UNIVERSIDAD DE SANTIAGO DE CHILE
FACULTAD DE CIENCIA
Departamento de Matemática y Ciencia de la Computación

UNIVERSITEIT ANTWERPEN
FACULTEIT WETENSCHAPPEN
Departement Wiskunde

Sums of squares and the Kaplansky radical of arithmetic function fields

Gonzalo Esteban Manzano Flores

Profesores Guías:
Dr. David Grimm,
Dr. Karim Johannes Becher

Tesis para optar al grado de
Doctor en Ciencia Mención Matemática.

Villa alemana - Chile
2023

Nederlandse samenvatting

Het doel van deze thesis is het bestuderen van niet-triviale oplossingen van zekere homogene polynomen van graad 2 in een lichaam K van karakteristiek verschillend van twee. De belangrijkste resultaten bevinden zich in hoofdstukken 4 en 5. In hoofdstuk 4 bestuderen we de verzameling van elementen $a \in K$ verschillend van nul zodat de veelterm $X^2 - aY^2 - bZ^2$ een niet-triviale oplossing over K heeft voor elke $b \in K$ verschillend van nul. Deze verzameling, die het Kaplanskysradicaal wordt genoemd, is in feite een deelgroep van de multiplicatieve groep van K met de eigenschap dat het de kwadraten verschillend van nul in K bevat en het in de groep van sommen van twee kwadraten in K wordt gevat. Een redelijke vraag is dus of we voorbeelden kunnen vinden waar het radicaal verschillend is van de groep van kwadraten. Een eerste voorbeeld werd opgesteld door C. Cordes en achteraf voorzag M. Kula een ander voorbeeld van zo een lichaam met de extra eigenschap dat de groep van klassen van kwadraten eindig is. In deze thesis tonen we voorbeelden van lichamen waarvan de quotiëntgroep van het Kaplanskysradicaal modulo de kwadraten eindig is, en waarvan de groep van klassen van kwadraten oneindig is.

In hoofdstuk 5 bestuderen we niet-triviale oplossingen in een lichaam K van veeltermen van de vorm $X_1^2 + \cdots + X_{n-1}^2 - \sigma X_n^2$ voor een $n \in \mathbb{N}$ en waar $\sigma \in K$. Het bestuderen van de oplossingen van dit soort veeltermen is equivalent aan het bestuderen of een element een som van een bepaalde eindige hoeveelheid van kwadraten is. Op zo een manier kunnen we, voor een willekeurig lichaam K, het kleinste positieve gehele getal n definiëren zodat elke som van kwadraten in K een som van n kwadraten is (als zo een geheel getal bestaat). Dit getal wordt het Pythagorasgetal genoemd en we stellen het voor door $p(K)$. Een open vraag is de volgende: Als $p(K)$ eindig is, is $p(K(X))$ dan ook eindig? We weten dat als er een $n \in \mathbb{N}$ bestaat zodat $p(L) < 2^n$ voor elke eindige reële extensie L van K, dan geldt $p(K(X)) \leq 2^n$. In het geval dat $n = 1$, wordt zo een lichaam K erfelijk Pythagorisch genoemd. Daardoor is het vinden van een uniforme bovengrens voor elk functielichaam in één variabele over een erfelijk Pythagorisch lichaam equivalent aan het vinden van een bovengrens voor $p(K(X,Y))$. In samenwerking met mijn promotoren en mijn collega's N. Daans en M. Zaninelli hebben we aangetoond dat $p(F) \leq 5$ voor elk functielichaam F in één variabele over een erfelijk Pythagorisch lichaam K, wat impliceert dat $p(K(X,Y)) \leq 2^3 = 8$. Nochtans is het geweten dat als F een kwadratische extensie is van $K(X)$, dan is $p(F) \leq 4$. Daarom is het logisch, als $2 < p(F) \leq 4$ voor zo een F, om de quotiëntgroep van sommen van vier kwadraten modulo sommen van twee kwadraten in F te bestuderen. Deze quotiëntgroep noemen we de tweede Pfisterindex van F. In deze thesis karakteriseren we de tweede Pfisterindex van F in termen van een verzameling van

valuatieringen van F wanneer K een erfelijk Pythagorisch lichaam $\mathbb{R}((t_1))\dots((t_n))$ is. Bovendien vinden we een bovengrens van de tweede Pfisterindex in functie van het genus van F/K en van n, en tevens bewijzen we dat deze bovengrens optimaal is.

Resumen

Esta tesis tiene como propósito estudiar soluciones no triviales de ciertos polinomios homogéneos de grado dos en un cuerpo K de característica diferente de dos. Los principales resultados obtenidos se encuentran en los capítulos 4 y 5. En el capítulo 4, estudiamos el conjunto de elementos no ceros $a \in K$ tales que el polinomio $X^2 - aY^2 - bZ^2$ tiene solución no trivial en K para todo $b \in K$ diferente de cero. Este conjunto es de hecho un subgrupo del grupo multiplicativo de K, llamado el Radical de Kaplansky de K, el cual tiene la propiedad de que contiene a los cuadrados no ceros de K y está contenido en el grupo de sumas de dos cuadrados de K. Es natural preguntarse si podemos encontrar ejemplos de cuerpos en donde el radical es diferente del grupo de cuadrados. Un primer tal ejemplo, fue construido por C. Cordes y luego M. Kula dio otro ejemplo de un tal cuerpo con la propiedad adicional que su grupo de clases de cuadrados es finito. En esta tesis, construimos ejemplos de cuerpos cuyos grupos cocientes del Radical de Kaplansky módulo los cuadrados es finito, y cuyos grupos de clases de cuadrados son infinitos.

En el capítulo 5 estudiamos soluciones no triviales en un cuerpo K de poliniomios de la forma $X_1^2 + \cdots + X_{n-1}^2 - \sigma X_n^2$, para algún $n \in \mathbb{N}$ y donde $\sigma \in K$. Estudiar la existencia de soluciones de este tipo de polinomios es equivalente a estudiar si un elemento $\sigma \in K$ es una suma de una cierta cantidad finita de cuadrados. De esta forma, para un cuerpo arbitrario K, uno puede definir el menor entero positivo n (si tal entero existe) tal que cada suma de cuadrados es una suma de n cuadrados en K, el cual es llamado el número de Pythagoras de K y lo denotamos por $p(K)$. Una pregunta aún abierta es la siguiente: Si $p(K)$ es finito ¿ Es $p(K(X))$ también finito ? Lo que sabemos es que si para toda extensión real finita L de K, existe un $n \in \mathbb{N}$ tal que $p(L) < 2^n$, entonces $p(K(X)) \leq 2^n$. En el caso donde $n = 1$, un tal cuerpo K se llama hereditariamente pitagórico. Así, encontrar una cota uniforme para todo cuerpo de funciones en una variable sobre un cuerpo hereditariamene pitagórico K, es equivalente a encontrar una cota para $p(K(X,Y))$. En un trabajo en conjunto con mis supervisores y mis colegas N. Daans, M. Zaninelli, demostramos que $p(F) \leq 5$ para todo cuerpo de funciones en una variable F sobre un cuerpo hereditariamente pitagórico K, lo que equivale a decir que $p(K(X,Y)) \leq 2^3 = 8$. Sin embargo, se sabe que si F es una extensión cuadrática de $K(X)$, entonces $p(F) \leq 4$. De esta forma, si $2 < p(F) \leq 4$ para un tal F, es natural estudiar el grupo cociente de sumas de cuatro cuadrados módulo sumas de dos cuadrados en F. A este grupo cociente lo llamamos el *segundo índice de Pfister de* F. Caracterizamos el segundo índice de Pfister de F en términos de ciertas valoraciones de F, cuando $K = \mathbb{R}((t_1))\ldots((t_n))$, y damos una cota optimal explícita en términos del género de F/K.

To Antu and Ingrid.

Acknowledgments

First of all, I would like to thank Ingrid for supporting me unconditionally throughout my Phd period. To my son Antu for giving me the energy to be able to finish this process in the best possible way. To my parents for always being there when I need them. To my family and Ingrid's family, I want to thank you for all the support you have given in these years.

I thank the people of the USACH and in particular my colleagues with whom we started this walk together. To all my mathematical and non-mathematical friends that I made during these years of study, either in Talca, Valparaíso or Quilpué. I also like to thank my friends and colleagues in Antwerp, especially thanks to N. Daans, M. Zaninelli, P. Gupta, K. Bingol, S. Veraa, J. Ramos and A. Mertens. Many of the results of my thesis originated in discussions with them.

I would like to thank all the people who made my stay in Europe welcoming, in particular E. Becker and Inge for the pleasant stays in Dortmund.

I would like to thank my thesis supervisors D. Grimm and K. Becher for the trust they always had in me, his good disposition at all times, his patience and selfless delivery in not only this thesis, but also in training me as a mathematician.

To Enrique Reyes and Cristóbal Rivas for helping me throughout the administrative process of the USACH.

I would also like to thank G. Lucchini, Y. Hu, D. Barrera and P. Yatsyna for agreeing to be reviewers of my thesis. I thank each of them so much for their time and diligent corrections and suggestions, which helped to improve this thesis.

Finally, I gratefully acknowledge financial support by: Agencia Nacional de Investigación y Desarrollo (ANID/National Doctorate/2017-21170477 and Fondecyt/11150956). Universidad de Santiago de Chile (Proyecto Dicyt/041933G). FWO Odysseus Program (project G0E6114N). University of Antwerp (Bijzonder Onderzoeksfonds (BOF), project BOFDOCPRO4, 2533).

Gonzalo Esteban Manzano Flores
Enero, 2023

Table of Contents

Introduction

The study of sums of squares in function fields goes back to Hilbert's 17^{th} problem of the list of 23 problems that guided a lot of mathematical research since 1900: Given $f \in \mathbb{R}[X_1, \dots, X_n]$ such that $f(x_1, \dots, x_n) \geq 0$ for all $x_1, \dots, x_n \in \mathbb{R}$, is f a sums of squares in $\mathbb{R}(X_1, \dots, X_n)$? Artin gave an affirmative answer to this question in 1927, and in 1967 Pfister gave a quantitive complement to this answer by showing that f is a sum of 2^n squares in $\mathbb{R}(X_1, \dots, X_n)$. Moreover, if f has coefficients in $\mathbb{Q}$, then f is a sum of 2^{n+1} squares in $\mathbb{Q}(X_1, \dots, X_n)$, when $n \geq 2$, and a sum of five squares when $n = 1$. The latter general bound was a long standing conjecture by Colliot-Thélène and Janssen, which was finally proven in 2016 by Janssen, and the latter bound for $n = 1$ was shown by Pourchét in 1971. These results motivated the definition of the Pythagoras number $p(K)$ of a field K as the least positive integer such that every sum of squares in K is a sum of $p(K)$ squares, together with the question how $p(K)$ relates to $p(K(X))$. This question is widely open for a field K in general, for example it is not even known whether $p(K) < \infty$ implies $p(K(X)) < \infty$. Note that an affirmative answer to this would in particular imply the finiteness of $p(K(X_1, \dots, X_n))$ for any field K with finite Pythagoras number. It is known however, that the finitess of $p(K(X))$ is equivalent to the existence of a uniform upper bound for the Pythagoras numbers of all finite extensions of K, see Theorem 2.3.10. Nevertheless, it is not clear whether $p(K(X, Y)) < \infty$ when there exists a uniform upper bound on the Pythagoras numbers of all finite extensions of K.

In Chapter 5 we will consider the case where K is hereditarily pythagorean, that is, K is real and $p(L) = 1$ for all finite real extensions L/K. In Section 5.1 we will show in Theorem 5.1.8 that $p(K(X, Y)) \leq 8$. More precisely, we will show the following result, which is part of a joint work with K. Becher, N. Daans, D. Grimm and M. Zaninelli.

Theorem 0.0.1 (Theorem 5.1.7)**.** *Let K be a hereditarily pythagorean field. Let F/K be a function field in one variable. Then $p(F) \leq 5$.*

In this thesis we set $\mathbb{N} = \{0, 1, 2, \dots\}$. We assume in the sequel that K is a hereditarily pythagorean field. Two crucial ingredients to prove Theorem A are, the existence of a henselian valuation v on K whose residue field has at most two field orderings, shown by L. Bröcker (Theorem 2.3.5), and on the other hand, a recent local-global principle by V. Mehmeti (Theorem 2.1.11) for quadratic forms over function fields in one variable over a field with a complete absolute value. It is not clear at the moment that this thesis is written whether 5 is the optimal uniform bound. In the case where the residue field of the aforementioned valuation v on K is uniquely ordered, we

get the improved bound $p(F) \leq 3$. In both cases, the proof is by reducing the general situation to the situation where K has at most two orderings. Since this property is stable under finite real extensions of K, we can bound the Pythagoras number of function fields over K (Section 2.3). In [62] it was shown for all function fields F/K of genus zero that $p(F) \leq 3$ if F is nonreal and $p(F) = 2$ if F is real. In [9] it was shown that $p(F) \leq 4$ for all hyperelliptic function fields F/K, and that moreover, the index of the multiplicative group of nonzero sums of two squares inside the group of nonzero sums of four squares in F, is finite in the case where the value group of the aforementioned henselian valuation v on K is of finite rank as a $\mathbb{Z}$-module. To simplify the wording, for a field L we denote by $\mathsf{S}_4(L)$ and $\mathsf{S}_2(L)$ the group of nonzero sums of 4 squares and the group of nonzero sums of 2 squares in L, respectively, and we call $|\mathsf{S}_4(L)/\mathsf{S}_2(L)|$ the *second Pfister index of* L. Under the additional hypothesis that the residue field of the valuation v on K is uniquely ordered we extend the aforementioned result from [9] on the finiteness of the second Pfister index to arbitrary function fields in one variable F/K, in Section 5.2. More precisely, we prove for the set $\mathcal{X}(F/v)$ of equivalence classes of valuations on F whose residue fields are nonreal and do not contain $\sqrt{-1}$, and moreover restrict to K as coarsenings of v, the following:

Theorem 0.0.2 (Theorem 5.2.5)**.** *Let $n \in \mathbb{N}$. Assume that K is a hereditarily pythagorean field carrying a henselian valuation with value group $(\mathbb{Z}^n, \leq_{\mathsf{lex}})$ and uniquely ordered residue field. Let F/K be a function field in one variable. Then*

$$|\mathsf{S}_4(F)/\mathsf{S}_2(F)| = 2^{|\mathcal{X}(F/v)|}.$$

To obtain the finiteness of $\mathsf{S}_4(F)/\mathsf{S}_2(F)$, it is enough to show that $2^{|\mathcal{X}(F/v)|}$ is an upper bound. The proof of this inequality uses an iterated application of a local-global principle for quadratic forms (Theorem 2.1.10) due to J.-L. Colliot-Thélène, R. Parimala and V. Suresh. This local-global principle is a discrete version of the more recently obtained local-global principle by V. Mehmeti, which we used to prove Theorem *A*. It is possible that the finiteness result can be also obtained in the non-discrete situation when we only require the so-called rational rank of v to be finite. However to obtain the reverse inequality $|\mathsf{S}_4(F)/\mathsf{S}_2(F)| \geq 2^{|\mathcal{X}(F/v)|}$, we use a variation of weak approximation due to P. Ribenboim (Theorem 1.5.1).

In the special case where $K = \mathbb{R}((t_1))\dots((t_n))$ the finiteness of $\mathsf{S}_4(F)/\mathsf{S}_2(F)$ was already shown in [4]. Moreover, if F/K is hyperelliptic of genus g, it follows from [9, Theorem 3.10] that $|\mathsf{S}_4(F)/\mathsf{S}_2(F)| \leq 2^{n(g+1)}$. In Section 5.3 we will show that this bound is optimal:

Theorem 0.0.3 (Theorem 5.3.8)**.** *Let $n, g \in \mathbb{N}$. Assume that K is a hereditarily pythagorean field carrying a henselian valuation v with value group $(\mathbb{Z}^n, \leq_{\mathsf{leq}})$ and uniquely ordered residue field. Let $f = -\prod_{i=0}^{g}(X^2 + t^{2i}) \in K[X]$, for some $t \in K$ such that $v(t) = (1, 0, \dots, 0) \in \mathbb{Z}^n$. Set $F = K(X)(\sqrt{f})$. Then g is the genus of F/K and*

$$|\mathsf{S}_4(F)/\mathsf{S}_2(F)| = 2^{n(g+1)}.$$

Observing that these examples are nonreal, we conjecture that for the second Pfister index of any function field to be $2^{n(g+1)}$, the function field has to be nonreal, and we show this in certain

cases in Section 5.4. In fact, we believe that, if the function field is real, then its second Pfister index is at most 2^{ng}. In the case where $g = 0$, this is true due to the previously mentioned result shown in [62] that any real function field of genus zero over any hereditarily pythagorean field has Pythagoras number 2, whereby its second Pfister index is trivial. We first extend this result to real quadratic twists of certain totally positive hyperelliptic function fields in Theorem 5.4.2 when K satisfies the hypothesis of Theorem B. Then we focus on the case $n = 1$ and give a precise description of all hyperelliptic function fields F/K of genus g with second Pfister index 2^{g+1} (Theorem 5.4.4). In particular we show that they are all nonreal. Finally we show that the latter is also true for non hyperelliptic function fields of genus g with second Pfister index 2^{g+1} (Theorem 5.4.5).

In Section 5.5 we stay in the situation where $n = 1$, that is, where K is the fraction field of a henselian discrete valuation ring T with uniquely ordered residue field. In [61] it was shown that any real function field of good reduction with respect to T has Pythagoras number 2. We use techniques from arithmetic geometry to relate the reduction type of a curve of genus one to the second Pfister index of its function field. We first focus on the case of elliptic curves, that is, curves of genus one with a rational point. In this case, the second Pfister index is bounded by 2, and since its function field is real, it is enough to characterize all the elliptic curves whose function fields have Pythagoras number 3. In fact, we show in Theorem 5.5.1 that all such elliptic curves have reduction type I_{2n} for some $n \in \mathbb{N}$, and we give a formula for a Weierstrass equation to obtain all elliptic function fields of Pythagoras number 3. We believe that this result can be extended to non-elliptic curves of genus one, that is, we conjecture that, if the function field is nonreal and its second Pfister index is 4, then the curve is of reduction type I_{2n} for some $n \in \mathbb{N}$. To support the conjecture, we consider the example of the curve $Y^2 = -(X^2+1)(X^2+t^2)$ over $\mathbb{R}((t))$ and we show that its function field has second Pfister index 4 and reduction type I_2 (Theorem 5.5.2). The fact that the second Pfister index is 4, was already shown in [9, Example 5.12] with different methods.

The reduction type of a curve over a discretely valued field is closely related to the notion of reduction graph. The latter is a combinatorial representation of the special fiber of an arithmetic surface over the valuation ring. At the end of Chapter 4 we relate the topology of the reduction graph of a regular model with the normal crossings property of a function field over a discretely valued field to the Kaplansky radical, which is the primary object of interest of all Chapter 4.

The *Kaplansky radical* $R(K)$ of a field K is defined as the subgroup of $K^\times$ whose elements are norms under every quadratic field extension of K. It is clear that $K^{\times 2} \subseteq R(K) \subseteq K^\times$, and for most natural fields one has that either $K^{\times 2} = R(K)$ or $R(K) = K^\times$. This group was first used implicitly by Kaplansky in [31] to study fields with a unique quaternion division algebra. In [12] C. Cordes introduced the name Kaplansky radical and constructed a first example of a field K such that $K^{\times 2} \subsetneqq R(K) \subsetneqq K^\times$. However in this example it was not clear whether the quotient $R(K)/K^{\times 2}$ was finite. We call $R(K)/K^{\times 2}$ the *radical square class group*. In [34] M. Kula gave another example of a field K as before which additionally has finite square class group and therefore in particular also finite radical square class group. In Section 4.4, for any $g \in \mathbb{N}$ we construct a field with infinite square class group and finite radical square class group of cardinality 2^g.

Theorem 0.0.4 (Theorem 4.4.6). *Let $g \in \mathbb{N}$. Let T be a complete discrete valuation ring with fraction K and such that -1 is not a square in the residue field. Let $f = \prod_{i=1}^{g+1}(X^2 + t^{2i}) \in K[X]$, for some uniformizer t of T. Then $F = K(X)(\sqrt{f})$ is a function field of genus g such that*

$$|R(F)/F^{\times 2}| = 2^g.$$

Observe that $F^\times/F^{\times 2}$ is infinite for the field F of Theorem D. The inequality $|R(F)/F^{\times 2}| \leq 2^g$ is shown in more generality (Theorem 4.4.3), based on the description of the failure of the local-global principle for squares in terms of the topology of the reduction graph of a regular model of F over T, due to D. Harbater, J. Hartmann and D. Krashen ([25, Theorem 9.6]). Our contribution is to relate the genus of F/K to the topology of this reduction graph (Section 3.2).

We also study the question whether the same bound holds under the weaker condition that the base field K is neither euclidean nor quadratically closed. Note that any discretely valued field falls in this category. When F/K is of genus zero, the bound from Theorem D predicts that $R(F) = F^{\times 2}$. We confirm this:

Theorem 0.0.5 (Theorem 4.3.1). *Let K be a field which is neither euclidean nor quadratically closed. Let F/K be a function field of genus zero. Then $R(F) = F^{\times 2}$.*

This generalizes the same result for the special case of the rational function field in [6, Proposition 3.4]. In Section 4.2 we consider the case of hyperelliptic function fields of genus $g \geq 1$, where we obtain a weaker bound compared to the bound from Theorem D.

Theorem 0.0.6 (Theorem 4.2.14). *Let $g \in \mathbb{N}$. Assume that K is neither euclidean nor quadratically closed. Let F/K be a hyperelliptic function field of genus g. Then*

$$|R(F)/F^{\times 2}| \leq 2^{2g+2}.$$

The basis for Theorems E and F is that, if K is neither euclidean nor quadratically closed, then $R(F)$ is contained in the group $\mathcal{L}(F)$ of local squares of F with respect to the K-trivial valuations on F (Theorem 4.1.2). If moreover K is complete with respect to a discrete valuation, we can describe $R(F)$ precisely as the group of local squares of F with respect to a larger set of valuations (Theorem 4.1.3). In the case where K is euclidean or quadratically closed this characterization of the Kaplansky radical in terms of local squares is not valid. Nevertheless the techniques for the previous case allow us to bound the group of local squares modulo squares.

Theorem 0.0.7 (Theorem 4.2.4). *Let K be a field and let $g \in \mathbb{N}$. Let F/K be a hyperelliptic function field of genus g. Then $|\mathcal{L}(F)/F^{\times 2}| \leq 2^{2g+1}$ in the case where K is quadratically closed, and $|\mathcal{L}(F)/F^{\times 2}| \leq 2^{2g+2}$ in the case where K is euclidean.*

In the special case where $K = \mathbb{C}$ we show that $|\mathcal{L}(F)/F^{\times 2}| = 2^{2g}$ for every hyperelliptic function field $F/\mathbb{C}$. This result could be reformulated in terms of the order of the 2-torsion part of the

Picard group of $F/\mathbb{C}$ (Theorem 4.2.8), which yields the same equality for an arbitrary function field of genus g over $\mathbb{C}$.

This summarizes the main results of the thesis which are all concentrated in Chapter 4 and Chapter 5. The purpose of the first three chapters is to prepare technical lemmas and preliminary results from underlying theories that are used as a tool in the final two chapters.

Chapter 1

Valuations and function fields

This chapter is introductory. Our main reference for valuation theory is [17] and for the theory of function fields is [59]. In Section 1.1 we recall the notion of valuations, extensions of valuations and dependent valuation rings. In Section 1.2 we treat the case of valuations having value group $\mathbb{Z}^n$ endowed with the lexicographic order. In Section 1.3 we study the theory of function fields in one variable and the notion of genus. In Section 1.4 we study residually transcendental valuations on function fields in one variable. In Section 1.5 we study Ribenboim's Approximation Theorem and we show an application of this.

1.1 Valuations and valuation rings

Let K be a field. An *ordered abelian group* is an additive abelian group Γ endowed with a total order such that, if $a \leq b$, then $a+c \leq b+c$, for all $a, b, c \in \Gamma$. Sometimes we write $(\Gamma, \leq)$ for an ordered abelian group to emphasize the order $\leq$ on Γ. A *valuation* v *on* K is a map $v : K \to \Gamma \cup \{\infty\}$, where Γ is an ordered abelian group, such that, for all $x, y \in K$, the following hold:

1. $v(x) = \infty$ if and only if $x = 0$,
2. $v(xy) = v(x) + v(y)$,
3. $v(x + y) \geq \min\{v(x), v(y)\}$.

Let $x, y \in K$. For a valuation v on K, one can easily verify that, if $v(x) \neq v(y)$, then

$$v(x + y) = \min\{v(x), v(y)\};$$

see for example [17, Pag. 20]. For a ring R, let $R^\times$ denote its group of invertible elements. A *valuation ring of* K is a subring $\mathcal{O} \subseteq K$ such that, for every $x \in K^\times$, we have $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$. A *valuation ring* is by definition a valuation ring of its fraction field. A valuation ring is an integral domain and a local ring; see [53, Proposition 2.1.1]. For a valuation ring $\mathcal{O}$, we denote by $\kappa_\mathcal{O}$ its residue field $\mathcal{O}/\mathfrak{m}$, where $\mathfrak{m}$ is the unique maximal ideal of $\mathcal{O}$, and we denote by $\Gamma_\mathcal{O}$ its value group $K^\times/\mathcal{O}^\times$. Let v be a valuation on K. Set

$$\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}.$$

Using the fact that $v(x^{-1}) = -v(x)$ for all $x \in K^\times$, one can easily verify that $\mathcal{O}_v$ is a valuation ring of K, and its maximal ideal, which we denote by $\mathfrak{m}_v$, is the set $\{x \in K^\times \mid v(x) > 0\}$. Set $\kappa_v = \kappa_{\mathcal{O}_v}$, and call this the *residue field of* v. We denote by Γ_v the value group $v(K^\times)$. Note that $\mathcal{O}_v^\times = \{x \in K^\times \mid v(x) = 0\}$. The residue in κ_v of an element $a \in \mathcal{O}_v$ will be denoted by $\overline{a}$. We call two valuations v and w on K *equivalent* if $\mathcal{O}_v = \mathcal{O}_w$. Two valuations v, w on K are equivalent if and only if there exists an isomorphism of ordered abelian groups $\gamma : \Gamma_w \to \Gamma_v$ such that $v = \gamma \circ w$; see [17, Proposition 2.1.3]. For a valuation ring $\mathcal{O}$ of K, we define

$$v_{\mathcal{O}} : K \longrightarrow K^\times/\mathcal{O}^\times \cup \{\infty\},$$
$$x \mapsto \begin{cases} x\mathcal{O}^\times, & \text{if } x \neq 0, \\ \infty & \text{if } x = 0, \end{cases}$$

where we consider $K^\times/\mathcal{O}^\times$ as an ordered abelian group, with respect to the ordering defined by setting $a\mathcal{O}^\times \leq b\mathcal{O}^\times$ whenever $b\mathcal{O} \subseteq a\mathcal{O}$, for $a, b \in K^\times$.

