_F} \mathcal{O}(P)$. Consider $P \in \mathfrak{X}_F$. Since $\Sigma F^2 \subseteq P$, it follows by Lemma 3.2.17 that $\mathcal{H} \subseteq \mathcal{O}(P)$. Hence $\mathcal{H} \subseteq \mathcal{H}(F)$. Let now $x \in \bigcap_{P \in \mathfrak{X}_F} \mathcal{O}(P)$. Then

$\mathfrak{X}_F = \bigcup_{n\in\mathbb{N}} H_{n-x^2}$. By Theorem 3.2.15 we have that $(\mathfrak{X}_F, \tau_F)$ is compact, hence there exist $k, n_1, \dots n_k \in \mathbb{N}$ such that $\mathfrak{X}_F = \bigcup_{i=1}^{k} H_{n_i - x^2}$. Set $m = \mathsf{max}\{n_1, \dots, n_k\}$. Then $\mathfrak{X}_F = H_{m-x^2}$, that is, $m - x^2 \in P$ for every $P \in \mathfrak{X}_F$. By Theorem 1.2.15, we conclude that $m - x^2 \in \Sigma F^2$. Therefore $\bigcap_{P\in\mathfrak{X}_F} \mathcal{O}(P) \subseteq \mathcal{H}$, whence the statement is proven. □

Chapter 4

The Pythagoras number of function fields

In this chapter we show that the Pythagoras number of a function field in one variable over a number field is at most 6. This was originally proven by F. Pop in his unpublished preprint [Pop90]. The argument we present is inspired by Pop's one, but uses different techniques.

4.1 Function fields in one variable

This section presents several known results from the literature about Pythagoras numbers of function fields in one variable, which will be used in the remainder of this dissertation. In the following overview we largely rely on [Pfi95].

All fields mentioned in the previous chapters have Pythagoras number 2^n or $2^n + 1$ for some $n \in \mathbb{N}$. For nonreal fields, this is simply by Proposition 1.2.4 and Theorem 1.2.6. Though for some time only real fields of Pythagoras number 2^n or $2^n + 1$ for some $n \in \mathbb{N}$ were known, it was eventually proven by D. Hoffmann that every positive integer occurs as the Pythagoras number of some real field [Ho99]. Nevertheless, to this date the only known examples of real fields with Pythagoras number not contained in $\{2^n, 2^n+1 \mid n \in \mathbb{N}\} \cup \{\infty\}$ are constructed by an infinite iteration of function field extensions. In particular, no field of Pythagoras number not in $\{2^n, 2^n+1 \mid n \in \mathbb{N}\} \cup \{\infty\}$ is known that is finitely generated over any proper subfield. It is indeed an open problem to understand the behaviour of the Pythagoras number under field extensions with a real base field. It has been a crucial discovery by J.W.S. Cassels [Cas64, Theorem 2] that $p(K(X)) > p(K)$ holds whenever K is real. However, we do not know yet whether the Pythagoras number grows slowly or fast when passing from a real field to the rational function field over it. To this date, a few examples of K are known where $p(K(X)) = p(K) + 2$ [Pfi95, Example 7.1.11], [BL11, Example 7.16], but there is no confirmed example where $p(K(X)) > p(K) + 2$. Nevertheless, in most of the known situations, the growth is minimal. For example, this is the case for number fields, for which we have the following.

4.1.1 Theorem (Pourchet, Hsia, Johnson)**.** *Let K be a number field. If K is real, then $p(K(X)) = p(K) + 1$, otherwise $p(K(X)) = s(K) + 1$.*

Proof. See [HJ74]. □

Note that the work of Hsia and Johnson in [HJ74] completed the work of Pourchet, who had shown the following in [Pou71].

4.1.2 Theorem (Pourchet)**.** *For any number field K, we have $p(K(X)) \leqslant 5$.*

Proof. See [Pou71]; in Chapter 6, we give an extended exposition of Pourchet's proof. □

A simple computation shows that the growth of the Pythagoras number in a rational extension is minimal also for the field $\mathbb{R}$, that is, $p(\mathbb{R}(X)) = 2$. The fields K that satisfy $p(K(X)) = 2$ were characterized by E. Becker in [Bec78].

We say that a field K is *hereditarily pythagorean* if it is real and if every finite real field extension of K is pythagorean.

4.1.3 Example. A real closed field is hereditarily pythagorean.

4.1.4 Theorem (Becker)**.** *A field K is hereditarily pythagorean if and only if $-1 \notin K^{\times 2}$ and $p(K(X)) = 2$.*

Proof. Whenever K is real, it has been shown in [Bec78, Theorem III.4] that K is hereditarily pythagorean if and only if $p(K(X)) = 2$. On the other hand, if $-1 \notin K^{\times 2}$ and $p(K(X)) = 2$, then K is real by Proposition 1.2.8, whence the statement. □

4.1.5 Proposition. *Let (K, v) be a valued field such that Kv is hereditarily pythagorean and v is henselian. Then K is hereditarily pythagorean.*

Proof. Consider a real finite field extension L/K. Since v is henselian, it extends uniquely to a valuation w on L, and w is also henselian non-dyadic. Since L/K is finite, it follows by the Fundamental Inequality (Theorem 2.2.4) that Lw/Kv is a finite extension. Since w is henselian non-dyadic, it follows by Proposition 2.4.6 that Lw is a real field. Since Kv is henselian, we have that $p(Lw) = 1$. Therefore $p(L) = 1$, by Theorem 2.4.9. This shows that K is hereditarily pythagorean. □

4.1.6 Proposition. *For a hereditarily pythagorean field K, the field $K(\!(t)\!)$ is hereditarily pythagorean.*

Proof. The statement follows from Theorem 4.1.4 and [BGVG14, Theorem 6.9]. □

4.1.7 Corollary. *For a hereditarily pythagorean field K and $n \in \mathbb{N}$, the field $K(\!(t_1)\!)\dots(\!(t_n)\!)$ is hereditarily pythagorean.*

Proof. The statement follows from Proposition 4.1.6 by induction. □

The behaviour of the Pythagoras number for arbitrary function fields in one variable is even more obscure, and even finding upper bounds is remarkably complicated. A fundamental result concerning the Pythagoras number of function fields in one variable over $\mathbb{R}$ was obtained by E. Witt in [Wi34]. Below we give a more general version of it, where $\mathbb{R}$ is replaced by a hereditarily euclidean field.

Let K be a field. We say that K is *euclidean* if K is real and $K^\times = K^{\times 2} \cup -K^{\times 2}$. We say that K is *hereditarily euclidean* if K is real and every real finite field extension of K is euclidean.

4.1.8 Theorem (Witt)**.** *Let K be a hereditarily euclidean field and F/K a function field in one variable. Then $p(F) = 2$.*

Proof. See [ELP73, Theorem F]. □

The inequality $p(F) \geqslant 2$ from Theorem 4.1.8 can be proven much more generally.

4.1.9 Theorem. *Let F/K be a finitely generated transcendental field extension where $\mathsf{char}(K) \neq 2$. Then $p(F) \geqslant 2$.*

Proof. The statement follows for example from [Lam05, Corollary VIII.5.9]. □

In the following statement, a characterisation is given of all the base fields over which every function field in one variable has Pythagoras number exactly 2.

4.1.10 Theorem. *Let K be a field such that $-1 \notin K^2$. Then K is hereditarily euclidean if and only if $p(F) = 2$ for every function field in one variable F/K.*

Proof. Assume that K is hereditarily euclidean and let F/K be a function field in one variable. Since $\mathsf{char}(K) \neq 2$, it follows by Theorem 4.1.9 that $p(F) \geqslant 2$. The inequality $p(F) \leqslant 2$ follows by [ELP73, Theorem F]. Therefore $p(F) = 2$. If K is not hereditarily euclidean, then $p\left(K(X)(\sqrt{-(1+X^2)})\right) \geqslant 3$, by [TI03, Theorem 4]. □

Function fields in one variable over $\mathbb{Q}$ have also been studied for a long time. We reserve the next section to their study.

4.2 Function fields over a number field

In [CT86, Theorem 2], J.L. Colliot-Thélène exploited the local-global principle obtained by K. Kato in [Kat86] to show that the Pythagoras number of a function field in one variable over $\mathbb{Q}$ is at most 7. Later F. Pop strengthened this bound to 6 in the preprint [Pop90]. At this date, a more recent version is available on Pop's webpage [Pop23]. Besides Kato's local-global principle, Pop's argument uses classical geometric tools, plus a trick to obtain a certain identity in $\mathbb{Q}_2$. In this section, we present an alternative proof for the upper bound $p(F) \leqslant 6$ for any function field in one variable $F/\mathbb{Q}$. Our argument differs from Pop's one in the tools that it involves, among which is the real holomorphy ring of F. It turns out that the algebraic properties of the latter, which were discussed in Chapter 3, are all what is necessary to retrieve the aforementioned bound, using Pop's trick and Kato's local-global principle, by means of elementary observations. The innovation contained in this section does not rely in the statements themselves, but rather in their proofs, and in particular in the proofs of Theorems 4.2.6 and 4.2.8. Our methods also produce a neat proof that $\Sigma K[X]^2 = \Sigma_5 K[X]^2$ for every number field K; see Corollary 4.2.8.

We begin by rewriting Kato's local-global principle advantageously. Let F/K be a field extension. We call F/K *regular* if it is separable and K is relatively algebraically closed in F. If F/K is regular, it follows by [Jac75, Corollary IV.10.1], that $F \otimes_K E$ is a domain for every field extension E/K. Let E/K be a field extension. If E/K or F/K is regular, we denote $EF = \mathsf{Frac}(E \otimes_K F)$.

4.2.1 Lemma. *Let $F/\mathbb{Q}$ be a function field in one variable, let K be the relative algebraic closure of $\mathbb{Q}$ in F and let w be an absolute value on K. Then we have the following:*

(1) *F/K is regular.*

(2) *$F \otimes_K K^w$ is a domain, and FK^w/K^w is a function field in one variable.*

(3) *F/K is the function field of a smooth projective curve over K.*

Proof. (1) As $\mathsf{char}(K) = 0$, we have that F/K is separable. By assumption, K is relatively algebraically closed in F. Therefore F/K is regular.

(2) Since F/K is regular, it follows by [Jac75, Corollary IV.10.1] that $F \otimes_K K^w$ is a domain, and by [Liu06, Proposition 1.13 and Example 1.15] that FK^w/K^w is a function field in one variable.

(3) As F/K is a function field in one variable, we get by [Liu06, Proposition 7.3.13] that F/K is the function field of a normal projective curve $\mathcal{C}$ over K. Then $\mathcal{C}$ is regular, by [Liu06, Proposition 4.1.12; see also Example 4.2.9]. Since $\mathsf{char}(K) = 0$, we have that K is perfect. Therefore $\mathcal{C}$ is smooth, by [Liu06, Corollary 4.3.33]. □

Let K be a field. Recall from Section 2.3 that we denote by $\mathcal{W}_K$ the set of absolute values on K. Given $w \in \mathcal{W}_K$, we say that w is *dyadic* if it is non-archimedean and corresponds to a dyadic valuation on K, and *non-dyadic* otherwise.

4.2.2 Proposition. *Let $F/\mathbb{Q}$ be a function field in one variable and let K be the relative algebraic closure of $\mathbb{Q}$ in F. Then $p(FK^w) \leqslant 3$ for every $w \in \mathcal{W}_K$ non-dyadic.*

Proof. Let $w \in \mathcal{W}_K$ and set $L = FK^w$. Then L/K^w is a function field in one variable, by Lemma 4.2.1 (2). Recall from Section 2.3 that K^w is a local field. If $K \simeq \mathbb{R}$, then $p(L) \leqslant 2$, by Theorem 4.1.8. Otherwise $s(L) \leqslant s(K^w) \leqslant 2$, by Proposition 2.4.13, and thus $p(L) \leqslant 3$, by Proposition 1.2.4. □

4.2.3 Theorem (Kato)**.** *Let $F/\mathbb{Q}$ be a function field in one variable and let $f \in \Sigma F^2$. Then $f \in \Sigma_4 F^2$ if and only if $f \in \Sigma_4 (F \otimes_{\mathbb{Q}} \mathbb{Q}_2)^2$.*

Proof. If $f \in \Sigma_4 F^2$, then $f \in \Sigma_4 (F \otimes_{\mathbb{Q}} \mathbb{Q}_2)^2$, trivially. Assume that $f \in \Sigma_4 (F \otimes_{\mathbb{Q}} \mathbb{Q}_2)^2$. Let $K \subseteq F$ be the relative algebraic closure of $\mathbb{Q}$ in F and consider $w \in \mathcal{W}_K$ dyadic. Then $\mathbb{Q}_2 \subseteq K^w$, and we have a natural homomorphism $h : F \otimes_{\mathbb{Q}} \mathbb{Q}_2 \to F \otimes_K K^w$. Since $f \in \Sigma_4 (F \otimes_{\mathbb{Q}} \mathbb{Q}_2)^2$ and h is a ring homomorphism, we obtain that $f \in \Sigma_4 (F \otimes_K K^w)^2$. Together with Proposition 4.2.2, this shows that $f \in \Sigma_4 (FK^w)^2$ for all $w \in \mathcal{W}_K$. Recalling from [Lam05, §III.2] that $\langle\langle -1, -1 \rangle\rangle_{FK^w}$ is the norm form of the quaternion algebra $(-1, -1)_{FK^w}$, we get that f is a norm of $(-1, -1)_{FK^w}$. Observe that F is the function field of a smooth projective curve $\mathcal{C}$ over K, by Lemma 4.2.1 (3). Recall that $\mathcal{C}$ is proper; see e.g. [Liu06, Proposition 3.3.16]. Furthermore, FK^w is the function field of the base change of $\mathcal{C}$ to K^w.

In view of this, it follows by [Kat86, Theorem 0.8 (2)] and [MS82, Theorem 12.2] that $\langle\langle -1, -1, f \rangle\rangle_F$ is hyperbolic; see also the discussion on [Kat86, page 146]. Therefore $f \in \Sigma_4 F^2$, by Proposition 1.1.5. □

4.2.4 Corollary (Colliot-Thélène)**.** *Let $F/\mathbb{Q}$ be a nonreal function field in one variable. Then $p(F) \leqslant 5$.*

Proof. Since F is nonreal, we have that $-1 \in \Sigma F^2$. By Proposition 2.4.14, we have that $-1 \in \Sigma_4 {\mathbb{Q}_2}^2$. Since $\mathbb{Q}_2 \subseteq F \otimes_{\mathbb{Q}} \mathbb{Q}_2$, we obtain that $-1 \in \Sigma_4 (F \otimes_{\mathbb{Q}} \mathbb{Q}_2)^2$. It follows by Theorem 4.2.3 that $-1 \in \Sigma_4 F^2$, whereby $p(F) \leqslant 5$. □

The following example shows that the bound in Corollary 4.2.4 is optimal.

4.2.5 Example. Let $K = \mathbb{Q}(\sqrt{-7})$ and $F = K(X)$. Then $s(F) = 4$, by Theorem 1.1.10, and $p(F) = 5$, by Proposition 1.2.8.

Let F be a field. Recall from Section 3.2 that the real holomorphy ring of F is defined as $\mathcal{H}(F) = \bigcap \mathcal{R}(F)$ where $\mathcal{R}(F)$ is the set of real valuation rings of F.

4.2.6 Theorem (Pop)**.** *Let $F/\mathbb{Q}$ be a real function field in one variable. Then we have the following:*

(1) $\mathcal{H}(F)^\times \cap \Sigma F^2 \subseteq \Sigma_5 F^2$.

(2) $\Sigma F^2 = \Sigma_2 F^2(\Sigma F^2 \cap \mathcal{H}(F)^\times)$.

Proof. (1) Consider $f \in \mathcal{H}(F)^\times \cap \Sigma F^2$. Clearly we have $(f+1)^2/f \in \mathcal{H}(F) \cap \Sigma F^2$. By Lemma 3.2.16, there exists $a \in \mathbb{R}^{\times 2}$ such that $(\tilde{f}(P)+1)^2/\tilde{f}(P) \leqslant a$ for all $P \in \mathfrak{X}(F)$. Let $k \in \mathbb{N}$ be such that $k \geqslant \mathsf{max}\{2, \log_2(a)/2\}$ and set

$$g = f - (f+1)^2/2^{2k}.$$

We will show that $g \in \Sigma F^2$ and $g \in \Sigma_4(F \otimes_{\mathbb{Q}} \mathbb{Q}_2)^2$. Consider an ordering P on F. Then $\tilde{g}(P) = \tilde{f}(P) - (\tilde{f}(P)+1)^2/2^{2k}$. Since $(\tilde{f}(P)+1)^2/\tilde{f}(P) \leqslant a$ and $2^{2k} \geqslant a$, we obtain $\tilde{g}(P) \geqslant 0$. Thus $\mathsf{Im}(\tilde{g}) \subseteq [0,\infty)$, and $g \in \Sigma F^2$, by Lemma 3.2.16 (3). Moreover, we have

$$\begin{aligned} 2^{2k} g = 2^{2k} f - f^2 - 2f - 1 &= -1\left(f^2 + 2f(1-2^{2k-1}) + 1\right) \\ &= -1\left((f+1-2^{2k-1})^2 + 2^{2k}(1-2^{2k-2})\right) \end{aligned}$$

Since $k \geqslant 2$, we have that $2k-2 \geqslant 2$. Therefore $1 - 2^{2k-2} \equiv 1 \mathsf{\ mod\ } 4$. It follows by [Lam05, Corollary VI.2.24] that $1 - 2^{2k-2} \in \Sigma_2 {\mathbb{Q}_2}^2$. By Proposition 2.4.14, we have that $-1 \in \Sigma_4 {\mathbb{Q}_2}^2$. Thus $2^{2k} g \in \Sigma_4(F \otimes_{\mathbb{Q}} \mathbb{Q}_2)^2$, by Theorem 1.1.16. Since $F/\mathbb{Q}$ is a function field in one variable, we conclude by Theorem 4.2.3 that $2^{2k} g \in \Sigma_4 F^2$, whereby $g \in \Sigma_4 F^2$. Since $f = g + ((f+1)/2^k)^2$, we conclude that $f \in \Sigma_5 F^2$. Hence $\mathcal{H}(F)^\times \cap \Sigma F^2 \subseteq \Sigma_5 F^2$.

(2) The inclusion $\Sigma_2 F^2(\Sigma F^2 \cap \mathcal{H}(F)^\times) \subseteq \Sigma F^2$ is clear. In order to prove the opposite inclusion, consider $f \in (\Sigma F^2)^\times$ and set $g = f/(1+f^2)$. Note that $g \in \mathcal{H}(F)$, by Lemma 3.2.1, hence $g \in \Sigma F^2 \cap \mathcal{H}(F)$. Recall that $\mathcal{H}(F/\mathbb{Q}) = \mathcal{H}(F)$. By Lemma 3.2.7, there exists $a \in (\Sigma_2 \mathcal{H}(F)^2)^\times$ such that $a\mathcal{H}(F) = g\mathcal{H}(F)$, that is, such that $g/a \in \mathcal{H}(F)^\times$. Then $f = a(1+f^2) \cdot g/a$, where $g/a \in \Sigma F^2 \cap \mathcal{H}(F)^\times$ and $a(1+f^2) \in \Sigma_2 F^2$ by Theorem 1.1.16. Therefore $\Sigma F^2 \subseteq \Sigma_2 F^2(\Sigma F^2 \cap \mathcal{H}(F)^\times)$, which concludes the proof. □

4.2.7 Corollary (Pop). *Let $F/\mathbb{Q}$ be a function field in one variable. Then $p(F) \leqslant 6$.*

Proof. By Theorem 4.2.6, we get $\Sigma F^2 = \Sigma_2 F^2(\Sigma F^2 \cap \mathcal{H}(F)^\times)$ and $\Sigma F^2 \cap \mathcal{H}(F)^\times \subseteq \Sigma_5 F^2$. Furthermore $\Sigma_5 F^2 \cdot \Sigma_2 F^2 \subseteq \Sigma_6 F^2$, by Theorem 1.1.16. Thus $\Sigma F^2 \subseteq \Sigma_2 F^2 \cdot \Sigma_5 F^2 \subseteq \Sigma_6 F^2$, and $p(F) \leqslant 6$. □

The bound obtained in Corollary 4.2.7 is the best upper bound for the Pythagoras number of function fields in one variable over $\mathbb{Q}$ that is currently available in the literature. Nonetheless, no such field of Pythagoras number 6 is known at the moment, leaving the question open whether this bound is optimal or not. We have already mentioned that Pourchet showed in [Pou71] that $p(K(X)) \leqslant 5$ for every number field K. Furthermore, Corollary 4.2.4 shows that the bound 6 is not optimal when we restrict to nonreal function fields in one variable over $\mathbb{Q}$, and Theorem 4.2.6 shows that even for real ones, a large class of elements actually consists of sums of 5 squares. As witnessed by the following statement, the techniques developed here also provide a nice conceptual argument that another large set of sums of squares (morally half of them) in a rational function field over $\mathbb{Q}$ consists of sums of five squares.

4.2.8 Corollary. *Let K be a real number field and $f \in \Sigma K[X]^2$ square-free in $K[X]$ such that* $\deg(f) \in 4\mathbb{Z}$. *Then $f \in \Sigma_5 K[X]^2$.*

Proof. Set $\mathcal{H} = \mathcal{H}(K(X))$ and $S = \{\mathcal{O}_v \mid v \text{ real valuation on } K(X)\}$, so that $\mathcal{H} = \mathcal{H}_S$. Denote by $\mathcal{P}_K$ the set of monic irreducible polynomials in $K[X]$, and, for $p \in \mathcal{P}_K$, by

v_p the p-adic valuation on $K(X)$; denote further by v_∞ the degree-valuation on $K(X)$. Recall from Proposition 3.2.8 that a nontrivial valuation on a number field is nonreal. Hence any real valuation on $K(X)$ is trivial on K, and is thus equivalent to either v_∞ or v_p for some $p \in \mathcal{P}_K$; see Example 2.1.3 (*d*). Observe further that $\mathcal{H}^\times = \bigcap_{\mathcal{O}\in S} \mathcal{O}^\times$, by Proposition 3.1.10.

Let $k \in \mathbb{N}$ be such that $\deg(f) = 4k$ and set $g = f/(1+X^2)^{2k}$. Observe first that $v_\infty(g) = 4k - \deg(f) = 0$, that is, $g \in \mathcal{O}_{v_\infty}^\times$. Consider now $p \in \mathcal{P}_K$ such that v_p is real. Let $n \in \mathbb{N}$, $f_1, \dots, f_n \in K[X]$ be such that $f = \Sigma_{i=1}^n f_i^2$. By Proposition 2.4.2, we have $v_p(g) = 4k(\mathsf{min}\{v_p(f_i) \mid 1 \leqslant i \leqslant n\} - \mathsf{min}\{v_p(1), v_p(X)\})$. Since f is square-free, there exists $i \in \{1, \dots, n\}$ such that p does not divide f_i in $K[X]$, whereby $v_p(f_i) = 0$. Since $v_p(f_j) \geqslant 0$ for every $1 \leqslant j \leqslant n$, $v_p(1) = 0$ and $v_p(X) \geqslant 0$, we get by Proposition 2.4.2 that $v_p(1+X^2) = v_p(f) = 0$. Hence $v_p(g) = 0$, that is, $g \in \mathcal{O}_{v_p}^\times$.

This shows that $g \in \mathcal{H}(K(X))^\times$. Since $f \in \Sigma K(X)^2$, we have $g \in \Sigma K(X)^2$. Therefore $g \in \Sigma_5 K(X)^2$, by Theorem 4.2.6. Thus $f = ((1+X^2)^k)^2 g \in \Sigma_5 K(X)^2$ as well. By Theorem 1.1.21, we conclude that $f \in \Sigma_5 K[X]^2$. □

4.2.9 Question. *Does $p(F) \leqslant 5$ hold for every function field in one variable $F/\mathbb{Q}$?*

Chapter 5
A local-global principle for rational function fields

In Section 4.2, we have obtained a characterisation of sums of four squares in a function field in one variable over a number field from the local-global principle for 3-fold Pfister forms contained in [Kat86]. Kato's argument for such a local-global principle mostly relies on classical cohomological instruments. For the rational function field in one variable over a number field we provide here an alternative, simpler argument for Kato's local-global principle, based on standard quadratic form theory and valuation theory. The central idea of this argument is to combine Springer's theorem for non-dyadic discretely valued fields and Milnor's exact sequence, and it is due to P. Gupta, who showed it to the author for the base field $\mathbb{Q}$ and for the 3-fold Pfister forms $\langle\langle -1,-1,a\rangle\rangle_{\mathbb{Q}(X)}$ where $a \in \Sigma\mathbb{Q}(X)^2$.

In Section 5.1 we study quadratic forms on discretely valued fields in order to develop the tools that we will later apply in Section 5.2 to obtain the local-global principle. Finally, in Section 5.3, we state the local-global principle explicitly for several fields.

5.1 Quadratic forms over rational function fields

In this section, we study the behaviour of quadratic forms over discretely valued fields, and in particular over rational function fields equipped with the p-adic valuation for an irreducible polynomial p. In order to do this, we fix a field K of characteristic different from 2.