Proposition 1.1.1. *Let $\mathcal{O}$ be a valuation ring of K. Then $v_{\mathcal{O}}$ is a valuation on K such that $\mathcal{O}_{v_{\mathcal{O}}} = \mathcal{O}$.*

Proof. See [17, Proposition 2.1.2]. □

For a valuation ring $\mathcal{O}$ of K, we call $v_{\mathcal{O}}$ the *valuation on K associated to $\mathcal{O}$*. The value group of a valuation determines the arithmetic properties of the valuation ring. For example, if Γ_v is order-isomorphic to $\mathbb{Z}$, then $\mathcal{O}_v$ is a local principal ideal domain which is not a field; see [14, Theorem 16.2.7]. Given two ordered abelian groups $(G, \leq)$ and $(G', \leq')$, we can induce the product $G \times G'$ with the lexicographic order $\leq_{\mathsf{lex}}$, that is, for $g, h \in G, g', h' \in G'$, we have that $(g, g') \leq_{\mathsf{lex}} (h, h')$ if and only if, either $g < h$, or $g = h$ and $g' \leq' h'$. Similarly, we can define the lexicographic order $\leq_{\mathsf{lex}}$ on $\mathbb{Z}^n$, for some $n \in \mathbb{N}$ with $n \geq 2$. If Γ_v is order-isomorphic to $(\mathbb{Z}^n, \leq_{\mathsf{lex}})$, for some $n \in \mathbb{N}$, then $\mathcal{O}_v$ is a ring of Krull dimension n, which is noetherian only when $n \leq 1$; see Theorem 1.2.1.

A subgroup Δ of an ordered abelian group Γ is called *convex in* Γ if for each $\gamma \in \Gamma, \delta \in \Delta$ with $0 \leq \gamma \leq \delta$ we have $\gamma \in \Delta$. The *rank* of an ordered abelian group Γ is defined as the number of its proper convex subgroups, and we denote this number by $\mathsf{rk}(\Gamma)$. Note that the trivial group $\{0\}$ is the unique group with rank 0. Given a valuation v on K, we set $\mathsf{rk}(v) = \mathsf{rk}(\Gamma_v)$, and we call this the rank of v. We will apply terms defined for valuations also to valuation rings and vice versa when the translation is straightforward.

Proposition 1.1.2. *Let v be a rank-one valuation on K. Then Γ_v is order-isomorphic to a non-trivial subgroup of $(\mathbb{R}, +, 0, \leq)$ with the ordering induced by natural ordering on $\mathbb{R}$.*

Proof. See [17, Proposition 2.1.1]. □

For $n \in \mathbb{N}$, we denote by $\Omega_n(K)$ the set of valuation rings of K of rank n, and we denote by $\Omega(K)$

the set of valuation rings of K of finite rank, that is,

$$\Omega(K) = \bigcup_{i\in\mathbb{N}} \Omega_i(K).$$

Let Γ be an ordered abelian group and let Δ be a convex subgroup of Γ. For $\gamma, \gamma' \in \Gamma$, we set $\gamma+\Delta \leq \gamma'+\Delta$ if and only $\gamma \leq \gamma'$ or $\gamma+\Delta = \gamma'+\Delta$. In this way, we obtain an ordering on the quotient group Γ/Δ. Clearly, the set of convex subgroups of an ordered abelian group Γ is linearly ordered by the inclusion, and since there is a bijective correspondence between the convex subgroups of Γ/Δ and the convex subgroups of Γ that contain Δ, we have that

$$\mathsf{rk}(\Gamma/\Delta) = \mathsf{rk}(\Gamma) - \mathsf{rk}(\Delta),$$

whenever Γ has finite rank.

Given two valuation rings $\mathcal{O}, \mathcal{O}'$ of K, we say that $\mathcal{O}'$ is a *coarsening of* $\mathcal{O}$, or that $\mathcal{O}$ is a *refinement of* $\mathcal{O}'$, if $\mathcal{O} \subseteq \mathcal{O}'$.

Example 1.1.3. Let $\mathcal{O}$ be a valuation ring of K and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$. Since the localization $\mathcal{O}_\mathfrak{p}$ of $\mathcal{O}$ at $\mathfrak{p}$ is a valuation ring of K, we have that $\mathcal{O}_\mathfrak{p}$ is a coarsening of $\mathcal{O}$.

Proposition 1.1.4. *Let v be a valuation on K. There is an inclusion inverting bijection between the set of convex subgroups of Γ_v and the set of prime ideals of $\mathcal{O}_v$. Under this bijection, a convex subgroup Δ of Γ_v is mapped to the prime ideal $\mathfrak{p}_\Delta = \{x \in K \mid v(x) > \delta \text{ for every } \delta \in \Delta\}$, and a prime ideal $\mathfrak{p}$ of $\mathcal{O}_v$ is mapped to the convex subgroup $\Delta_\mathfrak{p} = \{\gamma \in \Gamma_v \mid \gamma, -\gamma < v(x) \text{ for every } x \in \mathfrak{p}\}$.*

Proof. See [17, Lemma 2.3.1]. □

Proposition 1.1.5. *Let $\mathcal{O}, \mathcal{O}'$ be two valuation rings of K such that $\mathcal{O}'$ is a coarsening of $\mathcal{O}$. Let $\mathfrak{m}$ and $\mathfrak{m}'$ be the maximal ideals of $\mathcal{O}$ and $\mathcal{O}'$ respectively. Then $\mathfrak{m}' \subseteq \mathfrak{m}$. Moreover $\mathcal{O}' = \mathcal{O}_{\mathfrak{m}'}$.*

Proof. Consider $x \in \mathfrak{m}' \setminus \{0\}$. Then $x^{-1} \notin \mathcal{O}'$. Since $\mathcal{O}'$ is a coarsening of $\mathcal{O}$, we have $x^{-1} \notin \mathcal{O}$, hence $x \in \mathfrak{m}$. Thus $\mathfrak{m}' \subseteq \mathfrak{m}$. In order to show that $\mathcal{O}' = \mathcal{O}_{\mathfrak{m}'}$, we need to show that any nonzero element $x \in \mathcal{O}'$ has the form $x = a/b$, for some $a \in \mathcal{O}$ and $b \in \mathcal{O}' \setminus \mathfrak{m}'$. If $x \in \mathcal{O}$, then $x = x/1 \in \mathcal{O}_{\mathfrak{m}'}$. We consider the case where $x \in \mathcal{O}' \setminus \mathcal{O}$. Hence $x^{-1} \in \mathcal{O} \subseteq \mathcal{O}'$, whereby x is invertible in $\mathcal{O}'$. Thus $x^{-1} \notin \mathfrak{m}'$, hence $x = 1/x^{-1} \in \mathcal{O}_{\mathfrak{m}'}$. □

Remark 1.1.6. Note that, given a valuation v on K, the correspondence in Theorem 1.1.4 also gives a bijection between convex subgroups of Γ_v and coarsenings of $\mathcal{O}_v$, by Theorem 1.1.5.

Lemma 1.1.7. *Let v, v' be valuations on K such that $\mathcal{O}_{v'}$ is a coarsening of $\mathcal{O}_v$. Then $\Gamma_{v'}$ is order-isomorphic to $\Gamma_v/\Delta_{\mathfrak{m}_{v'}}$.*

Proof. Without loss of generality, we may assume that $\Gamma_v = K^\times/\mathcal{O}_v^\times$ and $\Gamma_{v'} = K^\times/\mathcal{O}_{v'}^\times$. We observe that we have a surjective order-preserving group homomorphism $\psi : K^\times/\mathcal{O}_v^\times \to K^\times/\mathcal{O}_{v'}^\times$ sending $x\mathcal{O}_v^\times$ to $x\mathcal{O}_{v'}^\times$. Since $\mathcal{O}_v^\times \subseteq \mathcal{O}_{v'}^\times$, we have that $\ker(\psi) = \mathcal{O}_{v'}^\times/\mathcal{O}_v^\times$. We claim that $\mathcal{O}_{v'}^\times/\mathcal{O}_v^\times \subseteq \Delta_{\mathfrak{m}_{v'}}$. Let

$a \in \mathcal{O}_{v'}^\times$, and let $x \in \mathfrak{m}_{v'}$. Then $xa^{-1}, xa \in \mathfrak{m}_{v'}$. Since $\mathfrak{m}_{v'} \subseteq \mathfrak{m}_v$, we have that $xa^{-1}, xa \in \mathfrak{m}_v$, whereby $a\mathcal{O}_v^\times \in \Delta_{\mathfrak{m}_{v'}}$, because $x \in \mathfrak{m}_{v'}$ was arbitrarily chosen. Therefore $\mathcal{O}_{v'}^\times/\mathcal{O}_v^\times \subseteq \Delta_{\mathfrak{m}_{v'}}$. The other inclusion is clear by Theorem 1.1.6 and by Theorem 1.1.4. Therefore $\Gamma_{v'} \simeq \Gamma_v/\Delta_{\mathfrak{m}_{v'}}$ by the First Isomorphism Theorem. □

Let v be a valuation on K. We say that a valuation v' on K is a *coarsening of* v if there exists a surjective homomorphism of ordered abelian groups $\varphi : \Gamma_v \to \Gamma_{v'}$ such that $v' = \varphi \circ v$. Note that, in this case $\ker(\varphi)$, will be always a convex subgroup of Γ_v.

Proposition 1.1.8. *Let v be a valuation on K and v' a coarsening of v. For $x \in \mathcal{O}_{v'}^\times$, the value $v(x)$ only depends on the residue $x + \mathfrak{m}_{v'}$ in $\kappa_{v'}$. In particular, v induces a valuation $\overline{v} : \kappa_{v'} \to \Delta_{\mathfrak{m}_{v'}} \cup \{\infty\}$ such that $\overline{v}(x + \mathfrak{m}_{v'}) = v(x)$ for all $x \in \mathcal{O}_{v'}^\times$.*

Proof. Let $x, y \in \mathcal{O}_{v'}$ be such that $x - y \in \mathfrak{m}_{v'}$ and $x, y \notin \mathfrak{m}_{v'}$. Since $\mathfrak{m}_{v'} \subseteq \mathfrak{m}_v$ by Theorem 1.1.5, and since y is invertible in $\mathcal{O}_{v'}$, we have that $x/y - 1 = (x - y)y^{-1} \in \mathfrak{m}_{v'} \subseteq \mathfrak{m}_v$, and hence $v(x) = v(y)$. Moreover, for all $a \in \mathcal{O}_v \setminus \mathfrak{m}_{v'}$ we have $v(a) \in \Delta_{\mathfrak{m}_{v'}}$, because $\Delta_{\mathfrak{m}_v'} = \mathcal{O}_{v'}^\times/\mathcal{O}_v^\times$. Hence $\overline{v}$ is a valuation on $\kappa_{v'}$. □

Let v be a valuation on K and v' a coarsening of v. The valuation $\overline{v}$ on $\kappa_{v'}$, defined in Theorem 1.1.8 is called the *residual valuation of v modulo v'*.

Proposition 1.1.9. *Let v be a valuation on K and v' a coarsening of v. Let $\overline{v}$ be the residual valuation of v modulo v'. Then $\kappa_v = \kappa_{\overline{v}}$.*

Proof. Consider the residue homomorphism $\varphi : \mathcal{O}_{v'} \to \kappa_{v'}$. Since, for every $x \in \mathcal{O}_v \setminus \mathfrak{m}_{v'}$ we have $x \in \mathcal{O}_{v'}^\times$, we obtain that $\varphi(\mathcal{O}_v) = \mathcal{O}_v/\mathfrak{m}_{v'} = \mathcal{O}_{\overline{v}}$. In particular, we have that $\kappa_{\overline{v}} = \mathcal{O}_{\overline{v}}/\mathfrak{m}_{\overline{v}} = (\mathcal{O}_v/\mathfrak{m}_{v'})/(\mathfrak{m}_v/\mathfrak{m}_{v'}) = \kappa_v$. □

Proposition 1.1.10. *Let v' be a valuation on K and w a valuation on $\kappa_{v'}$. Let $\varphi : \mathcal{O}_{v'} \to \kappa_{v'}$ be the residue homomorphism of v'. Let $\mathcal{O} = \varphi^{-1}(\mathcal{O}_w)$. Then $\mathcal{O}$ is a refinement of $\mathcal{O}_{v'}$.*

Proof. We clearly have that $\mathcal{O}$ is a subring of $\mathcal{O}_{v'}$. Let $x \in K^\times$ be such that $x \notin \mathcal{O}$. Then $\varphi(x) \notin \mathcal{O}_w$, and hence $\varphi(x^{-1}) \in \mathcal{O}_w$, whereby $x^{-1} \in \mathcal{O}$. This shows that $\mathcal{O}$ is a valuation ring of K. □

Let v' be a valuation on K and w a valuation on $\kappa_{v'}$. Let $\varphi : \mathcal{O}_{v'} \to \kappa_{v'}$, be the residue homomorphism of v'. Let $\mathcal{O} = \varphi^{-1}(\mathcal{O}_w)$. A valuation v on K corresponding to $\mathcal{O}$ is called a *composition of v' with w*.

Proposition 1.1.11. *Let $r, d \in \mathbb{N}$. Let v be a rank-$(d + r)$ valuation on K, and let v' be a rank-r coarsening of v. Let $\overline{v}$ be the residual valuation of v modulo v'. Then $\overline{v}$ is of rank d and any composition of v' with $\overline{v}$ has rank $r + d$.*

Proof. Since $\Gamma_{\overline{v}} = \Delta_{\mathfrak{m}_{v'}}$, it follows by Theorem 1.1.7 that $\overline{v}$ has rank d. Let ν a composition of v' with $\overline{v}$. Consider the order-preserving group homomorphism $\psi : K^\times/\mathcal{O}_\nu^\times \to K^\times/\mathcal{O}_{v'}$ given by $x\mathcal{O}_\nu \mapsto x\mathcal{O}_{v'}^\times$. Since $\ker(\psi) = \mathcal{O}_{v'}^\times/\mathcal{O}_\nu^\times = (\mathcal{O}_{v'}/\mathfrak{m}_{v'})^\times/(\mathcal{O}_\nu/\mathfrak{m}_{v'})^\times = \kappa_{v'}^\times/\mathcal{O}_{\overline{v}}^\times \simeq \Gamma_{\overline{v}}$, where the latter is an isomorphism of ordered abelian groups, we obtain that $\Gamma_\nu/\Gamma_{\overline{v}} \simeq \Gamma_{v'}$, whereby $\mathsf{rk}(\nu) = d + r$. □

Remark 1.1.12. Let $r, d \in \mathbb{N}$. Let v be a rank-r valuation on K. Theorem 1.1.11 gives a bijection between refinements of $\mathcal{O}_v$ of rank $d + r$ and valuation rings of κ_v of rank d. The valuations corresponding to one another under this bijections have the same residue fields, by Theorem 1.1.9.

Lemma 1.1.13. *Let v be a valuation on K and v' a coarsening of v. Let $\overline{v}$ be the residual valuation of v modulo v'. Let $a \in \mathcal{O}_v^\times K^{\times 2} \cap \mathcal{O}_{v'}^\times$. Then $\overline{a} \in \mathcal{O}_{\overline{v}}^\times \kappa_{v'}^{\times 2}$.*

Proof. There exists $c \in K^\times$ such that $ac^{-2} \in \mathcal{O}_v^\times$. Since $\mathcal{O}_v \subseteq \mathcal{O}_{v'}$, we have that $\mathcal{O}_v^\times \subseteq \mathcal{O}_{v'}^\times$. Hence $a/c^2 \in \mathcal{O}_{v'}^\times$, and thus $c \in \mathcal{O}_{v'}^\times$. Let $\varphi : \mathcal{O}_{v'} \to \kappa_{v'}$ be the residue homomorphism of v'. Since $\varphi(\mathcal{O}_v^\times) = \mathcal{O}_{\overline{v}}^\times$, we have that $\varphi(ac^{-2}) \in \mathcal{O}_{\overline{v}}^\times$. Therefore $\overline{a} \in \mathcal{O}_{\overline{v}}^\times \kappa_{v'}^{\times 2}$. □

Let L/K be a field extension. Let $\mathcal{O}$ be a valuation ring of K. We say that a valuation ring $\mathcal{O}'$ of L is an *extension of* $\mathcal{O}$ if $\mathcal{O}' \cap K = \mathcal{O}$. Let v be a valuation on a field K. We call the pair (K, v) a *valued field*. We call a valuation w on L an *extension of v to L* if $w|_K = v$, and we call $(L, w)/(K, v)$ *an extension of valued fields*. Note that if w is an extension of v, we have that $\kappa_v \subseteq \kappa_w, \mathfrak{m}_w \cap \mathcal{O}_v = \mathfrak{m}_v$, and $\mathcal{O}_w$ is an extension of $\mathcal{O}_v$. We call $e(w/v) = [w(L^\times) : v(K^\times)]$ the *ramification index* of the extension $(L, w)/(K, v)$. We say that w (resp. $\mathcal{O}_w$) is an *unramified* extension of v (resp. of $\mathcal{O}_v$) if $e(w/v) = 1$, that is, if $w(L^\times) = v(K^\times)$.

Proposition 1.1.14. *Let L/K be a field extension and w a valuation on L. Then there exists an intermediate extension $K \subseteq M \subseteq L$ such that $w|_M$ is unramified over $w|_K$, and such that M is maximal with this property.*

Proof. Let X be the set of intermediate extensions N between K and L, such that $w|_N$ is unramified over $w|_K$. This set is nonempty, as it contains K. Endowed with the partial ordering by inclusion, we observe that any totally ordered subset Y of X has as a supremum the field $\bigcup_{N \in Y} N$ in X. By Zorn's Lemma, we have thus that X contains a maximal element. □

We call a field M satisfying the statement of Theorem 1.1.14 *a maximal unramified subextension of L/K with respect to w*.

A valuation ring $\mathcal{O}$ of K is called *henselian* if it has a unique extension to any algebraic field extension of K. Let v be a valuation on K corresponding to $\mathcal{O}$. For $f \in \mathcal{O}_v[X]$, let ∂f denote the formal derivative of f and $\overline{f} \in \kappa_v[X]$ denote the image of f via the residue map $\mathcal{O}_v[X] \to \kappa_v[X]$. By [17, Theorem 4.1.3], $\mathcal{O}_v$ is henselian if and only if for each $f \in \mathcal{O}_v[X]$ and $a \in \mathcal{O}_v$ such that $\overline{f}(\overline{a}) = 0$ and $\partial\overline{f}(\overline{a}) \neq 0$, there exists $\alpha \in \mathcal{O}$ such that $f(\alpha) = 0$ and $\overline{\alpha} = \overline{a}$. We say that a valuation v on K is *henselian* if $\mathcal{O}_v$ is henselian. Note that a field is always a henselian valuation ring.

The following example is inspired from [22, Example 1.1.14].

Example 1.1.15. Let $K = \bigcup_{n=1}^{\infty} \mathbb{C}((t^{1/n}))$. This field is called the field of *Puiseux series in the variable* t over $\mathbb{C}$. Let v_t be the t-adic valuation on $\mathbb{C}((t))$. Since v_t is henselian and $K/\mathbb{C}((t))$ is algebraic, there exists a unique extension w of v to K, which is henselian. In this case $\Gamma_w = \mathbb{Q}$.

A valuation ring $\mathcal{O}$ such that $\Gamma_{v_\mathcal{O}} = \mathbb{Z}$ is called a *discrete valuation ring*. An element $t \in \mathcal{O}$ such that $v_\mathcal{O}(t) = 1$ is called a *uniformizer of* $\mathcal{O}$.

Lemma 1.1.16. *Let $\mathcal{O}$ be a henselian discrete valuation ring of K. Let t be a uniformizer of $\mathcal{O}$. Let $\alpha \in K^\times$. Then $\alpha \in K^{\times 2}$ if and only if $\alpha = t^{2n}u$, for some $n \in \mathbb{Z}, u \in K$ such that $v(u) = 0$ with $\overline{u} \in \kappa_\mathcal{O}^{\times 2}$.*

Proof. See [35, VI. Corollary 1.2]. □

Proposition 1.1.17. *Assume that $K^\times = K^{\times 2} \cup -K^{\times 2}$. Then K has no discrete valuation ring.*

Proof. By the sake of a contradiction, we assume that there exists a discrete valuation ring $\mathcal{O}$ of K. Let t be a uniformizer of $\mathcal{O}$. If $t \in K^{\times 2}$, then $v_\mathcal{O}(t) \in 2\mathbb{Z}$, contradiction. If $t \in -K^{\times 2}$, then $v_\mathcal{O}(t) \in 2\mathbb{Z}$, because $v(-1) = 0$, contradiction. Therefore K has no discrete valuation ring. □

Proposition 1.1.18. *Let v be a valuation on K and v' a coarsening of v. Let $\overline{v}$ be the residual valuation of v modulo v'. Then v is henselian if and only if v' and $\overline{v}$ are henselian.*

Proof. See [17, Corollary 4.1.4]. □

Let $\mathcal{O}_1, \mathcal{O}_2$ be two valuation rings of K. We denote by $\mathcal{O}_1\mathcal{O}_2$ the smallest subring of K containing $\mathcal{O}_1$ and $\mathcal{O}_2$. We observe that $\mathcal{O}_1\mathcal{O}_1$ is a valuation ring of K; see [17, Pag 43]. Indeed, if there exists $x \in K \setminus \mathcal{O}_1\mathcal{O}_2$, then $x \notin \mathcal{O}_1, \mathcal{O}_2$, and hence $x^{-1} \in \mathcal{O}_1, \mathcal{O}_2$, whereby $x^{-1} \in \mathcal{O}_1\mathcal{O}_2$. We call $\mathcal{O}_1$ and $\mathcal{O}_2$ *dependent* if $\mathcal{O}_1\mathcal{O}_2$ if is a proper subring of K, otherwise $\mathcal{O}_1$ and $\mathcal{O}_2$ are called *independent*.

Proposition 1.1.19. *Let $\mathcal{O}_1, \mathcal{O}_2$ be two distinct valuation rings of K of rank one. Then $\mathcal{O}_1$ and $\mathcal{O}_2$ are independent.*

Proof. This follows directly from the fact that rank-1 valuation rings are maximal proper subrings; see [17, Corollary 2.3.2]. □

Proposition 1.1.20. *Assume that K does not carry a henselian valuation with separably closed residue field. Let n be a positive integer. Let v be a henselian valuation of rank n on K. Then for $1 \leq i \leq n$, the rank-i coarsening of v is up to equivalence the unique henselian rank-i valuation on K.*

Proof. We prove the statement by induction on n. Assume $n = 1$. Then $\mathcal{O}_v$ is a henselian valuation ring of K of rank one. If there were another henselian rank-one valuation ring of K, it would be independent with $\mathcal{O}_v$, by Theorem 1.1.19. But, this would contradict [17, Theorem 4.4.1], since K

is not separably closed. Hence $\mathcal{O}_v$ is the unique rank-one henselian valuation ring of K. Assume now that $n > 1$. Let $\mathcal{O}'$ be a coarsening of $\mathcal{O}$ of rank $n-1$. We have that $\mathcal{O}'$ is a henselian valuation ring by Theorem 1.1.18. Let v, v' be two valuations corresponding to $\mathcal{O}$ and $\mathcal{O}'$ respectively. Since K is a field carrying a henselian valuation v' of rank $n-1$, it follows from the induction hypothesis that for every $1 \leq i \leq n-1$, there exists a unique henselian valuation ring of rank i. Let $\overline{v}$ be the residual valuation of v modulo v'. Then $\mathcal{O}_{\overline{v}}$ is a henselian valuation ring of rank 1 of $\kappa_{v'}$, by Theorem 1.1.18 and by Theorem 1.1.12. Since distinct rank one valuations are independent and $\kappa_{v'}$ is not separably closed, $\mathcal{O}_{\overline{v}}$ is the unique henselian valuation ring of $\kappa_{v'}$ of rank one. Since rank-one valuation rings of $\kappa_{v'}$ correspond bijectively to rank n valuation rings of K by Theorem 1.1.12, $\mathcal{O}_v$ is the unique henselian valuation of rank n of K. □

Let v be a valuation on K. We call v *nondyadic* if $v(2) = 0$. A valued field (K, v) is called *nondyadic* is v is nondyadic. The following result describes quadratic extensions of nondyadic valued fields.

Proposition 1.1.21. *Let $a \in K^\times \setminus K^{\times 2}$ and let $(K, v) \subseteq (K(\sqrt{a}), v')$ be an extension of nondyadic valued fields. If $v(a) \in 2\Gamma_v$, then the extension v'/v is unramified and $\kappa_{v'} = \kappa_v(\sqrt{\overline{u}})$ for any $u \in aK^{\times 2} \cap \mathcal{O}_v^\times$. If $v(a) \notin 2\Gamma_v$, then $[\Gamma_{v'} : \Gamma_v] = 2, \kappa_v = \kappa_{v'}$ and v' is the unique extension of v to $K(\sqrt{a})$.*

Proof. This follows from [17, Theorem 3.3.4, Fundamental Inequality]. See also [5, Corollary 2.2] for a proof. □

An *absolute value* $|\ |$ *on* K is a map $|\ | : K \to \mathbb{R}_{\geq 0}$ such that, for all $x, y \in K$, the following hold:

1. $|x| > 0$ for all $x \neq 0$, and $|0| = 0$,
2. $|xy| = |x| + |y|$,
3. $|x + y| \leq |x| + |y|$.

We say that an absolute value $|\ |$ on K is *non-archimdean* if $|x + y| \leq \max\{|x|, |y|\}$, for all $x, y \in K$. Let v be a rank-one valuation on K. Then Γ_v is order-isomorphic to a non-trivial subgroup of $\mathbb{R}$; see Theorem 1.1.2. Thus, one can define a non-archimedean absolute value by setting $|x|_v = e^{-v(x)}$, for $x \in K^\times$ and $|0| = 0$; see [52, 2.1.A]. Since an absolute value defines a metric on K, by [52, 1.5.K], we say that K is *complete with respect to* v if every Cauchy sequence from K with respect to the metric $|\ |_v$ converges to some element of K.

Let v be rank-one valuation on K. There exists a valued field extension $(K^v, \hat{v})$ of (K, v) such that K^v is complete with respect to $\hat{v}$. Note that, by [17, Corollary 1.3.2], $\hat{v}$ is a henselian valuation and, by [17, Theorem 1.3.4], $\hat{v}$ is an unramified extension of v with $\kappa_{\hat{v}} = \kappa_v$. Moreover, $(K^v, \hat{v})$ is unique up to isomorphism of valued fields, that is, if there exists another extension of valued fields $(L, w)/(K, v)$ such that L is complete with respect to w, then there exists an isomorphism $\varphi : K^v \to L$ such that $w \circ \varphi = \hat{v}$; see [17, Theorem 2.4.3]. Thus, we call $(K^v, \hat{v})$ *the completion of* (K, v).

Lemma 1.1.22. *Let $n \in \mathbb{N}$. Let v be a henselian valuation of rank n on K. Let v_1 be a coarsening of v of rank one, and let $(K^{v_1}, \hat{v}_1)$ be the completion of (K, v_1). Let v' be a composition of $\hat{v}_1$ with $\overline{v}$. Then v' is a henselian valuation on K^{v_1} of rank n such that $\mathcal{O}_{v'} \cap K = \mathcal{O}_v$ and $\kappa_{v'} = \kappa_v$.*

Proof. Let $\overline{v}$ be the residual valuation of v modulo v_1. We note that $\mathcal{O}_{v'} \cap K = \mathcal{O}_v$. Furthermore, since $\overline{v}$ and $\hat{v}_1$ are henselian valuations, by Theorem 1.1.18, we have that v' is a henselian valuation on K^{v_1}. Since v and v_1 are of rank n and 1, respectively, it follows by Theorem 1.1.11 that v' is of rank n. Moreover, it follows by Theorem 1.1.9 that $\kappa_{v'} = \kappa_v$. □

Let G be an ordered abelian group. Since G is abelian, it is naturally a $\mathbb{Z}$-module, and we may consider $G \otimes_{\mathbb{Z}} \mathbb{Q}$. We denote by $\mathsf{rr}(G)$ the dimension of $G \otimes_{\mathbb{Z}} \mathbb{Q}$ as a $\mathbb{Q}$-vector space. Note that $\mathsf{rr}(G) = \mathsf{rr}(H) + \mathsf{rr}(G/H)$ for any subgroup H of G and that $\mathsf{rk}(G) \leq \mathsf{rr}(G)$; see [17, Proposition 3.4.1].

For a field extension L/K, we denote by $\mathsf{trdeg}(L/K)$ the transcendence degree of L/K.

Theorem 1.1.23. *Let L/K be a field extension. Let v be a valuation on K of finite rank, and let w be an extension of v to L. Then*

$$\mathsf{rk}(\Gamma_w) \leq \mathsf{rk}(\Gamma_v) + \mathsf{trdeg}(L/K).$$

Proof. We have that $\mathsf{trdeg}(\kappa_w/\kappa_v) + \mathsf{dim}_{\mathbb{Q}}(\Gamma_w/\Gamma_v \otimes_{\mathbb{Z}} \mathbb{Q}) \leq \mathsf{trdeg}(L/K)$, by [17, Theorem 3.4.3]. Moreover, since $\mathsf{rk}(\Gamma_w) - \mathsf{rk}(\Gamma_v) \leq \mathsf{dim}_{\mathbb{Q}}(\Gamma_w/\Gamma_v \otimes_{\mathbb{Z}} \mathbb{Q})$ by [17, Proposition 3.4.1], we can conclude that $\mathsf{rk}(\Gamma_w) \leq \mathsf{rk}(\Gamma_v) + \mathsf{trdeg}(L/K)$. □

Proposition 1.1.24. *Let v be a valuation on K. Then there exists a unique extension w of v to the rational function field $K(X)$ such that $w(X) = 0$ and such that the residue $\overline{X} \in \kappa_w$ is transcendental over κ_v. Moreover, for $n \in \mathbb{N}$ and $a_0, \ldots, a_n \in K$ we have that*

$$w\left(\sum_{i=0}^{n} a_i X^i\right) = \min_{0 \leq i \leq n} \{v(a_i)\}.$$

In particular, we have that $\kappa_w = \kappa_v(\overline{X})$ and w is an unramified extension of v.

Proof. See [17, Corollary 2.2.2]. □

The extension w of a valuation v on K to $K(X)$ with the above properties is called the *Gauss extension of v to $K(X)$ with respect to X*.

The following Lemma will be used in the context of sums of squares in fields in Section 5.1. This helps to reduce a problem from the case of a valuation with infinite rank to a valuation of finite rank; see Theorem 5.1.6.

Lemma 1.1.25. *Let v be a henselian valuation on a field K. Let K_0 be a finitely generated field such that $K_0 \subseteq K$. Then there exists an intermediate extension $K_0 \subseteq K' \subseteq K$ such that $v|_{K'}$ is henselian of finite rank and $\kappa_{v|_{K'}} = \kappa_v$.*

Proof. Let $v_0 = v|_{K_0}$. By Theorem 1.1.14 there exists a maximal unramified subextension K_1 of K/K_0 with respect to v. Let $v_1 = v|_{K_1}$. We claim that $\kappa_v = \kappa_{v_1}$. Assume for the sake of a contradiction the existence of $x \in \mathcal{O}_v^\times$ such that $\overline{x} \in \kappa_v \setminus \kappa_{v_1}$. Consider first the case that $\bar{x}$ is transcendental over κ_{v_1}. In particular x is transcendental over K_1; see for example [17, Theorem 3.2.4]. Then, $v|_{K_1(x)}$ is the Gauss extension of v_1 to $K_1(x)$ with respect to x by Theorem 1.1.24, whereby it is unramified, which contradicts the fact that (K_1, v_1) is a maximal unramified extension. Consider now the case that $\overline{x}$ is algebraic over κ_{v_1}. Let $f \in \mathcal{O}_{v_1}[X]$ be a monic polynomial such that $\overline{f} \in \kappa_{v_1}[X]$ is the minimal polynomial of $\overline{x}$ over κ_{v_1}. Since v is henselian, there exists $y \in \mathcal{O}_v$ such that $f(y) = 0$ and $\overline{y} = \overline{x}$. Since $\overline{f}$ is irreducible, one sees easily that f is irreducible over K_1 (e.g. [17, Remark 4.1.2]). Since f is monic, f is the minimal polynomial of y. Hence $[K_1(y) : K_1] = \deg(\overline{f}) = [\kappa_{v_1}(\overline{x}) : \kappa_{v_1}]$ and $[\kappa_{v_1}(\overline{x}) : \kappa_{v_1}] > 1$, because $\overline{x} \notin \kappa_{v_1}$. It follows from [17, Theorem 3.3.4] that $e(v|_{K_1}/v_1)\deg(\overline{f}) \leq [K_1(y) : K_1]$. This implies that $(K_1(y), v|_{K_1(y)})$ is a proper unramified extension of (K_1, v_1), and hence of (K_0, v_0) contained in K. This contradicts the fact that (K_1, v_1) is a maximal unramified extension of (K_0, v_0). Therefore $\kappa_{v_1} = \kappa_v$. Since K_0 is a finitely generated field and $v_1|_{\mathbb{Q}}$ is either trivial or equivalent to a $\mathbb{Z}$-valuation on $\mathbb{Q}$, we conclude that $\mathsf{rk}(\Gamma_{v_1}) < \infty$, by Theorem 1.1.23. Let K' be the relative algebraic closure of K_1 in K and let $v' = v|_{K'}$. We claim that v' has finite rank. Since $\mathsf{trdeg}(K'/K_1) = 0$, we conclude by Theorem 1.1.23 that $\mathsf{rk}(\Gamma_{v'}) < \infty$, whence $\mathsf{rk}(\Gamma_{v'}) < \infty$. Finally, (K', v') is henselian, by [17, Corollary 4.1.5], and such that $\kappa_{v'} = \kappa_v$. □

1.2 Discrete valuations of finite rank

Let $n \in \mathbb{N}$. We call a valuation having value group $(\mathbb{Z}^n, \leq_{\mathsf{lex}})$ a $\mathbb{Z}^n$-*valuation*. Note that $(\mathbb{Z}^0, \leq_{\mathsf{lex}})$ is the trivial additive group. Let K be a field. We denote by $V_n(K)$ the set of $\mathbb{Z}^n$-valuations on K. We set

$$V(K) = \bigcup_{i \in \mathbb{N}} V_i(K).$$

Let $n, d \in \mathbb{N}$ with $d \leq n$. We denote by $\pi_d : \mathbb{Z}^n \to \mathbb{Z}^d$ the projection on the first d components. Note that π_d is a homomorphism of ordered abelian groups with respect to the lexicographic orders on $\mathbb{Z}^n$ and $\mathbb{Z}^d$. Dually, we denote by $\pi^d : \mathbb{Z}^n \to \mathbb{Z}^d$ the projection on the last d components of $\mathbb{Z}^n$. Note that π^d is a group homomorphism, but it is not order-preserving when $d < n$.

Let $v \in V(K)$ and set $n = \mathsf{rk}(v)$. For $1 \leq i \leq n$, we denote by e_i^n the n-tuple $(e_1, \ldots, e_n)$ such that

$$e_j = \begin{cases} 1 & \text{if } j = (n+1) - i \ , \\ 0 & \text{if } j \neq (n+1) - i \ . \end{cases}$$

Note that e_1^n is the minimal positive element of $\mathbb{Z}^n$. An n-tuple $(t_1, \ldots, t_n) \in K^n$ is called a *parametrical system of* v if $v(t_i) = e_i^n$ for all $1 \leq i \leq n$.

Proposition 1.2.1. *Let $v \in V(K)$ be a valuation and set $n = \mathsf{rk}(v)$. Then the Krull dimension of $\mathcal{O}_v$ is n, and $\mathfrak{m}_v$ is generated by any element $t \in K^\times$ with $v(t) = e_1^n$.*

Proof. It follows by [17, Lemma 2.3.1] that the Krull dimension of $\mathcal{O}_v$ is n. Let $(t_1,\dots,t_n)\in K^n$ be a parametrical system of v. Clearly $t_1\in\mathfrak{m}_v$. Let $a\in\mathfrak{m}_v$, and let $a_1,\dots,a_n\in\mathbb{Z}$ be such that $v(a)=(a_1,\dots,a_n)$. Then $at_1^{-a_1}\cdots t_n^{-a_n}\in\mathcal{O}_v^\times$. Let $u\in\mathcal{O}_v^\times$ be such that $a=t_1^{a_1}\cdots t_n^{a_n}u$. Since

$$(a_1,\dots,a_n-1)+e_1^n>0,$$

and e_1^r is the minimal positive element of $(\mathbb{Z}^n,\leq_{\mathsf{lex}})$, we have $(a_1,\dots,a_n-1)\geq(0,\dots,0)$, and hence $t_1^{a_1}\cdots t_n^{a_n-1}\in\mathcal{O}_v$. Thus a belongs to the ideal of $\mathcal{O}_v$ generated by t_1. This shows that $\mathfrak{m}_v=(t_1)$. □

Proposition 1.2.2. *Let $n,r\in\mathbb{N}$ with $r\leq n$. Let v be a $\mathbb{Z}^n$-valuation on K. Then $\pi_r\circ v$ is a $\mathbb{Z}^r$-valuation. Moreover, it is up to equivalence the unique rank-r coarsening of v.*

Proof. Since π_r is order-preserving, we have that $\pi_r\circ v\in V_r(K)$ and it is a coarsening of v. Now let v' be a rank-r coarsening of v. It follows by Theorem 1.1.7 that $(\Gamma_{v'},\leq)$ is order-isomorphic to $(\mathbb{Z}^r,\leq_{\mathsf{lex}})$. Using the fact that the convex subgroups of $\mathbb{Z}^n$ are linearly ordered by inclusion, we have that $\mathcal{O}_{v'}=\mathcal{O}_{\pi_r\circ v}$, by Theorem 1.1.6, that is, $\pi_r\circ v$ is equivalent to v'. □

In the case of valuations in $V(K)$, we can explicitly construct residual valuations and compositions of valuations. The latter depend on the choice of a parametrical system as follows.

Proposition 1.2.3. *Let $n,r\in\mathbb{N}$ with $r\leq n$. Let v be a $\mathbb{Z}^n$-valuation on K and set $v_r=\pi_r\circ v$. Then $\Delta_{\mathfrak{m}_{v_r}}=\{0\}^r\times\mathbb{Z}^{n-r}$ and the residual valuation $\overline{v}$ of v modulo v_r, is given by $\overline{v}(x+\mathfrak{m}_{v_r})=(\pi^{n-r}\circ v)(x)$.*

Proof. Since $\Delta_{\mathfrak{m}_{v_r}}$ is a convex subgroup of $\mathbb{Z}^n$ of rank r, we have that $\Delta_{\mathfrak{m}_{v_r}}=\{0\}^r\times\mathbb{Z}^{n-r}$. Let $x\in\mathcal{O}_{v_r}^\times$. Then there exist $a_{n-r},\dots,a_n\in\mathbb{Z}$ such that $v(x)=(0,\dots,0,a_{n-r},\dots,a_n)$. Thus, it follows by Theorem 1.1.8 that $\overline{v}(x+\mathfrak{m}_{v_r})=(a_{n-r},\dots,a_n)=(\pi^r\circ v)(x)$. □

Proposition 1.2.4. *Let $d\in\mathbb{N}$. Let v' be a $\mathbb{Z}^r$-valuation on K and let w be a $\mathbb{Z}^d$-valuation on $\kappa_{v'}$. Let $(t_1,\dots,t_n)\in K^r$ be a parametrical system of v'. The valuation $v:K\to\mathbb{Z}^r\times\mathbb{Z}^d\cup\{\infty\}$, given by $v(a)=(v'(a),w(\overline{u}))$, where $a=t_1^{a_1}\dots t_r^{a_r}u$ for some $u\in\mathcal{O}_{v'}^\times$, is a composition of v' with w.*

Proof. Clearly v is a $\mathbb{Z}^{r+d}$-valuation on K and v' is a coarsening of v, by Theorem 1.2.2. Let $x\in\mathcal{O}_v\setminus\mathfrak{m}_{v'}$. Then $v(\overline{x})=(0,\dots,0,w(\overline{x}))\geq(0,\dots,0)$, which implies that $\overline{x}\in\mathcal{O}_w$. Therefore v is a composition of v' with w. □

Let $d\in\mathbb{N}$. Let v' be a $\mathbb{Z}^r$-valuation on K and let w be a $\mathbb{Z}^d$-valuation on $\kappa_{v'}$. Let $(t_r,\dots,t_1)\in K^r$ be a parametrical system of v'. We call the valuation v defined in Theorem 1.2.4, the *composition of v' with w with respect to $(t_1,\dots,t_r)$*.

Lemma 1.2.5. *Let $n\in\mathbb{N}$. Let $v,v'\in V_n(K)$ be equivalent. Then $v=v'$ if and only if there exist $t_2,\dots,t_n\in K^\times$ such that $v(t_i)=v'(t_i)=e_i^n$ for every $2\leq i\leq n$.*

Proof. Assume that there exist $t_2,\dots,t_n\in K^\times$ such that $v(t_i)=v'(t_i)=e_i^n$ for $2\leq i\leq n$. Let $t_1\in K^\times$ be such that $v(t_1)=e_1^n$. Since there exists an order-isomorphism $\gamma:\mathbb{Z}^n\to\mathbb{Z}^n$ such that $\gamma\circ v=v'$

and $\gamma(e_1^n) = e_1^n$, we have that $v'(t_1) = e_1^n$. Let $a \in K^\times$. Then there exist $a_1, \dots, a_n \in \mathbb{Z}$ such that $v(a) = (a_1, \dots, a_n)$ in $\mathbb{Z}^n$. Then $at_1^{-a_1} \cdots t_n^{-a_n} \in \mathcal{O}_v^\times$. Hence $v'(at_1^{-a_1} \cdots t_n^{-a_n}) = 0$ and $v'(a) = (a_1, \dots, a_n)$. This shows that $v = v'$. The other implication is trivial. □

In the following, we show some examples of fields carrying a $\mathbb{Z}^n$-valuation.

Examples 1.2.6. (1) Let n be a positive integer, and let k be a field. We consider $K_n = k((t_1)) \dots ((t_n))$ the field of iterated Laurent series over k. By induction on n, we show that there exists a $\mathbb{Z}^n$-valuation v on K_n such that $(t_1, \dots, t_n) \in K_n^n$ is a parametrical system of v. For $n = 1$, the valuation v_{t_1} on K_1, given by $v_{t_1}(\sum_{i=m}^{\infty} a_i t_1^i) = m$, when $a_m \in k^\times$, is a $\mathbb{Z}$-valuation on K_1 such that t_1 is a parametrical system v_{t_1}. Let $n > 1$. Let v' be the t_n-adic valuation on K_n, that is, the $\mathbb{Z}$-valuation corresponding to the valuation ring $K_{n-1}[\![t_n]\!]$. By the induction hypothesis, since $\kappa_{v'} = K_{n-1}$, we may consider a $\mathbb{Z}^{n-1}$-valuation w on K_{n-1} such that $(t_1, \dots, t_{n-1}) \in \kappa_{v'}^{n-1}$ is a parametrical system of w. Let v be the composition of v' with w with respect to t_n. Hence v is a $\mathbb{Z}^n$-valuation on K_n, and since $v(t_n) = (v'(t_n), w(\overline{1})) = (1, 0, \dots, 0) = e_n^n$, we have that $(t_1, \dots, t_n) \in K_n^n$ is a parametrical system of v. Note that different choices of uniformizers of v' can lead to distinct $\mathbb{Z}^n$-valuations on K_n (e.g. $t_n t_1$ instead of t_n). Moreover, by Theorem 1.1.18 and since v' is henselian, v is a henselian valuation on K_n.

(2) Let n be a positive integer. Let $E_n = k(t_1, \dots, t_n)$ be the field of fractions of the polynomial ring $k[t_1, \dots, t_n]$ over k. For $n = 1$, we can consider the t_1-adic valuation on $k(t_1)$. Assume $n > 1$. Let v' be the t_n-adic valuation on E_n, considering t_n as a linear polynomial over E_{n-1}. Since $\kappa_{v'} = E_{n-1}$, using the same argument as above, we may consider a $\mathbb{Z}^n$-valuation v on E_n such that $(t_1, \dots, t_n) \in E_n^n$ is a parametrical system of v.

(3) Let $n \in \mathbb{N}$. Let K' be the relative algebraic closure of E_n in K_n. Let v be the henselian $\mathbb{Z}^n$-valuation on K_n as defined in (1). By Theorem 1.2.5 we have that $v|_{E_n}$ is the $\mathbb{Z}^n$-valuation on E_n as defined in (2). Hence $v|_{K'}$ is a $\mathbb{Z}^n$-valuation on K' such that $\kappa_{v'} = k$. Furthermore, by [17, Corollary 4.1.5] the valuation $v|_{K'}$ is henselian.

We call $W \subseteq \Omega(K)$ *saturated* if for all $\mathcal{O} \in W$ we have $\mathcal{O}' \in W$ for every coarsening $\mathcal{O}'$ of $\mathcal{O}$. Let $S, S' \subseteq V(K)$. We say that S and S' are *equivalent* if $\{\mathcal{O}_v \mid v \in S\} = \{\mathcal{O}_v \mid v \in S'\}$. We say that $S \subseteq V(K)$ is *coherent* if

- S is a set of pairwise non-equivalent valuations,
- and, if $v \in S$ is a $\mathbb{Z}^n$-valuation, then $\pi_i \circ v \in S$, for all $0 \leq i \leq n$.

Proposition 1.2.7. *Let $S \subseteq V(K)$ be such that $W = \{\mathcal{O}_v \mid v \in S\}$ is finite and saturated. Then there exists a coherent set $S' \subseteq V(K)$ equivalent to S.*

Proof. Let $n = \max\{\dim \mathcal{O}_v \mid v \in S\}$. We prove the statement by induction on n. If $n = 1$, there is nothing to show, since every subset of $V_1(K)$ is a set of pairwise of non-equivalent $\mathbb{Z}$-valuations, which is trivially coherent. Assume now that $n > 1$. By the induction hypothesis, we have that for any $S \subseteq \bigcup_{1\leq i\leq n-1} V_i(K)$ such that $W = \{\mathcal{O}_v \mid v \in S\}$ is finite and saturated, there exists a coherent set $S' \subseteq V(K)$ with $W = \{\mathcal{O}_v \mid v \in S'\}$. Let $S \subseteq \bigcup_{1\leq i\leq n} V_i(K)$ be such that $W = \{\mathcal{O}_v \mid v \in S\}$ is finite and saturated. Without loss of generality, we may assume that S consist of a set of non-equivalent valuations. Let $S_{n-1} = S \setminus V_n(K)$. Then, by the induction hypothesis, S_{n-1} is equivalent to a coherent subset S'_{n-1} of $\bigcup_{1\leq i\leq n-1} V_i(K)$. Let $v \in S'_{n-1}$. Let $V_v = \{w \in S \mid \mathcal{O}_w \subsetneq \mathcal{O}_v\}$. Let $(t_1, \ldots, t_{n-1}) \in K^{n-1}$ be a parametrical system of v. For $w \in V_v$, let $\overline{w}$ be the residual valuation of w modulo v. Let w' be the composition of v and $\overline{w}$, with respect to $(t_1, \ldots, t_{n-1})$. Thus, for every $w \in V_v$, we can define a $\mathbb{Z}^n$-valuation w' on K, which is equivalent to w, by Theorem 1.1.12. Let $S(v) = \{w' \mid w \in V_v\}$. Then $S(v) \cup S'_{n-1}$ is a coherent set equivalent to $V_v \cup S'_{n-1}$. We obtain that

$$S' = \bigcup_{v\in S'_{n-1}\cap V_{n-1}(K)} S(v) \cup S'_{n-1},$$

is a coherent finite set equivalent to S. □

1.3 Function fields in one variable

Let K be a field. A field extension F/K is called a *function field in one variable* if it is finitely generated of transcendence degree one, that is, there exists a transcendental element $X \in F$ such that $F/K(X)$ is a finite extension. Let F/K be a function field in one variable. The relative algebraic closure $\tilde{K}$ of K in F is called the *field of constants of* F/K. Note that $\tilde{K}/K$ is a finite field extension; see [59, Corollary 1.1.16]. We say that F/K is *ruled* if $F = \tilde{K}(X)$ for some $X \in F$.

Let $F = K(X)$ be the rational function field in one variable X. Let $p \in K[X]$ be a monic irreducible polynomial. We consider

$$\mathcal{O}_p = \left\{ \frac{p^n f}{g} \mid n \in \mathbb{N}, f, g \in K[X], p \nmid f, g \right\},$$

the localization of $K[X]$ at $pK[X]$. Then $\mathcal{O}_p$ is a valuation ring of F and the function $v : K(X) \to \mathbb{Z} \cup \{\infty\}$, defined by $v(\frac{p^n f}{g}) = n$ and $v(0) = \infty$, for $n \in \mathbb{Z}, f, g \in K[X] \setminus pK[X]$, is a $\mathbb{Z}$-valuation v on F such that $\mathcal{O}_v = \mathcal{O}_p$. We denote this valuation by v_p and call it *the p-adic valuation on* $K(X)$. We note that $\kappa_{v_p} = K[X]/(p)$, which is a finite extension of K. We consider also the function $v_\infty : F \mapsto \mathbb{Z} \cup \{\infty\}$, defined by $v_\infty(f/g) = \deg f - \deg g$, for $f, g \in K[X] \setminus \{0\}$ and $v_\infty(0) = \infty$. Clearly v_∞ is a valuation on F and

$$\mathcal{O}_{v_\infty} = \left\{ \frac{f}{g} \mid f, g \in K[X], \deg f \leq \deg g \right\}.$$

Note that $\kappa_{v_\infty} = K$. Let $\mathcal{P}_K$ denote the set of all monic irreducible polynomials over K, and let $\mathcal{P}'_K = \mathcal{P}_K \cup \{\infty\}$.

Proposition 1.3.1. *Let v be a valuation on $K(X)$ such that $v|_K$ is trivial. Then v is equivalent to v_p for some $p \in \mathcal{P}'_K$.*

Proof. See [17, Theorem 2.1.4]. □

Proposition 1.3.2. *Let F/K be a function field in one variable. Let v be a valuation on F such that $v|_K$ is trivial. Then v is equivalent to a $\mathbb{Z}$-valuation and κ_v is a finite field extension of K.*

Proof. Let $X \in F$ be a transcendental element. Then $F/K(X)$ is a finite extension. By Theorem 1.3.1, $v|_{K(X)}$ is equivalent to v_p for some $p \in \mathcal{P}'_K$, and hence $\kappa_{v|_{K(X)}}/K$ is a finite field extension. Hence κ_v/K is a finite field extension, by [17, Theorem 3.3.5]. It follows by Theorem 1.1.23 that $\mathsf{rk}(v) = 1$, and since $\Gamma_v/\mathbb{Z}$ is finite, we have that v is equivalent to a $\mathbb{Z}$-valuation. □

We call a function field in one variable F/K *regular* if $K = \tilde{K}$ and if there exists $X \in F$ such that $F/K(X)$ is a finite separable extension. Note that the second condition is automatically satisfied when K is perfect; see [59, Proposition 3.10.2].