Given a non-dyadic $\mathbb{Z}$-valuation v on K and a Pfister form ϕ over K, we say that ϕ is *unramified with respect to* v if $\phi \simeq \langle\langle a_1,\dots,a_m\rangle\rangle_K$ for some $m \in \mathbb{N}$ and $a_1,\dots,a_m \in \mathcal{O}_v^\times$, and *ramified with respect to* v otherwise.

5.1.1 Example. In this chapter we are especially interested in the n-fold Pfister form $2^n \times \langle 1\rangle_K$ for $n \in \mathbb{N}$. This is obviously unramified with respect to any valuation on K.

The next statement describes the structure of a ramified Pfister form and will help us defining its residue form.

5.1.2 Lemma. *Let v be a non-dyadic $\mathbb{Z}$-valuation on K and π a uniformizer of v. Let $m \in \mathbb{N}^+$ and let ϕ be an m-fold Pfister form over K that is ramified with respect to v. Then there exists an $(m-1)$-fold Pfister form ψ over K that is unramified with respect to v and $u \in \mathcal{O}_v^\times$ such that $\phi \simeq \psi \perp u\pi\psi$.*

Proof. Up to isometry, we may assume that $\phi \simeq \langle\langle a_1,\dots,a_{k-1},a_k\pi,\dots,a_m\pi\rangle\rangle_K$ for some $a_1,\dots,a_m \in \mathcal{O}_v^\times$ and $1 \leqslant k \leqslant m$. Observe that $\langle\langle a_j\pi, a_{j+1}\pi\rangle\rangle_K \simeq \langle\langle -a_ja_{j+1}, a_{j+1}\pi\rangle\rangle_K$ for every $k \leqslant j \leqslant m-1$. Hence we may assume, up to isometry, that $k = m$. Therefore the statement follows by setting $u = a_m$ and $\psi = \langle\langle a_1,\dots,a_{m-1}\rangle\rangle_K$. □

Let v be a non-dyadic $\mathbb{Z}$-valuation on K and ϕ a Pfister form over K. If ϕ is unramified with respect to v, we let $m \in \mathbb{N}$ and $a_1, \dots, a_m \in \mathcal{O}_v^\times$ be such that $\phi \simeq \langle\langle a_1, \dots, a_m \rangle\rangle_K$, and we set $\overline{\phi}^v = \langle\langle \overline{a}_1^v, \dots, \overline{a}_m^v \rangle\rangle_{Kv}$. If ϕ is ramified with respect to v, we let ψ be an $(m-1)$-fold Pfister form over K as in Lemma 5.1.2, and we set $\overline{\phi}^v = \overline{\psi}^v$. We call $\overline{\phi}^v$ the *residue form of ϕ with respect to v.*

5.1.3 Remark. By [Lam05, Corollary VI.1.5], the residue form $\overline{\phi}^v$ only depends on ϕ, and not on the choice of $a_1, \dots, a_m$ and ψ, up to Witt equivalence. By Theorem 1.1.17, a Pfister form over K is isotropic if and only if it is hyperbolic. Hence $\overline{\phi}^v$ only depends on ϕ, up to isometry.

5.1.4 Lemma. *Let v be a non-dyadic $\mathbb{Z}$-valuation on K, $m \in \mathbb{N}^+$ and $a_1, \dots, a_m \in \mathcal{O}_v^\times$. If $\langle \overline{a}_1^v, \dots, \overline{a}_m^v \rangle_{Kv}$ is isotropic, then there exists $t \in D_K(\langle a_1, \dots, a_m \rangle)$ such that $v(t) = 1$.*

Proof. Assume that $\langle \overline{a}_1^v, \dots, \overline{a}_m^v \rangle_{Kv}$ is isotropic and let $x_1, \dots, x_m \in \mathcal{O}_v$ be such that $\overline{a}_1^v \overline{x}_1^{v2} + \dots + \overline{a}_m^v \overline{x}_m^{v2} = 0$ and $(\overline{x}_1^v, \dots, \overline{x}_m^v) \neq (0, \dots, 0)$. Up to a permutation of the indices, we may assume that $\overline{x}_1^v \neq 0$, that is, $x_1 \in \mathcal{O}_v^\times$. Since $\overline{a}_1^v \overline{x}_1^{v2} + \dots + \overline{a}_m^v \overline{x}_m^{v2} = 0$, we have that $v(a_1x_1^2 + \dots + a_mx_m^2) \geqslant 1$. If $v(a_1x_1^2 + \dots + a_mx_m^2) = 1$, then the statement is already shown. Otherwise, let $\pi \in K$ be such that $v(\pi) = 1$. We have that

$$a_1(x_1 + \pi)^2 + a_2x_2^2 + \dots + a_mx_m^2 = (a_1x_1^2 + \dots + a_mx_m^2) + 2a_1x_1\pi + a_1\pi^2.$$

Since $v(a_1x_1^2 + a_2x_2^2 + \dots + a_mx_m^2), v(a_1\pi^2) \geqslant 2$ and $v(2a_1x_1\pi) = v(\pi) = 1$, we conclude that $v\big(a_1(x_1 + \pi)^2 + \dots + a_mx_m^2\big) = 1$, whereby the statement is proven. □

5.1.5 Corollary. *Let v be a non-dyadic $\mathbb{Z}$-valuation on K and ϕ a Pfister form over K that is ramified with respect to v. Then $\overline{\phi}^v$ is anisotropic.*

Proof. By Lemma 5.1.2, there exists a Pfister form ψ over K that is unramified with respect to v and a uniformizer π of v such that $\phi \simeq \psi \perp \pi\psi$ and $\overline{\phi}^v = \overline{\psi}^v$. For the sake of a contradiction, assume that $\overline{\phi}^v$ is isotropic. Then there exists $\pi' \in D_K(\psi)$ with $v(\pi') = 1$, by Lemma 5.1.4. Since ψ is a Pfister form, it follows by Theorem 1.1.15 that $\pi'\psi \simeq \psi$. Set $u = \pi/\pi'$. Then $u \in \mathcal{O}_v^\times$, and $\psi \perp \pi\psi \simeq \psi \perp u\psi$, which contradicts the hypothesis that ϕ is ramified with respect to v. □

5.1.6 Lemma. *Let F/E be a field extension and ϕ a Pfister form over E. Let further v be a non-dyadic $\mathbb{Z}$-valuation on E and w a non-dyadic $\mathbb{Z}$-valuation on F such that v is equivalent to $w|_E$ and $[wF : wE]$ is finite and odd. Then $\overline{(\phi_F)}^w = (\overline{\phi}^v)_{Fw}$.*

Proof. If ϕ is unramified with respect to v, then ϕ_F is unramified with respect to w, since $\mathcal{O}_v = \mathcal{O}_w \cap E$, and thus $\overline{\phi_F}^w = (\overline{\phi}^v)_{Fw}$. Assume now that ϕ is ramified with respect to v. Then there exists a uniformizer $\pi \in E$ of v and a Pfister form ψ over E that is unramified with respect to v such that $\phi = \psi \perp \pi\psi$, by Lemma 5.1.2. Let $t \in E$ be a uniformizer of w and let $u \in \mathcal{O}_w^\times$ be such that $\pi = ut^{w(\pi)}$. Then $w(\pi) = [wF : wE]$, which is odd by assumption. Hence $\phi_F = \psi_F \perp ut^{w(\pi)}\psi_F \simeq \psi_F \perp ut\psi_F$. Therefore $\overline{(\phi_F)}^w = \overline{(\psi_F)}^w = (\overline{\psi}^v)_{Fw} = (\overline{\phi}^v)_{Fw}$. □

The following statement is a special case of Springer's Theorem, which plays a crucial role in the study of quadratic forms over discretely valued fields.

5.1.7 Theorem (Springer)**.** *Let v be a complete non-dyadic $\mathbb{Z}$-valuation on K and let ϕ be a Pfister form over K. Then ϕ is anisotropic if and only if $\overline{\phi}^v$ is anisotropic.*

Proof. The statement follows from [Lam05, Proposition VI.1.9], using Lemma 5.1.2 when ϕ is ramified with respect to v. □

In the rest of this section we study the behaviour of residue forms in the context of p-adic valuations on $K(X)$, and more specifically their behaviour under specific field extensions of $K(X)$. We denote by $\mathcal{P}_K$ the set of monic irreducible polynomials in $K[X]$. As in Example 2.1.3 (b), given $p \in \mathcal{P}_K$, we denote by v_p the p-adic valuation on $K(X)$.

5.1.8 Lemma. *Let L/K be a field extension and $p \in \mathcal{P}_K$. Let $\alpha \in L$ be a root of p and denote by w the $(X-\alpha)$-adic valuation on $L(X)$. Then $w(p)$ is odd and $w|_{K(X)} = w(p)\cdot v_p$.*

Proof. Since $\mathsf{char}(K) \neq 2$, there exist $p' \in \mathcal{P}_K$ separable and $n \in \mathbb{N}$ odd such that $p(X) = p'(X^n)$. Since p' is separable and $p'(\alpha^n) = p(\alpha) = 0$, there exists $q \in L[X]$ such that $p = (X-\alpha)^n \cdot q$ and $q(\alpha) \neq 0$. Hence $w(p) = n$ and $w|_{K(X)} = n \cdot v_p$, by the definition of w. □

Let $p \in \mathcal{P}_K$ and let ϕ be a Pfister form over $K(X)$. Since v_p is non-dyadic, we may call ϕ *unramified at p* if ϕ is unramified with respect to v_p. We also call *residue form of ϕ modulo p* the residue form of ϕ modulo v_p.

5.1.9 Corollary. *Let $p \in \mathcal{P}_K$ and ϕ a Pfister form over $K(X)$ that is anisotropic over $K(X)^{v_p}$. Let L/K be a field extension, $\alpha \in L$ a root of p and denote by w the $(X-\alpha)$-adic valuation on $L(X)$. Assume that $(\overline{\phi}^{v_p})_L$ is anisotropic. Then $\phi_{L(X)^w}$ is anisotropic.*

Proof. Set $E = K(X)^{v_p}$, $v = \widehat{v}_p$ and $F = L(X)^w$. By Lemma 5.1.8, we have that $w(p)$ is odd, therefore $[wL(X) : wK(X)] = w(p)$ is odd. Identify $K(X)v_p$ with $K(\alpha) \subseteq L$. By Lemma 5.1.6, we find $(\overline{\phi}^{v_p})_L = \overline{\phi_{L(X)}}^{w}$. Hence $(\overline{\phi}^{v_p})_L = \overline{\phi_F}^{\widehat{w}}$, which is then anisotropic. Since $\widehat{w}$ is complete and non-dyadic, it follows by Theorem 5.1.7 that ϕ_F is anisotropic. □

5.2 A local-global principle for rational function fields

In this section we use Milnor's Exact Sequence and the tools developed in Section 5.1 to obtain a Local-Global Principle for rational function fields. We formulate our main result (Theorem 5.2.2) in a very general context. This will prove useful in Section 5.3, where it will be applied to different situations. In order to do this, we fix a field K of characteristic different from 2. We first rework Milnor's Exact Sequence in the following way.

5.2.1 Theorem. *Let ϕ be a quadratic form over $K(X)$. If ϕ is not hyperbolic, then there exists $p \in \mathcal{P}_K$ such that $\phi_{K(X)^{v_p}}$ is not hyperbolic.*

Proof. Suppose that $\phi_{K(X)^{v_p}}$ is hyperbolic for every $p \in \mathcal{P}_K$. By Milnor's Exact Sequence (see [Lam05, Milnor's Theorem IX.3.1]), there exists a quadratic form ψ over K such that ϕ is Witt equivalent to $\psi_{K(X)}$. By the assumption on ϕ, we have that $\psi_{K(X)^{v_p}}$ is hyperbolic for every $p \in \mathcal{P}$. This holds in particular for $p = X$, for which we have $K(X)^{v_p} \simeq K(\!(X)\!)$ and $K(X)v_p \simeq K$. Hence ψ is hyperbolic over $K(\!(X)\!)$. It follows by Theorem 5.1.7 that ψ is hyperbolic. Thus ϕ is hyperbolic as well. □

Let $\mathcal{E}$ be a set of field extensions of K and $m \in \mathbb{N}^+$. We say that *$\mathcal{E}$ is local-global for K at m* if for every $p \in \mathcal{P}_K$, $f_1, \dots, f_m \in K[X] \smallsetminus pK[X]$ such that $\langle\langle \overline{f_1}^{v_p}, \dots, \overline{f_m}^{v_p} \rangle\rangle_{K(X)v_p}$ is anisotropic, there exist $L \in \mathcal{E}$ and $\alpha \in L$ such that $p(\alpha) = 0$ and $\langle\langle f_1(\alpha), \dots, f_m(\alpha) \rangle\rangle_L$ is anisotropic. This is equivalent to saying that, for every $p \in \mathcal{P}_K$ and m-fold Pfister form

ϕ on $K(X)$ that is unramified at p and such that $\overline{\phi}^{v_p}$ is anisotropic, there exist $L \in \mathcal{E}$ and $\alpha \in L$ such that $p(\alpha) = 0$ and $\overline{\phi_{L(X)}}^{v}$ is anisotropic where v is the $(X-\alpha)$-adic valuation on $L(X)$. We say that $\mathcal{E}$ *is local-global for* K if it is local-global for K at every $m \in \mathbb{N}^+$. By convention, we assume that any set of field extensions of K is *local-global for* K *at* 0.

5.2.2 Theorem (Local-Global Principle)**.** *Let* $m \in \mathbb{N}^+$ *and let* $\mathcal{E}$ *be a set of field extensions of* K*. Assume that* $\mathcal{E}$ *is local-global for* K *at* m *and* $m-1$*. Then every anisotropic* m*-fold Pfister form over* $K(X)$ *is anisotropic over* $L(X)$ *for some* $L \in \mathcal{E}$*.*

Proof. Let ϕ be an anisotropic m-fold Pfister form over $K(X)$. By Theorem 5.2.1, there exists $p \in \mathcal{P}_K$ such that $\phi_{K(X)^{v_p}}$ is not hyperbolic, and thus anisotropic, by Theorem 1.1.17. Set $\ell = m$ if ϕ is unramified at p, and $\ell = m-1$ otherwise. Then $\overline{\phi}^{v_p}$ is an ℓ-fold Pfister form over $K(X)v_p$, by Lemma 5.1.2, and is anisotropic, by Theorem 5.1.7. Let $f_1, \dots, f_\ell \in \mathcal{O}_{v_p}^{\times} \cap K[X]$ be such that $\overline{\phi}^{v_p} \simeq \langle\langle \overline{f}_1^{v_p}, \dots, \overline{f}_\ell^{v_p} \rangle\rangle_{K(X)v_p}$. By the hypothesis on $\mathcal{E}$, there exists $L \in \mathcal{E}$ and $\alpha \in L$ such that $p(\alpha) = 0$ and $\langle\langle f_1(\alpha), \dots, f_l(\alpha) \rangle\rangle_L$ is anisotropic. Let v be the $(X-\alpha)$-adic valuation on $L(X)$. Since $\langle\langle f_1(\alpha), \dots, f_l(\alpha) \rangle\rangle_L = \overline{\phi_{L(X)}}^{v}$, it follows by Corollary 5.1.9 that $\phi_{L(X)^v}$ is anisotropic. Since $L(X)$ embeds into $L(X)^v$, we conclude that $\phi_{L(X)}$ is anisotropic. □

5.3 Applications

In this section we apply Theorem 5.2.2 to obtain several local-global principles for Pfister forms over rational function fields. Besides Theorem 5.2.2, the main ingredient is the Hasse-Minkowski Local-Global Principle (Theorem 2.3.11), which is used in the argument of Lemma 5.3.1.

Recall from Section 2.3 that a *global field* is a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_q(X)$ for some $q \in \mathbb{N}$ prime, and that for a field K we call $\mathcal{W}_K$ the set of absolute values on K.

For a field K and $p \in \mathcal{P}_K$, we set $K_p = K[X]/(p)$, and we identify $K(X)v_p$ with K_p.

5.3.1 Lemma. *Let* K *be a global field such that* $\mathsf{char}(K) \neq 2$*. Then the set*

$$\{K_p^w \mid p \in \mathcal{P}_K,\ w \in \mathcal{W}_{K_p}\}$$

is local-global for K*.*

Proof. Consider $p \in \mathcal{P}_K$, $m \in \mathbb{N}^+$ and $f_1, \dots, f_m \in K[X] \smallsetminus pK[X]$ such that the form $\langle\langle \overline{f}_1^{v_p}, \dots, \overline{f}_m^{v_p} \rangle\rangle_{K_p}$ is anisotropic. Since K_p/K is finite, K_p is a global field. By Theorem 2.3.11, there exists $w \in \mathcal{W}_{K_p}$ such that $\langle\langle \overline{f}_1^{v_p}, \dots, \overline{f}_m^{v_p} \rangle\rangle_{K_p^w}$ is anisotropic. Consider a root $\alpha \in K_p^w$ of p. Then $\langle\langle f_1(\alpha), \dots, f_m(\alpha) \rangle\rangle_{K_p^w} \simeq \langle\langle \overline{f}_1^{v_p}, \dots, \overline{f}_m^{v_p} \rangle\rangle_{K_p^w}$ is anisotropic. This shows that the set $\{K_p^w \mid p \in \mathcal{P}_K,\ w \in \mathcal{W}_{K_p}\}$ is local-global for K at m. Since $m \in \mathbb{N}^+$ was taken arbitrary, we obtain the statement. □

We recover a local-global principle for Pfister forms over the rational function field over a global field. When restricted to 3-fold Pfister forms, it can be seen as a special case of the local-global principle for 3-fold Pfister forms from [Kat86, p. 146] that we used to obtain Theorem 4.2.3.

5.3.2 Theorem. *Let* K *be a global field with* $\mathsf{char}(K) \neq 2$ *and let* ϕ *be an anisotropic Pfister form over* $K(X)$*. Then there exists* $w \in \mathcal{W}_K$ *such that* $\phi_{K^w(X)}$ *is anisotropic.*

Proof. By Lemma 5.3.1, the set $\{K_p^w \mid p \in \mathcal{P}_K,\ w \in \mathcal{W}_{K_p}\}$ is local-global for K. By Theorem 5.2.2, there exist $p \in \mathcal{P}_K$ and $\tilde{w} \in \mathcal{W}_{K_p}$ such that ϕ is anisotropic over $K_p^{\tilde{w}}(X)$. Set $w = \tilde{w}|_K$. Then $w \in \mathcal{W}_K$, and K^w naturally embeds into $K_p^{\tilde{w}}$, by Corollary 2.3.6. Thus $K^w(X)$ embeds into $K_p^{\tilde{w}}(X)$. Hence ϕ is anisotropic over $K^w(X)$. □

Recall from Section 2.3 that an absolute value is *dyadic* if it is non-archimedean and corresponds to a dyadic valuation, and *non-dyadic* otherwise. We obtain the following local-global principles, for sums of two and of four squares respectively.

5.3.3 Corollary. *Let K be a global field and $h \in \Sigma\, K[X]^2$. Then $h \in \Sigma_2 K[X]^2$ if and only if $h \in \Sigma_2 K^w(X)^2$ for all $w \in \mathcal{W}_K$ non-archimedean such that $|Kw| \not\equiv 1 \bmod 4$.*

Proof. For $h = 0$, the statement holds trivially. Assume that $h \neq 0$. If $h \in \Sigma_2 K[X]^2$, then $h \in \Sigma_2 K^w(X)^2$ for all $w \in \mathcal{W}_K$. Vice versa, assume that $h \in \Sigma_2 K^w(X)^2$ for all $w \in \mathcal{W}_K$ non-archimedean such that $|Kw| \not\equiv 1 \bmod 4$. If $\mathsf{char}(K) = 2$, then $h \in K[X]^2$, trivially. Assume that $\mathsf{char}(K) \neq 2$. Consider $w \in \mathcal{W}_K$. If w is archimedean, then $K^w \simeq \mathbb{R}$ or $K^w \simeq \mathbb{C}$, by Example 2.3.8 (a); thus $p(K^w(X)) = 2$. If w is non-archimedean and $|Kw| \equiv 1 \bmod 4$, then $s(K^w(X)) = s(K^w) = 1$, by Proposition 2.4.13, and thus $p(K^w(X)) \leqslant 2$, by Proposition 1.2.4. In either case, we obtain $h \in \Sigma_2 K^w(X)^2$. By the assumption on h, this shows that $\langle\!\langle -1, h\rangle\!\rangle_{K^w(X)}$ is isotropic for every $w \in \mathcal{W}_K$. Therefore $\langle\!\langle -1, h\rangle\!\rangle_{K(X)}$ is isotropic, by Theorem 5.3.2. Hence $h \in \Sigma_2 K(X)^2$, by Theorem 1.1.18, and thus $h \in \Sigma_2 K[X]^2$, by Theorem 1.1.21. □

5.3.4 Corollary. *Let $h \in \Sigma\mathbb{Q}[X]^2$. Then $h \in \Sigma_2\mathbb{Q}[X]^2$ if and only if $h \in \Sigma_2\mathbb{Q}_p(X)^2$ for every prime $p \in \mathbb{N}$ such that $p \not\equiv 1 \bmod 4$.*

Proof. The statement follows from Corollary 5.3.3 and from the fact that, for every prime $p \in \mathbb{N}$, $\mathbb{Q}_p$ is, up to isomorphism, the unique completion of $\mathbb{Q}$ having residue field of characteristic p; see Example 2.3.9. □

5.3.5 Corollary. *Let K be a global field and $h \in \Sigma\, K[X]^2$. Then $h \in \Sigma_4 K[X]^2$ if and only if $h \in \Sigma_4 K^w(X)^2$ for every dyadic $w \in \mathcal{W}_K$.*

Proof. For $h = 0$, the statement holds trivially. If $\mathsf{char}(K) \neq 0$, then $s(K) \leqslant 2$; thus $\Sigma K(X)^2 = \Sigma_4 K(X)^2$, by Corollary 1.2.5, and the statement is trivial. Assume now that $h \neq 0$ and $\mathsf{char}(K) = 0$. If $h \in \Sigma_4 K[X]^2$, then $h \in \Sigma_4 K^w(X)^2$ for every $w \in \mathcal{W}_K$. Vice versa, assume $h \in \Sigma_4 K^w(X)^2$ for every dyadic $w \in \mathcal{W}_K$. Consider $w \in \mathcal{W}_K$ non-dyadic. If w is archimedean, then $K^w \simeq \mathbb{R}$ or $K^w \simeq \mathbb{C}$, by Example 2.3.8 (a), thus $p(K^w(X)) = 2$. If w is non-archimedean, then $s(K^w(X)) = s(K^w) \leqslant 2$, by Proposition 2.4.13, thus $p(K^w(X)) \leqslant 3$, by Proposition 1.2.4. In either case we get $h \in \Sigma_4 K^w(X)^2$. This shows that $\langle\!\langle -1, -1, h\rangle\!\rangle_{K^w(X)}$ is isotropic for all $w \in \mathcal{W}_K$. Hence $\langle\!\langle -1, -1, h\rangle\!\rangle_{K(X)}$ is isotropic, by Theorem 5.3.2. Therefore $h \in \Sigma_4 K(X)^2$, by Theorem 1.1.18, and thus $h \in \Sigma_4 K[X]^2$, by Theorem 1.1.21. □

5.3.6 Corollary. *Let $h \in \Sigma\mathbb{Q}[X]^2$. Then $h \in \Sigma_4\mathbb{Q}[X]^2$ if and only if $h \in \Sigma_4\mathbb{Q}_2(X)^2$.*

Proof. The statement follows from Corollary 5.3.5, together with the fact that $\mathbb{Q}_2$ is, up to isomorphism, the unique dyadic completion of $\mathbb{Q}$; see Example 2.3.9. □

Another application of Theorem 5.2.2 provides a local-global principle for Pfister forms over $K(\!(t_1)\!)\cdots(\!(t_n)\!)(X)$, where K is a global field and $n \in \mathbb{N}$. Before proving this local-global principle, we briefly study finite field extensions of iterated formal power series.

5.3.7 Lemma. *Let K be a field, $n \in \mathbb{N}$ and $F/K(\!(t_1)\!)\cdots(\!(t_n)\!)$ a finite field extension. Then F is K-isomorphic to $E(\!(s_1)\!)\cdots(\!(s_n)\!)$ for some finite field extension E/K.*

Proof. The statement follows by induction from the case where $n = 1$. Assume therefore that $n = 1$, and denote $t = t_1$ for simplicity. By [OM73, Theorem 14:1], the complete discrete valuation ring $K\llbracket t\rrbracket$ extends to a unique valuation ring $\mathcal{O}$ of F, which is also complete and discrete. Let κ be the residue field of $\mathcal{O}$. By [Sta, Lemma 10.160.8] (Cohen's Structure Theorem), there exists a subfield E of $\mathcal{O}$ such that the residue map of $\mathcal{O}$ induces an isomorphism $E \simeq \kappa$; see also [Sta, Remark (1) after Definition 10.160.4]. By [Sta, Lemma 10.160.10 (2)], there exists an E-isomorphism $\mathcal{O} \simeq E\llbracket s\rrbracket$, and thus an E-isomorphism $F \simeq E(\!(s)\!)$. Since $\mathcal{O}$ extends $K\llbracket t\rrbracket$, the residue field of $K\llbracket t\rrbracket$, which is K, embeds naturally in κ, and it follows by Theorem 2.2.4 that $[\kappa : K] \leqslant [F : K(\!(t)\!)] < \infty$, whereby κ/K is finite. Since $E \simeq \kappa$, we may see E as a finite extension of K, and thus there exists a K-isomorphism $F \simeq E(\!(s)\!)$. □

Given a field extension L/K, we call *finite intermediate field extension of L/K* any finite field extension F/K where F is a subfield of L.