We fix a regular function field in one variable F/K. We denote by $\mathcal{V}(F/K)$ the set of $\mathbb{Z}$-valuations on F which are trivial on K. The *divisor group* $\mathsf{Div}(F)$ is defined as the free abelian group generated by the valuations in $\mathcal{V}(F/K)$. We write an element $D \in \mathsf{Div}(F)$ as formal sum $D = \sum_{v\in\mathcal{V}(F/K)} n_v v$, with $n_v \in \mathbb{Z}$, and $n_v = 0$ for almost all $v \in \mathcal{V}(F/K)$. Note that, if $D = \sum_{v\in\mathcal{V}(F/K)} n_v v$ and $D' = \sum_{v\in\mathcal{V}(F/K)} n'_v v$ are two divisors, then

$$D + D' = \sum_{v\in\mathcal{V}(F/K)} (n_v + n'_v)v,$$

and the neutral element in $\mathsf{Div}(F)$ is the divisor $\sum_{v\in\mathcal{V}(F/K)} n_v v$, where $n_v = 0$ for all $v \in \mathcal{V}(F/K)$. For a divisor $D = \sum_{v\in\mathcal{V}(F/K)} n_v v \in \mathsf{Div}(F)$ and $v \in \mathcal{V}(F/K)$, we denote $v(D) := n_v$.

We can define a partial ordering $\leq$ on $\mathsf{Div}(F)$ as follows: for $D_1, D_2 \in \mathsf{Div}(F)$, we set $D_1 \leq D_2$ if and only if $v(D_1) \leq v(D_2)$ for all $v \in \mathcal{V}(F/K)$. We define the *degree of a divisor* D as

$$\deg D = \sum_{v\in\mathcal{V}(F/K)} n_v[\kappa_v : K].$$

Let $x \in F^\times$. We denote $(x) = \sum_{v\in\mathcal{V}(F/K)} v(x)v$. It follows by [59, Corollary 1.3.4] that $v(x) = 0$ for all but finitely many $v \in \mathcal{V}(F/K)$. Hence $(x) \in \mathsf{Div}(F)$, and it is called the *principal divisor of* x.

We define $\mathsf{Princ}(F) = \{(x) \in \mathsf{Div}(F) \mid x \in F^\times\}$. Note that, since $(x) + (y) = (xy)$ for all $x, y \in F^\times$, we have that $\mathsf{Princ}(F)$ is a subgroup of $\mathsf{Div}(F)$. We define

$$\mathsf{Cl}(F) = \mathsf{Div}(F)/\mathsf{Princ}(F),$$

the divisor class group of F/K. For a divisor $D \in \mathsf{Div}(F)$, we denote its class by $[D] \in \mathsf{Cl}(F)$. Thus, for two divisors $D, D' \in \mathsf{Div}(F)$, we have $[D] = [D']$ if and only if $D' = D + (x)$, for some $x \in F^\times$.

In the following, we define the genus of F/K. Let $A \in \mathsf{Div}(F)$. We define the space

$$\mathcal{L}(A) = \{x \in F \mid (x) \geq -A\}.$$

It follows from [59, Lemma 1.4.6] that $\mathcal{L}(A)$ is a vector space over K and by [59, Proposition 1.4.9] that $\dim_K \mathcal{L}(A)$ is finite. Since K is algebraically closed in F, we have $\mathcal{L}(0) = K$ and $\mathcal{L}(A) = \{0\}$

whenever $\deg A < 0$, because for every $x \in F$ transcendental over K there exist $v, v' \in \mathcal{V}(F/K)$ with $v(x) > 0$ and $v'(x) < 0$ by [59, Corollary 1.1.20]. By [59, Proposition 1.4.14] there exists $\gamma \in \mathbb{Z}$ such that $\deg A - \dim \mathcal{L}(A) \leq \gamma$ for every divisor $A \in \mathsf{Div}(F)$. The genus of the regular function field F/K is

$$g(F/K) := \max\{\deg A - \dim \mathcal{L}(A) + 1 \mid A \in \mathsf{Div}(F)\}.$$

Note that, since $\deg(0) - \dim \mathcal{L}(0) + 1 = 0$, we have that $g \geq 0$. If $K \neq \tilde{K}$, we define the genus of F/K as $g(F/\tilde{K})$.

Theorem 1.3.3. *Assume that $g(F/K) = 0$. Then the following hold:*

1. *There exists a divisor $A \in \mathsf{Div}(F)$ of degree 2, and a transcendental element $X \in F$ such that $[F : K(X)] = 2$.*
2. *F is a rational function field over K if and only if there exists a divisor $A \in \mathsf{Div}(F)$ of degree one.*

Proof. See [63, Theorem 4.1.7]. □

Proposition 1.3.4. *Assume $\mathsf{char}(K) \neq 2$. Let F/K be a regular function field in one variable. Then $g(F/K) = 0$ if and only if there exist $a, b \in K^\times$ and $X \in F$ transcendental such that $F = K(X)(\sqrt{aX^2 + b})$.*

Proof. If $g(F/K) = 0$, then the result follows from [32, Theorem 5.7.2]. If there exist $a, b \in K^\times$ and $X \in F$ transcendental such that $F = K(X)(\sqrt{aX^2 + b})$, then $g(F/K) = 0$, by [32, Theorem 5.7.3]. □

Example 1.3.5. Let $F = \mathbb{R}(X)\left(\sqrt{-(X^2+1)}\right)$. We claim that $F/\mathbb{R}$ is a nonruled function field in one variable of genus zero. Clearly by Theorem 1.3.4, $F/\mathbb{R}$ is of genus zero. Since $-1 = X^2 + \left(\sqrt{-(X^2+1)}\right)^2$, there cannot be a divisor with residue field $\mathbb{R}$. In particular $F/\mathbb{R}$ is not rational, by Theorem 1.3.3.

We call a regular function field in one variable F/K such that there exists a transcendental element $X \in F$ with $[F : K(X)] = 2$ a *hyperelliptic function field*.

Note that the rational function field is a hyperelliptic function field because $[K(X) : K(X^2)] = 2$. It is known that every function field in one variable of genus 2 over a perfect field is hyperelliptic; see [59, Lemma 6.2.2].

Remark 1.3.6. Assume $\mathsf{char}(K) \neq 2$. Let F/K be a hyperelliptic function field. Then there exist $X, Y \in F$ such that $F = K(X, Y)$ and $Y^2 = f(X)$, for some non-constant square-free polynomial f in $K[X]$.

Proposition 1.3.7. *Assume $\mathsf{char}(K) \neq 2$. Let $f \in K[X]$ be a non-constant square-free polynomial. Set $F = K(X)(\sqrt{f})$. Then $g(F/K) = \lfloor \frac{\deg f - 1}{2} \rfloor$.*

Proof. See [63, Corollary 4.3.7]. □

Note that in the literature, an additional requirement for F/K to be called hyperelliptic is that $g(F/K) \geq 2$, i.e. that $\deg f \geq 5$, where $f \in K[X]$ is a square-free polynomial such that $F = K(X)(\sqrt{f})$. If one can find a square-free polynomial $f \in K[X]$ with $\deg f = 3$ such that F is isomorphic to $K(X)(\sqrt{f})$, then F/K is called an *elliptic function field*.

If K is a field carrying a $\mathbb{Z}$-valuation, we can describe a hyperelliptic function field F/K as follows.

Lemma 1.3.8. *Assume that K carries a $\mathbb{Z}$-valuation v. Let $f \in K[X]$ be a non-constant square-free polynomial of degree d, and let $F = K(X)(\sqrt{f})$. Then F is K-isomorphic to*

$$K(X)(\sqrt{\alpha \cdot q_1 \cdots q_r}),$$

for some $r \in \mathbb{N}, q_1, \ldots, q_r \in \mathcal{O}_v[X]$ monic irreducible such that $d = \sum_{i=1}^{r} \deg q_i$, and where $\alpha = 1$ if d is odd and otherwise α is the leading coefficient of f.

Proof. Since $\mathsf{Frac}(\mathcal{O}_v) = K$, we can assume that $f \in \mathcal{O}_v[X]$. Let $d = \deg f$. Let $a_0, \ldots, a_d \in \mathcal{O}_v$ be such that $f = \sum_{i=0}^{d} a_i X^i$. Since F is the function field of $Y^2 = f(X)$, multiplying by $a_d^{2(d-1)}$, we have that $(a_d^{d-1}Y)^2 = a_d^{d-1} g(X)$, where $g = \sum_{i=0}^{d} b_i X^i$, where $b_d = a_d^d$ and $b_i = a_i a_d^{d-1}$ for all $0 \leq i \leq d-1$. Replacing $X' = a_d X$, and $Y' = a_d^{d-1} Y$, we have that F is K-isomorphic to $K(X')\left(\sqrt{a_d^{d-1} g(X')}\right)$. Write $g(X') = q_1(X') \ldots q_r(X')$, where $q_i(X') \in K[X']$ are monic irreducible polynomials, for some $r \in \mathbb{N}$. Since $\mathcal{O}_v$ is a Unique Factorization Domain, by Gauss' Lemma, we may assume that $q_1(X'), \ldots, q_r(X') \in \mathcal{O}_v[X']$, which concludes the proof. □

Given a field extension L/E, we say that E is *existentially closed* in L if every system of polynomial equations over E which has a solution over L also has a solution over E.

Theorem 1.3.9. *Assume that K carries a henselian valuation v of rank one. Then K is existentially closed in K^v.*

Proof. See [33, Theorem 5.9]. □

Let $F/K, K'/K$ be two field extensions such that K is relatively algebraically closed either in F or in K'. Since K is perfect, $F \otimes_K K'$ is a domain; see [30, Corollary 1, pag. 203]. The fraction field of $F \otimes_K K'$ is called *the compositum of F and K' over K*. Note that the compositum of F with K' over K is an extension of F and of K'.

Lemma 1.3.10. *Let F/K be a function field in one variable. Let K' be a field extension of K such that K is relatively algebraically closed in K'. Let E be the compositum of F' and K' over K. Then E/K' is a function field in one variable.*

Proof. We write F as the fraction field of $K(X)[Y_1,\dots,Y_r]/(g_1,\dots,g_s)$ for some $s,r \in \mathbb{N}$, and where $g_i \in K(X)[Y_1,\dots,Y_r]$ are polynomials defining a prime ideal $I = (g_1,\dots,g_s)$. Since we have an exact sequence

$$0 \to I \to K(X)[Y_1,\dots,Y_r] \to K(X)[Y_1,\dots,Y_r]/I \to 0.$$

Observe that by [38, Proposition 1.2.2, (a)], every field extension is flat. Hence K'/K is flat, and then we have that the sequence

$$0 \to I \otimes_K K' \to K(X)[Y_1,\dots,Y_r] \otimes_K K' \to K(X)[Y_1,\dots,Y_r]/I \otimes_K K' \to 0$$

is also exact. Hence we obtain that $K(X)[Y_1,\dots,Y_r]/I \otimes_K K' \simeq K'(X)[Y_1,\dots,Y_r]/I'$, where $I' = I \cdot K'(X)[Y_1,\dots,Y_r]$. Therefore E is the fraction field of a finitely generated $K'(X)$-algebra of Krull dimension 1 by [56, Theorem], whereby E/K' is a function field in one variable. □

Let v be a henselian valuation on K. It follows by [65, Theorem 32.19, pag 357] that K is separably algebraically closed in K^v. Hence the compositum of F with K^v over K exists for any field extension F/K.

Theorem 1.3.11. *Assume that K carries a henselian valuation of rank one. Let F/K be a function field in one variable. Let E be the compositum of F and K^v over K. Then F is existentially closed in E.*

Proof. It follows from Theorem 1.3.9 that K is existentially closed in K^v. The result follows from [13, Lemma 7.2]. □

1.4 Residually transcendental valuations

In this section, we fix a valued field (K,v). Let F/K be a function field in one variable. An extension w of v to F is called *residually transcendental* if κ_w/κ_v is transcendental.

We recall that, for a valuation ring $\mathcal{O}$ of a field E, the corresponding valuation on E with valuation ring $\mathcal{O}$ and value group $E^\times/\mathcal{O}^\times$ is denoted by $v_\mathcal{O}$. We say that an extension $\mathcal{O}$ of $\mathcal{O}_v$ to F is *residually transcendental* if $\kappa_\mathcal{O}/\kappa_v$ is transcendental.

Lemma 1.4.1. *Let F/K be a function field in one variable. Let w be a residually transcendental extension of v to F. Then Γ_w is order-isomorphic to Γ_v and κ_w/κ_v is a function field in one variable.*

Proof. We first claim that κ_w/κ_v is a function field in one variable. Let $\alpha \in \kappa_w$ be a transcendental element over κ_v and let $\theta \in \mathcal{O}_w^\times$ be such that $\overline{\theta} = \alpha$. It follows by [17, Theorem 3.2.4] that $K(\theta)/K$ is transcendental. Let $w' = w|_{K(\theta)}$. By Theorem 1.1.24, w' is the Gauss extension of v with respect to θ and $\Gamma_{w'} = \Gamma_v$. Hence $\kappa_{w'} = \kappa_v(\alpha)$. Since F/K is a function field in one variable, we have that

$F/K(\theta)$ is a finite extension, which implies that $\kappa_w/\kappa_v(\alpha)$ is a finite field extension, whereby κ_w/κ_v is a function field in one variable.

Since $F/K(\theta)$ is finite, we have that $\Gamma_w/\Gamma_{w'}$ is finite, by [17, Corollary 3.2.3], whereby Γ_w/Γ_v is finite. Let $d = [\Gamma_w : \Gamma_v]$. It follows by [17, Theorem 3.2.4, (1)] that for every $\gamma \in \Gamma_w$ there exists an $n \in \mathbb{N}$ such that $\gamma n \in \Gamma_v$. In particular $d\gamma \in \Gamma_v$ for every $\gamma \in \Gamma_w$. Then the function $\Gamma_w \to \Gamma_v$, given by $\gamma \mapsto d\gamma$ is clearly a group isomorphism such that if $\gamma \leq \gamma'$, for $\gamma, \gamma' \in \Gamma_w$, then $d\gamma \leq d\gamma'$. Therefore Γ_w is order-isomorphic to Γ_v. □

Let F/K be a function field in one variable. We recall from Section 1.1, that $\Omega_i(F)$ denotes the set of valuation rings of F of rank i, for $i \in \mathbb{N}$. We define a set of equivalence classes of valuation extensions of coarsenings of v to F in the following way. For $i \in \mathbb{N}$, let $\Omega_i(F/v)$ denote the set of valuation rings $\mathcal{O} \in \Omega_i(F)$ such that $v_{\mathcal{O}}$ is a residually transcendental extension of a coarsening of v. We set

$$\Omega(F/v) = \bigcup_{i \in \mathbb{N}} \Omega_i(F/v).$$

Proposition 1.4.2. *Let $n \in \mathbb{N}$ and let $v \in V_n(K)$. Let F/K be a function field in one variable. Let $\mathcal{O} \in \Omega(F/v)$. Then $v_{\mathcal{O}}$ is a $\mathbb{Z}^r$-valuation, for some $r \leq n$.*

Proof. This follows directly from Theorem 1.2.2 and Theorem 1.4.1. □

For $i \in \mathbb{N}$, we set $\Omega_i^*(F/v) = \{\mathcal{O} \in \Omega_i(F/v) \mid \kappa_{\mathcal{O}}/\kappa_{\mathcal{O}\cap K}$ is nonruled $\}$. We set

$$\Omega(F/v) = \bigcup_{i \in \mathbb{N}} \Omega_i^*(F/v).$$

Proposition 1.4.3. *Let v be a valuation on K. Let F/K be a ruled extension. Let w be a residually transcendental extension of v. Then κ_w/κ_v is ruled.*

Proof. See [45, Theorem 3.3]. □

Lemma 1.4.4. *Let F/K be a function field in one variable. Then $\Omega^*(F/v)$ is saturated.*

Proof. Let w be a valuation on F such that $\mathcal{O}_w \in \Omega^*(F/v)$. Let w' be a coarsening of w. We claim that $\mathcal{O}_{w'} \in \Omega^*(F/v)$. It follows by [17, Theorem 3.2.4] that $\kappa_{w'}/\kappa_{w'|_K}$ is transcendental, and hence is a function field in one variable, by Theorem 1.4.1. Let $\overline{w}$ be the residual valuation of w modulo w'. Let $\nu = w|_K$. Note that $w'|_K$ is a coarsening of ν. Let $\overline{\nu}$ be the residual valuation of ν modulo $w'|_K$. If $\kappa_{w'}/\kappa_{w'|_K}$ were, then $\kappa_{\overline{w}}/\kappa_{\overline{v}}$ would be ruled, by Theorem 1.4.3, which is a contradiction. Therefore $\mathcal{O}_{w'} \in \Omega^*(F/v)$. □

Let F/K be a function field in one variable. It is natural to wonder whether the set $\Omega^*(F/v)$ is finite. We shall give a positive answer in Theorem 1.4.6 under the assumption that $v \in V(K)$. Assuming that v is a $\mathbb{Z}$-valuation on K, it was shown by K. Becher and D. Grimm that there exists a bound of $\Omega^*(F/v)$ depending on the genus of F/K.

Theorem 1.4.5 (Becher-Grimm)**.** *Assume that K carries a $\mathbb{Z}$-valuation v such that κ_v perfect. Let F/K be a regular function field in one variable. Then*

$$|\Omega^*(F/v)| \leq g(F/K) + 1.$$

Proof. See [3, Theorem 5.3]. □

In Section 5.2 we will relate this result to sums of squares in fields and we will show in Theorem 5.4.4 that the above bound is optimal.

Theorem 1.4.6. *Let n be a positive integer. Assume that K carries a $\mathbb{Z}^n$-valuation v. Let F/K be a function field in one variable. Then $\bigcup_{1\leq i\leq n}\Omega_i^*(F/v)$ is finite.*

Proof. We prove the statement by induction on n. If $n = 1$, then v is a $\mathbb{Z}$-valuation on K, and it follows by Theorem 1.4.5 that $\Omega_1^*(F/v)$ is finite. Assume now that $n > 1$. By the induction hypothesis, for any positive integer $s < n$, for any field L carrying a $\mathbb{Z}^s$-valuation v' and for any function field in one variable E/L, the set $\bigcup_{1\leq i\leq s}\Omega_i^*(E/v')$ is finite. Let $v_1 = \pi_1 \circ v$ and let $\overline{v}$ be the residual valuation of v modulo v_1. Then $\overline{v}$ is a $\mathbb{Z}^{n-1}$-valuation on κ_{v_1}, by Theorem 1.1.11. Let $r \in \{1,\dots,n\}$. We claim that $\Omega_r^*(F/v)$ is finite. If $r = 1$, then this follows by Theorem 1.4.5. Assume $r > 1$. Let w be a valuation on F such that $\mathcal{O}_w \in \Omega_r^*(F/v)$. Let $w_1 = \pi_1 \circ w$. It follows by Theorem 1.4.4 and by Theorem 1.4.1 that $\mathcal{O}_{w_1} \in \Omega_1^*(F/v)$ and that $\mathcal{O}_{w_1}$ is an extension of $\mathcal{O}_{v_1}$. Since $\kappa_{w_1}/\kappa_{v_1}$ is a function field in one variable and $\overline{v}$ is a $\mathbb{Z}^{n-1}$-valuation on κ_{v_1}, we have that $\Omega_{r-1}^*(\kappa_{w_1}/\overline{v})$ is finite. Furthermore, we have that $\mathcal{O}_w$ is determined by the induce valuation ring $\mathcal{O}_{\overline{w}} \in \Omega_{r-1}^*(\kappa_{w_1}/\overline{v})$, where $\overline{w}$ is the residual valuation of w modulo w_1, by Theorem 1.1.12. Hence, we have that $|\Omega_r^*(F/v)| = \sum_{\mathcal{O}\in\Omega_1^*(F/v)}|\Omega_{r-1}^*(\kappa_{\mathcal{O}}/\overline{v})|$, where $\overline{v}$ is the residual valuation of v modulo $v_{\mathcal{O}}$. Since for every $\mathbb{Z}$-valuation ν on F the set $\Omega_{r-1}(\kappa_\nu/\overline{v})$ is finite, we have that the set $\Omega_r^*(F/v)$ is finite, and since r was arbitrarily taken, we obtain the statement. □

1.5 Ribenboim's approximation theorem

Let v, v' be two valuations on K and let w be a coarsening of v and v'. There exist surjective order-homomorphisms $\varphi_{v,w} : \Gamma_v \to \Gamma_w, \varphi_{v',w} : \Gamma_{v'} \to \Gamma_w$ such that $w = \varphi_{v,w} \circ v$ and $w = \varphi_{v',w} \circ v'$. Then there exists an order-preserving isomorphism

$$\psi_{v,v'} : \Gamma_v/\ker(\varphi_{v,w}) \to \Gamma_{v'}/\ker(\varphi_{v',w}),$$

given by the composition $\Gamma_v/\ker(\varphi_{v,w}) \to \Gamma_w$ with $\Gamma_w \to \Gamma_{v'}/\ker(\varphi_{v',w})$.

Let v, v' be two valuations on K. We call a pair $(\gamma_v, \gamma_{v'}) \in \Gamma_v \times \Gamma_{v'}$ *compatible* if $\psi_{v,v'}(\gamma_v + \ker(\varphi_{v,w})) = (\gamma_{v'} + \ker(\varphi_{v',w}))$, where w is a coarsening of v and v' such that $\mathcal{O}_w = \mathcal{O}_{v'}\mathcal{O}_{v'}$.

Theorem 1.5.1 (P. Ribenboim)**.** *Let V be a finite set of valuations on K. For $v \in V$, let $\gamma_v \in \Gamma_v$. Then there exists $x \in K$ such that $v(x) = \gamma_v$ for all $v \in V$ if and only if $(\gamma_v)_{v\in V}$ is pairwise compatible.*

Proof. See [51, Theorem 5]. □

Let $S \subseteq V(K)$ coherent. Note that for valuations $v, v' \in S$ a pair $(\gamma_v, \gamma_{v'}) \in \Gamma_v \times \Gamma_{v'}$ is compatible if $\pi_r(\gamma_v) = \pi_r(\gamma_{v'})$, where r is the rank of $\mathcal{O}_v\mathcal{O}_{v'}$.

Let $n \in \mathbb{N}$. We recall that π^1 is the projection on the last component of $\mathbb{Z}^n$. Let $S \subseteq V(K)$ be a finite coherent set. We define the group homomorphism

$$\Phi_S : K^\times \to \prod_{v \in S} \mathbb{Z}, a \mapsto (\pi^1(v(a)))_{v \in S}. \tag{1.1}$$

Proposition 1.5.2. *Let K be a field. Let $S \subseteq V(K)$ be a finite coherent set. Then Φ_S is surjective.*

Proof. Let $(e_v)_{v \in S}$ be the canonical basis of $\prod_{v \in S} \mathbb{Z}$ as a $\mathbb{Z}$-module. For every $v \in S$, we show that there exists $x_v \in K^\times$ such that $\Phi_S(x_v) = e_v$. Consider $v \in S$ and let $\gamma_v = e_{\mathsf{rk}(v)}(v)$. For $w \in S$, where $\mathcal{O}_w$ is a refinement of $\mathcal{O}_v$, let $\gamma_w = e_{\mathsf{rk}(v)}(w)$ in Γ_w, otherwise $\gamma_w = 0$. We claim that for every $w, w' \in S$, the pair $(\gamma_w, \gamma_{w'}) \in \Gamma_w \times \Gamma_{w'}$ is compatible. Let $w, w' \in S$. If $\mathcal{O}_w, \mathcal{O}_{w'}$ are both not refinements of v, then $(\gamma_w, \gamma_{w'})$ are trivially compatible. Assume $\mathcal{O}_w$ is a refinement of $\mathcal{O}_v$ and $\mathcal{O}_{w'}$ is not a refinement of $\mathcal{O}_v$. It follows from Theorem 1.2.2 that $\mathcal{O}_w \subseteq \mathcal{O}_v \subsetneq \mathcal{O}_w\mathcal{O}_{w'} \subseteq K$, because every valuation ring has a unique coarsening of a fixed rank. Let $d \in \mathbb{N}$ be such that $\mathcal{O}_w\mathcal{O}_{w'} \in \Omega_d(K)$. Then $d < \mathsf{rk}(v) \leq \mathsf{rk}(w)$ and hence $\pi_d(\gamma_w) = 0 = \pi_d(\gamma_{w'})$ in $\mathbb{Z}^d$. Finally, assume that $\mathcal{O}_w$ and $\mathcal{O}_{w'}$ are refinements of $\mathcal{O}_v$. Let $d \in \mathbb{N}$ be such that $\mathcal{O}_w\mathcal{O}_{w'} \in \Omega_d(K)$. Then $\mathcal{O}_w\mathcal{O}_{w'} \subseteq \mathcal{O}_v$ and hence $\mathsf{rk}(v) \leq d < \mathsf{rk}(w), \mathsf{rk}(v) \leq d < \mathsf{rk}(w')$. Thus, we have $\pi_d(\gamma_w) = \pi_d(\gamma_{w'})$, that is, $(\gamma_w, \gamma_{w'})$ are compatible. Therefore, for every $w, w' \in S$, the pair $(\gamma_w, \gamma_{w'}) \in \Gamma_w \times \Gamma_{w'}$ is compatible. By Theorem 1.5.1 there exists $x_v \in K^\times$ such that $w(x_v) = \gamma_w$ for all $w \in W$. Hence $\pi^1(v(x_v)) = \pi^1(\gamma_v) = 1$, and $\pi^1(w(x_v)) = 0$ for all $w \in S \setminus \{v\}$. Therefore $\Phi_S(x_v) = e_v$. Since $v \in S$ was arbitrarily chosen, we conclude that Φ_S is surjective. □

Chapter 2

Quadratic forms over fields

In this chapter we recall some, basic well-known results from the theory of quadratic forms, with a focus on sums of squares and on the Kaplansky radical. Furthermore, we explain some new, preliminary results that will be used in Chapter 4 and Chapter 5. In Section 2.1 we introduce some basic, known results about quadratic forms over fields. In Section 2.2 we define the Pythagoras number of a field, and we compute this invariant and describe its relation with the Pythagoras number of the residue fields of certain valuations on the field. In Section 2.3 we recall the notion of a hereditarily pythagorean field and we bound the Pythagoras number of function fields in one variable over a hereditarily pythagorean field admitting precisely two orderings (Theorem 2.3.9). The latter will be a key ingredient of Theorem 5.1.7, where we bound the Pythagoras number of any function field in one variable over any hereditarily pythagorean field. This is a joint work with my supervisors and my colleagues from U. Antwerpen N. Daans and M. Zaninelli. Finally, in Section 2.4 we define the Kaplansky radical of a field and we collect some examples of fields for which the Kaplansky radical is known.