5.3.8 Theorem. *Let K be a field with $\mathsf{char}(K) \neq 2$ and K^{alg} an algebraic closure of K. For every finite intermediate field extension F/K of K^{alg}/K, let $\mathcal{E}_F$ be a set of field extensions of F. Set*

$$\mathcal{E} = \{L(\!(t)\!) \mid L \in \mathcal{E}_F \textit{ for some finite intermediate field extension } F/K \textit{ of } K^{alg}/K\}.$$

For $m \in \mathbb{N}^+$, if $\mathcal{E}_F$ is local-global for F at $m-1$ and m for every finite intermediate field extension F/K of K^{alg}/K, then $\mathcal{E}$ is local-global for $K(\!(t)\!)$ at m. In particular, if $\mathcal{E}_F$ is local-global for F for every finite intermediate field extension F/K of K^{alg}/K, then $\mathcal{E}$ is local-global for $K(\!(t)\!)$.

Proof. Let $m \in \mathbb{N}^+$ be such that $\mathcal{E}_F$ is local-global for F at $m-1$ and m for every finite intermediate field extension F/K of K^{alg}/K. In order to show that $\mathcal{E}$ is local-global for $K(\!(t)\!)$ at m, consider $p \in \mathcal{P}_{K(\!(t)\!)}$ and $f_1, \ldots, f_m \in K(\!(t)\!)[X] \smallsetminus (p)$ such that the m-fold Pfister form $\langle\!\langle \overline{f}_1^{v_p}, \ldots, \overline{f}_m^{v_p}\rangle\!\rangle_{K(\!(t)\!)_p}$ is anisotropic. Set $F = K(\!(t)\!)_p$ and let $\alpha \in F$ be such that $p(\alpha) = 0$ and $F = K(\!(t)\!)(\alpha)$. Then $\langle\!\langle f_1(\alpha), \ldots, f_m(\alpha)\rangle\!\rangle_F = \langle\!\langle \overline{f}_1^{v_p}, \ldots, \overline{f}_m^{v_p}\rangle\!\rangle_F$. Since $F/K(\!(t)\!)$ is finite, it follows by Lemma 5.3.7 that F is K-isomorphic to $E(\!(s_1)\!)\cdots(\!(s_n)\!)$ for some finite field extension E/K. We may thus assume that E is a subfield of K^{alg} and $F = E(\!(s)\!)$. Let v be the s-adic valuation on F. Set $l = m$ if $\langle\!\langle f_1(\alpha), \ldots, f_m(\alpha)\rangle\!\rangle_F$ is unimodular with respect to v, and $l = m-1$ otherwise. In view of Lemma 5.1.2 we may assume, up to a permutation of the indices $1, \ldots, l$, that $v(f_1(\alpha)) = \ldots = v(f_l(\alpha)) = 0$. As v is complete non-dyadic, $Fv = E$ and $\langle\!\langle f_1(\alpha), \ldots, f_m(\alpha)\rangle\!\rangle_F$ is anisotropic, and it follows by Theorem 5.1.7 that $\langle\!\langle \overline{f_1(\alpha)}^v, \ldots, \overline{f_l(\alpha)}^v\rangle\!\rangle_E$ is anisotropic. As E/K is a finite intermediate field extension of K^{alg}/K, the set $\mathcal{E}_E$ is local-global at m and $m-1$. Hence there exists $L \in \mathcal{E}_E$ such that $\langle\!\langle \overline{f_1(\alpha)}^v, \ldots, \overline{f_l(\alpha)}^v\rangle\!\rangle_L$ is anisotropic. By Theorem 5.1.7 applied to the t-adic valuation on $L(\!(t)\!)$, we conclude that $\langle\!\langle f_1(\alpha), \ldots, f_m(\alpha)\rangle\!\rangle_{L(\!(t)\!)}$ is anisotropic. This shows that $\mathcal{E}$ is local-global for $K(\!(t)\!)$ at m. The second part of statement follows trivially from the first. □

5.3.9 Corollary. *Let K be a global field with $\mathsf{char}(K) \neq 2$ and $n \in \mathbb{N}$. Then the set*

$$\{F^w(\!(t_1)\!)\cdots(\!(t_n)\!) \mid F/K \textit{ finite intermediate field extension of } K^{alg}/K,\ w \in \mathcal{W}_F\}$$

is local-global for $K(\!(t_1)\!)\cdots(\!(t_n)\!)$.

Proof. Consider $m \in \mathbb{N}^+$. Set

$$\mathcal{E} = \{F^w \mid F/K \text{ finite intermediate field extension of } K^{alg}/K,\ w \in \mathcal{W}_F\} \quad \text{and}$$

$$\mathcal{E}_n = \{F^w(\!(t_1)\!)\cdots(\!(t_n)\!) \mid F/K \text{ finite intermediate field extension of } K^{alg}/K,\ w \in \mathcal{W}_F\}.$$

Observe that

$$\{K_p^w \mid p \in \mathcal{P}_K,\ w \in \mathcal{W}_{K_p}\} \subseteq \mathcal{E},$$

and recall that $\{K_p^w \mid p \in \mathcal{P}_K,\ w \in \mathcal{W}_{K_p}\}$ is local-global for K at m, by Lemma 5.3.1. Then $\mathcal{E}$ is local-global for K at m, trivially. It follows by Theorem 5.3.8 via an elementary induction argument that the set $\mathcal{E}_n$ is local-global for $K(\!(t_1)\!)\cdots(\!(t_n)\!)$ at m. Since this holds for arbitrary $m \in \mathbb{N}^+$, this shows that $\mathcal{E}_n$ is local-global for $K(\!(t_1)\!)\cdots(\!(t_n)\!)$. □

5.3.10 Proposition. *Let K be a global field with $\mathsf{char}(K) \neq 2$ and $n \in \mathbb{N}$. Let ϕ be an anisotropic Pfister form over $K(\!(t_1)\!)\cdots(\!(t_n)\!)(X)$. Then there exists $w \in \mathcal{W}_K$ such that ϕ is anisotropic over $K^w(\!(t_1)\!)\cdots(\!(t_n)\!)(X)$.*

Proof. By Corollary 5.3.9, the set

$$\mathcal{E}_n = \{F^w(\!(t_1)\!)\cdots(\!(t_n)\!) \mid F/K \text{ finite intermediate field extension of } K^{alg}/K,\ w \in \mathcal{W}_F\}$$

is local-global for $K(\!(t_1)\!)\cdots(\!(t_n)\!)$. It follows by Theorem 5.2.2 that there exist a finite intermediate field extension F/K of K^{alg}/K and $\tilde{w} \in \mathcal{W}_F$ such that ϕ is anisotropic over $F^{\tilde{w}}(\!(t_1)\!)\cdots(\!(t_n)\!)(X)$. Set $w = \tilde{w}|_K$. Then $w \in \mathcal{W}_K$, and K^w naturally embeds into $F^{\tilde{w}}$, by Corollary 2.3.6. Thus $K^w(\!(t_1)\!)\cdots(\!(t_n)\!)(X)$ embeds into $F^{\tilde{w}}(\!(t_1)\!)\cdots(\!(t_n)\!)(X)$. Therefore ϕ is anisotropic over $K^w(\!(t_1)\!)\cdots(\!(t_n)\!)(X)$. □

Similarly as before, we specialize the result to sums of four squares.

5.3.11 Corollary. *Let K be a global field and $n \in \mathbb{N}$. Set $F = K(\!(t_1)\!)\cdots(\!(t_n)\!)$ and let $h \in \Sigma F[X]^2$. Then $h \in \Sigma_4 F[X]^2$ if and only if $h \in \Sigma_4 K^w(\!(t_1)\!)\cdots(\!(t_n)\!)(X)^2$ for every dyadic $w \in \mathcal{W}_K$.*

Proof. If $h \in \Sigma_4 F[X]^2$, then $h \in \Sigma_4 K^w(\!(t_1)\!)\cdots(\!(t_n)\!)(X)^2$ for every dyadic $w \in \mathcal{W}_K$, trivially. Vice versa, suppose that $h \in \Sigma_4 K^w(\!(t_1)\!)\cdots(\!(t_n)\!)(X)^2$ for all dyadic $w \in \mathcal{W}_K$. If $\mathsf{char}(K) \neq 0$, then $s(K) \leqslant 2$, by Corollary 1.2.5; thus $\Sigma F(X)^2 = \Sigma_4 F(X)^2$, by Proposition 1.2.4, and the statement holds trivially. Assume now that $\mathsf{char}(K) = 0$. Consider $w \in \mathcal{W}_K$ non-dyadic and set $L = K^w(\!(t_1)\!)\cdots(\!(t_n)\!)(X)$. If w is archimedean, then $K^w \simeq \mathbb{R}$ or $K^w \simeq \mathbb{C}$, by Example 2.3.8 (a); in the first case, we find that $p(L) = 2$ by Corollary 4.1.7 and Theorem 4.1.4, in the second case $p(L) = 2$ by Proposition 1.2.8. If w is non-archimedean, then it follows by Proposition 2.4.13 that $p(L) \leqslant 3$. In either case, we obtain $h \in \Sigma_4 L^2$. By the assumption, this shows that $\langle\!\langle -1, -1, h\rangle\!\rangle$ is isotropic over $K^w(\!(t_1)\!)\cdots(\!(t_n)\!)(X)$ for every $w \in \mathcal{W}_K$. By Proposition 5.3.10, we get that $\langle\!\langle -1, -1, h\rangle\!\rangle$ is isotropic over $F(X)$. Hence $h \in \Sigma_4 F(X)^2$, by Theorem 1.1.18, and thus $h \in \Sigma_4 F[X]^2$, by Theorem 1.1.21. □

5.3.12 Corollary. *Let $n \in \mathbb{N}$, $h \in \Sigma\mathbb{Q}(\!(t_1)\!)\cdots(\!(t_n)\!)[X]^2$. Then $h \in \Sigma_4\mathbb{Q}(\!(t_1)\!)\cdots(\!(t_n)\!)[X]^2$ if and only if $h \in \Sigma_4\mathbb{Q}_2(\!(t_1)\!)\cdots(\!(t_n)\!)(X)^2$.*

Proof. The statement follows from Corollary 5.3.11, together with the fact that $\mathbb{Q}_2$ is, up to isomorphism, the unique dyadic completion of $\mathbb{Q}$; see Example 2.3.9. □

Chapter 6
The Pythagoras number of a rational function field over a number field

Y. Pourchet proved in [Pou71] that the Pythagoras number of a rational function field over a number field is at most 5. Pourchet's exposition seems at a first glimpse to rely heavily on the assumption that the base field is a number field, but it does not make immediately clear which properties of number fields are necessary for the proof. In the following, we decompose Pourchet's argument into different steps and we highlight the hypotheses that are relevant for each step. It is interesting, in view of possible applications of this kind of argument to different settings, that each step turns out to require only milder assumptions than having a number field as a base field.

6.1 Representation of polynomials by quadratic forms

In this section we inquire whether and when it is possible to bound the degrees of the polynomials in the representation of a given polynomial by a quadratic form. More precisely, given a field K, $m, n \in \mathbb{N}$, an n-ary quadratic form ϕ over K and a polynomial $f \in D_{K[X]}(\phi)$ of degree $2m$, we investigate whether it is possible to find $f_1, \ldots, f_n \in K[X]$ such that $f = \phi(f_1, \ldots, f_n)$ and $\deg(f_i) \leqslant m$ for every $1 \leqslant i \leqslant n$.

Throughout this section it might help to keep in mind the following example, related to sums of five squares in $\mathbb{Q}_2[X]$. Consider $f \in \mathbb{Q}_2[X]$ of even degree. Recall from Section 2.4 that $s(\mathbb{Q}_2(X)) = s(\mathbb{Q}_2) = 4$, whereby $\mathbb{Q}_2(X) = \Sigma\mathbb{Q}_2(X)^2 = \Sigma_5\mathbb{Q}_2(X)^2$. It is thus easy to show that there exist $f_1, \ldots, f_5 \in \mathbb{Q}_2[X]$ such that $f = f_1^2 + \ldots + f_5^2$, by using the Cassels-Pfister Theorem (Theorem 1.1.21). It is possible, but more difficult, to show that there exist such $f_1, \ldots, f_5$ having $\deg(f_i) \leqslant \deg(f)/2$ for every $1 \leqslant i \leqslant 5$. This was shown in [Pou71, Theorem 1] as a crucial step to show that $p(\mathbb{Q}(X)) \leqslant 5$. In this section we discuss when and how these kind of problems can be solved; the following statements cover and extend the techniques for local fields developed in [Pou71, Étude Locale].

In the sequel, let K be a field of characteristic different from 2. Recall from Chapter 5 that we denote by $\mathcal{P}_K$ the set of monic irreducible polynomials with coefficients in K.

6.1.1 Lemma. *Let $a \in (K^\times \smallsetminus -K^{\times 2}) \cup \{-1\}$. Let $U \subseteq \mathcal{P}_K$ be finite and $g_1, g_2 \in K[X]$ such that, for all $p \in U$, p^2 does not divide $g_1^2 + ag_2^2$ in $K[X]$. Then there exist $|K|-1-2|U|$ pairs $(h_1, h_2) \in K[X] \times K[X]$ such that h_1 is coprime in $K[X]$ to any polynomial in U and $g_1^2 + ag_2^2 = h_1^2 + ah_2^2$; furthermore, for $|K| - 3 - 2|U|$ of these pairs, we also have* $\deg(h_1) = \mathsf{max}\{\deg(g_1), \deg(g_2)\}$.

Proof. For $x, y \in K^\times$ such that $ay^2 + 1 \neq 0$, we set

$$A_x = \frac{1}{2}\begin{pmatrix} x + x^{-1} & x - x^{-1} \\ x - x^{-1} & x + x^{-1} \end{pmatrix} \text{ and } B_y = \frac{1}{ay^2 + 1}\begin{pmatrix} ay^2 - 1 & 2ay \\ 2y & 1 - ay^2 \end{pmatrix}.$$

We will use the matrices $\{A_x\}_{x\in K^\times}$ to prove the statement for $a=-1$, and the matrices $\{B_y\}_{y\in K^\times}$ for $a\neq -1$. Set $\phi=\langle 1,a\rangle_K$. If $a=-1$, then for every $x\in K^\times$, we have $\phi\circ A_x=\phi$; if $-a\in K^\times\smallsetminus K^{\times 2}$, then $ax^2+1\neq 0$ and $\phi\circ B_x=\phi$ for every $x\in K^\times$.

Fix $p\in U$ and $\alpha\in K[X]/(p)$ such that $K[X]/(p)=K(\alpha)$. Consider $M,N\in \mathsf{M}_2(K)$ such that $\phi\circ M=\phi\circ N=\phi$ and $M\cdot(g_1,g_2)^t, N\cdot(g_1,g_2)^t\in (p)\times K[X]$, that is,

$$M\cdot(g_1(\alpha),g_2(\alpha))^t, N\cdot(g_1(\alpha),g_2(\alpha))^t\in\{0\}\times K(\alpha).$$

Assume that $a=-1$ and $M=A_x$, $N=A_y$ for $x,y\in K^\times$. From the first component, we obtain that $(x^2+1)g_1(\alpha)+(x^2-1)g_2(\alpha)=(y^2+1)g_1(\alpha)+(y^2-1)g_2(\alpha)=0$. Since p does not divide both g_1,g_2 and $x,y\in K^\times$, we have $g_1(\alpha)\neq 0$ or $g_2(\alpha)\neq 0$. Assume that $g_1(\alpha)\neq 0$. Then $x^2\neq 1$, otherwise $2=x^2+1=0$, which would contradict $\mathsf{char}(K)\neq 2$. Analogously we find $y^2\neq 1$. Thus $g_2(\alpha)/g_1(\alpha)=(x^2+1)/(1-x^2)=(y^2+1)/(1-y^2)$, whereby $x^2=y^2$. Similarly, we obtain that $x^2=y^2$ if $g_2(\alpha)\neq 0$. Hence $x=y$, or $x=-y$.

Assume that $a\notin -K^{\times 2}$ and $M=B_x$, $N=B_y$ for $x,y\in K^\times$. From the first component, we obtain that $(ax^2-1)g_1(\alpha)+2xg_2(\alpha)=(ay^2-1)g_1(\alpha)+2yg_2(\alpha)=0$. Since p does not divide both g_1,g_2 and $x,y\in K^\times$, we have $g_1(\alpha)\neq 0$. Therefore $2g_2(\alpha)/g_1(\alpha)=(1-ax^2)/x=(1-ay^2)/y$, whereby either $x=y$, or $x=-1/ay$.

If $a=-1$, we have shown that for every $p\in U$ there exist $x_p,y_p\in K$ such that $A_x\cdot(g_1,g_2)^t\notin K[X]\times(p)$ for any $x\in K\smallsetminus\{0,x_p,y_p\}$; set $S=\{0\}\cup\{x_p,y_p\mid p\in U\}$. If $a\notin -K^{\times 2}$, we have shown that, for every $p\in U$, there exist $x_p,y_p\in K$ such that $B_x\cdot(g_1,g_2)^t\notin K[X]\times(p)$ for any $x\in K\smallsetminus\{0,x_p,y_p\}$; set $S=\{0\}\cup\{x_p,y_p\mid p\in U\}$.

An elementary computation shows for every $x,y\in K^\times$ that $x=y$ if $a=-1$ and $A_x\cdot(g_1,g_2)^t=A_y\cdot(g_1,g_2)^t$, or if $a\notin -K^{\times 2}$ and $B_x\cdot(g_1,g_2)^t=B_y\cdot(g_1,g_2)^t$. Hence there exist $|K\smallsetminus S|\geqslant |K|-1-2|U|$ couples $(h_1,h_2)\in K[X]\times K[X]$ such that h_1 is coprime in $K[X]$ to every polynomial in U and $\phi(g_1,g_2)=\phi(h_1,h_2)$.

Set now $m=\max\{\deg(g_1),\deg(g_2)\}$. For every $i\in\{1,2\}$, let $c_i\in K$ be such that $g_i=c_iX^m+G_i$, for some $G_i\in K[X]$ such that $\deg(G_i)<m$. Consider $x\in K^\times$. Observe that $\mathtt{lc}((x^2+1)g_1+(x^2-1)g_2)=(x^2+1)c_1+(x^2-1)c_2$ and, analogously, $\mathtt{lc}((ax^2-1)g_1+2xg_2)=(ax^2-1)c_1+2xc_2$. Then there exist $x_0,y_0\in K^\times$ such that $\deg((x^2+1)g_1+(x^2-1)g_2))=m$ for every $x\in K^\times\smallsetminus\{x_0,y_0\}$, and x_1,y_1 such that $\deg((ax^2-1)g_1+2xg_2)=m$ for any $x\in K^\times\smallsetminus\{x_1,y_1\}$. Set $T=S\smallsetminus\{x_0,y_0\}$ if $a=-1$, otherwise $T=S\smallsetminus\{x_1,y_1\}$. Then there exist $|K\smallsetminus T|\geqslant |K|-1-2|U|$ couples $(h_1,h_2)\in K[X]\times K[X]$ such that h_1 is coprime in $K[X]$ to any polynomial in U, $\phi(g_1,g_2)=\phi(h_1,h_2)$ and $\deg(h_1)=m$. □

6.1.2 Corollary. *Let ϕ be a regular binary quadratic form over K, let $g\in D_{K[X]}(\phi)$ be square-free in $K[X]$ with $2\deg(g)<|K|-1$ and let $f\in K[X]$. Then there exist $f_1,f_2\in K[X]$ such that $f\equiv\phi(f_1,f_2)\ \mathsf{mod}\ g$.*

Proof. Observe that the statement only depends on ϕ up to isometry, thus we may assume that $\phi=c\langle 1,a\rangle_K$ for some $a,c\in K^\times$. Furthermore, we may assume $c=1$. Since $2\deg(g)<|K|-1$, g has at most $(|K|-2)/2$ monic irreducible factors. By Lemma 6.1.1, there exist $g_1,g_2\in K[X]$ such that g_1 is coprime to g and $g=g_1^2+ag_2^2$. Then we have $ag_2^2\equiv -g_1^2\ \mathsf{mod}\ g$, whence

$$\begin{aligned}4g_1^2f&=g_1^2(f+1)^2-g_1^2(f-1)^2\\&\equiv g_1^2(f+1)^2+ag_2^2(f-1)^2\ \mathsf{mod}\ g\\&\equiv\phi(g_1(f+1),g_2(f-1))\ \mathsf{mod}\ g.\end{aligned}$$

Let $h\in K[X]$ be an inverse of g_1 $\mathsf{mod}\ g$, that is, such that $g_1h\equiv 1\ \mathsf{mod}\ g$. Then we have that $\phi((f+1)/2,hg_2(f-1)/2)\equiv f\ \mathsf{mod}\ g$. □

6.1.3 Proposition. *Let $d \in \mathbb{N}$ and let ϕ be a regular d-ary quadratic form over K. Let $a \in D_K(\phi)$ and $\phi' \subseteq \phi$ be such that $\phi \simeq \langle a \rangle \perp \phi'$. Let $f \in K[X] \smallsetminus K$ be square-free and such that $\deg(f) < |K| - 1$. Assume that there exist $g \in K[X]$ not dividing f with $2\deg(g) = \deg(f)$ and $f_1, \dots, f_{d-1} \in K[X]$ such that $af \equiv \phi'(f_1, \dots, f_{d-1}) \bmod g$. Then there exists $F \in K[X]$ with $\deg(F) = \deg(f)$ such that $F/a - f \in K[X]^2$, $\mathtt{lc}(F) \in D_K(\phi)$ and ϕ_L is isotropic for every field extension L/K containing a root of F.*

Proof. Let $n \in \mathbb{N}$ be such that $\deg(f) = 2n$. By the hypotheses we have $n > 0$ and $d > 1$. Let $g \in K[X]$ not dividing f with $\deg(g) = n$, and let $f_1, \dots, f_{d-1} \in K[X]$ be such that $af \equiv \phi'(f_1, \dots, f_{d-1}) \bmod g$. Since we are working modulo g and $\deg(g) = n$, we may assume that $\deg(f_i) < n$ for $1 \leqslant i \leqslant d - 1$. Hence there exists $h \in K[X]$ with $\deg(h) = n$ and such that

$$af = \phi'(f_1, \dots, f_{d-1}) + agh.$$

Let U be the set of the common monic prime factors of $f_1, \dots, f_{d-1}$ in $K[X]$. Since $\deg(f_1), \dots, \deg(f_{d-1}) \leqslant n - 1$, it follows that $|U| \leqslant n - 1$. Since $2n < |K| - 1$, we obtain that $2|U| < |K| - 3$. Since f is square-free, we have for any $p \in U$ that p^2 does not divide gh. Set $g_1 = (g + h)/2$ and $g_2 = (g - h)/2$. Then $gh = g_1^2 - g_2^2$. By Lemma 6.1.1, there exist $h_1, h_2 \in K[X]$ with $\deg(h_2) \leqslant \deg(h_1) = n$ such that h_1 is coprime in $K[X]$ to every polynomial from U and $h_1^2 - h_2^2 = g_1^2 - g_2^2 = gh$. Therefore we have

$$af + ah_2^2 = \phi'(f_1, \dots, f_{d-1}) + ah_1^2.$$

Set $F = af + ah_2^2$. Then the choice of h_1 implies that $\phi_{K[X]/(p)}$ is isotropic for every prime factor p of F in $K[X]$. Since $\deg(f_i) < n$ for any $1 \leqslant i \leqslant d - 1$ and $\deg(h_1) = n$, we have that $\deg(F) = 2n$ and $\mathtt{lc}(F) = a \cdot \mathtt{lc}(h_1)^2$, and thus $\mathtt{lc}(F) \in D_K(\phi)$. □

6.1.4 Lemma. *Let ϕ be a regular quadratic form in at least two variables over K and let $k \in \mathbb{N}$. Then there exists a set $S \subseteq K[X]$ of monic, separable, pairwise coprime polynomials of degree $2k$ that are represented by ϕ over $K[X]$ with $|S| = |K^{\times 2}|$.*

Proof. Observe that it suffices to show the statement for the case where ϕ is binary; furthermore, the statement only depends on ϕ up to isometry, thus we may assume that $\phi = c\langle 1, a \rangle_K$ for some $a, c \in K^\times$. Finally, we may assume $c = 1$. thus we may assume that $\phi \simeq \langle 1, a \rangle_K$ for some $a \in K^\times$.

Assume first that $\mathsf{char}(K)$ does not divide k. Consider $b \in K^\times$. Set $g_b = X^{2k} + ab^2$. Then $g_b = \phi(X^k, b)$, thus g_b is represented by ϕ over $K[X]$. Since $\mathsf{char}(K)$ does not divide $2k$, we have that g_b is separable. Consider now $b_1, b_2 \in K^\times$ such that $b_1 \neq \pm b_2$. We have that $g_{b_1} - g_{b_2} = a(b_1^2 - b_2^2) \in K[X]^\times$, hence g_{b_1} and g_{b_2} are coprime in $K[X]$.

Assume now that $\mathsf{char}(K)$ divides k. Consider $b \in K^\times$. Set $g_b = X^{2k} + ab^2(X + 1)^2$. Then $g_b = \phi(X^k, b(X + 1))$, thus g_b is represented by ϕ over $K[X]$. Since $\mathsf{char}(K)$ divides k, the formal derivative of g_b is $2ab^2(X + 1)$, which is coprime to g_b in $K[X]$. Hence g_b is separable. Consider $b_1, b_2 \in K^\times$ such that $b_1 \neq \pm b_2$. Since $g_{b_1} - g_{b_2} = a(b_1^2 - b_2^2)(X + 1)^2$, we have that g_{b_1} and $g_{b_1} - g_{b_2}$ are coprime in $K[X]$, thus g_{b_1} g_{b_2} are coprime in $K[X]$.

In either case, we obtain the statement by setting $S = \{g_b \mid b \in K^\times\}$. □

6.1.5 Theorem. *Let ϕ be a regular quadratic form over K in at least 3 variables and let $f \in K[X]$ be square-free of even degree. If $\deg(f) \equiv 2 \bmod 4$, then assume further that f has a factor of odd degree. Let $a \in D_K(\phi)$. Then there exists $F \in K[X]$ with $\deg(F) \leqslant \deg(f)$, $F/a - f \in K[X]^2$, $\mathtt{lc}(F) \in D_K(\phi)$ and such that ϕ_L is isotropic for every extension L/K containing a root of F.*

Proof. If $\mathtt{lc}(f) \in D_K(\phi)$ and ϕ_L is isotropic for every extension L/K containing a root of f, set $F = af$. Then the statement holds trivially.

Assume now that $\mathtt{lc}(f) \notin D_K(\phi)$ or ϕ_L is anisotropic for some extension L/K containing a root of f. Observe that K is infinite, in view of [Lam05, Proposition II.3.4]. Let $d \in \mathbb{N}$ be such that ϕ is a regular d-ary quadratic form. Then $\phi \simeq \phi' \perp \langle a \rangle$ for some $(d-1)$-ary quadratic form ϕ' over K. We want to show, in order to apply Proposition 6.1.3, that there exist $g, f_1, \dots, f_{d-1} \in K[X]$ with $2\deg(g) = \deg(f)$ such that g does not divide f and $af \equiv \phi'(f_1, \dots, f_{d-1}) \bmod g$. If we show this for $d - 1 = 2$, then the same follows for all $d \geqslant 3$ by replacing ϕ' with a binary subform of it. We may thus assume that $d = 3$.

Suppose first that $\deg(f) = 4k$ for some $k \in \mathbb{N}$. By Lemma 6.1.4, there exist at least three separable pairwise coprime polynomials in $D_{K[X]}(\phi')$ of degree $2k$. Hence there exists $g \in D_{K[X]}(\phi')$ separable with $\deg(g) = 2k$ not dividing af. Since K is infinite, it follows by Corollary 6.1.2 that $af \equiv \phi'(f_1, f_2) \bmod g$ for some $f_1, f_2 \in K[X]$.

Suppose now that $\deg(f) = 4k + 2$ for some $k \in \mathbb{N}$ and that f has a factor of odd degree. Then f has an irreducible factor p of odd degree with $\deg(p) \leqslant 2k + 1$.

Assume first $\deg(p) \leqslant 2k - 1$ and set $m = k + (1 - \deg(p))/2$. Note that $m \geqslant 1$. By Lemma 6.1.4, there exist at least three separable pairwise coprime polynomials in $D_{K[X]}(\phi')$ of degree $2m$. Therefore there exists $h \in D_{K[X]}(\phi')$ separable, coprime to p, not dividing f and such that $\deg(h) = 2m$. Set $g = p \cdot h$. Then g does not divide af and $\deg(g) = 2k + 1$. Since h is separable, it is square-free. Since $h \in D_{K[X]}(\phi')$ and $\deg(h) < \deg(g) = 2k+1 < \infty$, it follows by Corollary 6.1.2 that there exist $f_1, f_2 \in K[X]$ such that $af \equiv \phi'(f_1, f_2)$ modulo every prime factor of h. Since $af \equiv 0 \equiv \phi'(0, 0) \bmod p$, it follows by the Chinese Remainder Theorem that there exist $\hat{f}_1, \hat{f}_2 \in K[X]$ such that $af = \phi'(\hat{f}_1, \hat{f}_2) \bmod g$.

Assume now that $\deg(p) = 2k+1$. Let $q \in K[X]$ be such that $f = pq$ and let $\lambda \in K^\times$ be such that $\lambda^2 \neq \mathtt{lc}(q)/\mathtt{lc}(p)$. Set $g = (q - \lambda^2 p)$. Then $\deg(g) = 2k+1$ and $f - \lambda^2 p^2 = pg$, therefore $af \equiv a(\lambda p)^2 \bmod g$, and $a(\lambda p)^2 \in D_{K[X]}(\phi)$. Since f is square-free, we have that p does not divide q. Hence p does not divide g. Therefore g does not divide $a\lambda^2 p^2$, that is, g does not divide f.

In either case we have shown that there exists $g \in K[X]$ satisying the hypothesis of Proposition 6.1.3. Hence the statement follows from Proposition 6.1.3. □

6.1.6 Corollary. *Let $m \in \mathbb{N}$ with $m \geqslant 2$, let ϕ be an m-fold Pfister form over K and $f \in K[X]$ square-free of even degree. If $\deg(f) \equiv 2 \bmod 4$, then assume further that f has a factor of odd degree. Let $a \in D_K(\phi)$. Then there exists $F \in D_{K[X]}(\phi)$ with $\deg(F) \leqslant \deg(f)$ such that $F/a - f \in K[X]^2$.*

Proof. By Theorem 6.1.5, there exists $F \in K[X]$ such that ϕ_L is isotropic for every field extension L/K containing a root of F, $\deg(F) \leqslant \deg(f)$, $F/a - f \in K[X]^2$ and $\mathtt{lc}(F) \in D_K(\phi)$. It follows by Theorem 1.1.24 that $F \in D_{K[X]}(\phi)$. □

Recall from Section 4.1 that K is *euclidean* if K is real and $K^\times = K^{\times 2} \cup -K^{\times 2}$.

6.1.7 Proposition. *Let ϕ be a Pfister form over K such that ϕ_L is isotropic for every quadratic field extension L/K. Then ϕ is universal or K is euclidean.*

Proof. If ϕ is isotropic, then ϕ is universal, by Corollary 1.1.7. Suppose that ϕ is anisotropic and let ψ be a quadratic form over K such that $\phi \simeq \langle 1 \rangle_K \perp \psi$. By Corollary 1.1.20, we have $D_K(\psi) \cup -K^2 = K$. Assume that ϕ is not universal. Then $D_K(\psi) = K \smallsetminus -K^2 = D_K(\phi)$. As $D_K(\phi)$ is a proper subgroup of $K^\times$, we get that

$K^\times/D_K(\phi) = \{D_K(\phi), -D_K(\phi)\}$ and $-D_K(\phi) = -K^{\times 2}$, thus $K^{\times 2} = D_K(\phi)$ and $K^\times = K^{\times 2} \cup -K^{\times 2}$. Furthermore, it follows by [Lam05, Kneser's Lemma VII.6.5] that K is real. Therefore K is euclidean. □

6.1.8 Corollary. *Assume that K is not euclidean. Let $m \in \mathbb{N}$ with $m \geqslant 2$ and ϕ an m-fold Pfister form over K such that ϕ_L is isotropic for every finite field extension L/K of even degree. Let $f \in K[X]$ be square-free of even degree and $a \in K^\times$. Then there exists $F \in D_{K[X]}(\phi)$ with $\deg(F) \leqslant \deg(f)$ and such that $F/a - f \in K[X]^2$.*

Proof. If f has a factor of odd degree, then the statement follows by Corollary 6.1.6. Assume now that f has no factor of odd degree. Set $F = af$. For any prime factor p of F, we have that $[K[X]/(p) : K] = \deg(p) \in 2\mathbb{N}^+$, hence ϕ is isotropic over $K[X]/(p)$ by the hypothesis. Since K is not euclidean, it follows by Proposition 6.1.7 that ϕ is universal, whereby $\mathtt{lc}(F) \in D_K(\phi)$. Therefore $F \in D_{K[X]}(\phi)$ by Theorem 1.1.24. □

Recall from Section 4.1 that K is a *local field* if it is isomorphic to $\mathbb{R}$, to $\mathbb{C}$, to a finite field extensions of $\mathbb{Q}_p$ or of $\mathbb{F}_p(\!(t)\!)$ for $p \in \mathbb{N}$ prime. We retrieve the following statement, contained in [Pou71, Théorème 1].

6.1.9 Corollary. *Assume that K is a nonreal local field. Let ϕ be a regular 4-ary quadratic form over K, let $a \in K^\times$ and let $f \in K[X]$ be square-free and of even degree. Then there exists $F \in D_{K[X]}(\phi)$ with $\deg(F) \leqslant \deg(f)$ such that $F/a - f$ is a square in $K[X]$.*

Proof. Recall that $D_{K[X]}(\phi) = D_{K(X)}(\phi) \cap K[X]$, by the Cassels-Pfister Theorem 1.1.21. If ϕ is isotropic, then $\phi_{K(X)}$ is universal by Proposition 1.1.23, whereby $D_{K[X]}(\phi) = K[X]$, and we retrieve the statement by setting $F = af$. Assume now that ϕ is anisotropic. Then it follows by [Lam05, Corollary VI.2.15] that ϕ is isometric to a 2-fold Pfister form over K, which is universal over K, by [Lam05, Corollary VI.2.11]. By [Lam05, Lemma VI.2.14], we conclude that ϕ_L is isotropic for every field extension L/K of even degree. Hence the statement follows from Corollary 6.1.8. □

We retrieve from Corollary 6.1.9 the example about polynomials over $\mathbb{Q}_2$ that was discussed at the beginning of this section.

6.1.10 Corollary. *Let $f \in \mathbb{Q}_2[X]$ be of even degree. Then there exist $f_1, \ldots, f_5 \in \mathbb{Q}_2[X]$ such that $\deg(f_i) \leqslant \deg(f)$ for any $1 \leqslant i \leqslant 5$ and $f = f_1^2 + f_2^2 + f_3^2 + f_4^2 + f_5^2$.*

Proof. Set $\phi = \langle 1,1,1,1\rangle_{\mathbb{Q}_2}$. Recall from Section 2.4 that $\mathbb{Q}_2 = \Sigma_4 {\mathbb{Q}_2}^2$, that is, ϕ is universal. Let $g \in \mathbb{Q}_2[X]$ be such that f/g^2 is square-free and $f/g^2 \in \mathbb{Q}_2[X]$. It follows by Corollary 6.1.9 that there exists $F \in D_{\mathbb{Q}_2[X]}(\phi)$ with $\deg(F) \leqslant \deg(f/g^2)$ and such that $-F + f/g^2 \in K[X]^2$. Therefore, there exist $h, F_1, F_2, F_3, F_4 \in \mathbb{Q}_2[X]$ such that $h^2 = -F + f/g^2$ and $F = \phi(F_1, F_2, F_3, F_4)$. Then $f/g^2 = F + h^2$, that is, $f = g^2F + g^2h^2$, and $2\deg(F_i), 2\deg(h) \leqslant \deg(f/g^2)$ for any $1 \leqslant i \leqslant 4$. We find that

$$f = (gF_1)^2 + (gF_2)^2 + (gF_3)^2 + (gF_4)^2 + (gh)^2,$$

and $2\deg(gF_i), 2\deg(gh) \leqslant \deg(f)$ for any $1 \leqslant i \leqslant 4$. Hence we obtain the statement by setting $f_i = gF_i$ for $1 \leqslant i \leqslant 4$ and $f_5 = gh$. □

6.2 Continuity of roots and quadratic forms

We fix a henselian valued field (K, v) of characteristic different from 2. In this section we show, for $n \in \mathbb{N}^+$, that being a sum of 2^n squares over $K[X]$ is a continuous property with respect to the v-adic topology. Roughly speaking, we show that changing by a little the coefficient of a polynomial which is a sum of 2^n squares produces another sum of 2^n squares. We are not aware of these results in the literature, though the techniques of root-continuity which we exploit have been mature for several years; see e.g. [Bri06]. In order to follow this section, it might help the reader to keep in mind that we are especially interested in fields K which are finite extensions of $\mathbb{Q}_2$. In Section 6.4, we will generalise these tools to arbitrary quadratic forms.

For this section, we fix an algebraic closure K^{alg} of K and we denote the unique extension of v to K^{alg} again by v, and the valuation ring of K^{alg} corresponding to v again by $\mathcal{O}_v$. The value group of the latter is $vK \otimes_{\mathbb{Z}} \mathbb{Q}$, and it contains the value group of the extension of v to any finite extension of K contained in K^{alg}; see [EP05, p. 78]. We denote the Gauss extension of v to $K^{alg}(X)$ with respect to X again by v.

6.2.1 Proposition. *Let $f \in K[X] \setminus \{0\}$ and let $\alpha \in K^{alg}$ be a root of f. Then we have $v(\alpha) \geqslant v(f) - v(\mathtt{lc}(f))$.*

Proof. Write $f = (X - \alpha)g$ with $g \in K^{alg}[X]$. Then $v(g) \leqslant v(\mathtt{lc}(g)) = v(\mathtt{lc}(f))$ and $v(X-\alpha) \leqslant v(\alpha)$. Hence $v(f) = v(g) + v(X-\alpha) \leqslant v(\alpha) + v(\mathtt{lc}(f))$. □

6.2.2 Proposition. *Let $f, g \in K[X] \setminus \{0\}$ with* $\deg(g) \leqslant \deg(f)$*. Let $\alpha \in K^{alg}$ be a root of f. Then we have*

$$v(g(\alpha)) \geqslant v(f-g) + \deg(f)(v(f) - v(\mathtt{lc}(f))).$$

Proof. Set $n = \deg(f)$ and let $a_0, b_0, \dots, a_n, b_n \in K$ be such that $f = \Sigma_{i=0}^n a_i X^i$ and $g = \Sigma_{i=0}^n b_n X^n$. Since $f(\alpha) = 0$, we have that

$$g(\alpha) = g(\alpha) - f(\alpha) = (b_n - a_n)\alpha^n + \ldots + (b_1 - a_1)\alpha + (b_0 - a_0).$$

We obtain that

$$\begin{aligned} v(g(\alpha)) &\geqslant \mathsf{min}\{v(b_k - a_k) + k \cdot v(\alpha) \mid 0 \leqslant k \leqslant n\} \\ &\geqslant \mathsf{min}\{v(b_k - a_k) \mid 0 \leqslant k \leqslant n\} + \mathsf{min}\{k \cdot v(\alpha) \mid 0 \leqslant k \leqslant n\} \\ &= v(g-f) + \mathsf{min}\{k \cdot v(\alpha) \mid 0 \leqslant k \leqslant n\}. \end{aligned}$$

By Proposition 6.2.1, we have $v(\alpha) \geqslant v(f) - v(a_n)$. Since $v(f) - v(a_n) \leqslant 0$, we obtain

$$\begin{aligned} \mathsf{min}\{k \cdot v(\alpha) \mid 0 \leqslant k \leqslant n\} &\geqslant \mathsf{min}\{k(v(f) - v(a_n)) \mid 0 \leqslant k \leqslant n\} \\ &= n(v(f) - v(a_n)). \end{aligned}$$

Hence $v(g(\alpha)) \geqslant v(f-g) + n(v(f) - v(a_n))$. □

6.2.3 Proposition. *Let $f, g \in K[X] \setminus \{0\}$ with* $\deg(g) = \deg(f)$ *and let $\alpha \in K^{alg}$ be a root of f. Then there exists a root $\beta \in K^{alg}$ of g such that*

$$v(\beta - \alpha) \geqslant \frac{v(f-g) - v(\mathtt{lc}(g))}{\deg(f)} + v(f) - v(\mathtt{lc}(f)).$$

Proof. Set $n = \deg(f)$. Let $\beta_1, \dots, \beta_n \in K^{alg}$ such that $g = \mathtt{lc}(g) \cdot \prod_{i=1}^n (X - \beta_i)$. Then

$$g(\alpha) = \mathtt{lc}(g) \cdot \prod_{i=1}^{n} (\alpha - \beta_i).$$

For the sake of a contradiction, assume that, for every $1 \leqslant i \leqslant n$, we have

$$v(\alpha - \beta_i) < (v(f-g) - v(\mathtt{lc}(g)))/n + v(f) - v(\mathtt{lc}(f)).$$

Then we have

$$\begin{aligned} v(g(\alpha)) &= v(\mathtt{lc}(g)) + \Sigma_{i=1}^{n} v(\alpha - \beta_i) \\ &< v(\mathtt{lc}(g)) + n\Big(\big(v(f-g) - v(\mathtt{lc}(g))\big)/n + v(f) - v(\mathtt{lc}(f))\Big). \end{aligned}$$

Hence $v(g(\alpha)) < v(f-g) + n(v(f) - v(\mathtt{lc}(f)))$, which contradicts Proposition 6.2.2. □

Recall from Section 2.2 that for $n \in \mathbb{N}$ and $F \in K^{alg}[X] \setminus \{0\}$ having precisely n roots in K^{alg}, we set $C_v(F) = -\infty$ if $n \leqslant 1$, and we set

$$C_v(F) = \mathsf{sup}\{v(\alpha_i - \alpha_j) \mid 1 \leqslant i < j \leqslant n\}$$

where $\alpha_1, \ldots, \alpha_n$ are the distinct roots of F in K^{alg} otherwise. Recall also that for $\alpha \in K^{alg}$, we set $C_v(\alpha/K) = C_v(F)$ where F is the minimal poynomial of α over K.

6.2.4 Proposition. *Let $F \in K[X] \setminus \{0\}$. For every root $\alpha \in K^{alg}$ of F, we have that $C_v(F) \geqslant C_v(\alpha/K)$ and, if F is monic with $v(F) \geqslant 0$, then $C_v(\alpha/K) \geqslant 0$ and $v(\alpha) \geqslant 0$.*

Proof. The first part of the statement follows directly from the definitions. Assume now that F is monic and $v(F) \geqslant 0$. Then $F \in \mathcal{O}_v[X]$, by the definition of the Gauss extension. Consider a root $\alpha \in K^{alg}$ of F. Since $\mathcal{O}_v$ is integrally closed, $F \in \mathcal{O}_v[X]$ and F is monic, we obtain that $\alpha \in \mathcal{O}_v$, that is, $v(\alpha) \geqslant 0$. Since this holds for all roots of F, we also conclude that $C_v(\alpha) \geqslant 0$. □

For $F \in K^{alg}[X] \setminus \{0\}$, we set

$$\gamma_v(F) = \deg(F) \cdot \big(C_v(F) - v(F) + v(\mathtt{lc}(F))\big) + v(\mathtt{lc}(F)).$$

6.2.5 Theorem. *Let $F, G \in K^{alg}[X] \setminus \{0\}$ with $v(F-G) > \gamma_v(F)$ and $\deg(G) = \deg(F)$, and let $\beta \in K^{alg}$ be a root of G. Then there exists a root $\alpha \in K^{alg}$ of F such that $v(\beta - \alpha) > C_v(F)$.*

Proof. Set $m = \deg(F)$. Let $F_0, G_0, \ldots, F_m, G_m \in K^{alg}$ be such that $F = \Sigma_{i=0}^{m} F_i X^i$ and $G = \Sigma_{i=0}^{m} G_i X^i$, and let $\alpha_1, \ldots, \alpha_m \in K^{alg}$ be such that $F = F_m \cdot \prod_{i=1}^{m}(X - \alpha_i)$. Furthermore, denote $M = \mathsf{max}\{v(\beta - \alpha_i) \mid 1 \leqslant i \leqslant m\}$. Observe that

$$mM \geqslant \Sigma_{i=1}^{m} v(\beta - \alpha_i) = v\left(\prod_{i=1}^{m}(\beta - \alpha_i)\right) = v(F(\beta)/F_m) = v(F(\beta)) - v(F_m).$$

Since $F(\beta) = (F-G)(\beta) = \Sigma_{i=1}^{m}(F_i - G_i)\beta^i$, we find

$$\begin{aligned} mM &\geqslant \mathsf{min}\{v(F_i - G_i) + iv(\beta) \mid 0 \leqslant i \leqslant m\} - v(F_m) \\ &\geqslant v(F-G) + \mathsf{min}\{iv(\beta) \mid 0 \leqslant i \leqslant m\} - v(F_m) \end{aligned}$$

By Proposition 6.2.1, we have $v(\beta) \geqslant v(G) - v(G_m)$ and $C_v(F) \geqslant v(F) - v(F_m)$. From the latter inequality, we find $\gamma_v(F) \geqslant v(F_m)$. Since $v(G-F) > \gamma_v(F)$, and by the definition of the Gauss extension, it follows that $v(G_m - F_m) \geqslant v(G-F) > v(F_m) \geqslant v(F)$.

In particular, we have $v(G-F) > v(F)$, whereby $v(G) = v(F)$, and $v(G_m - F_m) > v(F_m)$, whereby $v(G_m) = v(F_m)$. We obtain that $v(\beta) \geqslant v(F) - v(F_m)$, whence

$$\mathsf{min}\{iv(\beta) \mid 0 \leqslant i \leqslant m\} = m \cdot \mathsf{min}\{0, v(\beta)\} \geqslant m \cdot \mathsf{min}\{0, v(F) - v(F_m)\}.$$

Since $v(F_m) \geqslant v(F)$, we get that $\mathsf{min}\{0, v(F) - v(F_m)\} = v(F) - v(F_m)$. Therefore $mM \geqslant v(F-G) + m(v(F) - v(F_m)) - v(F_m)$. Since $v(F-G) > \gamma_v(F)$, we conclude that $mM > mC_v(F)$, whereby $M > C_v(F)$. By the definition of M, there exists a root $\alpha \in K^{alg}$ of F with $v(\beta - \alpha) > C_v(F)$. □

6.2.6 Proposition. *Let $F \in K[X]$ be separable. Then for every $G \in K[X]$ such that* $\deg(G) = \deg(F)$ *and $v(F-G) > \gamma_v(F)$, we have*

$$K[X]/(F) \simeq K[X]/(G).$$

Proof. Set $m = \deg(F)$ and let $\alpha_1, \ldots, \alpha_m \in K^{alg}$ denote the roots of F. Consider $1 \leqslant i \leqslant m$. By Theorem 6.2.5, there exists a root $\beta_i \in K^{alg}$ of G such that

$$v(\alpha_i - \beta_i) > C_v(F) \geqslant C_v(\alpha_i/K).$$

Therefore for $1 \leqslant i < j \leqslant m$, we have that

$$v(\beta_i - \beta_j) = v(\alpha_i - \alpha_j) \neq \infty.$$

Hence $\beta_1, \ldots, \beta_m$ are all different. Since $\deg(G) = m$, it follows that

$$G = \mathtt{lc}(G) \cdot (X - \beta_1) \cdot \cdots \cdot (X - \beta_m),$$

and in particular G is separable.

Consider now $1 \leqslant i \leqslant m$. By Theorem 2.2.14, we have that $K(\alpha_i) \subseteq K(\beta_i)$. We claim that $K(\alpha_i) = K(\beta_i)$. Assume, for the sake of a contradiction, that $K(\alpha_i) \subsetneq K(\beta_i)$. Since G is separable, there exists a $K(\alpha_i)$-automorphism σ of K^{alg} such that $\sigma(\beta_i) \neq \beta_i$. Hence $\beta_j = \sigma(\beta_i)$ for some $j \in \{1, \ldots, n\} \setminus \{i\}$. Since $v \circ \sigma = v$, we obtain

$$v(\alpha_i - \beta_j) = v(\sigma(\alpha_i - \beta_i)) = v(\alpha_i - \beta_i) > C_v(\alpha_i/K) \geqslant v(\alpha_i - \alpha_j).$$

Thus $v(\alpha_j - \beta_j) = v(\alpha_j - \alpha_i) \leqslant C_v(\alpha_i/K)$, which contradicts the way in which $\beta_1, \ldots, \beta_m$ were obtained. Hence $K(\alpha_i) = K(\beta_i)$ for every $1 \leqslant i \leqslant n$. Therefore

$$K[X]/(F) \simeq K(\alpha_1) \times \cdots \times K(\alpha_m) = K(\beta_1) \times \cdots \times K(\beta_m) \simeq K[X]/(G).$$

□

6.2.7 Corollary. *Let $m, k \in \mathbb{N}$ and let $F \in K[X] \cap \Sigma_{2^k} K(X)^2$ be separable of degree m. Then there exists $\gamma \in vK$ such that for every $G \in K[X]$ of degree m with $\mathtt{lc}(G) \in \Sigma_{2^k} K^2$ and $v(F-G) > \gamma$, we have $G \in \Sigma_{2^k} K[X]^2$.*

Proof. By Proposition 6.2.6, there exists $\gamma \in vK$ such that, for every $G \in K[X]$ of degree m such that $\mathtt{lc}(G) \in \Sigma_{2^k} K^2$ and $v(F-G) > \gamma$, we have that $K[X]/(F) \simeq K[X]/(G)$. Then $G \in \Sigma_{2^k} K[X]^2$, by Proposition 1.2.10. □

6.2.8 Corollary. *Assume that K is a non-archimedean local field and v is the valuation determined by K. Let $m \in \mathbb{N}$ and $F \in \Sigma_4 K[X]^2$ separable of degree m. Then there exists $\gamma \in vK$ such that, for any $G \in K[X]$ of degree m such that $v(F-G) > \gamma$, we have $G \in \Sigma_4 K[X]^2$.*

Proof. Recall from Section 2.4 that $K^v = \Sigma_4 K^{v2}$. Then the statement follows directly from Corollary 6.2.7. □

6.3 Pourchet's global theorem

In this section we use the local-global principle from Chapter 5 and the instruments that were developed in Sections 6.1 and 6.2 to retrieve the bound $p(K(X)) \leqslant 5$ for every number field K contained in [Pou71]. Before proving Pourchet's theorem, we develop a few more tools. The following statement is an application of the Weak Approximation (Theorem 2.1.9) to polynomials in one variable over a field.