2.1 General notions

We always denote by K a field of characteristic different from 2. Let $n \in \mathbb{N}$. A *quadratic form* in n variables over K is a homogeneous polynomial $\varphi \in K[X_1, \dots, X_n]$ of degree 2. We write $\varphi = \sum_{i,j=1}^{n} a_{ij} X_i X_j$, with $a_{ij} \in K$ for $1 \leq i, j \leq n$. Replacing the coefficients a_{ij} by $a'_{ij} = \frac{1}{2}(a_{ij} + a_{ji})$, we have a symmetric matrix $M_\varphi = (a'_{ij})_{i,j=1}^{n}$ associated to φ such that in terms of matrix notations $\varphi = X \cdot M_\varphi \cdot X^t$, where $X = (X_1, \dots, X_n)$ and X^t denotes the transpose of X. On the other hand, for every symmetric matrix M in $\mathbb{M}_n(K)$, we have that $\varphi = X \cdot M \cdot X^t$ is a quadratic form with $M_\varphi = M$. We say that a quadratic form φ in n-variables is *regular* if M_φ is invertible. Let $n, m \in \mathbb{N}$. Let φ and ψ be two quadratic forms over K in n and m, variables respectively. The orthogonal sum of φ and ψ, denoted by $\varphi \perp \psi$ is the quadratic form in $(n+m)$-variables defined as

$$\varphi \perp \psi = X \begin{pmatrix} M_\varphi & 0 \\ 0 & M_\psi \end{pmatrix} X^t$$

where $X = (X_1, \dots, X_{n+m})$. Let $a_{ij} \in K$ be such that $M_\psi = (a_{ij})_{i,j=1}^n$. The tensor product of φ and ψ, denote by $\varphi \otimes \psi$, is the quadratic form in nm-variables defined as

$$\varphi \otimes \psi = X \begin{pmatrix} a_{11}M_\varphi & a_{12}M_\varphi & \cdots & a_{1n}M_\varphi \\ a_{21}M_\varphi & a_{22}M_\varphi & \cdots & a_{2n}M_\varphi \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}M_\varphi & a_{n2}M_\varphi & \cdots & a_{nn}M_\varphi \end{pmatrix} X^t$$

where $X = (X_1, \dots, X_{nm})$. It is easy to see that, if φ and ψ are regular, then $\varphi \perp \psi$ and $\varphi \otimes \psi$ are regular. Let φ and ψ two quadratic forms in n-variables. We say that φ and ψ are *isometric* and denote by $\varphi \simeq \psi$ if there exists a matrix A in $\mathbb{GL}_n(K)$ such that $M_\varphi = A^t \cdot M_\psi \cdot A$. We set

$$\det(\varphi) = \det(M_\varphi)K^{\times 2},$$

in $K^\times/K^{\times 2}$, and we call it the *determinant of* φ. It is easy to see that, if $\varphi \simeq \psi$, then $\det(\varphi) = \det(\psi)$. The quadratic form φ is called *isotropic* if there exists $v \in K^n \setminus \{0\}$ such that $\varphi(v) = 0$, otherwise we say that φ is *anisotropic*. We set $D_K(\varphi) = \{\varphi(v) \mid v \in K^n\} \setminus \{0\}$. For $a_1, \dots, a_n \in K$, we denote by $\langle a_1, \dots, a_n \rangle$ the quadratic form $a_1X_1^2 + \cdots + a_nX_n^2$. We also denote by $\langle\ \rangle$ the empty quadratic form in 0-variables. It is known that every quadratic form is isometric to a quadratic form of the form $\langle a_1, \dots, a_n \rangle$ for some $a_1, \dots, a_n \in K$; see for example [35, I. Corollary 2.4].

Lemma 2.1.1. *Let $a, b \in K^\times$. If $c \in D_K\langle a, b\rangle$, then $\langle a, b\rangle \simeq \langle c, abc\rangle$.*

Proof. See [48, 2.1.3]. □

Lemma 2.1.2. *Let φ be a regular quadratic form over K, and let $a \in K^\times$. Then $a \in D_K(q)$ if and only if $\varphi \perp \langle -a\rangle$ is isotropic.*

Proof. See [35, I. Corollary 3.5]. □

The following Lemma characterizes the 3-dimensional quadratic forms with trivial determinant.

Lemma 2.1.3. *Let $a, b \in K^\times$ and let $\varphi = \langle -a, -b, ab\rangle$. The following facts hold:*

(1) If $D_K(\varphi) = K^{\times 2}$, then $\varphi \simeq \langle 1, 1, 1\rangle$ and K is pythagorean.

(2) If $D_K(\varphi) \neq K^{\times 2}$, then there exists $a', b' \in K^\times$ such that $\varphi \simeq \langle -a', -b', a'b'\rangle$ and $a'b' \notin K^{\times 2}$.

Proof. We show (1). Since $-a, -b, ab \in D_K(\varphi)$ and $D_K(\varphi) = K^{\times 2}$, we have that $\varphi \simeq \langle 1, 1, 1\rangle$. Hence $\mathsf{S}_3(K) = D_K(\varphi) = K^{\times 2}$, whereby K is pythagorean. We show (2). Let $c \in D_K(\varphi) \setminus K^{\times 2}$. Then $\langle -a, -b, ab\rangle \simeq \langle c, d, e\rangle$, for some $d, e \in K^\times$, by [35, I. 2.3]. Since $d(\varphi) = K^{\times 2}$, we have that $cde \in K^{\times 2}$, whereby $\varphi \simeq \langle c, d, cd\rangle$. Letting $a' = -d, b' = -cd$, we obtain the desired. □

It follows by Theorem 1.3.4 that every regular function field of genus zero F/K is the function of a conic $Y^2 = aX^2 + b$ over K, for some $a, b \in K^\times$, and thus, of the projective smooth conic

$abY^2 - a(bX)^2 - b(aZ)^2 = 0$. Thus, to a regular function field of genus zero $K(X)(\sqrt{aX^2+b})$ we can associate a 3-dimensional quadratic form $\langle -a, -b, ab\rangle$ over K. These two objects are related as follows.

Proposition 2.1.4. *Let $a, b, a', b' \in K^\times$. Then $K(X)(\sqrt{aX^2+b})$ is K-isomorphic to $K(X)(\sqrt{a'X^2+b'})$ if and only if $\langle -a, -b, ab\rangle \simeq \langle -a', -b', a'b'\rangle$.*

Proof. This follows directly by [35, III. Theorem 2.5] and by [19, Theorem 1.4.2]. □

We call a quadratic form φ *universal* if $D_K(\varphi) = K^\times$.

Example 2.1.5. Since for all $a \in K^\times$, we have $a = \left(\frac{a+1}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2$, the quadratic form $\langle 1, -1\rangle$ over K is universal.

We denote by $\mathbb{H}$ the quadratic form X_1X_2. Substituting $X_1 = Y_1 - Y_2$ and $X_2 = Y_1 + Y_2$, we obtain that $\mathbb{H} \simeq \langle a, -a\rangle$ for any $a \in K^\times$. A quadratic form φ is called *hyperbolic* if $\varphi \simeq m \times \mathbb{H} = \mathbb{H} \perp \ldots \perp \mathbb{H}$ for some $m \in \mathbb{N}$. If $\varphi \in K[X_1, \ldots, X_n]$ is a regular quadratic form in n variables, then we call n the *dimension of* φ and denote it by $\dim(\varphi)$. It follows by [35, I. Theorem 4.1] that, for every regular quadratic form φ, there exists a unique $m \in \mathbb{N}$ and an anisotropic quadratic form ψ such that

$$\varphi \simeq \psi \perp m \times \mathbb{H}.$$

We call two regular quadratic forms φ and ψ *Witt equivalent* if there exists $r, s \in \mathbb{N}$ and an anisotropic quadratic form λ such that $\varphi \simeq \lambda \perp r \times \mathbb{H}$ and $\psi \simeq \lambda \perp s \times \mathbb{H}$. For a quadratic form φ, we denote by $[\varphi]$ the class of φ modulo Witt equivalence. We set

$$WK = \{[\varphi] \mid \varphi \text{ regular quadratic form over K}\}.$$

The set WK is given the structure of conmutative ring by defining addition and multiplication for classes $[\varphi]$ and $[\psi]$ of regular quadratic forms φ and ψ as follows:

$$[\varphi] + [\psi] = [\varphi \perp \psi], \quad [\varphi] \cdot [\psi] = [\varphi \otimes \psi].$$

The classes of quadratic forms $[\langle\,\rangle]$ and $[\langle 1\rangle]$ are the additive and multiplicative neutral element of WK, respectively. The ring WK with the above operations is called the *Witt ring of* K. The elements of WK are in 1-to-1 correspondence with the isometry classes of all anisotropic forms; see [35, II. Proposition 1.4].

We denote by IK the ideal of WK consisting of the classes of even-dimensional regular quadratic forms. The ideal IK is called *the fundamental ideal of* WK.

Let $n \in \mathbb{N}$. We set $I^nK = (IK)^n$. We write

$$\langle\langle a_1, \ldots, a_n\rangle\rangle = \langle 1, -a_1\rangle \otimes \cdots \otimes \langle 1, -a_n\rangle$$

for $a_1, \ldots, a_n \in K^\times$. A quadratic form φ over K such that $\varphi \simeq \langle\langle a_1, \ldots, a_n\rangle\rangle$ for some $a_1, \ldots, a_n \in K^\times$ is called an *n-fold Pfister form*.

Theorem 2.1.6 (Pfister). *Let φ be a Pfister form over K. If φ is isotropic, then φ is hyperbolic.*

Proof. See [35, X. Theorem 1.7]. □

Proposition 2.1.7. *The ideal I^nK is generated as a group by the Witt classes of n-fold Pfister forms over K.*

Proof. See [35, X. Proposition 1.2]. □

Corollary 2.1.8. *We have $I^nK = 0$ if and only if every n-fold Pfister form over K is isotropic.*

Proof. This follows by Theorem 2.1.7 together with Theorem 2.1.6. □

Proposition 2.1.9. *Let $n \in \mathbb{N}$. Every $(n+1)$-fold Pfister form over K is hyperbolic if and only if every n-fold Pfister form over K is universal.*

Proof. Let φ be a Pfister form over K. Then the result follows from the fact that $D_K(\varphi)$ is equal to the set of elements $a \in K^\times$ such that $\langle 1, -a\rangle \otimes \varphi$ is hyperbolic; see for example [35, X. Theorem 1.8]. □

An important tool for studying isotropy of quadratic forms over concrete fields are local-global principles. A local-global principle for a given field states that a quadratic form is isotropic if and only if it is locally isotropic, where locally refers to considering the quadratic form over completions of the field with respect to some set of valuations. One very famous such example would be the local-global principle by Hasse-Minkowski, which states that a quadratic form over a number field K is isotropic if and only if is isotropic over all completions of K; see [35, Hasse-Minkowski principle 3.1]. Assume that K carries a $\mathbb{Z}$-valuation v. Let F/K be a function field in one variable. We say that a $\mathbb{Z}$-valuation w on F is v-divisorial if, either $w|_K$ is trivial or $w|_K$ is equivalent to v and κ_w/κ_v is a function field in one variable. We denote by $\mathcal{V}(F/v)$ the set of all v-divisorial valuations on F. Another important example would be the following.

Theorem 2.1.10 (Colliot-Thélène, Parimala, Suresh). *Assume that K carries a complete nondyadic $\mathbb{Z}$-valuation. Let F/K be a function field in one variable, and let φ be a regular quadratic form over F of dimension at least 3. Then φ is isotropic over F if and only if φ is isotropic over F^w for every $w \in \mathcal{V}(F/v)$.*

Proof. This follows from a analysis of the proof of [11, Theorem 3.1], whose statement unnecessarily assumed that the unique regular projective curve over K whose function field is isomorphic to F be smooth, and where the set of valuations in the statement was unnecessarily taken to be the set of all discrete valuations on F. See also [21, Theorem 6.1] for the statement as presented here. □

The following new local-global principle due to Mehmeti, will play a key role in our study of sums of squares in function fields in Chapter 5.

Let v be a valuation on K of rank one. Let F/K be a function field in one variable. We denote by $\mathcal{M}(F/v)$ the set of valuations w on F of rank one such that $w|_K$ is either trivial or $w|_K = v$.

Theorem 2.1.11 (V. Mehmeti)**.** *Assume that K carries a nondyadic complete rank-one valuation v. Let F/K be a function field in one variable. A regular quadratic form over F of dimension at least 3 is isotropic if and only if it is isotropic over F^w for every $w \in \mathcal{M}(F/v)$.*

Proof. See [40, Corollary 3.19, (2)] and [40, Remark 3.20]. □

Proposition 2.1.12. *Assume that $\mathsf{char}(K) \neq 2$. Assume that $I^2L = 0$ for all finite extensions L/K. Then $I^3F = 0$ for every function field in one variable F/K.*

Proof. We use the cohomological 2-dimension of a field E of characteristic different from 2, which is denoted by $cd_2(E)$, and for $\mu_2 = \{-1, 1\} \subseteq E^\times$ and $n \in \mathbb{N}$, we denote by $H^n(E, \mu_2)$, the n-th Galois cohomology group of E with coefficients in μ_2, as defined in [54, Chap. I. §2]. It follows by [15, Theorem 13.7, Theorem 14.3] that I^2L/I^3L is isomorphic to $H^2(L, \mu_2)$, whereby $H^2(L, \mu_2) = 0$, because $I^3L = 0$. By [54, Proposition 4.1.21'] we have that $cd_2(K) < 2$. Let F/K be a function field in one varable. Then it follows by [43, 6.5.14] that $cd_2(F) < 3$. Then, by [41, Theorem 12.2], we conclude that the reduced norm form of any quaternion algebra over F is surjective. This means that every 2-fold Pfister form over F is universal, whereby $I^3F = 0$, by Theorem 2.1.9. □

2.2 Sums of squares

Let K be a field. For $d \in \mathbb{N}$, let $\mathsf{S}_d(K)$ denote the set of nonzero sums of d squares in K. Let $\mathsf{S}(K) = \bigcup_{d \in \mathbb{N}} \mathsf{S}_d(K)$. Note that $\mathsf{S}(K)$ consists of all nonzero sums of squares in K, and that it is also a subgroup of $K^\times$. We also denote $\mathsf{S}_1(K)$ by $K^{\times 2}$.

The *Pythagoras number* $p(K)$ of K is the smallest positive integer d such that $\mathsf{S}(K) = \mathsf{S}_d(K)$ if such an integer d exists, otherwise it is infinite. The *level* $s(K)$ *of* a field K is the smallest integer d such that $-1 \in \mathsf{S}_d(K)$ if such an integer d exists, otherwise it is infinite. If $s(K) < \infty$ we say that K is *nonreal*, otherwise we say that K is *real*.

Theorem 2.2.1 (Pfister)**.** *For any $n \in \mathbb{N}$, $\mathsf{S}_{2^n}(K)$ is a subgroup of $K^\times$.*

Proof. See [35, X. Corollary 1.9]. □

Theorem 2.2.2 (Pfister)**.** *Assume that K is nonreal. Then $s(K)$ is a power of 2.*

Proof. See [35, XI. Theorem 2.2]. □

Corollary 2.2.3. *If K is nonreal, then $s(K) \leq p(K) \leq s(K)+1$. In particular, $p(K)$ is either 2^n or 2^n+1, for some $n \in \mathbb{N}$;*

Proof. See for example [48, Lemma 7.1.3]. □

Let n be a positive integer. We call $[\mathsf{S}_{2^n}(K) : \mathsf{S}_{2^{n-1}}(K)]$ the *n-th Pfister index of K*. We say that K has trivial n-th Pfister index if $[\mathsf{S}_{2^n}(K) : \mathsf{S}_{2^{n-1}}(K)] = 1$.

Remark 2.2.4. Clearly, if n is the largest integer such that the n-th Pfister index of K is nontrivial, then $2^{n-1} < p(K) \leq 2^n$. Moreover, if K is nonreal of level 2^n, for some $n \in \mathbb{N}$, then $\mathsf{S}(K) = \mathsf{S}_{2^n+1}(K)$, and hence $(n+1)$ is the largest integer such that the $(n+1)$-th Pfister index can be nontrivial.

The Theorem 2.2.4 might make it seem plausible that the Pythagoras number of a field is always either 2^n or 2^n+1, for some $n \in \mathbb{N}$. However, it was proved by D. Hoffmann in [29] that, for every $m \in \mathbb{N}$, there exists a field E such that $p(E) = m$. In the following we recall some examples where the Pythagoras number is known.

Examples 2.2.5. (1) Since $\mathsf{S}(\mathbb{R}) = \mathbb{R}_{\geq 0} = \mathbb{R}^{\times 2}$, we have that $p(\mathbb{R}) = 1$.

(2) Lagrange's four-square theorem states that every positive integer is a sum of four integer squares; see [35, XI. Theorem 1.4]. This implies that $p(\mathbb{Q}) \leq 4$. Since $7 \in \mathsf{S}_4(\mathbb{Q}) \setminus \mathsf{S}_3(\mathbb{Q})$, we can conclude that $p(\mathbb{Q}) = 4$.

(3) If K is a number field, then $p(K) \leq 4$. See for example [35, XI. Examples 5.9 (2)].

(4) [Pourchet, Hsia-Jonson] Let K be a number field. Then

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

See [48, Theorem 1.9, Chap. 7].

(5) Let $F = \mathbb{R}(X)$. We claim that $p(F) = 2$. Since $X^2+1 \notin F^{\times 2}$, we have $p(F) > 1$. Consider $f \in \mathsf{S}(F)$. Then $f = gh^2$, for some $g \in \mathsf{S}(F) \cap \mathbb{R}[X]$ and $h \in F^\times$. It is enough to show that $\mathsf{S}(F) \cap \mathbb{R}[X] \subseteq \mathsf{S}_2(F)$. Let $g \in \mathbb{R}[X]$. We can write

$$g = b(X-\alpha_1)^{\delta_1} \cdots (X-\alpha_r)^{\delta_r} q_1 \cdots q_n,$$

where $\alpha_1, \ldots, \alpha_r \in \mathbb{R}, b \in \mathbb{R}^\times, \delta_i \in \mathbb{N}$ and $q_1, \ldots, q_n \in \mathbb{R}[X]$ are monic quadratic irreducible polynomials. For $1 \leq i \leq n$, let $c_i, d_i \in \mathbb{R}$ be such that $q_i = X^2 + c_i X + d_i$. Let $1 \leq i \leq n$. Since q_i is irreducible over $\mathbb{R}$, we have that $c_i^2 - 4d_i \in -\mathbb{R}^{\times 2}$. Hence

$$q_i = \left(X - \frac{c_i}{2}\right)^2 + \left(\sqrt{\frac{4d_i - c_i^2}{4}}\right)^2.$$

Thus, if $g \in \mathsf{S}(F)$, then $g(x) \geq 0$ for all $x \in \mathbb{R}$. Hence $b \in \mathbb{R}^{\times 2}, \delta_i \in 2\mathbb{Z}$, for all $1 \leq i \leq r$, whereby $g \in \mathsf{S}_2(F)$. Therefore $p(F) \leq 2$.

The fifth example in Theorem 2.2.5 was generalized by E. Witt as follows.

Theorem 2.2.6 (E. Witt)**.** *Let $F/\mathbb{R}$ be a function field in one variable. Then $p(F) = 2$.*

Proof. See [66, I]. □

In what follows, we study the Pythagoras number of a valued field and its relation with the Pythagoras number of the residue field.

Proposition 2.2.7. *Let K be a field and v a nondyadic henselian valuation on K. Let $n \in \mathbb{N}$. Let $a_1, \dots, a_n \in \mathcal{O}_v^\times$, and let $\varphi = \langle a_1, \dots, a_n \rangle$ over K. If $\overline{\varphi} = \langle \overline{a_1}, \dots, \overline{a_n} \rangle$ is isotropic over κ_v, then φ is isotropic over K.*

Proof. Since the quadratic form $\overline{\varphi}$ is isotropic over κ_v, there exist $x_1, \dots, x_n \in \mathcal{O}_v$ not all in $\mathfrak{m}_v$ such that $a_1x_1^2 + \cdots + a_nx_n^2 \in \mathfrak{m}_v$. Without loss of generality, we may assume that $x_1 \in \mathcal{O}_v^\times$. Let $f(T) = a_1T^2 + a_2x_2^2 + \cdots + a_nx_n^2$, and $\overline{f}(T) = \overline{a_1}T^2 + \overline{a_2x_2^2 + \cdots + a_nx_n^2}$ in $\kappa_v[T]$. Then its formal derivate $\partial\overline{f}(T) = 2\overline{a_1}T \neq 0$, and thus $\overline{x_1} \in \kappa_v$ is a simple root of $\overline{f}$. Now, since $f \in \mathcal{O}_v[T]$, $f(\overline{x_1}) = 0$, there exists $\alpha \in \mathcal{O}_v$ such that $f(\alpha) = 0$ and $\overline{\alpha} = \overline{x_1}$, by Hensel's Lemma. Therefore $\alpha \in \mathcal{O}_v^\times$ and $\varphi(\alpha, x_2, \dots, x_n) = f(\alpha) = 0$. Hence φ is isotropic over K. □

We say that a valuation v on K is *real* or *nonreal*, respectively, if κ_v has the corresponding property.

Lemma 2.2.8. *Let v be a nonreal valuation on K. Then $s(\kappa_v) \leq s(K)$. Moreover, if v is a nondyadic henselian valuation, then $s(\kappa_v) = s(K)$.*

Proof. If K is real, then the inequality is trivial. Assume that K is nonreal, and let $d \in \mathbb{N}$ be such that $s(K) = d$. We claim that $s(\kappa_v) \leq d$. Since $s(K) \leq d$, there exist a positive integer n with $n \leq d$ and $a_0, \dots, a_n \in K^\times$ such that $a_1^2 + \cdots + a_n^2 = 0$ and $v(a_0) \leq \cdots \leq v(a_n)$. Set $b_i = a_0^{-1}a_i$ for $0 \leq i \leq n$. Then $-1 = b_1^2 + \cdots + b_n^2$ and $b_1, \dots, b_n \in \mathcal{O}_v$. Hence $-1 = \overline{b_1}^2 + \cdots + \overline{b_n}^2$ in κ_v, whereby $s(\kappa_v) \leq d$. Assume now that v is a nondyadic nonreal henselian valuation. Let $s = s(\kappa_v)$ and let $\varphi = (s+1) \times \langle 1 \rangle$. Then $\overline{\varphi} = (s+1) \times \langle \overline{1} \rangle$ is isotropic over κ_v. It follows from Theorem 2.2.7 that φ is isotropic over K, whereby K is nonreal with $s(K) \leq s(\kappa_v)$. Note that this implies implies that K is real if and only if κ_v is real. □

Lemma 2.2.9. *Let v be a valuation on K and let $d \in \mathbb{N}$. Then $v(a_1^2 + \cdots + a_d^2) = \min\{2v(a_i) \mid 1 \leq i \leq d\}$ holds for all $a_1, \dots, a_d \in K$ if and only if $d \leq s(\kappa_v)$. In particular, if $d \leq s(\kappa_v)$, then $\sigma \in \mathcal{O}_v^\times K^{\times 2}$ for all $\sigma \in \mathsf{S}_d(K)$.*

Proof. It follows by [4, Lemma 4.1]. □

Recall that an ordered abelian group is called discrete if there exists a minimal positive element.

Proposition 2.2.10. *Let v be a nonreal, nondyadic valuation on K such that Γ_v is discrete. Then $s(\kappa_v) < p(K)$.*

Proof. Let $d = s(\kappa_v)$. There exist $f \in \mathfrak{m}_v, x_1, \dots, x_d \in K$ such that $f = 1 + x_1^2 + \cdots + x_d^2$. Let $b = (1 - \frac{f}{2})^2 + x_1^2 + \cdots + x_d^2 = \frac{f^2}{4}$. Let $\gamma \in \Gamma_v$ be the minimal positive element and let $z \in K$ be such that $v(z) = \gamma$. Note that $\gamma \notin 2\Gamma_v$. Hence $0 < v(z) < 2v(f) = v(b)$. Let $\sigma = (z - (1 - \frac{f}{2}))^2 + x_1^2 + \cdots + x_d^2$. Since $\sigma = z(z - 2(1 - \frac{f}{2})) + b$, $0 < v(z) < v(b)$, and since $v(2 - f) = 0 < v(z)$, we have that $v(\sigma) = \gamma$. It follows by Theorem 2.2.9 that $\sigma \notin \mathsf{S}_d(K)$, and hence $s(\kappa_v) < p(K)$. □

For a field K, we set

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

Proposition 2.2.11. *Let v be a valuation on K. Then $p(\kappa_v) \leq p(K)$. If v is nondyadic and henselian, then $p(K) \leq p'(\kappa_v)$. In particular, if either $2\Gamma_v = \Gamma_v$ and v is nonreal, or v is real, then $p(K) = p(\kappa_v)$.*

Proof. First, we show that $p(\kappa_v) \leq p(K)$. If $p(K) = \infty$, then this is trivial. Assume $p(K) < \infty$. Let $d = p(K)$. Let $\sigma \in \mathcal{O}$ be such that $\overline{\sigma} \in \mathsf{S}(\kappa_v)$. There exist $n \in \mathbb{N}, x_1, \dots, x_n \in \mathcal{O}_v^\times$ and $m \in \mathfrak{m}_v$ such that $\sigma = x_1^2 + \cdots + x_n^2 + m$. Thus $x_1^2 + \cdots + x_n^2 \in \mathsf{S}_d(K)$, and hence there exist $y_1, \dots, y_d \in K$ such that $x_1^2 + \cdots + x_n^2 = y_1^2 + \cdots + y_d^2$. If $v(y_i) < 0$ for some $1 \leq i \leq d$, then $s(\kappa_v) + 1 \leq d$, by Theorem 2.2.9, whereby $p(\kappa_v) \leq s(\kappa_v) + 1 \leq d$. We may therefore assume that $y_1, \dots, y_d \in \mathcal{O}_v$, whereby $\overline{\sigma} = \overline{y_1}^2 + \cdots + \overline{y_d}^2 \in \mathsf{S}_d(\kappa_v)$. This shows that $p(\kappa_v) \leq p(K)$.

For the rest, we assume that v is nondyadic and henselian. It follows by Theorem 2.2.8 and Theorem 2.2.3 that $p(K) \leq s(K) + 1 = s(\kappa_v) + 1$ when K is nonreal. We now suppose that v is real. Let $\sigma \in \mathsf{S}(K)$ and let $r = p(\kappa_v)$. Then there exists $x \in K^\times$ such that $\sigma x^{-2} \in \mathcal{O}_v^\times$ and $\overline{\sigma x^{-2}} \in \mathsf{S}(\kappa_v)$, by Theorem 2.2.9 whence $\overline{\sigma x^{-2}} \in \mathsf{S}_r(\kappa_v)$. It follows by Theorem 2.2.7 that $\sigma \in \mathsf{S}_r(K)$. This shows that $p(K) \leq p(\kappa_v)$, and we conclude that $p(K) = p(\kappa_v)$. Assume now that v is nonreal and $2\Gamma_v = \Gamma_v$. Then $r \in \mathbb{N}$ and for every $\sigma \in \mathsf{S}(K)$ there exists $x \in K^\times$ such that $\sigma x^{-2} \in \mathcal{O}_v^\times$, and since $\overline{\sigma x^{-2}} \in \mathsf{S}_r(\kappa_v)$, we have that $\sigma \in \mathsf{S}_r(K)$, by Theorem 2.2.7. This shows that $p(K) \leq r = p(\kappa_v)$ and we conclude that $p(K) = p(\kappa_v)$. □

2.3 Hereditarily pythagorean fields

Let K be a field of characteristic different from 2. We say that $P \subsetneq K$ is an *ordering of K*, if it has the following properties:

$$P + P \subseteq P, P \cdot P \subseteq P \quad \text{and} \quad P \cup -P = K.$$

Theorem 2.3.1 (Artin-Schreier)**.** *Let $\sigma \in K^\times$. Then $\sigma \in \mathsf{S}(K)$ if and only if $\sigma \in P$ for all orderings P of K.*

Proof. See [35, VIII. Theorem 1.12]. □

Corollary 2.3.2. *K is real if and only if K admits an ordering.*

Proof. Assume that there exists an ordering P on K. If $-1 \in \mathsf{S}(K)$, then $-1 \in P$, by Theorem 2.3.1. Then $a = \left(\frac{a+1}{2}\right)^2 + (-1)\left(\frac{a-1}{2}\right)^2 \in P$, for all $a \in K$, because $K^{\times 2} \cup \{0\} \subseteq P$ and $P + P \subseteq P$. This contradicts the fact that $P \subsetneq K$. The other direction is clear. □

We say that K is *pythagorean* if $p(K) = 1$. A real pythagorean field is called *euclidean* if it allows only one ordering

Proposition 2.3.3. *Assume that K is real. Then K is euclidean if and only if $K^\times = K^{\times 2} \cup -K^{\times 2}$.*

Proof. See [35, VIII. Proposition 1.6]. □

The field K is called *hereditarily pythagorean* if K is real and every finite real extension of K is pythagorean. The fields $\mathbb{R}, \mathbb{R}((t_1))\dots((t_n))$ for $n \in \mathbb{N}$ and $\bigcup_{i=1} \mathbb{R}((t^{1/i}))$ are familiar examples of hereditarily pythagorean fields.

Hereditarily pythagorean fields were studied by E. Becker and by L. Bröcker in the 1970s; see [8] and [10].

Theorem 2.3.4 (Becker)**.** *Assume that K is real. Then K is hereditarily pythagorean if and only if every finite nonreal extension of K contains $\sqrt{-1}$.*

Proof. See [8, III, Theorem 1]. □

A valuation theoric description of these fields is the following.

Proposition 2.3.5. *The following are equivalent.*

(1) K is hereditarily pythagorean.

(2) There exists a henselian valuation on K whose residue field is hereditarily pythagorean and admits at most two orderings.

Proof. The implication (2) ⇒ (1) follows by Theorem 2.2.11 (2), Theorem 2.2.8 and by the fact that finite extensions of henselian valued fields are also henselian. For the other implication; see [10, Proposition 3.5]. □

For a field K, the quotient group $K^\times/K^{\times 2}$ is called the *square class group of K*. We call $q(K) = |K^\times/K^{\times 2}|$ the *square class number of K*. The square class group of fields carrying a henselian $\mathbb{Z}^n$-valuation has the following characterization.

Lemma 2.3.6. *Let $n \in \mathbb{N}$. Let v be a henselian $\mathbb{Z}^n$-valuation on K. Then*

$$q(K) = 2^n q(\kappa_v)$$

Proof. Let $(t_n, \dots, t_1) \in K^n$ be a parametrical system of v. Let $a \in K^\times$. Since $K = \mathsf{Frac}(\mathcal{O}_v)$, there exist $b, c \in \mathcal{O}_v$ such that $a = bc^{-1} = bc(c^{-1})^2$. Hence $a \in \{ut_1^{u_1} \cdots t_n^{u_n} h^2 \mid u_i \in \{0,1\}, u \in \mathcal{O}_v^\times \text{ and } h \in K^\times\}$. Moreover, for $u \in \mathcal{O}_v^\times$ we have $u \in K^{\times 2}$ if and only if $\overline{u} \in \kappa_v^{\times 2}$, by Hensel's Lemma. Therefore, we have that $q(K) \leq 2^n q(\kappa_v)$. The other inequality is clear. □

Lemma 2.3.7. *Let K be a pythagorean field admiting exactly two orderings. Then*

$$q(K) = 4.$$

Proof. Let P_1, P_2 be the two orderings of K. For $i = 1, 2$, we set $P_i^\times = P_i \setminus \{0\}$. We consider $\varphi : K^\times \to (K^\times/P_1^\times) \times (K^\times/P_2^\times)$ the group homomorphism given by $x \mapsto (xP_1^\times, xP_2^\times)$. It follows by Theorem 2.3.1 that $\ker(\varphi) = \mathsf{S}(K)$, and hence $\ker(\varphi) = K^{\times 2}$. Hence $q(K) \leq |K^\times/P_1^\times| \cdot |K^\times/P_2^\times|$. Moreover, by [35, VIII. Proposition 1.3 (4)] we have that $|K^\times/P_i^\times| = 2$ for $i = 1, 2$. Since P_1 and P_2 are not contained in one another, it follows that φ is surjective. Hence $q(K) = 4$. □

Proposition 2.3.8. *Let K be a hereditarily pythagorean field admiting exactly two orderings. Let L/K be a finite nonreal extension. Then $q(L) = 2$.*

Proof. We first assume that there exists a finite real extension K'/K and a finite tower of quadratic field extensions $K' = K_0' \subseteq K_1' \subseteq \ldots \subseteq K_r'$, for some $r \in \mathbb{N}$, such that K_r' contains L and $[K_r' : L]$ is odd. We claim that $q(L) = 2$. Let us fix $0 \leq j < r$. Let $E = K_j$, and let $M = K_{j+1}$. Since K has exactly two orderings, it follows by [10, Proposition 3.9] that every finite real extension of K has exactly two orderings, too. Thus, if K_j is real, then $q(K_j) = 4$, by Theorem 2.3.7. Moreover, if K_{j+1} is nonreal and K_j is real, then it follows by [35, VII. Theorem 3.8] that $q(K_{j+1}) = 2$, because $K_{j+1} = K_j(\sqrt{-1})$. Now, if K_j is nonreal, then $q(K_{j+1}) \leq 2$, by [35, Corollary 3.10]. Therefore, we can conclude that $q(K_r) \leq 2$, because K_r is nonreal. It follows by [35, VIII. Corollary 5.12] that $q(K_r) = 2$. Now, since the extension K_r/L is odd, we have an inclusion $L^\times/L^{\times 2} \to L'^\times/L'^{\times 2}$ and whereby $q(L) \leq q(L') \leq 2$. Since L/K is a finite extension, we use [35, VIII. Corollary 5.12] in order to conclude that $q(L) = 2$.

The proof concludes by proving the existence of a finite real extension K'/K together with a tower of quadratic extensions of K' with the above mentioned properties. For this, let F be the normal closure of L/K. Let $G = \mathsf{Gal}(F/K)$ and let $G' = \mathsf{Gal}(F/L)$. Let $r, r', q, q' \in \mathbb{N}$ be such that $|G| = 2^r q$ and $|G'| = 2^{r'} q'$, where q and q' are odd. Let H be a 2-Sylow subgroup of G'. Since H is a 2-subgroup of G, it follows by [37, Chap. I. Theorem 6.4] that there exists a 2-Sylow subgroup A of G containing H. Let $L' = F^H$, the fixed field of H in F, and let $K' = F^A$, the fixed field of A in F. Hence K'/K and L'/L are field extensions of odd degree both contained in F. Since G is a finite group, H is contained in a maximal proper subgroup of A, which is of index 2, by [14, Chap. 6. Theorem 1, (5)]. Repeating this same argument for this maximal proper subgroup, it can be seen that we can construct a sequence of subgroups $H = H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_d = A$, for some $d \in \mathbb{N}$ such that H_{i+1}/H_i is of order 2 for $i = 1, \dots, d$. By the Fundamental Theorem of Galois Theory (see [14, Chap. 14. Theorem 14]), there exists a finite tower of fields $K' = K_0' \subseteq K_1' \subseteq K_2' \subseteq \ldots \subseteq K_d' = L'$ where

K_i'/K_{i+1} is a quadratic extension for $1 \leq i \leq d$. Finally, since K'/K is odd, by [35, VIII. Proposition 2.2] we obtain that K' is real. □

Theorem 2.3.9. *Let K be a hereditarily pythagorean field admiting exactly two orderings. Let F/K be a function field in one variable. Then $p(F) \leq 4$.*

Proof. Let $L = K(\sqrt{-1})$. Let L'/L be a finite extension. Then L' is nonreal, and it follows by Theorem 2.3.8 that $q(L') = 2$. Therefore, by [35, XI. Theorem 6.4], every quadratic form over L' of dimension larger than 2 is isotropic, and in particular every 2-fold Pfister form is isotropic. Thus $I^2L' = 0$, by Theorem 2.1.8. Let F/K be a function field in one variable and let $F' = F(\sqrt{-1})$. Since $F'/K(\sqrt{-1})$ is a function field in one variable, we have that $I^3F' = 0$, by Theorem 2.1.12. The fact that $I^3F' = 0$ is equivalent to saying that every 3-fold Pfister form over F' is hyperbolic, by Theorem 2.1.8 and Theorem 2.1.6, and thus equivalent to say that every 2-fold Pfister form is universal, by Theorem 2.1.9. Therefore $\mathsf{S}(F) = \mathsf{S}_4(F)$ by [35, XI. Corollary 4.9], whereby $p(F) \leq 4$. □

Items 4 and 5 in Theorem 2.2.5 give us a hint that there might exist a general relation between $p(K)$ and $p(K(X))$. However, we do not even know whether the finiteness of $p(K)$ implies that $p(K(X))$ is finite whenever K is real. If K is real field and there exists $d \in \mathbb{N}$ with $p(L) \leq d$ for all finite real extensions L/K, then we know a bound for $p(K(X))$ as follows.

Theorem 2.3.10 (Pfister, Becher-Van Geel)**.** *Let $n \in \mathbb{N}$, and let K be a real field. Then the following are equivalent:*

(1) $p(K(X)) \leq 2^{n+1}$.

(2) $p(L) < 2^{n+1}$ *for all finite real extensions* L/K.

(3) $s(L) \leq 2^n$ *for all finite nonreal extensions* L/K.

Proof. For the equivalence (2) ⇔ (3); see [49, Satz 2] and [35, XI. 3]. For the other equivalences; see [9, Theorem 3.3]. □

Assume that K is real. It was shown by E. Becker in [8, Chap. III, Theorem 4] that $p(K(X)) = 2$ if and only if K is hereditarily pythagorean.

For $f \in K[X]$, we say that a root α of f is real or nonreal, respectively, if the field $K[\alpha]$ has the corresponding property.

Lemma 2.3.11. *Let K be a hereditarily pythagorean field. Let f be a monic irreducible polynomial in $K[X]$ with only nonreal roots. Then there exist $h_1, h_2 \in K[X]$ such that $f = h_1^2 + h_2^2$ with $\deg h_1 > \deg h_2$. Moreover, if w is a valuation on $K(X)$ such that $w(f) > 2w(h_1) = 2w(h_2)$, then $-1 \in \kappa_w^{\times 2}$.*

Proof. Set $K' := K[X]/(f)$. Then K' is a finite nonreal extension of K, whence $\sqrt{-1} \in K'$, by Theorem 2.3.4, and hence 2 divides $[K' : K] = \deg f$. Let $d \in \mathbb{N}$ be such that $\deg f = 2d$. Thus, we can write

$$f = (X^d + \alpha_{d-1}X^{d-1} + \cdots + \alpha_0)(X^d + \sigma(\alpha_{d-1})X^{d-1} + \cdots + \sigma(\alpha_0)),$$

where σ is the nontrivial K-automorphism of $K(\sqrt{-1})$ and where $\alpha_i = a_i + b_i\sqrt{-1}$ with $a_i, b_i \in K$ for $0 \leq i \leq d$. Let $h_1 = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0$ and let $h_2 = b_{d-1}X^{d-1} + \cdots + b_0$. Let $N : K(\sqrt{-1})(X) \to K(X)$ be the norm map of $K(\sqrt{-1})(X)/K(X)$. Hence $f = N(h_1 + \sqrt{-1}h_2) = h_1^2 + h_2^2$, and $\deg h_1 > \deg h_2$. Let w be a valuation on $K(X)$. If $w(f) > 2w(h_1) = 2w(h_2)$, then we have that $(h_1h_2^{-1})^2 + 1 = fh_2^{-2} \in \mathfrak{m}_w$, and hence

$$0 = \overline{fh_2^{-2}} = \left(\frac{\overline{h_1}}{\overline{h_2}}\right)^2 + \overline{1}$$

in κ_w. Therefore $-1 \in \kappa_w^{\times 2}$. □

For an example of a real pythagorean field which is not hereditarily pythagorean; see [48, Example 7.1.11]. The field K is called *hereditarily euclidean* if K is real and every finite real extension of K is euclidean.

Proposition 2.3.12. *Let K be a hereditarily pythagorean field. Then K is hereditarily euclidean if and only if it allows only one ordering.*

Proof. By definition, if K is hereditarily euclidean, then K is uniquely ordered. For the other implication, we consider a finite real extension L/K. If K is uniquely ordered, then L has exactly one ordering, by [10, Proposition 3.9]. Since K is hereditarily pythagorean, we have that L is pythagorean. This shows that K is hereditarily euclidean. □

Hereditarily euclidean fields were studied by R. Elman and A. R. Wadsworth in [18], from which the following result originates.

Proposition 2.3.13. *Let K be a real field. The following are equivalent.*

(1) K is hereditarily euclidean.

(2) $p(F) = 2$ for every function field in one variable F/K.

Proof. For the implication (2) ⇒ (1); see [9, Corollary 4.6]. The implication (1) ⇒ (2) was shown by Elman-Wadsworth; see [9, Theorem 4.5]. □

For a positive integer n, the field of iterated Laurent series $\mathbb{R}((t_1))\ldots((t_n))$ is an example of a hereditarily pythagorean field which is not hereditarily euclidean.

2.4 The Kaplansky radical

We recall here the *Kaplansky radical of* K introduced by C. Cordes in [12]. By this we refer to the set

$$R(K) = \bigcap_{a \in K^\times} D_K\langle 1, -a\rangle .$$

Since $a \in D_K\langle 1, -b\rangle$ for all $b \in K^\times$ is equivalent to saying that $D_K\langle 1, -a\rangle = K^\times$, we can describe $R(K)$ as the set of all $a \in K^\times$ such that $N : K(\sqrt{a})^\times \to K^\times$, the group homomorphism given by the norm map, is surjective.

Proposition 2.4.1. *Let K be a field. Then $R(K)$ is a subgroup of $K^\times$ such that*

$$K^{\times 2} \subseteq R(K) \subseteq \mathsf{S}_2(K).$$

Proof. Let $a \in K^\times$, and let $N : K(\sqrt{a})^\times \to K^\times$, be the group homomorphism given by the norm map. Using the fact that N is multiplicative and $N(K(\sqrt{a})^\times) = D_K\langle 1, -a\rangle$, we have that $D_K\langle 1, -a\rangle$ is subgroup of $K^\times$. In particular $R(K)$ is a subgroup of $K^\times$. Clearly $K^{\times 2} \subseteq R(K)$, and since $D_K\langle 1, 1\rangle = \mathsf{S}_2(K)$, we have $R(K) \subseteq \mathsf{S}_2(K)$. Hence $K^{\times 2} \subseteq R(K) \subseteq \mathsf{S}_2(K) \subseteq K^\times$. □

We say that K is *radical-free* if $R(K) = K^{\times 2}$. In the following, we recall some known examples of fields with $R(K) = K^\times$ or which are radical-free.

Examples 2.4.2. (1) Every pythagorean field is radical-free.

(2) Assume that K is nonreal with $q(K) = 2$ and $-1 \notin K^{\times 2}$. It is clear that $s(K) = 2$. Hence $-1 \in R(K)$, because $D_K\langle 1, 1\rangle = \mathsf{S}_2(K) = K^\times$, whereby $R(K) = K^\times$.

(3) We claim that $\mathbb{Q}$ is radical-free. For a prime $p \in \mathbb{N}$, let v_p be the p-adic valuation on $\mathbb{Q}$, and let $\mathbb{Q}_p$ denote the completion of $\mathbb{Q}$ with respect to v_p. Let $\mathbb{Z}^*$ be the set of square-free integers. Note that $\mathbb{Q}^\times = 2\mathbb{Q}^{\times 2} \cup \bigcup_{x \in \mathbb{Z}^* \setminus \{2\}} x\mathbb{Q}^{\times 2}$. We first show that $2 \notin R(\mathbb{Q})$. Using the fact that the quadratic form $\langle 1, -2, 11\rangle$ is not isotropic over $\mathbb{Q}_{11}$, because 2 is not a square in $\mathbb{F}_{11}$, we have that $\langle 1, -2, 11\rangle$ is anisotropic over $\mathbb{Q}$, by [35, VI. 3.1]. Hence $-11 \notin D_{\mathbb{Q}}\langle 1, -2\rangle$, and therefore $2 \notin R(\mathbb{Q})$.

Assume that $\mathbb{Q}^{\times 2} \subsetneq R(\mathbb{Q})$. Since $2 \notin R(\mathbb{Q})$, there exists $x \in \mathbb{Z}^* \setminus \{2\} \cap R(\mathbb{Q})$ and an odd prime number p dividing x. Since $\mathbb{F}_p^\times \neq \mathbb{F}_p^{\times 2}$, we can consider some $q \in \mathbb{Z}$ such that $\overline{q} \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$. Since $D_{\mathbb{Q}}\langle 1, -p\rangle = \mathbb{Q}^\times$, there exist $a, b \in \mathbb{Q}$ such that $q = a^2 - xb^2$. Now we have that $v_p(q) = 0$, which implies that $0 = v_p(a^2) < v_p(xb^2)$, whereby $\overline{q} = \overline{a}^2$ in $\mathbb{F}_p$, contradiction. Therefore $\mathbb{Q}^{\times 2} = R(\mathbb{Q})$.

4. If K is a field such that every quadratic form of dimension two is universal, then $R(K) = K^\times$ (and in such a case K is nonreal). In particular, if K is a finite field, then $R(K) = K^\times$, by [35, Proposition 3.4, II].

5. Let K be a field which is either algebraically closed or real closed. Let F/K be a function field in one variable. Then it follows by [35, Theorem of Tsen-Lang. Pag. 368] that, every quadratic form of dimension 2 is universal. Hence $R(F)F^\times$.

6. Let $F = K(X)$, the rational function field in one variable X over K. Assuming that $K(\sqrt{-1})$ is not quadratically closed, it was shown in [6, Proposition 3.4] that $R(F) = F^{\times 2}$.

A field K is called *hereditarily quadratically closed* if $L^\times = L^{\times 2}$ for every finite field extension L/K. The following generalization of Theorem 2.3.13 was shown by Elman-Wadsworth.

Proposition 2.4.3. *Assume that K is either hereditarily euclidean or hereditarily quadratically closed. Let F/K be a function field in one variable. Then*

$$R(F) = \mathsf{S}_2(F) = \mathsf{S}(F).$$

Proof. It was shown in [18, Proposition, (3)] that I^2F is torsion free. Then the proof follows by [35, Proposition 6.26]. □

Chapter 3

Arithmetic curves

In Chapter 1 we considered valuations on a function field extending a fixed valuation on the base field. In general, it is difficult to keep track of all those valuation extensions. If the base field valuation is discrete of rank one, however, one can keep track of the valuation extensions (at least the residually transcendental ones) by means of arithmetic-geometric models of the function field.

In this chapter, we will use standard definitions and notations in the theory of arithmetic geometry that can be found in [38]. Let X be a noetherian scheme. We denote by $\mathcal{O}_X$ its structure sheaf. For $x \in X$, we denote by $\mathcal{O}_{X,x}$ the stalk of $\mathcal{O}_X$ at x. We recall that $\mathcal{O}_{X,x}$ is a local ring. We denote by $\mathfrak{m}_{X,x}$ its maximal ideal and by $\kappa(x) = \mathcal{O}_{X,x}/\mathfrak{m}_{X,x}$ its residue field. A *prime divisor on* X is an irreducible closed subset of X of codimension one. We denote by $\mathsf{Div}(X)$ the free abelian group generated by the prime divisors of X. If X is integral and ξ is its generic point, then $\mathcal{O}_{X,\xi}$ is a field. We denote it by $\kappa(X)$ and call it *the function field of* X. If moreover X is a R-scheme of finite type, for some Dedekind domain R, then $\kappa(X)$ is a finitely generated field extension of K, where K is the fraction field of R.

In Section 3.1 we define the notion of arithmetic genus of a curve and describe its relation with the genus of its function field in the case where the curve is integral. In Section 3.2 we define a graph associated to a fibered surface and we show that its Betti number is bounded by the genus of the generic fiber. In Section 3.3 we use Tate's algorithm to describe the reduction type of certain elliptic curves. In Section 3.4 we construct the minimal regular model of a curve explicitly using blowing ups.

3.1 The arithmetic genus

In the following sections of the current chapter, T denotes a discrete valuation ring with perfect fraction field K, maximal ideal $\mathfrak{m}$ and residue field k. We fix an algebraic closure $\bar{k}$ of k.

In Section 1.3 we defined the genus of a function field in one variable F/K. In the case where K is relatively algebraically closed in F, we could take this as the genus of the unique corresponding normal projective curve C. However, in the case where K admits a $\mathbb{Z}$-valuation, we will also consider the reduction of C, which is a connected projective curve over the residue field k, but this curve

does not have to be regular, nor integral, nor reduced, so we need to extend the definition of the genus to arbitrary projective curves over a field.

In the following discussion of the genus of a curve over K we only need the field K and are not taking reference to $T, \mathfrak{m}$ or k. Let X be a projective curve over K, that is, a K-scheme admitting a closed K-immersion into $\mathbb{P}^n_K$ for some $n \in \mathbb{N}$ whose irreducible components are of dimension one. We sometimes write X/K to indicate that the curve X is given and considered over K. Let $\mathcal{M}$ be a coherent $\mathcal{O}_X$-module and $i \in \mathbb{N}$. We denote by $H^i(X, \mathcal{M})$ the i-th Čech cohomology; see [38, Definition 5.2.10]. We recall from [38, Theorem 5.3.2] that, as a K-vector space, $H^i(X, \mathcal{M})$ is finite-dimensional. In particular $H^0(X, \mathcal{M}) = \mathcal{M}(X)$; see [38, Proposition 5.2.6]. We define the *arithmetic genus of* X as

$$\mathfrak{g}(X/K) = 1 - \dim_K H^0_K(X, \mathcal{O}_X) + \dim_K H^1_K(X, \mathcal{O}_X).$$

We recall that, if X is an integral curve, then $\kappa(X)/K$ is a function field in one variable, and conversely for every function field F/K in one variable, there exists a unique integral regular projective curve X over K such that $\kappa(X) = F$; see [38, Proposition 7.3.13] and [38, Remark 7.3.14].

Proposition 3.1.1. *Let X/K be a geometrically integral projective curve. Then*

$$g(\kappa(X)/K) \leq \mathfrak{g}(X/K),$$

and the equality holds if and only if X is regular.

Proof. See [3, Proposition 2.1]. □

For a ring A, let $\mathsf{Nil}(A)$ be the nilradical of A. Let X be a projective curve over K. Let $\mathcal{N}_X$ denote the sheaf of ideals of $\mathcal{O}_X$ given by $\mathcal{N}_X(U) = \mathsf{Nil}(\mathcal{O}_X(U))$ for every open subset U of X. We define the sheaf $\mathcal{O}_X/\mathcal{N}_X$ as the sheafification of the presheaf given by $\mathcal{O}_X(U)/\mathcal{N}_X(U)$ for every open subset U of X. Note that $\mathcal{N}_X$ and $\mathcal{O}_X/\mathcal{N}_X$ are coherent $\mathcal{O}_X$-modules. We denote by X_{red} the projective curve $(X, \mathcal{O}_X/\mathcal{N}_X)$. Note that X and X_{red} are isomorphic as topological spaces, but not necessarily as schemes. In fact $\mathcal{O}_{X_{\mathsf{red}}}$ is a sheaf of reduced rings.