6.3.1 Lemma. *Let K be a field, let S be a finite set of pairwise independent valuations on K and $n \in \mathbb{N}$. For every $v \in S$, let $\gamma_v \in vK$ and let $g_v \in K^v[X]$ be such that $\deg(g_v) \leqslant n$. Then there exists $g \in K[X]$ such that $\deg(g) \leqslant n$ and $v(g - g_v) > \gamma_v$ for every $v \in S$.*

Proof. Consider $v \in S$. Let $a_{v0}, \dots, a_{vn} \in K^v$ be such that $g_v = \Sigma_{i=0}^n a_{vi} X^i$. Recall from Section 2.3 that K is dense in K^v with respect to the v-adic topology. Then for every $1 \leqslant i \leqslant n$ we may choose $b_{vi} \in K$ such that $v(b_{vi} - a_{vi}) > \gamma_v$.

By applying Theorem 2.1.9 $n+1$ times, we find $b_0, \dots, b_n \in K$ such that $v(b_i - b_{vi}) > \gamma_v$ for every $v \in S$ and $0 \leqslant i \leqslant n$. Set $g = \Sigma_{i=0}^n b_i X^i$. Then for every $v \in S$ we have that $v(g - g_v) = \mathsf{min}\{v(b_i - b_{vi}) \mid 0 \leqslant i \leqslant n\}$, whereby $v(g - g_v) > \gamma_v$, since $v(b_i - b_{vi}) > \gamma_v$ for every $0 \leqslant i \leqslant n$. □

Recall from Section 3.2 that given a real field K and an ordering P on K, we say that P is *archimedean* if for every $x \in K$ there exists $n \in \mathbb{N}$ such that $x \leqslant_P n$ (that is, $n - x \in P$); this is equivalent to having $\mathcal{O}(P) = K$. We say that a field is *archimedean* if it admits an archimedean ordering and is *totally archimedean* if it is real and if all of its orderings are archimedean; clearly, this amounts to the whole field being the only real valuation ring, and to having the whole field as real holomorphy ring.

6.3.2 Proposition. *Let K be a totally archimedean field, $f \in \Sigma K[X]^2$ square-free and $g \in K[X]$ such that $2\deg(g) \leqslant \deg(f)$. Then $g^2/f \in \mathcal{H}(K(X))$.*

Proof. Set $\mathcal{P} = \{p \in \mathcal{P}_K \mid K[X]/(p) \text{ is real}\}$. Consider $p \in \mathcal{P}$. Note that v_p is real, since $K(K)v_p = K[X]/(p)$. Since $f \in \Sigma K[X]^2$, it follows by Proposition 2.4.2 that $v_p(f) \in 2\mathbb{Z}$. Since f is square-free, we have that $v_p(f) \in \{0, 1\}$. Therefore $v_p(f) = 0$. This shows that $v_p(g^2/f) \geqslant 0$ for each $p \in \mathcal{P}$. Since K is totally archimedean, the only real valuation ring of K is K itself. It follows by Example 2.1.3 (d) that the only real valuation rings of $K(X)$ are $\mathcal{O}_{v_\infty}$ and $\mathcal{O}_{v_p}$ where $p \in \mathcal{P}$. Therefore $g^2/f \in \mathcal{H}(K(X))$. □

6.3.3 Lemma. *Let K be a totally archimedean field. Let S be a finite set of valuations on K, let $f \in \Sigma\, K[X]^2$ be square-free and let $g \in K[X]$ be such that $2\deg(g) \leqslant \deg(f)$. For every $v \in S$, let $\gamma_v \in vK$. Then there exists $c \in K^\times$ such that $f - c^2 g^2 \in \Sigma\, K[X]^2$ and such that $v(c-1) > \gamma_v$ for every $v \in S$.*

Proof. Without loss of generality, we may assume that $\gamma_v \geqslant 0$ for every $v \in S$. By Theorem 2.1.9, there exists $x \in K^\times$ such that $v(x) > \gamma_v$ for every $v \in S$. Since K is totally archimedean, we have that $K = \mathcal{H}(K)$. Hence there exists $n \in \mathbb{N}$ such that $n - x^{-2} \in \Sigma\, K^2$. Set $y = nx^2$. Then $y - 1 \in \Sigma\, K^2$ and $v(y) > \gamma_v$ for every $v \in S$. Consider $k \in \mathbb{N}^+$ and set $c_k = 1 + y^k/(1-y^k) = 1/(1-y^k)$. For every $v \in S$, we have that $v(c_k - 1) = v(y^k/(1-y^k)) = kv(y)$, hence $v(c_k - 1) > \gamma_v$. In view of Proposition 6.3.2, we have $g^2/((y-1)^2 f) \in \mathcal{H}(K(X))$. By Theorem 3.2.18, there exists $m \in \mathbb{N}$ such that $m - g^2/((y-1)^2 f) \in \Sigma\, K(X)^2$. Thus $m^2 - g^2/((y-1)^2 f) \in \Sigma\, K(X)^2$, that is, $m^2(y-1)^2 - g^2/f \in \Sigma K(X)^2$. Since $y - 1 \in \Sigma\, K^2$, we have that $y^i - 1 \in \Sigma K^2$ for all

$i \in \mathbb{N}$, and thus $(y-1)(y^{m+1}+\cdots+y+1-m) \in \Sigma K^2$, whereby $y^m-1-m(y-1) \in \Sigma\, K^2$. Hence $(y^m-1)^2-(m(y-1))^2 \in \Sigma\, K^2$, thus $(y^m-1)^2-g^2/f \in \Sigma\, K(X)^2$. Therefore $c_m^{-2}-g^2/f \in \Sigma K(X)^2$, whence $f-c_m^2 g^2 \in \Sigma\, K(X)^2$. □

6.3.4 Example. Let K be a real number field, let $f \in \Sigma\, K[X]^2$ and $g \in K[X] \smallsetminus \{0\}$. Let S be a set of dyadic $\mathbb{Z}$-valuations on K. Then S is finite, by Theorem 2.2.4. For every $v \in S$, let $\gamma_v \in \mathbb{N}$. By Lemma 6.3.3, there exists $c \in K^\times$ such that $v(c-1) > \gamma_v - 2v(g)$ for every $v \in S$ and $f - c^2g^2 \in \Sigma\, K[X]^2$. Therefore $f-c^2g^2 \in \Sigma\, K[X]^2$ and for every $v \in S$ we have $v(c^2g^2-g^2) = v(c+1)+v(c-1)+2v(g) > \gamma_v$.

Finally, we retrieve Pourchet's upper bound for $p(K(X))$ where K is a number field. The following statements were originally proven in [Pou71, Théorème 2, Corollaire 4].

6.3.5 Lemma. *Let K be a real number field and let $f \in \Sigma\, K[X]^2$ be square-free. Then there exists $h \in K[X]$ such that $f-h^2 \in \Sigma\, K[X]^2$ and $f-h^2 \in \Sigma_4 K^v[X]^2$ for every dyadic valuation v on K.*

Proof. Set $\phi = \langle\langle -1,-1\rangle\rangle_K$. Since $f \in \Sigma K[X]^2$, we have that $\deg(f)$ is even. Let S be the set of dyadic $\mathbb{Z}$-valuations on K. Since $K/\mathbb{Q}$ is finite, it follows by Theorem 2.2.4 that S is finite. Consider $v \in S$. By Corollary 6.1.9, there exists $g_v \in K^v[X]$ with $\deg(f-g_v^2)=2n$ such that $f-g_v^2 \in D_{K^v[X]}(\phi)$. Let $h_v \in K^v[X]$ be such that $(f-g_v^2)/h_v^2$ is square-free in $K^v[X]$, and thus separable. By Corollary 6.2.8, there exists $\gamma_v \in \mathbb{Z}$ such that, for every $G \in K^v[X]$ such that $\deg(G) = \deg(f-g_v^2) - 2\deg(h_v)$ and $v((f-g_v^2)/h_v^2 - G) > \gamma_v$, we have $G \in D_{K^v[X]}(\phi)$.

By Lemma 6.3.1, there exists $g \in K[X]$ such that, for every $v \in S$, we have

$$v(g_v - g) > \mathsf{max}\{v(2g), \gamma_v - v(2g) + 2v(h_v)\}.$$

Consider $v \in S$. By the choice of g, we have that $v(g_v-g) > \gamma_v - v(2g) + 2v(h_v)$ and $v(g_v+g) = v(2g)$. Therefore

$$\begin{aligned} v((f-g^2)/h_v^2 - (f-g_v^2)/h_v^2) &= v(g_v^2-g^2) - 2v(h_v) \\ &= v(g_v-g)+v(g_v+g)-2v(h_v) \\ &> \gamma_v - v(2g) + v(2g) + 2v(h_v) - 2v(h_v) = \gamma_v. \end{aligned}$$

By the choice of γ_v, we obtain that $(f-g^2)/h_v^2 \in D_{K^v[X]}(\phi)$, whence $f-g^2 \in D_{K^v[X]}(\phi)$.

If $g=0$, then since $f \in \Sigma\, K[X]^2$, we may take $h=0$ to obtain the claim. Suppose $g \neq 0$. Then, by Lemma 6.3.3, there exists $c \in K^\times$ such that $f-c^2g^2 \in \Sigma\, K[X]^2$ and $v(c^2g^2-g^2) > \gamma_v + 2v(h_v)$ for all $v \in S$. Set $h = cg$. As $v((f-g^2)/h_v^2 - (f-h^2)/h_v^2) > \gamma_v$, and again by the choice of γ_v, we have that $(f-h^2)/h_v^2 \in D_{K^v[X]}(\phi)$ for every $v \in S$. Thus $f-h^2 \in D_{K^v[X]}(\phi)$ for every dyadic $\mathbb{Z}$-valuation v of K. □

6.3.6 Theorem (Pourchet)**.** *Let K be a number field, $f \in \Sigma K[X]^2$. Then $f \in \Sigma_5 K[X]^2$.*

Proof. If K is nonreal, then $s(K(X)) = s(K) \leqslant 4$, by Corollary 2.4.16. Therefore $p(K(X)) \leqslant s(K)+1 \leqslant 5$, by Proposition 1.2.4. Assume that K is real. For every $g \in K[X]$ such that g^2 divides f in $K[X]$, we have that $f \in \Sigma_5 K[X]^2$ if and only if $f/g^2 \in \Sigma_5 K[X]^2$. Thus we may assume that f is square-free. By Lemma 6.3.5, there exists $h \in K[X]$ such that $f-h^2 \in \Sigma K[X]^2$ and $f-h^2 \in \Sigma_4 K^v[X]^2$ for any dyadic $\mathbb{Z}$-valuation v on K. By Corollary 5.3.5 we get $f-h^2 \in \Sigma_4 K[X]^2$, whence $f \in \Sigma_5 K[X]^2$. □

6.4 Variations on root continuity

In this section we generalise the techniques developed in the second part of Section 6.2 to arbitrary quadratic forms. As in Section 6.2, we fix a henselian valued field (K, v) of characteristic different from 2 and an algebraic closure K^{alg} of K. We denote the unique extension of v to K^{alg} again by v.

6.4.1 Corollary. *Let $F \in K[X]$ be separable and let ϕ be an anisotropic quadratic form over K such that $\phi_{K[X]/(p)}$ is isotropic for every irreducible factor p of F in $K[X]$. Then there exists $\gamma \in vK$ such that for each $G \in K[X]$ with $\deg(G) = \deg(F)$ and $v(F-G) > \gamma$, and for every irreducible factor $p \in K[X]$ of G, we have that $\phi_{K[X]/(p)}$ is isotropic.*

Proof. Set $m = \deg(F)$ and $\gamma = \gamma_v(F)$. We claim that γ satisfies the desired properties. Consider $G \in K[X]$ of degree m such that $v(F - G) > \gamma$. Consider an irreducible factor p of G in $K[X]$ and a root $\beta \in K^{alg}$ of p. By Theorem 6.2.5, there exists a root $\alpha \in K^{alg}$ of F such that $v(\alpha - \beta) > C_v(F)$. Thus $v(\alpha - \beta) > C_v(\alpha/K)$, by Proposition 6.2.4. It follows by Theorem 2.2.14 that $K(\alpha, \beta)$ is purely inseparable over $K(\beta)$. As $\mathsf{char}(K) \neq 2$, we have that $[K(\alpha, \beta) : K(\beta)]$ is odd. Since $\phi_{K(\alpha)}$ is isotropic, it follows that $\phi_{K(\alpha,\beta)}$ is isotropic. Hence $\phi_{K(\beta)}$ is isotropic, by Theorem 1.1.9. □

6.4.2 Corollary. *Let ϕ be an anisotropic Pfister form over K and let $F \in D_{K[X]}(\phi)$ be square-free in $K[X]$. Then there exists $\gamma \in vK$ such that, for every $G \in K[X]$ such that $\deg(G) = \deg(F)$, $\mathtt{lc}(G) \in D_K(\phi)$ and $v(F - G) > \gamma$, we have that $G \in D_{K[X]}(\phi)$.*

Proof. By Theorem 1.1.24, we have that $\mathtt{lc}(F) \in D_K(\phi)$ and that $\phi_{K[X]/(p)}$ is isotropic for any irreducible factor p of F. By Corollary 6.4.1, there exists $\gamma \in vK$ such that, for any $G \in K[X]$ with $\deg(F) = \deg(G)$ and $v(F-G) > \gamma$, and for any irreducible factor p of G, we have that $\phi_{K[X]/(p)}$ is isotropic. By Theorem 1.1.24, we conclude for every $G \in K[X]$ with $\deg(F) = \deg(G)$, $\mathtt{lc}(G) \in D_K(\phi)$ and $v(F - G) > \gamma$, that $G \in D_{K[X]}(\phi)$. □

6.4.3 Example. We retrieve Corollary 6.2.8. Assume that v is a $\mathbb{Z}$-valuation and K is a non-archimedean local field that is complete with respect to v. Set $\phi = \langle\langle -1, -1 \rangle\rangle_K$ and recall from Section 4.1 that ϕ is universal. Let $F \in D_{K[X]}(\phi)$ be square-free. By Corollary 6.4.2, there exists $\gamma \in \mathbb{Z}$ such that, for any $G \in K[X]$ such that $\deg(F) = \deg(G)$ and $v(F - G) > \gamma$, we have that $G \in D_{K[X]}(\phi)$.

Chapter 7

Bounding the Pythagoras number by $2^n + 1$

In this chapter we provide a sufficient condition for a field K to satisfy $p(K) \leqslant 2^n + 1$ for a given $n \in \mathbb{N}$, and we show that said condition applies to several families of fields. After developing the new setup in the first two sections, we recover two upper bounds mentioned in the introduction: the one by Becher, Grimm and Van Geel for the Pythagoras number of a function field in one variable over $\mathbb{R}(\!(t)\!)$ and Y. Hu's one for the Pythagoras number of a finite field extension of $\mathbb{R}(\!(t_0, t_1)\!)$.

Our method relies on the presence of a local-global principle for certain quadratic forms. As such, this is a fairly standard approach. Indeed, let $n \in \mathbb{N}$ and let F be a field. We have already seen that, given $a \in \Sigma F^2$, the question whether $a \in \Sigma_{2^n+1} F^2$ can be reformulated in terms of isotropy of the $(2^n + 2)$-ary quadratic form $\Sigma_{i=1}^{2^n+1} X_i^2 - aX_0^2$. In our approach, however, we use a valuation theoretic local-global principle to characterise the sums of 2^n squares (rather than the sums of $2^n + 1$ squares) while aiming for the bound $p(F) \leqslant 2^n + 1$. This is reminiscent of Pop's and Pourchet's methods described in Chapter 4 and Chapter 6, where a description of the sums of 4 squares in the considered fields via local conditions is essential to write certain elements as sums of 5 squares. We focus thus on the quadratic forms $\Sigma_{i=1}^{2^n} X_i^2 - aX_0^2$ with $a \in (\Sigma F^2)^\times$, which are in particular Pfister neighbors. Due to the direct link of such forms to Galois cohomology classes, a local-global principle for such forms may be easier to establish than for the corresponding quadratic forms of dimension $2^n + 2$. As a matter of fact, function fields in one variable $F/\mathbb{Q}$ provide an example where a local-global criterion for sums of 4 squares in F is available (see Theorem 4.2.3), while a similar local-global criterion for being a sum of 5 squares is not known. Our method is elementary, up to the local-global ingredient.

7.1 Square-effective rings

Let F denote a field of characteristic different from 2. Our method for obtaining the bound $p(F) \leqslant 2^n + 1$ for $n \in \mathbb{N}$ depends on the presence of a certain subring $\mathcal{H}$ of F that provides a characterisation of $\Sigma_{2^n} F^2$. In this section we discuss which properties are required by such a ring.

Let $\mathcal{H}$ be a subring of F having F as its field of fractions. We set

$$p^*(\mathcal{H}) = \mathsf{inf}\{k \in \mathbb{N} \mid \mathcal{H}^\times \cap \Sigma F^2 \subseteq \Sigma_k F^2\} \in \mathbb{N} \cup \{\infty\}\,.$$

Note that if F is nonreal, then $-1 \in \mathcal{H}^\times \cap \Sigma F^2$, therefore $s(F) \leqslant p^*(\mathcal{H})$.

7.1.1 Proposition. *Assume that $\Sigma F^2 \subseteq F^2 \cdot ((1 + \Sigma F^2) \cap \mathsf{Jac}(\mathcal{H}))$. Then*

$$p(F) \leqslant p^*(\mathcal{H}) + 1\,.$$

Proof. We set $p = p^*(\mathcal{H})$. Consider $g \in \Sigma F^2$. By the hypothesis, there exist $c \in F$ and $f \in (1+\Sigma F^2) \cap \mathsf{Jac}(\mathcal{H})$ such that $g = c^2 f$. Since $f \in \mathsf{Jac}(\mathcal{H})$, we have $1-4f \in \mathcal{H}^\times$, and since $f \in 1+\Sigma F^2$, we have $4f-1 \in 3+4\,\Sigma F^2 \subseteq \Sigma F^2$. Hence $4f-1 \in \mathcal{H}^\times \cap \Sigma F^2 \subseteq \Sigma_p F^2$. We conclude that

$$g - (\tfrac{1}{2}c)^2 = (\tfrac{1}{2}c)^2(4f-1) \in \Sigma_p F^2\,,$$

whereby $g \in \Sigma_{p+1}F^2$. This shows that $\Sigma F^2 = \Sigma_{p+1}F^2$. □

We say that $\mathcal{H}$ is *square-effective* if, for every $f_1, f_2 \in F$, there exist $g_1, g_2 \in F$ such that $f_1^2+f_2^2 = g_1^2+g_2^2$ and $f_1\mathcal{H} + f_2\mathcal{H} = g_1\mathcal{H} \supseteq g_2\mathcal{H}$. Recall from Section 3.1 that a *Bézout domain* is a domain in which every finitely generated ideal is principal, and that Bézout domains are integrally closed.

7.1.2 Proposition. *Assume that $\mathcal{H}$ is square-effective. Let $k \in \mathbb{N}^+$. Then:*

(1) *$\mathcal{H}$ is a Bézout domain.*

(2) *For every $f_1,\dots,f_k \in F$, there exist $g_1,\dots,g_k \in F$ such that $f_1^2+\ldots+f_k^2 = g_1^2+\ldots+g_k^2$ and $f_1\mathcal{H}+\ldots+f_k\mathcal{H} = g_1\mathcal{H} \supseteq g_2\mathcal{H} \supseteq \cdots \supseteq g_k\mathcal{H}$.*

(3) *$\Sigma_k F^2 = F^2 \cdot (1+\Sigma_{k-1}\mathcal{H}^2)$.*

(4) *If $1+\Sigma_{k-1}\mathcal{H}^2 \subseteq \mathcal{H}^\times$, then $\mathcal{H} \cap \Sigma_k F^2 = \Sigma_k \mathcal{H}^2$.*

(5) *If $2 \in \mathcal{H}^\times$, then for every $\mathfrak{m} \in \mathsf{Max}(\mathcal{H})$, we have $\mathcal{H} \cap \Sigma_k F^2 \subseteq \Sigma_k\mathcal{H}^2 + \mathfrak{m}$.*

Proof. (1) Since $\mathcal{H}$ is square-effective, any ideal of $\mathcal{H}$ generated by two elements is principal. Therefore any finitely generated ideal of $\mathcal{H}$ is principal.

(2) We prove the statement by induction on k. For $k \leqslant 1$ there is nothing to show. Assume now that the statement holds for some $k \geqslant 1$. In order to prove the statement for $k+1$, we consider $f_0,\dots,f_k \in \mathcal{H}$. By the induction hypothesis, there exist $h_1,\dots,h_k \in F$ such that $f_1^2+\ldots+f_k^2 = h_1^2+\ldots+h_k^2$ and $f_1\mathcal{H}+\ldots+f_k\mathcal{H} = h_1\mathcal{H} \supseteq \cdots \supseteq h_k\mathcal{H}$. It follows that $f_0\mathcal{H}+\ldots+f_k\mathcal{H} = f_0\mathcal{H}+h_1\mathcal{H}$. As $\mathcal{H}$ is square-effective, we may choose $g_0, h \in F$ such that $f_0^2+h_1^2 = g_0^2+h^2$ and $f_0\mathcal{H}+h_1\mathcal{H} = g_0\mathcal{H} \supseteq h\mathcal{H}$. Then we have $f_0^2+\ldots+f_k^2 = g_0^2+h^2+h_2^2+\ldots+h_k^2$ and $f_0\mathcal{H}+\ldots+f_k\mathcal{H} = g_0\mathcal{H} \supseteq h\mathcal{H}+h_2\mathcal{H}+\ldots+h_k\mathcal{H}$. Again by the induction hypothesis, there exist $g_1,\dots,g_k \in F$ for which we have that $h^2+h_2^2+\ldots+h_k^2 = g_1^2+\ldots+g_k^2$ and $h\mathcal{H}+h_2\mathcal{H}+\ldots+h_k\mathcal{H} = g_1\mathcal{H} \supseteq g_2\mathcal{H} \supseteq \cdots \supseteq g_k\mathcal{H}$. We conclude that $f_0^2+\ldots+f_k^2 = g_0^2+\ldots+g_k^2$ and $f_0\mathcal{H}+\ldots+f_k\mathcal{H} = g_0\mathcal{H} \supseteq g_1\mathcal{H} \supseteq \cdots \supseteq g_k\mathcal{H}$.

(3) By (2), we have $\Sigma_k F^2 \subseteq F^2\cdot(1+\Sigma_{k-1}\mathcal{H}^2)$. The opposite inclusion holds trivially.

(4) Let $f \in \mathcal{H} \cap \Sigma_k F^2$. By (3), we obtain that $f = x^2 \cdot h$ for certain $x \in F$ and $h \in 1+\Sigma_{k-1}\mathcal{H}^2$. If $h \in \mathcal{H}^\times$, then since x is a root of $X^2 - fh^{-1}$ and $\mathcal{H}$ is integrally closed, we get that $x \in \mathcal{H}$, whereby $f \in \mathcal{H}^2 \cdot (1+\Sigma_{k-1}\mathcal{H}^2) \subseteq \Sigma_k\mathcal{H}^2$. Therefore, if $(1+\Sigma_{k-1}\mathcal{H}^2) \subseteq \mathcal{H}^\times$, then $\mathcal{H} \cap \Sigma_k F^2 = \Sigma_k\mathcal{H}^2$.