Proposition 3.1.2. *Let X/K be a projective curve such that $\mathcal{O}_X(X) = K$. Then*

$$\mathfrak{g}(X_{\mathsf{red}}/K) \leq \mathfrak{g}(X/K).$$

Proof. Let

$$0 \to \mathcal{N}_X \to \mathcal{O}_X \to \mathcal{O}_X/\mathcal{N}_X \to 0$$

be the exact sequence of $\mathcal{O}_X$-modules given by the natural homomorphisms

$$\mathcal{N}(U) \to \mathcal{O}_X(U) \to (\mathcal{O}_X/\mathcal{N}_X)(U)$$

for every open subset U of X. It follows by [38, Proposition 5.2.15] and by [38, Proposition 5.2.24], that the connecting homomorphism of cohomology $\delta : (\mathcal{O}_X/\mathcal{N}_X)(X) \mapsto H^1(X, \mathcal{N}_X)$ yields an exact

sequence of $\mathcal{O}_X(X)$-modules

$$0 \longrightarrow \mathcal{N}_X(X) \longrightarrow \mathcal{O}_X(X) \longrightarrow (\mathcal{O}_X/\mathcal{N})(X)$$
$$H^1(X,\mathcal{N}_X) \longrightarrow H^1(X,\mathcal{O}_X) \longrightarrow H^1(X,\mathcal{O}_X/\mathcal{N}_X) \longrightarrow 0$$

Since $\mathcal{N}_X(X) = \mathsf{Nil}(K) = 0$ and $\mathcal{O}_X(X) = K$, we have

$$\dim_K H^1(X,\mathcal{O}_X) - \dim_K H^1(X,\mathcal{N}_X) = 1 - \dim_K(\mathcal{O}_X/\mathcal{N}_X)(X) + \dim_K H^1(X,\mathcal{O}_X/\mathcal{N}_X),$$

and hence $\mathfrak{g}(X/K) - \dim_K H^1(X,\mathcal{N}_K) = \mathfrak{g}(X_{\mathsf{red}},K)$. Therefore $\mathfrak{g}(X_{\mathsf{red}}/K) \leq \mathfrak{g}(X/K)$. □

We call a 2-dimensional integral flat and projective T-scheme $\mathcal{C}$ a *fibered surface over* T. Let $\mathcal{C}$ be a fibered surface over T. The scheme $\mathcal{C}_k = \mathcal{C} \times_T k$ is called the *special fiber of* $\mathcal{C}$, and we call $\mathcal{C}_K = \mathcal{C} \times_T K$ the *generic fiber of* $\mathcal{C}$. By [38, Lemma 8.3.3] the special fiber $\mathcal{C}_k$ is a projective curve over k, and $\mathcal{C}_K$ is an integral projective curve over K. Moreover, if $\mathcal{C}$ is normal, then the generic fiber $\mathcal{C}_K$ is normal. We recall that the projection $\mathcal{C}_K \to \mathcal{C}$ (resp. $\mathcal{C}_k \to \mathcal{C}$) is an open (resp. closed) immersion of T-schemes and that $\mathcal{C}$ is the disjoint union of their images. Note that the generic point η of $\mathcal{C}$ is in the generic fiber $\mathcal{C}_K$, whereby $\kappa(\mathcal{C}) = \kappa(\mathcal{C}_K)$. Given a function field in one variable F/K, any normal (resp. regular) fibered surface over T whose function field is K-isomorphic to F is called a *model* (resp. *regular model*) *of* F/T. Similarly, given an integral curve C/K, any normal (resp. regular) fibered surface over T whose generic fiber $\mathcal{C}_K$ is K-isomorphic to C is called a *model* (resp. *regular model*) *of* C/T.

Lemma 3.1.3. *Let F/K be a regular function field in one variable. Then there exists a regular model of F/T.*

Proof. By [38, Proposition 7.3.13, (a)], there exists a regular projective curve C over K such that $F = \kappa(C)$. Moreover, since K is perfect, by [38, Proposition 4.3.30] we have that C is smooth over K. Then, by [38, Proposition 10.1.8] we can find a regular fibered surface $\mathcal{C}$ over T such that its function field is K-isomorphic to $\kappa(C)$, whereby to F. Hence $\mathcal{C}$ is a regular model of F/T. □

Proposition 3.1.4. *Let F/K be a regular function field in one variable. Let $\mathcal{C}$ be a regular model of F/T. Assume that $H^0(\mathcal{C}_k,\mathcal{O}_{\mathcal{C}_k}) = k$. Then*

$$\mathfrak{g}((\mathcal{C}_k)_{\mathsf{red}}/k) \leq g(F/K).$$

Proof. We have that F is the function field of a geometrically connected regular projective curve C over K, by [3, Lemma 2.5]. Hence C is geometrically integral. By Theorem 3.1.1, we have $g(F/K) = \mathfrak{g}(C/K)$. Let $\mathcal{C}$ be a regular model of F/T. Then $C = \mathcal{C}_K$. By [38, Corollary 8.3.6], we have $\mathfrak{g}(\mathcal{C}_k/k) = \mathfrak{g}(\mathcal{C}_K/K)$, whereby $g(F/K) = \mathfrak{g}(\mathcal{C}_k/k)$. Since $H^0(\mathcal{C}_k,\mathcal{O}_{\mathcal{C}_k}) = \mathcal{O}_{\mathcal{C}_k}(\mathcal{C}_k) = k$, we obtain by Theorem 3.1.2 that $\mathfrak{g}((\mathcal{C}_k)_{\mathsf{red}}/k) \leq g(F/K)$. □

Remark 3.1.5. It seems that the hypothesis $H^0(\mathcal{C}_k, \mathcal{O}_{\mathcal{C}_k}) = k$ in Theorem 3.1.4 is automatically satisfied when assuming $\mathsf{char}(k) = 0$, by [50, Proposition 6.4.2].

3.2 Reduction of curves

In this section, we associate to a fibered surface $\mathcal{C}$ a reduction graph $\mathcal{G}(\mathcal{C})$ following [25], and we bound its Betti number in terms of the genus of its generic fiber $\mathcal{C}_K$. For this, we compute it with a different reduction graph $\mathcal{B}(\mathcal{C})$ associated to $\mathcal{C}$, introduced in [38, Definition 10.1.48], whose Betti number is known to be bounded by the genus; see Theorem 3.2.1. The Betti number of $\mathcal{G}(\mathcal{C})$ will be used in Section 4.4 to bound the size of the Kaplansky radical of a function field in one variable F/K in terms of the genus of F/K.

Let $\mathcal{C}$ be a fibered surface over T. We denote by $\mathcal{V}$ the of irreducible components of $\mathcal{C}_k$. We define the graph $\mathcal{B}(\mathcal{C})$ associated to $\mathcal{C}$ as follows:

(1) The set $\mathcal{V}$ is the set of vertices of $\mathcal{B}(\mathcal{C})$.

(2) For $\Gamma_1, \Gamma_2 \in \mathcal{V}$, we assign $\Gamma_1 \cdot \Gamma_2$ distinct edges between Γ_1 and Γ_2, where $\Gamma_1 \cdot \Gamma_2$ is the intersection number of Γ_1 and Γ_2 as defined in [38, Definition 9.1.15]. We denote by $\mathcal{E}$ the set of edges of $\mathcal{B}(\mathcal{C})$.

We denote by $\beta(\mathcal{C})$ the *Betti number* of the graph $\mathcal{B}(\mathcal{C})$, which is given by the formula

$$\beta(\mathcal{C}) = |\mathcal{E}| - |\mathcal{V}| + 1.$$

Proposition 3.2.1. *Let $\mathcal{C}$ be a regular fibered surface over T. Then*

$$\beta(\mathcal{C}) \leq \mathfrak{g}((\mathcal{C}_k)_{\mathsf{red}}/k).$$

Proof. See [38, Proposition 10.1.51]. □

Corollary 3.2.2. *Let F/K be a regular function field in one variable. Let $\mathcal{C}$ be a regular model of F/T. Assume that $H^0(\mathcal{C}_k, \mathcal{O}_{\mathcal{C}_k}) = k$. Then*

$$\beta(\mathcal{C}) \leq g(F/K).$$

Proof. It follows by Theorem 3.2.1 that $\beta(\mathcal{C}) \leq \mathfrak{g}((\mathcal{C}_k)_{\mathsf{red}}/k)$, and by Theorem 3.1.4 we have $\mathfrak{g}((\mathcal{C}_k)_{\mathsf{red}}/k) \leq g(F/K)$. □

In the sequel, X denotes a noetherian integral regular scheme. We denote by X^1 the set of all points of codimension one and by X^0 the set of all closed points. Let $D \in \mathsf{Div}(X)$. Since every prime divisor on X is given by the Zariski closure $\overline{\{x\}}$ of a point x of codimension one of X, we may write

$$D = \sum_{x \in X^1} n_x(D)\overline{\{x\}}$$

where $n_x(D) \neq 0$ for only finitely many $x \in X^1$. Let $U \subseteq X$ be an open subscheme. Then $U^1 \subseteq X^1$, and we thus obtain a natural projection $\mathsf{Div}(X) \to \mathsf{Div}(U)$ which is a group homomorphism.

We set $F = \kappa(X)$. Let $x \in X^1$. Since X is regular, $\mathcal{O}_{X,x}$ is a noetherian regular local domain of Krull dimension one, and in particular it is normal, whereby $\mathcal{O}_{X,x}$ is a discrete valuation ring of F; see [14, Chap. 16. Theorem 7]. We call v_x the $\mathbb{Z}$-valuation on F such that $\mathcal{O}_{v_x} = \mathcal{O}_{X,x}$. We set $X_x = \mathsf{Spec}(\mathcal{O}_{X,x})$.

Proposition 3.2.3. *Let X be a noetherian integral regular scheme. Let $f \in \kappa(X)$. Then $v_x(f) \neq 0$ for only finitely many $x \in X^1$.*

Proof. See for example [26, Chap. II. Lemma 6.1]. □

For $f \in F^\times$, we set

$$(f)_X = \sum_{x \in X^1} v_x(f)\overline{\{x\}}.$$

By Theorem 3.2.3 we have $(f)_X \in \mathsf{Div}(X)$, and it is called the *principal divisor given by f*.

Proposition 3.2.4. *Let X be a noetherian integral regular scheme. Let $x \in X$ and $D \in \mathsf{Div}(X_x)$. Then D is principal.*

Proof. Since $\mathcal{O}_{X,x}$ is regular and hence a unique factorization domain, by [2, Theorem 5], we have that every height-one prime ideal is principal, whereby every divisor in $\mathsf{Div}(X_x)$ is principal. □

For $D \in \mathsf{Div}(X)$ and $x \in X$, we say that x lies on D if $x \in \Gamma$ for some divisor Γ in the support of D. Let $x \in X^0$ lying on a divisor $D \in \mathsf{Div}(X)$. Let U be an open affine neighborhood of x. Let $\mathfrak{m}$ be the prime ideal of $\mathcal{O}_X(U)$ corresponding to x. Since $\mathcal{O}_{X,x}$ is the localization of of $\mathcal{O}_X(U)$ at $\mathfrak{m}$, we have a bijection between the set of prime ideals of $\mathcal{O}_X(U)$ contained in $\mathfrak{m}$ and the set of prime ideals of $\mathcal{O}_{X,x}$. Thus, we have a group homomorphism $\pi_x : \mathsf{Div}(X) \to \mathsf{Div}(X_x)$, defined on the level of prime divisors by $\Gamma \mapsto 0$ if $x \notin \Gamma$, and otherwise $\Gamma \mapsto \mathfrak{p}\mathcal{O}_{X,x}$, where $\mathfrak{p} \subseteq \mathcal{O}_X(U)$ is the prime ideal corresponding to $\Gamma \cap U$. Hence, by Theorem 3.2.4 for any $D \in \mathsf{Div}(X)$, there exists some $f \in F^\times$ such that $\pi_x(D) = (f)_{X_x}$.

Let $\mathcal{C}$ be a regular fibered surface over T. Let $D \in \mathsf{Div}(\mathcal{C})$ and let $x \in \mathcal{C}^0$ be a point lying on D. We say that D has *normal crossings at x* if there exist prime elements $p_1, p_2 \in \mathcal{O}_{\mathcal{C},x}$ generating $\mathfrak{m}_{\mathcal{C},x}$ and such that $\pi_x(D) = (p_1^{n_1} p_2^{n_2})_{\mathcal{C}_x}$ for some $n_1, n_2 \in \mathbb{Z}$. We say that D is a *normal crossing divisor* if D has normal crossings at every closed point $x \in \mathcal{C}$.

Let Γ be an irreducible component of $\mathcal{C}_k$, and let η be its generic point. Then $\mathcal{O}_{\mathcal{C},\eta}$ is a discrete valuation ring extending T. Let v be a $\mathbb{Z}$-valuation on $\kappa(\mathcal{C})$ such that $\mathcal{O}_v = \mathcal{O}_{\mathcal{C},\eta}$. The ramification index $e(v/v|_K)$ is called the *multiplicity of* Γ in $\mathcal{C}_k$. We associate to $\mathcal{C}_k$ the divisor:

$$\sum_{i=1}^{r} n_i \Gamma_i,$$

on $\mathcal{C}$, where $\Gamma_1, \ldots, \Gamma_r$ are the irreducible components of $\mathcal{C}_k$, and $n_1, \ldots, n_r$ are the respective multiplicities.

Let $\mathcal{C}$ be a regular fibered surface over T. We say that $\mathcal{C}$ *has normal crossings* if $\mathcal{C}_k$, as a divisor on $\mathcal{C}$, has normal crossings.

Proposition 3.2.5. *Assume that k is perfect. Let $\mathcal{C}$ be a regular fibered surface over T with normal crossings property. Let T' be an unramified extension of T with residue field $\bar{k}$. Then $\mathcal{C}' = \mathcal{C} \times_T T'$ is a regular fibered surface over T' with normal crossings property.*

Proof. Since $\mathcal{C}$ is a flat projective scheme over T, we have that $\mathcal{C}'$ is a flat projective scheme over T', by [38, Corollary 3.3.32] and [38, Proposition 4.3.3, (e)]. We have that both $\mathcal{C}'_{\bar{k}} = \mathcal{C}_k \times_k \bar{k}$ and $\mathcal{C}'_{K'} = \mathcal{C}_K \times_K K'$ are curves over $\bar{k}$ and K', by [38, Proposition 3.2.7] and thus $\dim(\mathcal{C}') = 2$. We claim that $\mathcal{C}'$ is regular. By [38, Corollary 4.2.17] it is enough to show regularity only for closed points. Let $x \in \mathcal{C}^0$. Since T' is an unramified extension of T, the second projection $p : \mathcal{C}' \to \mathcal{C}$ is unramified by [38, Proposition 4.3.22]. Hence $\mathfrak{m}_{\mathcal{C}',x} = \mathfrak{m}_{\mathcal{C},p(x)}\mathcal{O}_{\mathcal{C}',x}$, whereby the regularity of $\mathcal{O}_{\mathcal{C},p(x)}$, implies the regularity of $\mathcal{O}_{\mathcal{C}',x}$. Therefore $\mathcal{C}'$ is regular. Let $t \in T$ be an uniformizer. Since the closed subscheme $\mathcal{C}_k$ is given by the sheaf of ideals generated by t in $\mathcal{O}_{\mathcal{C}}$, we have that by the normal crossings property that $t = p_1^{n_1} p_2^{n_2}$, for some $n_1, n_2 \in \mathbb{N}$ and irreducible elements $p_1, p_2 \in \mathcal{O}_{\mathcal{C},p(x)}$ that generate $\mathfrak{m}_{\mathcal{C},p(x)}$. Since t is also a uniformizer of T', we have that $\mathcal{C}'_{\bar{k}}$ is the closed subscheme of $\mathcal{C}'$ defined by the sheaf of ideal generated by t in $\mathcal{O}_{\mathcal{C}'}$. Considering the equality $t = p_1^{n_1} p_2^{n_2}$ in $\mathcal{O}_{\mathcal{C}',x}$, and the fact that p_1 and p_2 also generate the ideal $\mathfrak{m}_{\mathcal{C}',x}$, we can conclude that $\mathcal{C}'_{\bar{k}}$ has normal crossings at x. Therefore $\mathcal{C}'$ has normal crossings property. □

Let $\mathcal{C}$ be a fibered surface over T. Let Γ be an irreducible component of $\mathcal{C}_k$ and $x \in \Gamma$. Let $\mathfrak{p}$ be the prime ideal of height one of $\mathcal{O}_{\mathcal{C},x}$ corresponding to the preimage of Γ under the morphism $\mathcal{C}_x \to \mathcal{C}$. By Theorem 3.2.4 there exists $f \in \kappa(\mathcal{C})^\times$ such that $\mathfrak{p} = (f)$. Let $\widehat{\mathcal{O}}_{\mathcal{C},x}$ be the completion of $\mathcal{O}_{\mathcal{C},x}$ with respect to $\mathfrak{m}_{\mathcal{C},x}$; see [38, Pag. 18]. An irreducible factor of f in $\widehat{\mathcal{O}}_{\mathcal{C},x}$ is called a *branch of* Γ *at* x.

In [25, Section 6], the authors define a bipartite reduction graph $\mathcal{G}(\mathcal{C})$ associated to $\mathcal{C}$ as follows. Let $\mathcal{V}$ be the set of irreducible components of $\mathcal{C}_k$. Let $\mathcal{P}$ be the set of all singularities on $(\mathcal{C}_k)_{\mathsf{red}}$.

(1) The set $\mathcal{V} \cup \mathcal{P}$ is the set of vertices of $\mathcal{G}(\mathcal{C})$.

(2) For $\Gamma \in \mathcal{V}$ and $p \in \mathcal{P}$, the edges of $\mathcal{G}(\mathcal{C})$ which connect p and Γ correspond to the branches on Γ at p.

Let $\mathcal{E}$ be the set of edges of $\mathcal{G}(\mathcal{C})$. We denote by $b(\mathcal{C})$ the *Betti number* of the graph $\mathcal{G}(\mathcal{C})$ given by the formula

$$b(\mathcal{C}) = |\mathcal{E}| - |\mathcal{V} \cup \mathcal{P}| + 1.$$

Proposition 3.2.6. *Let $\mathcal{C}$ be a regular fibered surface over T. Let Γ be an irreducible component of $\mathcal{C}_k$, and let $p \in \Gamma$ be a closed point such that Γ is regular at p. Then there is only one branch of Γ at p.*

Proof. Let $f \in \mathcal{O}_{\mathcal{C},p}$ be a generator of the prime ideal of $\mathcal{O}_{\mathcal{C},p}$ corresponding to Γ; see Theorem 3.2.4. Since $\mathcal{O}_{\mathcal{C},p}$ is regular local and Γ is regular at p, there exists $g \in \mathcal{O}_{\mathcal{C},p}$ such that $\mathfrak{m}_{\mathcal{C},p} = (f, g)$. We have that $\mathfrak{m}_{\mathcal{C},p}\widehat{\mathcal{O}}_{\mathcal{C},p}$ is the maximal ideal of $\widehat{\mathcal{O}}_{\mathcal{C},p}$; see for example [38, Thereom 1.3.16]. By [38, Lemma 4.2.26], $\widehat{\mathcal{O}}_{\mathcal{C},p}$ is regular, and by [38, Corollary 4.2.15] the quotient $\widehat{\mathcal{O}}_{\mathcal{C},p}/(g)$, is a regular local ring of dimension 1, that is, a discrete valuation ring. Moreover, $f + (g)$ is a generator of the maximal ideal of $\widehat{\mathcal{O}}_{\mathcal{C},p}/(g)$, which implies that f is an irreducible element of $\widehat{\mathcal{O}}_{\mathcal{C},p}$, and hence there is only one branch of Γ at p. □

Proposition 3.2.7. *Let $\mathcal{C}$ be a regular fibered surface over T with normal crossings property. Let $\mathcal{V}$ be the set of irreducible components of $\mathcal{C}_k$. Let $\mathcal{P}$ be the set of closed points of $\mathcal{C}_k$ at which distinct irreducible components of $\mathcal{C}_k$ meet. Then $b(\mathcal{C}) = |\mathcal{P}| - |\mathcal{V}| + 1$.*

Proof. By normal crossings, every $\Gamma \in \mathcal{V}$ is regular, by [38, Proposition 9.1.8]. Then for every $p \in \mathcal{P}$, there exist exactly two edges, by Theorem 3.2.6. Hence $|\mathcal{E}| = 2|\mathcal{P}|$. Therefore $b(\mathcal{C}) = |\mathcal{E}| - |\mathcal{P}| - |\mathcal{V}| + 1 = |\mathcal{P}| - |\mathcal{V}| + 1$. □

Proposition 3.2.8. *Assume that k is algebraically closed. Let $\mathcal{C}$ be a regular fibered surface over T with normal crossings. Then $b(\mathcal{C}) = \beta(\mathcal{C})$.*

Proof. Let $\mathcal{V}$ be the set of irreducible components of $\mathcal{C}_k$ and let $\mathcal{P}$ be the set of all closed points of $\mathcal{C}_k$ at which distinct irreducible components of $\mathcal{C}_k$ meet. Let $\mathcal{E}$ be the set of edges of $\mathcal{B}(\mathcal{C})$. Let $\Gamma_1, \Gamma_2 \in \mathcal{V}$ be a pair intersecting at a closed point. Then $\Gamma_1 \cdot \Gamma_2 = 1$ by [38, Proposition 9.1.8 (b), (iii)], because every point on $\mathcal{C}_k$ is rational. This implies that $|\mathcal{E}| = |\mathcal{P}|$, and hence $b(\mathcal{C}) = \beta(\mathcal{C})$, by Theorem 3.2.7. □

Proposition 3.2.9. *Let F/K be a regular function field in one variable. Let $\mathcal{C}$ be a regular model over T with normal crossings. Assume that $H^0(\mathcal{C}_k, \mathcal{O}_{\mathcal{C}_k}) = k$ and that each irreducible component of $\mathcal{C}_k$ intersects at least two other irreducible components. Then*

$$b(\mathcal{C}) \leq g(F/K).$$

Proof. By [38, Lemma 10.3.32] there exists a discrete valuation ring T' containing T such that T' is unramified over T and such that its residue field is equal to $\bar{k}$. Let $\mathcal{C}' = \mathcal{C} \times_T T'$. Let $\pi : \mathcal{C}' \to \mathcal{C}$ denote the morphism of the base change from k to $\bar{k}$. Let $\mathcal{V}$ and $\mathcal{V}'$ be the set of all irreducible components of $\mathcal{C}_k$ and $\mathcal{C}'_{\bar{k}}$, respectively. Let $\mathcal{P}$ and $\mathcal{P}'$ be the set of all closed points of $\mathcal{C}_k$ and $\mathcal{C}'_{\bar{k}}$, at which distinct irreducible components of $\mathcal{C}_k$ and $\mathcal{C}'_{\bar{k}}$ meet, respectively. Note that by Theorem 3.2.5 we have that $\mathcal{C}'_{\bar{k}}$ is a normal crossing divisor on $\mathcal{C}'$, and hence $b(\mathcal{C}') = |\mathcal{P}'| - |\mathcal{V}'| + 1$ and $b(\mathcal{C}) = |\mathcal{P}| - |\mathcal{V}| + 1$, by Theorem 3.2.7.

We claim that $b(\mathcal{C}) \leq b(\mathcal{C}')$. For this, we need to show that $|\mathcal{V}'| - |\mathcal{V}| \leq |\mathcal{P}'| - |\mathcal{P}|$. For a point $x \in \mathcal{P}$, we have that $|\pi^{-1}(x)| = [\kappa(x) : k]$ and for a curve $\Gamma \in \mathcal{V}$, we have that $|\pi^{-1}(\Gamma)| = [\ell_\Gamma : k]$, where ℓ_Γ is the relative algebraic closure of k in $\kappa(\Gamma)$. We note that, if $x \in \Gamma$, then $\ell_\Gamma \subseteq \kappa(x)$, whereby $[\kappa(x) : k] \geq [\ell_\Gamma : k]$. For $x \in \mathcal{P}$, we set $i(x) = [\kappa(x) : k]$. Since $\mathcal{C}$ has normal crossings, for $x \in \mathcal{P}$,

there exist precisely two curves $\Gamma_x, \Gamma'_x \in \mathcal{V}$ intersecting at x. In this case, we set $e_x = [\ell_{\Gamma_x} : k], e'_x = [\ell'_{\Gamma_x} : k]$. By the assumption, every vertex of $\mathcal{G}(\mathcal{C})$ has at least two edges. For $x \in \mathcal{P}$, we have that $i(x) \geq \max\{e_x, e'_x\}$, and hence we obtain that

$$\sum_{x\in\mathcal{P}}(i(x)-1) \geq \sum_{x\in\mathcal{P}}(\max\{e_x,e'_x\}-1) \geq \sum_{x\in\mathcal{P}}(\frac{1}{2}e_x-\frac{1}{2})+\sum_{x\in\mathcal{P}}(\frac{1}{2}e'_x-\frac{1}{2}).$$

Clearly $\sum_{x\in\mathcal{P}}(\frac{1}{2}e_x-\frac{1}{2})+\sum_{x\in\mathcal{P}}(\frac{1}{2}e'_x-\frac{1}{2}) \geq \sum_{\Gamma\in\mathcal{V}}([\ell_\Gamma : k]-1)$, and hence we have that $|\mathcal{V}'|-|\mathcal{V}| \leq |\mathcal{P}'|-|\mathcal{P}|$, whereby $b(\mathcal{C}) \leq b(\mathcal{C}')$.