(5) Let $\mathfrak{m} \in \mathsf{Max}(\mathcal{H})$. Since $\mathcal{H}$ is square-effective, so is $\mathcal{H}_\mathfrak{m}$. Assume first $s(\mathcal{H}/\mathfrak{m}) \geqslant k$. Then $1+\Sigma_{k-1}\mathcal{H}_\mathfrak{m}^2 \subseteq \mathcal{H}_\mathfrak{m}^\times$, since $\mathcal{H}/\mathfrak{m} \simeq \mathcal{H}_\mathfrak{m}/\mathfrak{m}\mathcal{H}_\mathfrak{m}$. By Proposition 7.1.2 (4), we obtain $\mathcal{H}_\mathfrak{m} \cap \Sigma_k F^2 = \Sigma_k \mathcal{H}_\mathfrak{m}^2$. Again using that $\mathcal{H}/\mathfrak{m} \simeq \mathcal{H}_\mathfrak{m}/\mathfrak{m}\mathcal{H}_\mathfrak{m}$, we get $\mathcal{H} \cap \Sigma_k F^2 \subseteq \Sigma_k\mathcal{H}^2 + \mathfrak{m}$. Assume now that $k > s(\mathcal{H}/\mathfrak{m})$. Then $-1 \in \Sigma_{k-1}\mathcal{H}^2 + \mathfrak{m}$. Using this and the identity $x = \left(\frac{x+1}{2}\right)^2 + (-1)\left(\frac{x-1}{2}\right)^2$ for $x \in \mathcal{H}$, we conclude that $\mathcal{H} \subseteq \Sigma_k\mathcal{H}^2 + \mathfrak{m}$. □

7.1.3 Theorem. *Assume that $\mathcal{H}$ is square-effective and $(1+\Sigma F^2) \cap \mathsf{Jac}(\mathcal{H}) \neq \emptyset$. Then*

$$p(F) \leqslant p^*(\mathcal{H}) + 1\,.$$

Proof. Set $\mathsf{M}(\mathcal{H}) = (1 + \Sigma F^2) \cap \mathsf{Jac}(\mathcal{H})$. If $0 \in \mathsf{M}(\mathcal{H})$, then F is nonreal, and therefore $p(F) \leqslant s(F) + 1 \leqslant p^*(\mathcal{H}) + 1$. Assume now that $0 \notin \mathsf{M}(\mathcal{H})$. Since $\mathsf{M}(\mathcal{H}) \neq \emptyset$ by the hypothesis, we may fix an element $g \in \mathsf{M}(\mathcal{H})$. Then $g^2 \in F^{\times 2} \cap \mathsf{M}(\mathcal{H})$, whereby we find $F^2 = F^2 g^2 \subseteq F^2 \cdot \mathsf{M}(\mathcal{H})$. Since $\mathsf{M}(\mathcal{H}) \cdot (1 + \Sigma\mathcal{H}^2) \subseteq \mathsf{M}(\mathcal{H})$, we conclude that $F^2 \cdot (1+\Sigma\mathcal{H}^2) \subseteq F^2 \cdot \mathsf{M}(\mathcal{H}) \cdot (1+\Sigma\mathcal{H}^2) \subseteq F^2 \cdot \mathsf{M}(\mathcal{H})$. By Proposition 7.1.2 (3), we obtain that $\Sigma F^2 \subseteq F^2 \cdot (1+\Sigma\mathcal{H}^2) \subseteq F^2 \cdot \mathsf{M}(\mathcal{H})$. Now the statement follows from Proposition 7.1.1. □

We will mainly consider the condition that $\mathcal{H}$ is square-effective in combination with the condition that $1 + \mathcal{H}^2 \subseteq \mathcal{H}^\times$.

7.1.4 Lemma. *Assume that $1 + \mathcal{H}^2 \subseteq \mathcal{H}^\times$. Then $f^2 + g^2 \in \mathcal{H}^\times$ for every $f, g \in \mathcal{H}$ with $f\mathcal{H} + g\mathcal{H} = \mathcal{H}$.*

Proof. Consider $f, g \in \mathcal{H}$ such that $f^2+g^2 \notin \mathcal{H}^\times$. Then $f^2+g^2 \in \mathfrak{m}$ for some $\mathfrak{m} \in \mathsf{Max}(\mathcal{H})$. If $f \notin \mathfrak{m}$, then there exists $h \in \mathcal{H}$ such that $fh \equiv 1 \bmod \mathfrak{m}$, whereby we obtain that $1 + (gh)^2 \equiv h^2(f^2 + g^2) \equiv 0 \bmod \mathfrak{m}$, which contradicts the hypothesis that $1 + \mathcal{H}^2 \subseteq \mathcal{H}^\times$. Therefore $f \in \mathfrak{m}$, and similarly we obtain that $g \in \mathfrak{m}$. Hence $f\mathcal{H} + g\mathcal{H} \subseteq \mathfrak{m}$ and in particular $f\mathcal{H} + g\mathcal{H} \neq \mathcal{H}$. □

7.1.5 Proposition. *The following are equivalent:*

(*i*) *$\mathcal{H}$ is square-effective and $1 + \mathcal{H}^2 \subseteq \mathcal{H}^\times$.*

(*ii*) *$\mathcal{H}$ is a Bézout domain and $\mathcal{H}^\times \cap (\mathcal{H}^2 + \mathcal{H}^2) = \mathcal{H}^{\times 2}(1 + \mathcal{H}^2)$.*

Proof. ($i \Rightarrow ii$) Condition (i) evidently implies that $\mathcal{H}^{\times 2}(1 + \mathcal{H}^2) \subseteq \mathcal{H}^\times \cap (\mathcal{H}^2 + \mathcal{H}^2)$ and thus, by Proposition 7.1.2, that $\mathcal{H}$ is a Bézout domain. It remains to show that $\mathcal{H}^\times \cap (\mathcal{H}^2 + \mathcal{H}^2) \subseteq \mathcal{H}^{\times 2}(1 + \mathcal{H}^2)$. Consider $f \in \mathcal{H}^\times \cap (\mathcal{H}^2 + \mathcal{H}^2)$. Since $\mathcal{H}$ is square-effective, there exist $g_1, g_2 \in F$ such that $f = g_1^2 + g_2^2$ and $g_1\mathcal{H} \supseteq g_2\mathcal{H}$. We then have that $f = g_1^2(1 + (g_1^{-1}g_2)^2)$, and $g_1^{-1}g_2 \in \mathcal{H}$. Since $1 + \mathcal{H}^2 \subseteq \mathcal{H}^\times$, we have that $f \in g_1^2\mathcal{H}^\times \cap \mathcal{H}^\times$, whereby $g_1^2 \in \mathcal{H}^\times$. Since $\mathcal{H}$ is integrally closed, we conclude that $g_1 \in \mathcal{H}^\times$, whereby $f = g_1^2(1 + (g_1^{-1}g_2)^2) \in \mathcal{H}^{\times 2} \cdot (1 + \mathcal{H}^2)$.

($ii \Rightarrow i$) Assume that $\mathcal{H}$ is a Bézout domain and $\mathcal{H}^\times \cap (\mathcal{H}^2 + \mathcal{H}^2) = \mathcal{H}^{\times 2}(1 + \mathcal{H}^2)$. Then clearly $1+\mathcal{H}^2 \subseteq \mathcal{H}^\times$. It remains to show that $\mathcal{H}$ is square-effective. To this purpose, consider $f_1, f_2 \in F$, not both equal to zero. Since $\mathcal{H}$ is a Bézout domain and its fraction field is F, there exists $g \in F^\times$ such that $f_1\mathcal{H} + f_2\mathcal{H} = g\mathcal{H}$. Then $f_1g^{-1}, f_2g^{-1} \in \mathcal{H}$ and $\mathcal{H} = f_1g^{-1}\mathcal{H} + f_2g^{-1}\mathcal{H}$. Since $1 + \mathcal{H}^2 \subseteq \mathcal{H}^\times$, it follows by Lemma 7.1.4 that $f_1^2g^{-2} + f_2^2g^{-2} \in \mathcal{H}^\times$. Since $\mathcal{H}^\times \cap (\mathcal{H}^2 + \mathcal{H}^2) \subseteq \mathcal{H}^{\times 2}(1 + \mathcal{H}^2)$, we may choose $l_1 \in \mathcal{H}^\times$, $l_2 \in \mathcal{H}$ such that $f_1^2g^{-2} + f_2^2g^{-2} = l_1^2 + l_2^2$. Letting $g_1 = gl_1$ and $g_2 = gl_2$, we obtain that $f_1^2+f_2^2 = g_1^2+g_2^2$ and $f_1\mathcal{H}+f_2\mathcal{H} = g_1\mathcal{H} \supseteq g_2\mathcal{H}$. This shows that $\mathcal{H}$ is square-effective. □

7.1.6 Lemma. *Assume that $1 + \mathcal{H}^2 \subseteq \mathcal{H}^\times$. Let $\mathcal{M}$ be a finite subset of* $\mathsf{Max}(\mathcal{H})$ *and $f_1, f_2 \in \mathcal{H}$ such that $f_1^2 + f_2^2 \notin \bigcup\mathcal{M}$. Then there exist $g_1 \in \mathcal{H} \smallsetminus \bigcup\mathcal{M}$ and $g_2 \in \mathcal{H}$ such that $f_1^2 + f_2^2 = g_1^2 + g_2^2$.*

Proof. Consider $G_1 = (X^2 - 1)f_1 + 2Xf_2$ and $G_2 = 2Xf_1 + (1 - X^2)f_2$ in $\mathcal{H}[X]$ and observe that $G_1^2 + G_2^2 = (1 + X^2)^2 \cdot (f_1^2 + f_2^2)$. Consider $\mathfrak{m} \in \mathcal{M}$. Since $1 + \mathcal{H}^2 \subseteq \mathcal{H}^\times$, we have $\mathsf{char}(\mathcal{H}/\mathfrak{m}) \neq 2$, whereby $|\mathcal{H}/\mathfrak{m}| > 2$. Hence there exists $x_\mathfrak{m} \in \mathcal{H}$ such that $G_1(x_\mathfrak{m}) \notin \mathfrak{m}$. Since $\mathcal{M}$ is finite, by the Chinese Remainder Theorem, there exists $x \in \mathcal{H}$ with $x \equiv x_\mathfrak{m} \bmod \mathfrak{m}$ for all $\mathfrak{m} \in M$, whereby we find $G_1(x) \in \mathcal{H} \smallsetminus \bigcup\mathcal{M}$. We now set $g_i = (1 + x^2)^{-1}G_i(x)$ for $i = 1, 2$ to obtain the desired conclusion. □

7.1.7 Proposition. *Assume that $\mathcal{H}$ is semilocal and $1 + \mathcal{H}^2 \subseteq \mathcal{H}^\times$. Then*

$$\mathcal{H}^\times \cap (\mathcal{H}^2 + \mathcal{H}^2) = \mathcal{H}^{\times 2}(1 + \mathcal{H}^2)\,.$$

Proof. Let $f_1, f_2 \in \mathcal{H}$ with $f_1^2 + f_2^2 \in \mathcal{H}^\times$. We have $\mathcal{H} \smallsetminus \bigcup \mathsf{Max}(\mathcal{H}) = \mathcal{H}^\times$, and since by the hypothesis $\mathsf{Max}(\mathcal{H})$ is finite, we can apply Lemma 7.1.6 to choose $g_1 \in \mathcal{H}^\times$ and $g_2 \in \mathcal{H}$ such that $f_1^2 + f_2^2 = g_1^2 + g_2^2 = g_1^2(1 + (g_1^{-1}g_2)^2) \in \mathcal{H}^{\times 2} \cdot (1 + \mathcal{H}^2)$. This shows that $\mathcal{H}^\times \cap (\mathcal{H}^2 + \mathcal{H}^2) \subseteq \mathcal{H}^{\times 2} \cdot (1 + \mathcal{H}^2)$. The opposite inclusion is obvious, because $1 + \mathcal{H}^2 \subseteq \mathcal{H}^\times$. □

7.1.8 Corollary. *Assume that $\mathcal{H}$ is a semilocal Bézout domain with $1+\mathcal{H}^2 \subseteq \mathcal{H}^\times$. Then $\mathcal{H}$ is square-effective.*

Proof. This follows by Proposition 7.1.7 and Proposition 7.1.5. □

7.2 Semilocal Bézout rings

Let $n \in \mathbb{N}^+$ and let F be a field of characteristic different from 2. In this section we present a technique to search for a subring $\mathcal{H}$ of F satisfying the hypotheses of Corollary 7.1.8 and Theorem 7.1.3 and such that $p^*(\mathcal{H}) \leqslant 2^n$, so as to show that $p(F) \leqslant 2^n + 1$.

We call a semilocal Bézout domain $\mathcal{H}$ *square-effective of order n* if

$$1 + \Sigma_{2^n - 1}\mathcal{H}^2 \subseteq \mathcal{H}^\times \quad \text{and} \quad (1 + \Sigma_{2^n}\mathcal{H}^2) \cap \mathsf{Jac}(\mathcal{H}) \neq \emptyset\,.$$

By Corollary 7.1.8, the first of the two conditions implies that $\mathcal{H}$ is square-effective. We can reformulate each of the two conditions in terms of levels of residue fields.

7.2.1 Proposition. *Let $\mathcal{H}$ be a semilocal Bézout ring of F. Let $S \subseteq \Omega(F)$ be such that $\mathcal{H} = \mathcal{H}_S$. Then $\mathcal{H}$ is square-effective of order n if and only if the residue field of every $\mathcal{O} \in S$ has level n.*

Proof. Note that such S exists and is finite, by Proposition 3.1.8. Then the statement follows directly from Lemma 2.4.1. □

We say that F is *n-effective* if F has a semilocal Bézout ring that is square-effective of order n and such that $p^*(\mathcal{H}) \leqslant 2^n$.

7.2.2 Example. Note that F is square-effective of order n if and only if $s(F) = 2^n$. Therefore, if $s(F) = p(F) = 2^n$, then F is trivially n-effective.

7.2.3 Proposition. *Let $n \in \mathbb{N}^+$. If F is n-effective, then $2^n \leqslant p(F) \leqslant 2^n + 1$.*

Proof. Let $\mathcal{H}$ be a semilocal Bézout ring of F which is square-effective of order n and such that $p^*(\mathcal{H}) \leqslant 2^n$. Then we have $1+\mathcal{H}^2 \subseteq 1+\Sigma_{2^n-1}\mathcal{H}^2 \subseteq \mathcal{H}^\times$ and $(1+\Sigma_{2^n}\mathcal{H}^2)\cap\mathsf{Jac}(\mathcal{H}) \neq \emptyset$. Hence $p(F) \leqslant p^*(\mathcal{H}) + 1 \leqslant 2^n + 1$, by Theorem 7.1.3. If we had $\Sigma_{2^n}\mathcal{H}^2 \subseteq \Sigma_{2^n-1}\mathcal{H}^2$, then $1+\Sigma_{2^n}\mathcal{H}^2 \subseteq 1+\Sigma_{2^n-1}\mathcal{H}^2 \subseteq \mathcal{H}^\times$, which contradicts $(1+\Sigma_{2^n}\mathcal{H}^2)\cap\mathsf{Jac}(\mathcal{H}) \neq \emptyset$. Thus there exists $h \in \Sigma_{2^n}\mathcal{H}^2 \smallsetminus \Sigma_{2^n-1}\mathcal{H}^2$. By Proposition 7.1.2 (4), we have $\mathcal{H}\cap\Sigma_{2^n-1}F^2 = \Sigma_{2^n-1}\mathcal{H}^2$. Hence $h \notin \Sigma_{2^n-1}F^2$, whereby $p(F) \geqslant 2^n$. □

7.2.4 Corollary. *Let $n \in \mathbb{N}^+$. If F is nonreal and n-effective, then $s(F) = 2^n$.*

Proof. Assume that F is nonreal and n-effective. Then $s(F) \leqslant p(F) \leqslant s(F) + 1$, by Proposition 1.2.4, and $2^n \leqslant p(F) \leqslant 2^n + 1$, by Proposition 7.2.3. Since $s(F)$ is a 2-power and $n \geqslant 1$, the statement follows. □

Let $k \in \mathbb{N}^+$ and let $\mathcal{H}$ be a subring of F. We say that $\mathcal{H}$ *characterises sums of k squares in F* if

$$\left\{h \in \mathcal{H}^\times \cap \Sigma F^2 \mid h + \mathfrak{m} \in \Sigma_k(\mathcal{H}/\mathfrak{m})^2 \text{ for any } \mathfrak{m} \in \mathsf{Max}(\mathcal{H})\right\} \subseteq \Sigma_k F^2 .$$

This condition allows one to check whether a unit in $\mathcal{H}$ that is a sum of squares in F is a sum of k squares in F by inspecting residues modulo maximal ideals.

7.2.5 Example. Let $\mathcal{H}$ be a subring of F with fraction field F. Then for any $k \in \mathbb{N}^+$ with $p^*(\mathcal{H}) \leqslant k$, we have that $\mathcal{H}$ characterises sums of k squares in F.

7.2.6 Proposition. *Let $n \in \mathbb{N}^+$. Let R be a semilocal Bézout ring of F that characterises sums of 2^n squares in F. For every $\mathfrak{m} \in \mathsf{Max}(R)$, let $\mathcal{H}(\mathfrak{m})$ be a semilocal Bézout ring of $R/\mathfrak{m}$ that is square-effective of order n and such that $p^*(\mathcal{H}(\mathfrak{m})) \leqslant 2^n$. Then*

$$\mathcal{H} = \{f \in R \mid f + \mathfrak{m} \in \mathcal{H}(\mathfrak{m}) \textit{ for all } \mathfrak{m} \in \mathsf{Max}(R)\}$$

is a semilocal Bézout ring of F that is square-effective of order n, and $p^*(\mathcal{H}) \leqslant 2^n$.

Proof. Recall that

$$R = \bigcap_{\mathfrak{m} \in \mathsf{Max}(R)} R_{\mathfrak{m}}.$$

Similarly, for each $\mathfrak{m} \in \mathsf{Max}(R)$, we have

$$\mathcal{H}(\mathfrak{m}) = \bigcap_{\mathfrak{m}' \in \mathsf{Max}(\mathcal{H}(\mathfrak{m}))} \mathcal{H}(\mathfrak{m})_{\mathfrak{m}'} .$$

Fix $\mathfrak{m} \in \mathsf{Max}(R)$ and $\mathfrak{m}' \in \mathsf{Max}(\mathcal{H}(\mathfrak{m}))$. It follows by [Kap74, Theorem 107] that $R_{\mathfrak{m}}$ is a valuation ring of F with residue field $R/\mathfrak{m}$, and that $(\mathcal{H}(\mathfrak{m}))_{\mathfrak{m}'}$ is a valuation ring of $R/\mathfrak{m}$ with residue field $\mathcal{H}(\mathfrak{m})/\mathfrak{m}'$. Since $\mathcal{H}(\mathfrak{m})$ is square-effective of order n, we have that $s(\mathcal{H}(\mathfrak{m})/\mathfrak{m}') = 2^n$, by Proposition 7.2.1. Let $\pi_{\mathfrak{m}} : R_{\mathfrak{m}} \to R/\mathfrak{m}$ be the residue homomorphism of $R_{\mathfrak{m}}$. For a valuation ring $\mathcal{O}$ of $R/\mathfrak{m}$, we have that $\pi_{\mathfrak{m}}^{-1}(\mathcal{O})$ is a valuation ring of F having the same residue field as $\mathcal{O}$; see e.g. [EP05, p. 45]. Thus $\pi_{\mathfrak{m}}^{-1}(\mathcal{H}(\mathfrak{m}))$ is the intersection of finitely many valuation rings of F whose residue fields have level 2^n.

Since R is semilocal, we obtain that $\mathcal{H}$ is the intersection of finitely many valuation rings of F with residue field of level 2^n. Thus $\mathcal{H}$ is a semilocal Bézout ring of F, by Proposition 3.1.8, and it is square-effective of order n, by Proposition 7.2.1.

Let $f \in \mathcal{H}^\times \cap \Sigma F^2$. For every $\mathfrak{m} \in \mathsf{Max}(R)$, it follows by Proposition 7.1.2 (5) that $f + \mathfrak{m} \in \Sigma(R/\mathfrak{m})^2$. By definition of $\mathcal{H}$ we have that $f + \mathfrak{m} \in \mathcal{H}(\mathfrak{m})^\times \cap \Sigma(R/\mathfrak{m})^2$, and since $p^*(\mathcal{H}(\mathfrak{m})) \leqslant 2^n$ we obtain that $f + \mathfrak{m} \in \Sigma_{2^n}(R/\mathfrak{m})^2$. Since R characterises sums of 2^n squares in F, we find $f \in \Sigma_{2^n} F^2$. Thus $\mathcal{H}^\times \cap \Sigma F^2 \subseteq \Sigma_{2^n} F^2$, whereby $p^*(\mathcal{H}) \leqslant 2^n$. □

Let V be a set of valuations on F. We define

$$\mathcal{H}_V = \bigcap_{v \in V} \mathcal{O}_v .$$

For $k \in \mathbb{N}^+$, we say that V *characterises sums of k squares in F* if the ring $\mathcal{H}_V$ characterises sums of k squares in F.

7.2.7 Theorem. *Let $n \in \mathbb{N}^+$. If there exists a nonempty finite set V of valuations on F that characterises sums of 2^n squares in F and such that Fv is n-effective for every $v \in V$, then F is n-effective.*

Proof. Assume that V is such a set of valuations on F. Then $\mathcal{H}_V$ is a semilocal Bézout ring of F that characterises sums of 2^n squares in F. For every $v \in V$ we fix a semilocal Bézout ring $\mathcal{H}_v$ of Fv that is square-effective of order n. Set $R = \mathcal{H}_V$. For $\mathfrak{m} \in \mathsf{Max}(R)$, it follows by [Kap74, Theorem 107] that $\mathfrak{m} = \mathfrak{m}_v \cap R$ for some $v \in V$, and we set $\mathcal{H}(\mathfrak{m}) = \mathcal{H}_v$ for such a $v \in V$. In this setting, we obtain by Proposition 7.2.6 that the subring $\mathcal{H}$ constructed there is square-effective of order n and that $p^*(\mathcal{H}) \leqslant 2^n$. Hence F is n-effective. □

Recall from Section 2.1 that we denote by $\mathcal{V}_F$ the set of $\mathbb{Z}$-valuations on F.

7.2.8 Proposition. *Let $k \in \mathbb{N}$ with $k \geqslant 2$ and let V be a finite set of $\mathbb{Z}$-valuations on F such that $s(Fv) \geqslant k$ for all $v \in V$. Then V characterises sums of k squares if and only if $\Sigma_k F^2 = \Sigma F^2 \cap \bigcap_{v\in V} \Sigma_k F^{v2}$.*

Proof. Set $S = \{x \in \mathcal{H}_V^\times \cap \Sigma F^2 \mid x + \mathfrak{m}_v \in \Sigma_k (Fv)^2 \text{ for every } v \in V\}$ and

$$T = \Sigma F^2 \cap \bigcap_{v\in V} \Sigma_k F^{v2}.$$

Note that $\Sigma_k F^2 \subseteq T$. Hence we have to show that $S \subseteq \Sigma_k F^2$ if and only if $T \subseteq \Sigma_k F^2$. We claim that $T = F^2 \cdot S$. The statement then follows trivially from this equality.

Consider $v \in V$. Recall that v extends uniquely to a $\mathbb{Z}$-valuation $\widehat{v}$ on F^v with $F^v\widehat{v} = Fv$. We define $S_v = \{x \in \mathcal{O}_{\widehat{v}}^\times \cap \Sigma F^{v2} \mid x + \mathfrak{m}_{\widehat{v}} \in \Sigma_k(Fv)^2\}$. Since $s(Fv) \geqslant k \geqslant 2$, we obtain by Proposition 7.2.1 that $1 + \Sigma_{k-1}\mathcal{O}_{\widehat{v}}{}^2 \subseteq \mathcal{O}_{\widehat{v}}^\times$ and that $\widehat{v}(2) = 0$. It follows by Proposition 7.1.2 (3) and (5) that $\Sigma_k F^{v2} \subseteq F^{v2} S_v$. As F^v is henselian with respect to $\widehat{v}$ and $\widehat{v}(2) = 0$, we also have the converse inclusion. Hence $\Sigma_k F^{v2} = F^{v2} S_v$. This implies that $F^2(\Sigma F^2 \cap S_v) \subseteq \Sigma F^2 \cap \Sigma_k F^{v2}$. Using that $\widehat{v}F^v = vF$ and $F^v\widehat{v} = Fv$, we also obtain the opposite inclusion. Therefore we have $\Sigma F^2 \cap \Sigma_k F^{v2} = F^2(\Sigma F^2 \cap S_v)$. Hence

$$T = \bigcap_{v\in V} (\Sigma F^2 \cap \Sigma_k F^{v2}) = \bigcap_{v\in V} F^2(\Sigma F^2 \cap S_v).$$

Observe that $S = \Sigma F^2 \cap \bigcap_{v\in V} S_v \subseteq \bigcap_{v\in V} F^2(\Sigma F^2 \cap S_v) = T$. Hence it remains to be shown that $T \subseteq F^2 \cdot S$. To this purpose, consider $f \in T \smallsetminus \{0\}$. For every $v \in V$ we fix $g_v \in F$ and $h_v \in S_v$ such that $f = g_v^2 h_v$. Since V is a finite set of $\mathbb{Z}$-valuations on F, which are necessarily pairwise independent, we can apply the Approximation Theorem 2.1.9 to obtain an element $g \in F^\times$ such that $v(g - g_v) > v(g_v)$ for every $v \in V$. It follows that $f/g^2 \in \bigcap_{v\in V} S_v$. Hence $f \in F^2(\Sigma F^2 \cap \bigcap_{v\in V} S_v) = F^2 \cdot S$. □

We say that a class $\mathcal{C}$ of quadratic forms over F *satisfies the local-global principle with respect to $\mathcal{V}_F$* if, for every form $q \in \mathcal{C}$ that is isotropic over F^v for every $v \in \mathcal{V}_F$, q is isotropic over F.

7.2.9 Corollary. *Let $k \in \mathbb{N}$ with $k \geqslant 2$. Suppose that the quadratic forms over F of the shape $\Sigma_{i=1}^k X_i^2 - aX_0^2$ with $a \in F^\times$ over F satisfy the local-global principle with respect to $\mathcal{V}_F$ and that the set $V = \{v \in \mathcal{V}_F \mid p(F^v) > k\}$ is finite. Then V characterises sums of k squares in F.*

Proof. It follows from the hypotheses that

$$\Sigma_k F^2 = \Sigma F^2 \cap \bigcap_{v\in\mathcal{V}_F} \Sigma_k F^{v2} = \Sigma F^2 \cap \bigcap_{v\in V} \Sigma_k F^{v2}.$$

For any $v \in V$, we have $k < p(F^v) \leqslant s(Fv) + 1$, whereby $s(Fv) \geqslant k$. Hence the statement follows from Proposition 7.2.8. □

7.3 Function fields in one variable

The tools developed in the previous sections can be used to compute the Pythagoras numbers of certain function fields in one variable over $k(\!(t)\!)$ for some base fields k. Note that any field k is relatively algebraically closed in $k(\!(t)\!)$, and in particular any irreducible polynomial in $k[X]$ remains irreducible in $k(\!(t)\!)[X]$.

7.3.1 Proposition. *Let $n \in \mathbb{N}$. Let k be a real field such that $p(L) \leqslant 2^n$ for any finite field extension L/k. Let $h \in k[X]$ be irreducible and such that $h \in \Sigma k(X)^2 \smallsetminus \Sigma_{2^{n+1}-1} k(X)^2$. Then*

$$p\left(k(\!(t)\!)(X)\big(\sqrt{(tX-1)h}\big)\right) = 2^{n+1} + 1\,.$$

Proof. We set $K = k(\!(t)\!)$, $f = (tX-1)h \in K[X]$ and $F = K(X)(\sqrt{f})$. Let K' and k' denote the root fields of h over K and over k, respectively. Observe that K'/K and k'/k are finite extensions, and that the t-adic valuation on K extends to a $\mathbb{Z}$-valuation on K' with residue field k', and hence K' can be identified with $k'(\!(t)\!)$. In particular we obtain $K'^{\times} = (k'^{\times} \cup tk'^{\times}) \cdot K'^{\times 2}$. As $p(k') \leqslant 2^n$, it follows that $\Sigma K'^2 = K'^{\times 2}(\Sigma_{2^n} K'^2 \cup t\,\Sigma_{2^n} K'^2)$. In particular $|(\Sigma K'^2)^{\times}/(\Sigma_{2^n} K'^2)^{\times}| \leqslant 2$. Set $m = n+1$. By [BVG09, Theorem 3.10], we obtain that $|(\Sigma F^2)^{\times}/(\Sigma_{2^m} F^2)^{\times}| \leqslant 2$.

Consider the Gauss extension to $K(X)$ of the t-adic valuation on K with respect to the variable X, and denote by v an extension of this valuation to F. Note that $vK(X) = vK = \mathbb{Z}$ and that $K(X)v$ can be naturally identified with $k(X)$. Then $\overline{f}^{v} = -h$, whereby $Fv = k(X)(\sqrt{-h})$. As $-h \notin k(X)^2$, we have $[Fv : K(X)v] = 2 = [F : K(X)]$. By Corollary 2.2.7, it follows that $vF = vK(X) = vK = \mathbb{Z}$. Since $k(X)$ is real and $h \in \Sigma_{2^m} k(X)^2 \smallsetminus \Sigma_{2^m-1} k(X)^2$, we obtain by [Scha85, Theorem 4.4.3 (i)] that $s(Fv) = 2^m$. Since $vF = \mathbb{Z}$, it follows by Proposition 2.4.2 that $v(\Sigma_{2^m} F^2) \subseteq 2\mathbb{Z}$. As $tX \in \Sigma F^2$ and $v(tX) = 1$, we obtain that $p(F) > 2^m$ and $\mathcal{O}_v^{\times} \cap tX\,\Sigma_{2^m} F^2 = \emptyset$. Since $|\,\Sigma F^2/\,\Sigma_{2^m} F^2| \leqslant 2$, we conclude that $\Sigma F^2 = \Sigma_{2^m} F^2 \cup tX\,\Sigma_{2^m} F^2$ and $\Sigma F^2 \cap \mathcal{O}_v^{\times} = \Sigma_{2^n} F^2$. Hence $\mathcal{O}_v$ is a Bézout ring of F such that $p^*(\mathcal{O}_v) \leqslant 2^m$.

Since $s(Fv) = 2^m$, it follows by Proposition 7.2.1 that $\mathcal{O}_v$ is square-effective of order m. Hence F is m-effective, whereby $p(F) \leqslant 2^m + 1$, in view of Proposition 7.2.3. This proves that $p(F) = 2^m + 1$. □

7.3.2 Example. Let F denote the function field of the elliptic curve

$$Y^2 = (tX-1)(X^2+1)$$

over $\mathbb{R}(\!(t)\!)$. By applying Proposition 7.3.1 to $k = \mathbb{R}$ and $h = X^2+1$, we obtain a new argument that

$$p(F) = 3\,.$$

7.3.3 Remark. Let F as in Example 7.3.2. The observation that $3 \leqslant p(F) \leqslant 4$ goes back to [TVGY06, Example 3.10], and the equality $p(F) = 3$ to [BGVG14, Corollary 6.13]. The proof in [BGVG14] relies on a deep local-global principle from [CTPS12, Theorem 3.1], which is based on field patching and which uses further results from algebraic geometry, such as embedded resolutions of singularities. In Example 7.3.2, we have retrieved the equality $p(F) = 3$ from our new method and results from [BVG09]. This approach uses no algebraic geometry, and only Milnor's Exact Sequence for the rational function field $\mathbb{R}(\!(t)\!)(X)$ as a local-global ingredient (via the proof of [BVG09, Theorem 3.10]).

7.3.4 Example. As mentioned in the introduction, it was shown in [CEP71] that the polynomial $M(X,Y) = X^2Y^4 + X^4Y^2 - 3X^2Y^2 + 1 \in \mathbb{R}[X,Y]$ is a sum of 4 squares but not a sum of 3 squares in $\mathbb{R}(X,Y)$. We consider the field $K = \mathbb{R}(Y)(\!(t)\!)$. Then $M(X,Y) \in \Sigma_4 K(X)^2 \smallsetminus \Sigma_3 K(X)^2$. Furthermore, $M(X,Y)$ is irreducible in $\mathbb{R}(Y)[X]$, hence also in $K[X]$. We now consider the field

$$F = K(X)\left(\sqrt{(tX-1)M(X,Y)}\right).$$

By Proposition 7.3.1, we obtain that $p(F) = 5$.

7.3.5 Remark. Let F be as in Example 7.3.2. The observation that $p(F) \leqslant 5$ is not present in the literature, but could be obtained directly from the local-global principle in [CTPS12, Theorem 3.1]. In Example 7.3.4 we obtained the inequality using only Milnor's Exact Sequence for the rational function field $\mathbb{R}(Y)(\!(t)\!)(X)$ as a local-global ingredient (via the proof of [BVG09, Theorem 3.10]), thus by much more elementary means.

Note that Example 7.3.2 and Example 7.3.4 imply that the bounds in Proposition 7.3.7 and Corollary 7.3.10 are sharp for $n = 1$ and $n = 2$. After these examples of particular function fields in one variable, we now turn to consider base fields where our method gives us a bound on the Pythagoras numbers of all function fields in one variable.

Let $n \in \mathbb{N}$ and let K be a field. We call K a *$\mathcal{P}_n$-field* if $p(K(X)) \leqslant 2^{n+1}$ and if every function field in one variable F/K with $p(F) > 2^{n+1}$ is $(n+1)$-effective.

7.3.6 Example. If $p(E) \leqslant 2^{n+1}$ holds for every function field in one variable E/K, then K is a $\mathcal{P}_n$-field. This applies in particular to the following situations:

(*i*) To $K = \mathbb{R}(X_1, \dots, X_n)$, by [Pfi67, Theorem 1]; see also [Lam05, Theorem XI.4.10]. For $n = 0$ this result goes back to [Wi34].

(*ii*) More generally, if $K(\sqrt{-1})$ is a $\mathcal{C}_n$-field (that is, in terms of Tsen-Lang theory, if every homogeneous polynomial of degree $d \in \mathbb{N}^+$ in at least $d^n + 1$ variables has a nontrivial zero; see e.g. [Scha85, §2.15]). Indeed, this implies for any function field in one variable F/K that $F(\sqrt{-1})$ is a $\mathcal{C}_{n+1}$-field. In particular, every $(n+1)$-fold Pfister form over F represents all elements of $F(\sqrt{-1})$, whereby we obtain that $p(F) \leqslant 2^{n+1}$, by [Lam05, Corollary XI.4.9].

(*iii*) For $n \geqslant 2$ to $K = \mathbb{Q}(X_1, \dots, X_{n-1})$. This follows from [CTJ91, Theorem 4.1.2 (*c*)], which relies on two deep facts [CTJ91, Conjectures 2.1 and 2.5] proven later in [Jan16, Theorem 0.1] and [OVV07, Theorem 4.1].

The interest of the notion of $\mathcal{P}_n$-field lies in the following consequence.

7.3.7 Proposition. *Let $n \in \mathbb{N}$ and let K be a $\mathcal{P}_n$-field. Then $p(F) \leqslant 2^{n+1} + 1$ for every function field in one variable F/K.*

Proof. By Proposition 7.2.3, this follows from the definition of $\mathcal{P}_n$-field. □

We will now show for $n \in \mathbb{N}$ that the class of $\mathcal{P}_n$-fields is stable under passage from a field K to the formal power series field $K(\!(t)\!)$. To show this, we will use the methods developed in the previous sections.

A function field in one variable F/K is called *ruled* if there exist $\theta \in F$ and a finite field extension K'/K such that $F = K'(\theta)$, and *nonruled* otherwise.

7.3.8 Proposition. *Let $m \in \mathbb{N}^+$. Let K be a field such that $p(K(X)) \leqslant 2^m$. Let $F/K(\!(t)\!)$ be a function field in one variable and let $v \in \mathcal{V}_F$. Then $K \subseteq \mathcal{O}_v$, and if $p(F^v) > 2^m$, then Fv/K is a nonruled function field in one variable.*

Proof. If $K(\!(t)\!) \subseteq \mathcal{O}_v$, then $p(F^v) \leqslant p(K(X)) \leqslant 2^m$ by [BGVG14, Lemma 6.3]. Assume that $K(\!(t)\!) \nsubseteq \mathcal{O}_v$. Since v is a $\mathbb{Z}$-valuation, we obtain by [BGVG14, Proposition 2.2] that $\mathcal{O}_v \cap K(\!(t)\!) = K[\![t]\!]$. Hence $K \subseteq Fv$ and $K(\!(t)\!)v = K$. Since $p(K(X)) \leqslant 2^m$, it follows by [BGVG14, Corollary 4.13] that $p(L(X)) \leqslant 2^m$ holds for every finite field extension L/K, and hence also for every algebraic extension L/K.

Assume that Fv/K is algebraic. Then $p(Fv(X)) \leqslant 2^m$, and we conclude by using [BGVG14, Theorem 4.14] that $p(F^v(X)) \leqslant 2^m$. Thus $p(F^v) \leqslant 2^m$.

Consider now the case where Fv/K is transcendental. Then Fv/K is a function field in one variable, by Theorem 2.2.4. Suppose that Fv/K is ruled. Then $Fv = L(\theta)$ for a finite field extension L/K and some element $\theta \in Fv$ that is transcendental over K. Since $p(K(X)) \leqslant 2^m$, we get by [BGVG14, Corollary 4.13] that $p(Fv) = p(L(X)) \leqslant 2^m$. If Fv is real, then $p(F^v) = p(Fv) \leqslant 2^m$. If Fv is nonreal, then $s(F^v) = s(Fv) < 2^m$ by [BVG09, Theorem 3.5], and therefore $p(F^v) = s(F^v) + 1 \leqslant 2^m$. □

7.3.9 Theorem. *Let $n \in \mathbb{N}$. If K is a $\mathcal{P}_n$-field, then $K(\!(t)\!)$ is a $\mathcal{P}_n$-field.*

Proof. Let K be a $\mathcal{P}_n$-field. If $\mathsf{char}(K) = 2$, then $K(\!(t)\!)$ is trivially a $\mathcal{P}_n$-field. Assume now that $\mathsf{char}(K) \neq 2$. Since $p(K(X)) \leqslant 2^{n+1}$, we get by [BGVG14, Theorem 4.14] that $p(K(\!(t)\!)(X)) \leqslant 2^{n+1}$. Consider a function field in one variable $F/K(\!(t)\!)$ with $p(F) > 2^{n+1}$. Let $V = \{v \in \mathcal{V}_F \mid p(F^v) > 2^{n+1}\}$ and let

$$W = \{w \in \mathcal{V}_F \mid Fw/K \text{ nonruled function field in one variable}\}.$$

Then $V \subseteq W$, by Proposition 7.3.8, and W is finite, by [BGVG14, Corollary 3.9]. Therefore V is finite. By [CTPS12, Theorem 3.1], quadratic forms in at least 3 variables over F satisfy the local-global principle with respect to $\mathcal{V}_F$. Since $2^{n+1} + 1 \geqslant 3$, we conclude by Corollary 7.2.9 that V characterises sums of 2^{n+1} squares in F.

In particular, since $p(F) > 2^{n+1}$, we obtain that $V \neq \emptyset$. For every $v \in V$, the residue field Fv is $(n+1)$-effective by the hypothesis. Hence F is $(n+1)$-effective, by Theorem 7.2.7. This shows that $K(\!(t)\!)$ is a $\mathcal{P}_n$-field. □

We retrieve the following statement contained in [BGVG14, Theorem 6.13].

7.3.10 Corollary. *Let $n, r \in \mathbb{N}$. Let K be a field such that $p(E) \leqslant 2^{n+1}$ for every function field in one variable E/K. Let F be a function field in one variable over $K(\!(t_1)\!)\ldots(\!(t_r)\!)$. Then $p(F) \leqslant 2^{n+1} + 1$.*

Proof. It follows by Example 7.3.6, via an iterated application of Theorem 7.3.9, that $K(\!(t_1)\!)\ldots(\!(t_r)\!)$ is a $\mathcal{P}_n$-field. Hence F is 2^{n+1}-effective, and thus $p(F) \leqslant 2^{n+1} + 1$ by Proposition 7.2.3. □

7.4 Geometric global fields

For a domain R and $n \in \mathbb{N}$, we denote the ring of iterated formal power series by $R[\![t_1, \ldots, t_n]\!] = R[\![t_1]\!]\ldots[\![t_n]\!]$, and we set $R(\!(t_1, \ldots t_n)\!) = \mathsf{Frac}(R[\![t_1, \ldots t_n]\!])$. It was shown in [CDLR82, Corollary 5.14] that $p(\mathbb{R}(\!(t_1, t_2)\!)) = 2$. In [Hu15], Hu showed that that $p(\mathbb{R}(\!(t_1, t_2, t_3)\!)) = 4$, and that $p(F) \leqslant 3$ for every finite field extension F of $\mathbb{R}(\!(t_1, t_2)\!)$. In this section, we show that one can also obtain this bound by means of Proposition 7.2.3. To this aim, we study the discrete valuations on a finite field extension of the fraction field of a complete noetherian local domain. We will use standard notions of modern algebraic geometry and assume that the reader is familiar with basic scheme theory, for which our main reference will be [Liu06].

Let R be a commutative ring. By the *dimension of* R we refer to its Krull dimension and we denote it by $\dim R$. Assume now that R is a local ring. We denote by $\mathfrak{m}_R$ its unique maximal ideal and by κ_R the residue field $R/\mathfrak{m}_R$. Recall from Section 2.2 that R is *henselian* if for every monic polynomial $f \in R[X]$, any simple root of f in κ_R is the residue of a root of f in R. By Theorem 2.2.10, every complete local domain is henselian.

We will mostly focus on the case where R is 2-dimensional. We will show that in this case the fraction field of R has only finitely many discrete valuation rings whose residue field is a nonruled function field in one variable over κ_R.

7.4.1 Proposition. *Let $d \in \mathbb{N}^+$ and let R be a complete noetherian local domain with $\dim R = d$. Then there exist subrings $\mathcal{O} \subseteq R_0 \subseteq R$ such that $\mathcal{O}$ is a complete discrete valuation ring with residue field κ_R, $R_0 \simeq \mathcal{O}[\![t_1, \ldots, t_{d-1}]\!]$ and R is a finite R_0-algebra.*

Proof. By [Sta, Lemma 10.161.11], there exists a complete regular local domain R_0 such that R is a finite R_0-algebra and such that R_0 is either isomorphic to $\kappa_R[\![t_1, \ldots, t_d]\!]$ or to $\mathcal{O}[\![t_1, \ldots, t_{d-1}]\!]$ where $\mathcal{O}$ is a complete discrete valuation ring with residue field κ_R. In the first case, set $\mathcal{O} = \kappa_R[\![t_d]\!]$; then $\mathcal{O}$ is a complete discrete valuation ring with residue field κ_R. □

7.4.2 Lemma. *Let F be a field, R a henselian local subring of F and $\mathcal{O}$ a discrete valuation ring of F such that $R = \mathfrak{m}_R + R \cap \mathcal{O}$. Then $R \subseteq \mathcal{O}$.*

Proof. Since R is henselian, we have $1 + \mathfrak{m}_R \subseteq F^{\times n}$ for any $n \in \mathbb{N}$ coprime to $\mathsf{char}(\kappa_R)$. Since this holds for infinitely many natural numbers n and $\mathcal{O}$ is a discrete valuation ring, we conclude that $1 + \mathfrak{m}_R \subseteq \mathcal{O}^\times$. In particular $\mathfrak{m}_R \subseteq \mathcal{O}$. Hence $R = \mathfrak{m}_R + R \cap \mathcal{O} \subseteq \mathcal{O}$. □

Let F be a field. Given $v \in \mathcal{V}_F$ and a subring $R \subseteq F$, we say that *v is centred on R* if $R \subseteq \mathcal{O}_v$; in this case, for $\mathfrak{p} \in \mathsf{Spec}(R)$, we say that *$v$ is centred on R in* $\mathfrak{p}$ if $\mathfrak{m}_v \cap R = \mathfrak{p}$.

Assume now that F is the function field of an integral scheme $\mathcal{X}$. For $x \in \mathcal{X}$, we denote by $\mathcal{O}_{\mathcal{X},x}$ the stalk of $\mathcal{X}$ at x, by $\mathfrak{m}_x$ its maximal ideal, and we set $\kappa(x) = \mathcal{O}_{\mathcal{X},x}/\mathfrak{m}_x$. For $v \in \mathcal{V}_F$, we say that *v is centred on $\mathcal{X}$ in x* if $\mathcal{O}_{\mathcal{X},x} \subseteq \mathcal{O}_v$ and $\mathfrak{m}_v \cap \mathcal{O}_{\mathcal{X},x} = \mathfrak{m}_x$.

In the sequel let R be a complete regular local domain that is not a field. We denote by E the fraction field of R and we consider a finite field extension F/E.

7.4.3 Proposition. *Every $\mathbb{Z}$-valuation on F is centred on R in a nonzero prime ideal of R.*

Proof. Set $d = \dim R$. Since $d > 0$, it follows by Proposition 7.4.1 that there exist subrings $\mathcal{O} \subseteq R_0 \subseteq R$ such that R is a finite R_0-algebra, $\mathcal{O}$ is a complete discrete valuation ring and $R_0 \simeq \mathcal{O}[\![t_1, \ldots, t_{d-1}]\!]$. Let $K \subseteq F$ be the fraction field of $\mathcal{O}$. Since $\mathcal{O}$ is complete, we have that $\mathcal{O}$ is the unique discrete valuation ring of K; see [BGVG14, Proposition 2.2]. Let $v \in \mathcal{V}_F$. We have that $\mathcal{O}_v \cap K = K$ or $\mathcal{O}_v \cap K = \mathcal{O}$, so in any case $\mathcal{O} \subseteq \mathcal{O}_v$. Therefore

$$R_0 = \mathfrak{m}_{R_0} + \mathcal{O} \subseteq \mathfrak{m}_{R_0} + (R_0 \cap \mathcal{O}_v).$$

Since R_0 is complete and in particular henselian, we obtain by Lemma 7.4.2 that $R_0 \subseteq \mathcal{O}_v$. Since R is a finite R_0-algebra, and thus an integral extension of R_0, we obtain that $R \subseteq \mathcal{O}_v$. It follows that $\mathfrak{m}_v \cap R \in \mathsf{Spec}(R)$. Since F/E is a finite field extension, the restriction of v to E is nontrivial. As E is the fraction field of R, we conclude that $\mathfrak{m}_v \cap R \neq \{0\}$. □

In the sequel we will use some results from algebraic geometry, including resolution of singularities for surfaces [Lip75, p. 193], for which we need the following observation.

7.4.4 Remark. By [Sta, Proposition 15.52.3] a complete notherian local ring is excellent, and hence in particular universally catenary and a Nagata ring. Here, this applies for R as well as for the integral closure of R in F, which is again a complete noetherian local ring by [HS06, Theorem 4.3.4].

7.4.5 Proposition. *Assume that* $\dim(R) = 2$. *Let* $v \in \mathcal{V}_F$ *and let* $\mathfrak{p} = \mathfrak{m}_v \cap R$. *Then one of the following holds:*

(*i*) $\mathfrak{p}$ *is a principal ideal of height* 1 *of* R *and there exists a complete discrete valuation ring of* Fv *whose residue field is a finite field extension of* κ_R.

(*ii*) $\mathfrak{p} = \mathfrak{m}_R$ *and* Fv *is either an algebraic extension of* κ_R *or a function field in one variable over* κ_R.

Proof. In view of Proposition 7.4.3, we have $\{0\} \subsetneq \mathfrak{p} \subseteq \mathfrak{m}_R$. Since R is a regular local ring, it is a unique factorization domain, by [Liu06, Theorem 4.2.16]. Hence any height-1 prime ideal of R is principal.

Assume first that $\mathfrak{p} \neq \mathfrak{m}_R$. Since R is local and 2-dimensional, we obtain that $\mathfrak{p}$ is a principal ideal of height 1, $\mathcal{O}_v \cap E = R_{\mathfrak{p}}$ and $R/\mathfrak{p}$ is a 1-dimensional complete local domain with residue field κ_R. Since $\mathcal{O}_v \cap E = R_{\mathfrak{p}}$, we have $Ev \simeq \mathsf{Frac}(R/\mathfrak{p})$.

By Proposition 7.4.1, there exists a complete discrete valuation ring $\mathcal{O}$ with residue field κ_R that is a subring of $R/\mathfrak{p}$ and such that $R/\mathfrak{p}$ is a finite $\mathcal{O}$-algebra. Let K be the fraction field of $\mathcal{O}$. Then Ev/K is finite. Thus Fv/K is finite. By [OM73, Theorem 14:1], it follows that Fv has a complete discrete valuation ring $\mathcal{O}'$ such that $\mathcal{O}' \cap K = \mathcal{O}$, whose residue field is a finite extension of the residue field of $\mathcal{O}$, which is κ_R.

Assume now that $\mathfrak{p} = \mathfrak{m}_R$. As $\dim R = 2$, it follows by [Liu06, Theorem 8.3.26 (a)] that $\mathsf{tr\,deg}(Ev/\kappa_R) \leqslant 1$. Since the extension F/E is finite, we obtain that $\mathsf{tr\,deg}(Fv/\kappa_R) \leqslant 1$. If $\mathsf{tr\,deg}(Fv/\kappa_R) = 0$, then Fv/κ_R is algebraic. Assume that $\mathsf{tr\,deg}(Fv/\kappa_R) = 1$. Let S be the integral closure of R in F. In view of the properties of S that were pointed out in Remark 7.4.4, we obtain by [Liu06, Theorem 8.3.26 (b)] that there exists an integral scheme $\mathcal{X}$, a proper birational morphism $\mathcal{X} \to \mathsf{Spec}(S)$ and $x \in \mathcal{X}$ of codimension 1 such that $\mathcal{O}_v = \mathcal{O}_{\mathcal{X},x}$. Since any proper morphism is of finite type, $\mathcal{O}_{\mathcal{X},x}$ is a finitely generated S-algebra, and hence also a finitely generated R-algebra. Thus Fv/κ_R is a finitely generated extension. Hence Fv/κ_R is a function field in one variable. □

Let $\mathcal{X}$ be a scheme. A *model of* $\mathcal{X}$ is a scheme $\mathcal{X}'$ together with a birational proper morphism $\mathcal{X}' \to \mathcal{X}$. For $i \in \mathbb{N}$, we denote by $\mathcal{X}^{(i)}$ the set of points of $\mathcal{X}$ of codimension i.

7.4.6 Corollary. *Assume that* $\dim R = 2$. *Let S be the integral closure of R in F and let* $v \in \mathcal{V}_F$. *There exists a model* $\mathcal{X}$ *of* $\mathsf{Spec}(S)$ *on which v is centred in a point of* $\mathcal{X}^{(1)}$ *if and only if Fv is either a function field in one variable over* κ_R *or a complete discretely valued field whose residue field is a finite extension of* κ_R.

Proof. Set $\mathcal{X}_0 = \mathsf{Spec}(S)$ and $\mathfrak{p} = \mathfrak{m}_v \cap S$. Since S is integral over R, the height of $\mathfrak{p}$ in S is equal to the height of $\mathfrak{p} \cap R = \mathfrak{m}_v \cap R$ in R, and hence it follows by Proposition 7.4.5 that it is either 1 or 2. Hence $\mathfrak{p} \in \mathcal{X}_0^{(1)}$ or $\mathfrak{p} \in \mathcal{X}_0^{(2)}$.

Assume first that $\mathfrak{p} \in \mathcal{X}_0^{(1)}$. Then $\mathcal{X}_0$ itself is a model of $\mathsf{Spec}(S)$ such that v is centred in a point of $\mathcal{X}_0^{(1)}$, and by Proposition 7.4.5, Fv is a complete discretely valued field whose residue field is a finite extension of κ_R.

Assume now that $\mathfrak{p} \in \mathcal{X}_0^{(2)}$. Recall that E is the fraction field of R. We consider the chain of field extensions $\kappa_R \subseteq \kappa(\mathfrak{p}) \subseteq Ev \subseteq Fv$. Since S is an integral extension of R, $\kappa(\mathfrak{p})/\kappa_R$ is an algebraic extension. By [Liu06, Theorem 8.3.26 (*b*)], there exists a model $\mathcal{X}$ of $\mathcal{X}_0$ such that v is centred in a point of $\mathcal{X}^{(1)}$ if and only if the extension $Fv/\kappa(\mathfrak{p})$ is transcendental, that is, if and only if Fv/κ_R is transcendental. Assume that we are in this case. Since the extension F/E is finite, so is Fv/Ev. Hence Ev/κ_R is transcendental. It follows by Proposition 7.4.5 that Ev/κ_R is a function field in one variable. As the extension Fv/Ev is finite, we obtain that Fv/κ_R is a function field in one variable. □

Let $\mathcal{X}$ be a scheme. Given $x \in \mathcal{X}$, we denote by $V(x)$ the Zariski closure of $\{x\}$ in $\mathcal{X}$, considered with its reduced scheme structure induced by $\mathcal{X}$.

7.4.7 Proposition. *Assume that* $\dim R = 2$. *Let S be the integral closure of R in F and let $\mathcal{X}$ be a regular model of* $\mathsf{Spec}(S)$. *Let $v \in \mathcal{V}_F$ and let x be the centre of v on $\mathcal{X}$. Assume that $x \in \mathcal{X}^{(2)}$. If $Fv/\kappa(x)$ is transcendental, then Fv/κ_R is a ruled function field in one variable.*

Proof. In view of the properties of S mentioned in Remark 7.4.4 and since $Fv/\kappa(x)$ is transcendental, it follows by [Liu06, Theorem 8.3.26 (*b*)] that

$$\mathsf{tr\,deg}(Fv/\kappa(x)) = 1 = \dim \mathcal{O}_{\mathcal{X},x} - 1.$$

We set $\mathcal{X}_0 = \mathcal{X}$ and $x_0 = x$. For $i \in \mathbb{N}$ we define recursively $\pi_{i+1} : \mathcal{X}_{i+1} \to \mathcal{X}_i$ as the blowing up of $\mathcal{X}_i$ along the regular subscheme $V(x_i)$ and denote by x_{i+1} the centre of v on $\mathcal{X}_{i+1}$. By [Liu06, Theorem 8.1.19 (*a*) and Proposition 8.1.12 (*b*)], it follows for every $i \in \mathbb{N}$ that $\mathcal{X}_{i+1}$ is a regular model of $\mathcal{X}_i$, and hence of $\mathsf{Spec}(S)$. Furthermore, it follows by [Liu06, Exercise 8.3.14] that there exists $n \in \mathbb{N}^+$ such that $x_n \in \mathcal{X}_n^{(1)}$, $\mathcal{O}_v = \mathcal{O}_{\mathcal{X}_n,x_n}$ and $x_i \in \mathcal{X}_i^{(2)}$ for $0 \leqslant i < n$. In particular we have $Fv = \kappa(x_n)$ and, by [Liu06, Theorem 8.2.5], $\kappa(x_i)/\kappa_R$ is a finite extension for every $0 \leqslant i < n$. Since $x_n \in \mathcal{X}_n^{(1)}$ and since the exceptional fibre $\pi_{i+1}^{-1}x_i$ is an irreducible subscheme of $\mathcal{X}_{i+1}$ of dimension 1, we obtain by [Liu06, Theorem 8.1.19 (*b*)] that $V(x_n) \simeq \mathbb{P}^1_{\kappa(x_{n-1})}$, and we conclude that x_n is the generic point of $\pi_{i+1}^{-1}x_i$. Therefore $\kappa(x_n)/\kappa(x_{n-1})$ is a rational function field in one variable. Since $Fv = \kappa(x_n)$ and $\kappa(x_{n-1})/\kappa_R$ is a finite extension, we conclude that Fv/κ_R is a ruled function field in one variable. □

We obtain an analogue to [BGVG14, Theorem 5.3].

7.4.8 Proposition. *Suppose* $\dim R = 2$. *Then there exist only finitely many $\mathbb{Z}$-valuations on F whose residue fields are nonruled function fields in one variable over κ_R.*

Proof. Let S be the integral closure of R in F. Then S is excellent; see Remark 7.4.4. Hence, by [Lip75, p. 193], there exists a regular model $\eta : \mathcal{X} \to \mathsf{Spec}(S)$ of $\mathsf{Spec}(S)$. We denote by $\iota : \mathsf{Spec}(S) \to \mathsf{Spec}(R)$ the morphism of schemes corresponding to the inclusion $R \to S$. Denote by $\mathcal{X}_s$ the fibre of $\eta \circ \iota$ over $\mathfrak{m}_R$. Since η is birational, its image is dense in $\mathsf{Spec}(S)$, hence $\mathcal{X}_s$ has dimension at most 1. Since $\mathcal{X}_s$ is a closed subscheme of $\mathcal{X}$ of dimension at most 1, it has only finitely many irreducible components, and hence we conclude that $\mathcal{X}_s \cap \mathcal{X}^{(1)}$ is finite.

Consider now an arbitrary $v \in \mathcal{V}_F$ such that Fv/κ_R is a nonruled function field in one variable. We claim that $\mathcal{O}_v = \mathcal{O}_{\mathcal{X},x}$ for some $x \in \mathcal{X}_s \cap \mathcal{X}^{(1)}$. Since $\mathcal{X}_s \cap \mathcal{X}^{(1)}$ is finite, this will establish the statement.

Let $x \in \mathcal{X}$ be the centre of v on $\mathcal{X}$. Since Fv/κ_R is a function field in one variable, it follows by Proposition 7.4.5 that v is centred in $\mathfrak{m}_R$ on R, that is, $x \in \mathcal{X}_s$. Since Fv/κ_R

is a nonruled function field in one variable, it follows by Proposition 7.4.7 that $x \in \mathcal{X}^{(1)}$. Since $\mathcal{X}$ is regular, it follows that $\mathcal{O}_{\mathcal{X},x}$ is a discrete valuation ring of F. Since $\mathcal{O}_{\mathcal{X},x} \subseteq \mathcal{O}_v$, we obtain that $\mathcal{O}_{\mathcal{X},x} = \mathcal{O}_v$. □

7.4.9 Proposition. *Let $m \in \mathbb{N}^+$, let K be a field such that $p(K(X)) \leqslant 2^m$ and let $F/K(\!(t_1, t_2)\!)$ be a finite field extension. Set $V = \{v \in \mathcal{V}_F \mid p(F^v) > 2^m\}$. Then V is finite and, for every $v \in V$, we have that Fv/K is a nonruled function field in one variable.*

Proof. Recall from Section 4.1 that we set $p'(L) = \mathsf{min}\{p(L), s(L)+1\} \in \mathbb{N} \cup \{\infty\}$ for any field L. Consider a finite field extension L/K. By [BGVG14, Corollary 4.6], the hypothesis on K implies that $p(L(X)) \leqslant 2^m$. Moreover, if L is nonreal, then it follows by [BVG09, Theorem 3.5] that $s(L(X)) = s(L) < 2^m$. In any case $p'(L) \leqslant p'(L(X)) \leqslant 2^m$.

Consider $v \in \mathcal{V}_F$. Recall that $p(F^v) = p'(Fv)$. If Fv/K is either algebraic or a ruled function field in one variable, then $p(F^v) = p'(Fv) \leqslant 2^m$. If Fv carries a complete $\mathbb{Z}$-valuation w such that $(Fv)w/K$ is finite, then $p(F^v) = p'(Fv) = p'((Fv)w) \leqslant 2^m$.

In view of Proposition 7.4.5, this shows for every $v \in V$ that Fv/K is a nonruled function field in one variable. We conclude by Proposition 7.4.8 that V is finite. □

7.4.10 Theorem. *Let $n \in \mathbb{N}$, let K be a $\mathcal{P}_n$-field and let $F/K(\!(t_1, t_2)\!)$ be a finite field extension. Then*

$$p(F) \leqslant 2^{n+1} + 1\,.$$

Proof. We set $V = \{v \in \mathcal{V}_F \mid p(F^v) > 2^{n+1}\}$. Then V is finite, by Proposition 7.4.9. Let S the integral closure of $K[\![t_1, t_2]\!]$ in F. Recall that S is a 2-dimensional noetherian complete local ring by [HS06, Theorem 4.3.4], and that F is the fraction field of S. We may assume that $\mathsf{char}(F) = 0$, since otherwise we trivially have that $p(F) \leqslant 3 \leqslant 2^{n+1}+1$. Hence $\mathsf{char}(K) = 0$ and thus also the residue field of S has characteristic 0. It follows by [HHK15, Corollary 4.7] that quadratic forms in at least 3 variables satisfy the local-global principle with respect to $\mathcal{V}_F$. Since $2^{n+1} + 1 \geqslant 3$, we conclude by Corollary 7.2.9 that V characterises sums of 2^{n+1} squares F. In particular, if $V = \emptyset$, then $p(F) \leqslant 2^{n+1}$.

Assume $V \neq \emptyset$. Consider $v \in V$. By Proposition 7.4.9, Fv/K is a function field in one variable. If $p(Fv) > 2^{n+1}$, then Fv is $(n+1)$-effective, since K is a $\mathcal{P}_n$-field. Assume that $p(Fv) \leqslant 2^{n+1}$. Then, since $2^{n+1} < p(F^v) \leqslant p(Fv) + 1$, we have that $p(F^v) = 2^{n+1} + 1$ and $s(Fv) = p(Fv) = 2^{n+1}$. By Example 7.2.2, it follows that Fv is $(n+1)$-effective. Hence Fv is $(n+1)$-effective for every $v \in V$. We conclude by Theorem 7.2.7 that F is $(n+1)$-effective. In particular $p(F) \leqslant 2^{n+1} + 1$, by Proposition 7.2.3. □

7.4.11 Corollary. *Let $n \in \mathbb{N}$ be such that $p(E) \leqslant 2^{n+1}$ holds for every function field in one variable E/K. Let $r \in \mathbb{N}$ and let $F/K(\!(t_1)\!)\ldots(\!(t_r)\!)(\!(t_{r+1}, t_{r+2})\!)$ be a finite field extension. Then*

$$p(F) \leqslant 2^{n+1} + 1.$$

Proof. The hypothesis implies that K is a $\mathcal{P}_n$-field; see Example 7.3.6. By an iterated application of Theorem 7.3.9, we obtain that $K(\!(t_1)\!)\ldots(\!(t_r)\!)$ is a P_n-field as well. Hence $p(F) \leqslant 2^{n+1} + 1$, by Theorem 7.4.10. □

7.4.12 Remark. As mentioned in the introduction, for $K = \mathbb{R}$, $r = 0$ and $n = 0$, the bound in Corollary 7.4.11 gives an alternative proof of [Hu15, Theorem 5.1]. Corollary 7.4.11 also applies when K is an extension of transcendence degree n of $\mathbb{R}$ (or of transcendence degree $n - 1 \geqslant 1$ of $\mathbb{Q}$) and gives that $p(F) \leqslant 2^{n+1} + 1$ for any field F as in the statement. When $n \geqslant 2$, this is an improvement compared to the bound $p(F) < 2^{n+2}$, which one could derive from [Hu17, Corollary 4.7] by using [BVG09, Theorem 3.5]; this was first pointed out to us by Y. Hu.

7.4.13 Question. *Is* $\mathbb{R}((t_1, t_2))$ *a* $\mathcal{P}_1$*-field?*

Bibliography

[AMD69] M. F. Atiyah, I. G. MacDonald. *Introduction to commutative algebra.* Addison-Wesley-Longman, 1969.

[Ar27] E. Artin. Über die Zerlegung definiter Funktionen in Quadrate. *Abh. Math. Sem. Univ. Hamburg* 5 (1927), 100–115.

[AS27] E. Artin, O. Schreier. Algebraische Konstruktion reeller Körper. *Abh. Math. Sem. Univ. Hamburg* 5 (1927), 85–99.

[Ba78] R. Baeza. *Quadratic forms over semilocal rings.* Lecture Notes in Mathematics, Vol. 655. Springer-Verlag, Berlin-New York, 1978.

[Bec78] E. Becker. *Hereditarily-pythagorean fields and orderings of higher level.* Monografias de Matemática, Vol. 29. Instituto de matemática pura e aplicada, Rio de Janeiro, 1978.

[Bec82] E. Becker. The real holomorphy ring and sums of 2nth powers. *Real algebraic geometry and quadratic forms (Rennes, 1981),* Lecture Notes in Math. 959, Springer, Berlin-New York (1982), 139–181.

[BGVG14] K. J. Becher, D. Grimm, J. Van Geel. Sums of squares in algebraic function fields over a complete discretely valued field. *Pacific J. Math* 267 (2014), 257–276.

[BL11] K. J. Becher, D. B. Leep The length and other invariants of a real field. *Math. Z. 269* (2011), no.1-2, 235–252.

[BVG09] K. J. Becher, J. Van Geel. Sums of squares in function fields of hyperelliptic curves. *Math. Z.* 261 (2009), 829–844.

[Bo98] N. Bourbaki. *Commutative algebra. Chapters 1–7.* Translated from the French. Elements of Mathematics (Berlin). Springer-Verlag, 1998.

[Bri06] D. Brink. New light on Hensel's lemma. *Expo. Math.* 24 (2006), no. 4, 291–306.

[Cas64] J. W. S. Cassels. On the representation of rational functions as sums of squares. *Acta Arith.* 9 (1964), 79–82.

[CC86] A. Charnow, E. Charnow. Fields for which the principal axis theorem is valid. *Math. Mag. 59 (1986)*, no. 4, 222–225.

[CEP71] J. W. S. Cassels, W. J. Ellison, A. Pfister. On sums of squares and on elliptic curves over function fields. *J. Number Theory* 3 (1971), 125–149.

[CDLR82] M. D. Choi, Z. D. Dai, T. Y. Lam, B. Reznick. The Pythagoras number of some affine algebras and local algebras. *J. Reine Angew. Math.* 336 (1982), 45–82.

[CT86] J. L. Colliot-Thélène. Appendix to ”A Hasse principle for two-dimensional global fields” by K. Kato. *J. Reine Angew. Math.* 366 (1986), 181–183.

[CTJ91] J. L. Colliot-Thélène, U. Jannsen. Sommes de carrés dans les corps de fonctions. *C. R. Acad. Sci. Paris Sér. I Math.* 312 (1991), 759–762.

[CTPS12] J. L. Colliot-Thélène, R. Parimala, Suresh Venapally. Patching and local-global principles for homogenous spaces over function fields of p-adic curves. *Comment. Math. Helv.* 87 (2012), no 4, 1011–1033.

[De22] C. F. Degen. Adumbratio Demonstrationis Theorematis Arithmetici Maxime Universalis. *Mémoires de l'Académie Impériale des Sciences de St. Pétersbourg, pour les années 1817 et 1818* 8 (1822), 207–219.

[Ef06] I. Efrat. *Valuations, orderings, and Milnor K-theory.* Mathematical Surveys and Monographs, 124. American Mathematical Society, Providence, RI, 2006.

[ELP73] R. Elman, T. Y. Lam, A. Prestel. On some Hasse principles over formally real fields. *Math. Z.* 134 (1973), 291–301.

[EP05] A. J. Engler, A. Prestel. Valued Fields. Springer Monographs in Mathematics. *Springer-Verlag, Berlin,* 2005.

[Eu48] L. Euler. 1748. Extract of a letter from Mr. Leonhard Euler..., *Phil. Trans.* 44 (1748), 373-375.

[Eu51] L. Euler. Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum. *Novi Commentarii academiae scientiarum Petropolitanae 5* (1760), 13–58.

[FJ08] M. D. Fried; M. Jarden. *Field arithmetic. 3rd edition.* Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge 11. Springer, Berlin, 2008.

[Gi92] R. Gilmer. Multiplicative ideal theory. Corrected reprint of the 1972 edition. Queen's Papers in Pure and Applied Mathematics 90. *Queen's University, Kingston,* 1992.

[Ha23] H. Hasse. Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen. *J. Reine Angew. Math.* 152 (1923), 129–148.

[He81] T. Heath. *A history of Greek mathematics. Vol. II. From Aristarchus to Diophantus.* Corrected reprint of the 1921 original. Dover Publications, Inc. New York (1981).

[HHK15] D. Harbater, J. Hartmann, D. Krashen. Refinements to patching and applications to field invariants. *Amer. J. Math.* 137 (2015).

[Hi88] D. Hilbert. Ueber die Darstellung definiter Formen als Summe von Formenquadraten. *Math. Ann. 32* (1888), no. 3, 342–350.

[Hi02] D. Hilbert. Mathematical problems. *Bull. Amer. Math. Soc.* 8 (1902), no. 10, 437–479.

[HJ74] J. S. Hsia, R.P. Johnson. On the representation in sums of squares for definite functions in one variable over an algebraic number field. *Amer. J. Math.* 96 (1974).

[Ho99] D. W. Hoffmann. Pythagoras numbers of fields. *J. Amer. Math. Soc.* 12 (1999), 839–848.

[HS06] C. Huneke, I. Swanson. Integral closure of ideals, rings, and modules. London Mathematical Society Lecture Note Series 336. *Cambridge University Press, Cambridge,* 2006.

[Hu15] Y. Hu. The Pythagoras number and the u-invariant of Laurent series fields in several variables. *J. Algebra* 426 (2015), 243–258.

[Hu17] Y. Hu. A cohomological Hasse principle over two-dimensional local rings. *Int. Math. Res. Not. IMRN* (2017), 4369–4397.

[Hur22] A. Hurwitz. Über die Komposition der quadratischen Formen. *Math. Ann. 88* (1922), no. 1-2, 1–25.

[Hur98] A. Hurwitz. Über die Composition der quadratischen Formen von beliebig vielen Variabeln. *Goett. Nachr.* (1898) 309–316.

[Jac75] N. Jacobson. *Lectures in abstract algebra. III. Theory of fields and Galois theory.* Graduate Texts in Mathematics, No. 32. Springer-Verlag, New York-Heidelberg, 1975.

[Jac89] N. Jacobson. *Basic algebra II*, Second edition. W. H. Freeman and Company, New York, 1989.

[Jan16] U. Jannsen. Hasse principles for higher-dimensional fields. *Ann. of Math.* 183 (2016), 1–71.

[Kap74] I. Kaplansky. *Commutative rings.* Revised edition. University of Chicago Press, Chicago, Ill., London, 1974.

[Kat86] K. Kato. A Hasse principle for two-dimensional global fields. With an appendix by J.-L. Colliot-Thélène. *J. Reine Angew. Math.* 366 (1986), 142–183.

[Lag70] J. L. Lagrange, Démonstration d'un théorème d'arithmétique, Nouv. Mém. *Acad. Roy. Sc. de Berlin* (1770), 123–133.

[Lam05] T. Y. Lam. *Introduction to quadratic forms over fields.* Graduate Studies in Mathematics, Providence, RI, 2005.

[Lam81] T. Y. Lam. Orderings, Valuations and Quadratic Forms. Regional Conference Series in Mathematics No 52, *American Mathematical Society, Providence, RI* (1981).

[Lan02] S. Lang. Algebra. *Revised third edition.* Graduate Texts in Mathematics 211. *Springer-Verlag, New York,* 2002.

[Lip75] J. Lipman. Introduction to resolution of singularities. *Algebraic geometry (Proc. Sympos. Pure Math., Vol. 29, Humboldt State Univ., Arcata, Calif., 1974),* Amer. Math. Soc., Providence, RI (1975), 187–230.

[Liu06] Q. Liu. *Algebraic Geometry and Arithmetic Curves.* Translated from the French by Reinie Erné. Oxford Graduate Texts in Mathematics 6. Oxford Science Publications. *Oxford University Press,* Oxford, 2002.

[Mat86] H. Matsumura. *Commutative ring theory.* Translated from the Japanese by M. Reid. Second edition. Cambridge Studies in Advanced Mathematics 8. *Cambridge University Press,* Cambridge, 1989.

[Mo67] T. S. Motzkin. The arithmetic-geometric inequality. *Inequalities (Proc. Sympos. Wright-Patterson Air Force Base, Ohio, 1965)*, Academic Press (1967), 205–224.

[MS82] A. Merkurjev, A. Suslin K-cohomology of Severi-Brauer varieties and the norm residue homomorphism.*Izv. Akad. Nauk SSSR Ser. Mat.46* (1982), no.5, 1011–1046, 1135–1136.

[MSV93] M. Mornhinweg, D. Shapiro, K. G. Valente. The principal axis theorem over arbitrary fields. *Amer. Math. Monthly 100 (1993)*, no. 8, 749–754.

[Neug57] O. Neugebauer. *The exact sciences in antiquity.* 2nd. ed. Brown University Press, Providence, RI (1957).

[Neuk99] J. Neukirch. *Algebraic number theory.* Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] 322. Springer-Verlag, Berlin, 1999.

[OM73] T. O'Meara. *Introduction to quadratic forms.* Reprint of the 1973 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2000.

[OVV07] D. Orlov, A. Vishik, V. Voevodsky. An exact sequence for $K_*^M/2$ with applications to quadratic forms. *Ann. of Math.* 165 (2007), 1–13.

[PD01] A. Prestel, C. N. Delzell. *Positive polynomials.* From Hilbert's 17th problem to real algebra. Springer Monographs in Mathematics.

[Pfi65a] A. Pfister. Zur Darstellung von -1 als Summe von Quadraten in einem Körper. *J. London Math. Soc.* 40 (1965), 159–165.

[Pfi65b] A. Pfister. Multiplikative quadratische Formen. *Arch. Math. (Basel) 16* (1965), 363–370.

[Pfi67] A. Pfister. Zur Darstellung definiter Funktionen als Summe von Quadraten. *Invent. Math.* 4 (1967), 229–237.

[Pfi95] A. Pfister. Quadratic forms with applications to algebraic geometry and topology. London Mathematical Society Lecture Note Series 217. *Cambridge University Press*, Cambridge, 1995.

[Pol70] B. Pollak. Orthogonal groups over global fields of characteristic 2. *J. Algebra* 15 (1970), 589–595.

[Pop90] F. Pop. Summen von Quadraten in arithmetischen Funktionenkörpern (1990). *Preprint,* `https://www.math.upenn.edu/~pop/Research/files-Res/dimen1.ps`

[Pop23] F. Pop. On the Pythagoras number of function fields of curves over umber fields (2023). *Preprint,* `https://www2.math.upenn.edu/~pop/Research/files-Res/Oct-2022_Moshe-Vol-1.pdf`

[Pou71] Y. Pourchet. Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques. *Acta Arith.* 19 (1971), 89–104.

[Pre78] A. Prestel. Remarks on the Pythagoras and Hasse number of real fields. *J. Reine Angew. Math.* 303/304 (1978), 284–294.

[Pre84] A. Prestel. *Lectures on formally real fields.* Lecture Notes in Mathematics 1093. Springer-Verlag, Berlin, 1984.

[Ra22] J. Radon. Lineare Scharen orthogonaler Matrizen. *Abh. Math. Sem. Univ. Hamburg 1* (1922), no. 1, 1–14.

[Scha85] W. Scharlau. *Quadratic and Hermitian forms.* Grundlehren der mathematischen Wissenschaften 270. Springer-Verlag, Berlin, 1985.

[Sche10] C. Scheiderer. Hilbert's theorem on positive ternary quartics: a refined analysis. *J. Algebraic Geom. 19* (2010), no. 2, 285–333.

[Si21] C. Siegel. Darstellung total positiver Zahlen durch Quadrate. *Math. Z.* 11 (1921), no. 3-4, 246–275.

[Sp52] T. A. Springer. Sur les formes quadratiques d'indice zéro. *C. R. Acad. Sci. Paris* 234 (1952), 1517–1519.

[Sta] The Stacks project authors, *The Stacks project.* `https://stacks.math.columbia.edu` (2022).

[TVGY06] S. V. Tikhonov, J. Van Geel, V. I. Yanchevskiĭ. Pythagoras numbers of function fields of hyperelliptic curves with good reduction. *Manuscripta Math.* 119 (2006), 305–322.

[TI03] S. V. Tikhonov, V. I. Yanchevskiĭ. Pythagoras numbers of function fields of genus zero curves defined over hereditarily Pythagorean fields. *Proceedings of the International Conference on Mathematics and its Applications (ICMA 2004)*, 438–443, Kuwait Univ. Dep. Math. Comput. Sci., Kuwait (2005).

[Wa76] W. C. Waterhouse. Self-adjoint operators and formally real fields. *Duke Math. J. 43* (1976), no. 2, 237–243.

[Wi34] E. Witt. Zerlegung reeller algebraischer Funktionen in Quadrate. Schiefkörper über reellem Funktionenkörper. *J. Reine Angew. Math.* 171 (1934), 4–11.

[Wi37] E. Witt: Theorie der quadratischen Formen in beliebigen Korpern, *J. Reine Angew. Math. 176* (1937), 31-44.

[ZS60] O. Zariski, P. Samuel. *Commutative algebra.* Vol. II. Reprint of the 1960 edition. Graduate Texts in Mathematics 29. Springer-Verlag, New York-Heidelberg, 1975.

Index