By Theorem 3.2.8 we have that $b(\mathcal{C}')$. Furthermore, by Theorem 3.2.2 we have that $\beta(\mathcal{C}') \leq g(F/K)$, whereby $b(\mathcal{C}) \leq g(F/K)$. □

Let $\mathcal{C}$ be a regular fibered surface over T. We say that $\mathcal{C}$ is *minimal* if every birational map $\mathcal{C}' \to \mathcal{C}$ of regular fibered surfaces over T extends to a morphism. Then this is further equivalent to saying that every birational morphism $\mathcal{C}' \to \mathcal{C}$ of arithmetic surfaces over T is an isomorphism if $\mathfrak{g}(\mathcal{C}_K/K) \geq 1$; see [38, Corollary 9.3.24].

Geometrically, we can understand a minimal regular fibered surface over T as follows. Let $\mathcal{C}$ be a regular fibered surface over T. Let $D \in \mathsf{Div}(\mathcal{C})$ be a prime divisor. We set $k' = H^0(D, \mathcal{O}_D)$, which is a finite field extension of k, by [38, Corollary 3.3.21]. The divisor D is called an *exceptional divisor* if $D \simeq \mathbb{P}^1_{k'}$ and $D^2 = -[k' : k]$. An exceptional divisor is a curve on $\mathcal{C}$ such that can be contracted to a regular point; see [38, Definition 9.3.1].

Proposition 3.2.10. *Let $\mathcal{C}$ be fibered surface over T. Then $\mathcal{C}$ is minimal if and only if it does not contain an exceptional divisor.*

Proof. See [38, Theorem 9.2.2]. □

Let C/K be an integral projective curve such that $\mathfrak{g}(C/K) \geq 1$. We call a fibered surface $\mathcal{C}$ over T a *minimal regular model of* C/T if $\mathcal{C}$ is a regular model of C/T that is minimal.

Proposition 3.2.11. *Let C/K be an integral projective curve with $\mathfrak{g}(C/K) \geq 1$. Then there exists a minimal regular of C/T and it is unique.*

Proof. The existence of a minimal regular model follows by [38, Proposition 10.1.8], and it is unique up to isomorphism by definition. □

Example 3.2.12. Assume $T = \mathbb{R}[\![t]\!]$. Let $\mathcal{C} \subseteq \mathbb{A}^3_T$ be the scheme

$$\mathsf{Spec}(T[X,Y,Z]/t - XZ, Y^2 + (X^2+1)(1+Z^2)).$$

We will see in Theorem 3.4.2 that $\mathcal{C}$ is an affine chart of the minimal regular model over T of a smooth projective curve of genus one over $K = \mathbb{R}((t))$. For a ring A and $f_1, \ldots, f_n \in A$, let $V(f_1, \ldots, f_n) = \{\mathfrak{p} \in \mathsf{Spec}(A) \mid (f_1, \ldots, f_n) \subseteq \mathfrak{p}\}$, where $(f_1, \ldots, f_n)$ is the ideal of A generated by

$f_1, \dots, f_n$. The special fiber $\mathcal{C}_k = V(t)$ is given by the scheme

$$\mathsf{Spec}(\mathbb{R}[X,Y,Z]/(XZ, Y^2 + (X^2+1)(1+Z^2)).$$

Written as a divisor, $\mathcal{C}_k = \Gamma_1 + \Gamma_2$, where Γ_1 is the irreducible component $V(Z, Y^2 + X^2 + 1)$ and Γ_2 is the irreducible component $V(X, Y^2 + Z^2 + 1)$. We claim that $\mathcal{C}_k$ is a normal crossing divisor on $\mathcal{C}$. Let p be the intersection point of Γ_1 with Γ_2 in $\mathcal{C}$, which is given by $V(\mathfrak{m})$ for the maximal ideal $\mathfrak{m} = (t, X, Z, Y^2+1)$ of $T[X,Y,Z]$. By [38, Proposition 1.8] it is enough to show that $\mathcal{C}_k$ has normal crossings at p, because p is the unique singular point of $\mathcal{C}_k$. Since $\Gamma_1 = V(t, Z)$, $\Gamma_2 = V(t, X)$ and $t = XZ$, we have that $\Gamma_1 = V(Z)$ and $\Gamma_2 = V(X)$. Let $\mathcal{C}_p = \mathsf{Spec}(\mathcal{O}_{\mathcal{C},p})$. Hence $\mathcal{C}_k$ as a divisor on $\mathcal{C}_p$ is given by (XZ). Since

$$\begin{aligned}\mathcal{O}_{\mathcal{C},p}/(X,Z) &= T[X,Y,Z]_{\mathfrak{m}}/(t - XZ, Y^2 + (X^2+1)(1+Z^2), X, Z)\\ &= T[Y]/(t, Y^2+1) = \mathbb{C},\end{aligned}$$

we have that $\mathcal{C}_k$ has normal crossings at p. Therefore $\mathcal{C}$ has normal crossings. Thus, $\mathcal{G}(\mathcal{C})$ is the graph given by the two vertices Γ_1 and Γ_2 connected by a single edge that represents the intersection point p. Hence $b(\mathcal{C}) = 0$.

Let $T' = \mathbb{C}[[t]]$, and let $\mathcal{C}' = \mathcal{C} \times_T T'$. Since Γ_1 and Γ_2 are geometrically integral, we have that $\mathcal{C}'_{\mathbb{C}} = \Gamma_1 + \Gamma_2$, where Γ_1 and Γ_2 intersect at the two points $(X, Z, Y + \sqrt{-1})$ and $(X, Z, Y - \sqrt{-1})$. It follows by Theorem 3.2.5 that $\mathcal{C}_{\mathbb{C}}$ is a normal crossing divisor on $\mathcal{C}'$. Thus, $\mathcal{G}(\mathcal{C}')$ is the graph given by the two vertices Γ_1 and Γ_2 connected by two edges representing the intersection points. Hence $b(\mathcal{C}') = 1$.

Let X/K be a K-scheme, and let L/K be field extension. We define an *L-rational point of X* to be a pair (x, σ), where $x \in X$ and a K-homomorphism $\sigma : \kappa(x) \to L$. We denote by $X(L)$ the set of L-rational points. For a K-rational point $x \in X$ we simply say that x is a *rational point*.

Example 3.2.13. Let L be a field and let $n \in \mathbb{N}$. We denote by $\mathbb{P}(L^{n+1})$ the set of equivalence classes of $L^{n+1} \setminus \{0\}$, under the equivalence relation by

$$x \sim y \iff x = \lambda y, \text{ for some } \lambda \in L^{\times}.$$

The equivalence class of an element $(a_0, \dots, a_n) \in L^{n+1} \setminus \{0\}$ is denoted by $[a_0 : \dots : a_n] \in \mathbb{P}(L^{n+1})$. We observe that there is a bijection from $\mathbb{P}(L^{n+1})$ to $\mathbb{P}^n_K(L)$; see [38, Lemma 2.3.43].

Proposition 3.2.14. *Assume that T is henselian. Let $\mathcal{C}$ be a fibered surface over T. Let L/K be a finite extension. Let T' be an extension of T to L and let ℓ be the residue field of T'. If $\mathcal{C}_K$ admits an L-rational point, then $\mathcal{C}_k$ admits an ℓ-rational point.*

Proof. We write

$$\mathcal{C} = \mathsf{Proj}(T[X_0, \dots, X_m]/(f_1, \dots, f_r)),$$

for some homogeneous polynomials $f_1, \dots, f_r \in T[X_0, \dots, X_m]$. Then

$$\mathcal{C}_K = \mathsf{Proj}(K[X_0, \dots, X_m]/(f_1, \dots, f_r))$$

and

$$\mathcal{C}_k = \mathsf{Proj}(k[X_0, \dots, X_m]/(\overline{f_1}, \dots, \overline{f_r})),$$

where $\overline{f_i}$ is the polynomial obtained from f_i when replacing its coefficients in T by the corresponding residues in k. Let $(q, \sigma) \in \mathcal{C}_K(L)$. In particular $\kappa(q) \subseteq L$. Write $(q, \sigma) \in \mathbb{P}^m_K(L)$ as a projective tuple $[x_0 : \dots : x_m] \in \mathbb{P}(L^{m+1})$ satisfying $f_1(x_0, \dots, x_m) = \cdots = f_r(x_0, \dots, x_m) = 0$. Let $s \in L$ be a uniformizer of T'. For $i \in \{0, \dots, m\}$ we write $x_i = s^{n_i} u_i$, where $n_i \in \mathbb{Z}$ and $u_i \in T'^{\times}$. Multiplying by s^{-n}, for $n = \min\{n_i \mid 0 \le i \le m\}$, we may assume that $x_0, \dots, x_m \in T'^{m+1}$ and $x_k \in T'^{\times}$, for some $k \in \{0, \dots, m\}$. Therefore $[\overline{x_0} : \dots : \overline{x_m}] \in \mathbb{P}(\ell^{m+1})$, and for all $i \in \{0, \dots, r\}$ we have $\overline{f_i}(\overline{x_0}, \dots, \overline{x_m}) = 0$. In particular $\mathcal{C}_k(\ell) \neq \varnothing$. □

3.3 Reduction of elliptic curves

In this section, we will describe and use Tate's algorithm to calculate the geometry of certain regular models of elliptic curves, which is usually referred to in the literature as the Kodaira-Néron *reduction type*. This will later, in Section 5.5, be used to study how properties of sums of squares in a function field in one variable of genus one relate to its reduction type.

An *elliptic curve over* K is defined as a pair (E, O) where E is a smooth curve of genus one over K and O is a rational point. Given an elliptic curve $(E, \mathcal{O})$ over K, $E(K)$ is endowed with the structure of an abelian group having the point O as neutral element; see [57, III. 2. The Group Law]. We generally denote by E/K an elliptic curve without mentioning the point O.

We recall that T denotes a discrete valuation ring with perfect fraction field K, maximal ideal $\mathfrak{m}$ and residue field k. We fix an algebraic closure $\bar{k}$ of k.

Since for every smooth projective curve C over K (or equivalently any function field F/K in one variable over K), there exists a unique minimal regular model $\mathcal{C}$ over T, by Theorem 3.2.11, we may use this to define a further arithmetic-geometric invariant for F/K, namely the *reduction type* of C/K (or equivalently the *reduction type of* F/T, respectively), based on the special fiber of said minimal regular model. We will focus mainly on the situation of curves of genus one. In the literature, the Kodaira-Néron types are listed for all possible elliptic curves over K, and they are grouped in the following families and typically represented by suggestive pictograms of the special fiber of the minimal regular model over $\bar{k}$; see for example [42, Pag. 124].

Consider an elliptic curve E/K. Let $\mathcal{C}$ be the minimal regular model of E/K. Then $\mathcal{C}_{\bar{k}} = \mathcal{C}_k \times_k \bar{k}$ has one the forms in [58, Figure 4.4. Pag 354]. In this section, we will describe only some of the Kodaira-Néron types.

Definition 3.3.1. *Let E/K be a smooth projective curve of genus one, and let $\mathcal{C}$ be the minimal regular model of E/K.*

- *We say that E is* of type I_0 *(or that E has* good reduction*) if $\mathcal{C}_{\bar{k}}$ is smooth. In this case $\mathcal{C}_k$ is a smooth projective curve of genus one.*

- *We say that E is* of type I_n, *for some integer $n \geq 2$, if $\mathcal{C}_{\bar{k}}$ consists of n non-singular rational curves arranged in a shape of an n-gon with tranversal intersections, that is, $\mathcal{C}_{\bar{k}} = \sum_{i=0}^{n-1} \Gamma_i$ satisfies the following:*

$$\Gamma_i \cdot \Gamma_j = \begin{cases} 1 & \text{if } j \equiv i \pm 1 \mod n, \\ -2 & \text{if } i = j. \\ 0 & \text{otherwise} \end{cases}$$

- *We say that E is* of type I_n^* *if $\mathcal{C}_{\bar{k}}$ consists of $n+1$ non-singular rational curves $F_0, \ldots, F_n$ of multiplicity 2, with four non-singular rational curves $\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4$ of multiplicity 1 satisfyng the following:*

  $\Gamma_i \cdot F_0 = \Gamma_j \cdot F_n = 1$, *for* $i = 1, 2$, $j = 3, 4$, *and* $\Gamma_i \cdot F_j = 0$ *otherwise.* $F_i \cdot F_{i+1} = 1$ *for all* $0 \leq i \leq n-1$, *and* $F_i \cdot F_j = 0$ *if* $j \neq i \pm 1$.

Other families $\mathsf{II}, \mathsf{III}, \mathsf{IV}, \mathsf{IV}^*, \ldots$, can be found in [58, IV. Theorem 8.2]. We do not need them here.

Proposition 3.3.2. *Let E/K be smooth projective curve. Let $\mathcal{C}$ be a model of E/K. If $\mathcal{C}_k$ is smooth, then $\mathcal{C}$ is the minimal regular model of E/K.*

Proof. Since $\mathcal{C}_k$ and $\mathcal{C}_K$ are smooth curves, we have that $\mathcal{C}$ is a regular model of E/K, by [38, Theorem 4.3.36]. By [58, VI. Proposition 7.3] we have that $\mathcal{C}_k^2 = 0$. Therefore $\mathcal{C}$ does not contain any exceptional, whereby $\mathcal{C}$ is minimal and $\mathcal{C}$ is the minimal regular model of E/K. □

Example 3.3.3. Let $\lambda \in T$ and $a \in T^\times$. Set $f = ZY^2 - (X - \lambda Z)(X^2 + aZ^2)$. Let E be the scheme $\mathsf{Proj}(K[X,Y,Z]/f(X,Y,Z))$, and let

$$\mathcal{C} = \mathsf{Proj}(T[X,Y,Z]/f(X,Y,Z)).$$

We first observe that the projective scheme $\mathcal{C}$ is a model of E/K by [38, Example 10.1.14]. Consider $\bar{f} = ZY^2 - (X - \overline{\lambda}Z)(X^2 + \overline{a}Z^2) \in k[X,Y,Z]$. Then $\mathsf{Proj}(k[X,Y,Z]/\bar{f})$ is the special fiber of $\mathcal{C}$. Furthermore, using the so-called Jacobian criterion [38, Theorem 4.2.19], one can show that $\mathcal{C}_k$ and $\mathcal{C}_K$ are smooth curves. Hence $\mathcal{C}$ is the minimal regular model of E/K, by Theorem 3.3.2. Moreover, since $\mathcal{C}_k$ is geometrically connected, we have that $\mathcal{C}_{\bar{k}}$ is a smooth curve of genus one. Therefore E is of type I_0.

Proposition 3.3.4. *Let F/K be a function field in one variable, and let $\mathcal{C}$ be a regular model of F/T. Let v be a $\mathbb{Z}$-valuation F such that $\mathcal{O}_v \cap K = T$ and such that κ_v/k is a nonruled function field in one variable. Then $\mathcal{O}_v = \mathcal{O}_{\mathcal{C},x}$ for some codimension one point $x \in \mathcal{C}$ lying on $\mathcal{C}_k$. In this case, the Zariski closure $\overline{\{x\}}$ of x is an irreducible component of $\mathcal{C}_k$ and $\kappa(\overline{\{x\}}) = \kappa_v$.*

Proof. See for example [4, Proposition 3.7]. □

Lemma 3.3.5. *Let T be a henselian discrete valuation ring with fraction field K and perfect residue field k. Let E/K be an elliptic curve of reduction type I_n^*, for some $n \in \mathbb{N}$, and let F/K be its function field. Then every residually transcendental extension of T to F is ruled.*

Proof. Let $\mathcal{C}$ be the minimal regular model of E/T, let T' be an unramified extension T' of T with residue field $\bar{k}$ (see Theorem 3.2.5), and let $\mathcal{C}' = \mathcal{C} \times_T T'$. Since E is of reduction type I_n^*, for some $n \in \mathbb{N}$, the special fiber $\mathcal{C}_{\bar{k}}$ is arranged as Theorem 3.3.1. Let $\mathcal{V}'$ be the set of irreducible components of $\mathcal{C}_{\bar{k}}$, and let $\mathcal{P}'$ be the set of those points on $\mathcal{C}_{\bar{k}}$ where two distinct irreducible components of $\mathcal{V}'$ intersect. Let $\mathcal{G}(\mathcal{C}')$ be the reduction graph associated to $\mathcal{C}'$ as defined in Section 3.2. We recall that the vertices of $\mathcal{G}(\mathcal{C}')$ are $\mathcal{V}' \cup \mathcal{P}'$, and a vertex $p \in \mathcal{P}'$ is connected by an unique edge with a vertex $\Gamma \in \mathcal{V}'$ if and only if $p \in \Gamma$. Since $\mathcal{C}_{\bar{k}}$ is a normal crossing divisor on $\mathcal{C}'$, there exists at most one edge between $p \in \mathcal{P}'$ and $\Gamma \in \mathcal{V}'$; see Theorem 3.2.7. Since $\mathcal{G}(\mathcal{C}')$ is a tree, we have that $\mathcal{G}(\mathcal{C}')$ has trivial Betti number, that is, $b(\mathcal{C}') = 0$. The natural action of $\mathsf{Gal}(\bar{k}/k)$ on $\mathcal{C}_{\bar{k}}$ induces a natural action on $\mathcal{V}'$ and on $\mathcal{P}'$, and hence on $\mathcal{G}(\mathcal{C}')$. Let v be a valuation corresponding to T. To prove the claim by contradiction, we assume that there exists a nonruled residually transcendental extension $\mathcal{O}$ of T to F. Let w be a valuation on F corresponding to $\mathcal{O}$. By Theorem 3.3.4 there exists an irreducible component of $\mathcal{C}_k$, which we denote by Γ_w such that $\kappa(\Gamma_w) = \kappa_w$. Let $\pi : \mathcal{C}_{\bar{k}} \to \mathcal{C}_k$ denote the morphism of base change from k to $\bar{k}$. By [3, Propositions 3.1 and 4.3], $\pi^{-1}(\Gamma_w)$ is an irreducible component of $\mathcal{C}_{\bar{k}}$ and it is the unique vertex γ in $\mathcal{G}(\mathcal{C}')$ whose stabilizer subgroup in $\mathsf{Gal}(\bar{k}/k)$ acts on the set of vertices that are connected by an edge to γ in such a way that every orbit has even cardinality. Moreover by [3, Corollary 3.5] the vertex $\pi^{-1}(\Gamma_w) \in \mathcal{V}'$ is the only vertex of $\mathcal{G}(\mathcal{C}')$ which is fixed by $\mathsf{Gal}(\bar{k}/k)$. Since $\mathcal{C}_K \simeq E$, we have that $\mathcal{C}_K$ admits a K-rational point. Thus, by Theorem 3.2.14 there exists a k-rational point x on $\mathcal{C}_k$, and $\pi^{-1}(x) \subseteq \mathcal{C}_{\bar{k}}$ consists of a unique point x', which is fixed by $\mathcal{G}$. Hence $x' \notin \mathcal{P}$. Moreover, since $\kappa(\Gamma_w)/k$ is not rational of genus zero, the point $x' \notin \pi^{-1}(\Gamma_w)$. We conclude that $x' \in \Gamma$, for some $\Gamma \in \mathcal{V}' \setminus \{\pi^{-1}(\Gamma_w)\}$. Since there exists $\sigma \in \mathsf{Gal}(\bar{k}/k)$ such that $\sigma(\Gamma) \neq \Gamma$, we conclude that $\sigma(x') \neq x'$, which is a contradiction, since $x' \notin \mathcal{P}'$. We conclude that every residually transcendental extension of T is ruled. □

Let E/K be an elliptic curve. It is known that there exists an isomorphism between E and a curve on $\mathbb{P}^2_K$ given by an equation of the form

$$y^2z + a_1xyz + a_3z^3 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

sending O to the point $[0 : 1 : 0] \in \mathbb{P}^2_K$, with coefficients $a_1, \ldots, a_6 \in K$; see [57, III. 3.1, (a)]. The latter is called a *Weierstrass equation for* E/K. To ease notation, we write the Weierstrass equation using coordinates $X = x/z$ and $Y = y/z$,

$$E : Y^2 + a_1XY + a_3 = X^3 + a_2X^2 + a_4X + a_6,$$

and remembering that there exists an extra point $[0 : 1 : 0]$, which is smooth by [57, III. 1.4]. Conversely, every curve given by a Weierstrass equation over K is an elliptic curve over K with point $[0 : 1 : 0]$ as the point O; see [57, III. 3.1, (c)]. Assuming that $a_1, \ldots, a_6 \in T$, we let

$$b_2 = a_1^2 + 4a_2,\ b_4 = a_1a_3 + 2a_4,\ b_6 = a_3^2 + 4a_6,\ b_8 = (b_2b_6 - b_4^2)/4.$$

We call the quantity $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ the *discriminant* of the Weierstrass equation. Let v be a $\mathbb{Z}$-valuation on K such that $\mathcal{O}_v = T$. Let $t \in K$ be such that $v(t) = 1$. We say that this

equation is *minimal for* E/K (with respect to T) if $v(\Delta)$ is minimal among all the discriminants of all Weierstrass equations for E/K with coefficients $a_1, \dots, a_6 \in T$. We define the polynomial

$$P(Z) = Z^3 + a_2 t^{-1} Z^2 + a_4 t^{-2} Z + a_6 t^{-3}.$$

There exists an algorithm due to J. Tate which computes the Kodaira-Néron reduction type of an elliptic curve from the coefficients of a Weierstrass equation for E/K; see [60]. In this section, we derive a consequence from Tate's algorithm.

Proposition 3.3.6. *Let E/K be an elliptic curve. Let $a_1, \dots, a_6 \in T$ be such that*

$$Y^2 + a_1 XY + a_3 = X^3 + a_2 X^2 + a_4 X + a_6$$

is a Weierstrass equation for E/K. Let Δ be its discriminant. Let v be a $\mathbb{Z}$-valuation corresponding to T. Assume that $a_3, a_4, a_6, \Delta \in \mathfrak{m}$. Let $n \in \mathbb{N}$ be such that $n = v(\Delta)$. Then the following statements hold:

(1) If $b_2 = a_1^2 + 4a_2 \in T^\times$, then E is of type I_n.

(2) Assume that $a_1, a_2 \in \mathfrak{m}, v(a_3) \geq 2, v(a_4) \geq 2$ and $v(b_6) \geq 3$. If $b_2 \in \mathfrak{m}$, then $P \in T[Z]$ and the following hold:

(i) If $\overline{P}(Z) \in K[Z]$ is separable, then E is of type I_0^*.

(ii) If $P(Z)$ has precisely two roots in $\bar{k}$, then E is of type I_{n-6}^*.

Proof. See [60]. See also [58, Tate's algorithm 9.4] for a proof using blowing-ups. □

Remark 3.3.7. The original algorithm [60] is a series of 11 steps which apply to any Weierstrass equation of a given elliptic curve. If we have a Weierstrass equation for an elliptic curve E/K and we get to the last step of the algorithm, this means that the equation was not minimal. Then by applying the change of variables $(X, Y) = (t^2 X', t^3 Y')$ we obtain another Weierstrass equation for E/K whose discriminant is $t^{-12}\Delta$, and we go back to the Step 1 and begin the algorithm again with this new equation. Therefore the algorithm will terminate.

Proposition 3.3.8. *Assume that $\mathsf{char}(k) \neq 2$. Let $\lambda \in T^\times$ and $a \in \mathfrak{m}$. Let E be the elliptic curve given by the Weierstrass equation $Y^2 = (X - \lambda)(X^2 + a^2)$. Then E is of type I_{2n} where $n = v(a)$.*

Proof. In this case, we have that $a_2 = -\lambda, a_4 = a^2, a_6 = -\lambda a^2$ and that $b_2 = -4\lambda, b_4 = 2a^2, b_6 = -4\lambda a^2, b_8 = 4\lambda^2 a^2 - a^4$. Hence

$$\Delta = -64a^2(\lambda^4 + 2\lambda^2 a^2 + a^4).$$

Let $n = v(a)$. Clearly $v(\Delta) = 2n$. Since $b_2 \in T^\times$, we have that E is type I_{2n}, by Theorem 3.3.6. □

Lemma 3.3.9. *Assume $\mathsf{char}(k) \neq 2, 3$. Let $\lambda, a \in T$. Let E/K be the elliptic curve given by the equation $Y^2 = (X - \lambda)(X^2 + a^2)$. Then this Weierstrass equation is minimal if and only if $\lambda \in T^\times$ or $v(a) = 1$ or $v(\lambda) = 1$.*

Proof. Set $c = 16\lambda^2 - 48a^2$ and let Δ be the discriminant of the equation $Y^2 = (X-\lambda)(X^2+a^2)$. By [57, VII. Remark 1.1], the equation is minimal if and only if $v(\Delta) < 12$ or $v(c) < 4$. Assume that either $\lambda \in T^\times$ or $v(a) = 1$ or $v(\lambda) = 1$. Then $v(c) < 4$ except possibly in the case where $\lambda, a \in T^\times$ or $v(\lambda) = v(a) = 1$. Assume that $\lambda, a \in T^\times$. We have

$$\Delta = -64a^2(\lambda^4 + 2\lambda^2a^2 + a^4)$$

and $c = 16(\lambda^2 - 3a^2)$. By contradiction, assume that $v(\Delta) > 12$ and $v(c) > 4$, that is, $\lambda^2 - 3a^2 \in \mathfrak{m}$ and $\lambda^4 + 2\lambda^2a^2 + a^4 \in \mathfrak{m}$. Hence $\overline{\lambda}^2 = 3\overline{a}^2$. Replacing $\overline{\lambda}^2$ by $\overline{3}\overline{a}^2$ in $\overline{\lambda}^4 + 2\overline{\lambda}^2a^2 + \overline{a}^4$, we obtain $9\overline{a}^4 + 6\overline{a}^4 + \overline{a}^4 = 0$. Hence $\overline{16} = 0$, contradiction. Therefore either $v(\Delta) < 12$ or $v(c) < 4$. Assume now that $\lambda = tu, a = th$ for some $u, h \in T^\times$. Then $\Delta = -64t^6h^2(u^4 + 2u^2h^2 + h^4)$ and $c = 16t^2(u^2 - 3h^2)$. Now, this case is similar to the above case. Hence we obtain one implication.

For the other direction, we assume that $\lambda = t^m u$ and $a = t^n h$, for some $u, h \in T^\times$ with $n, m > 1$. We have to show that the equation is not minimal. By the change of variable $(X, Y) = (t^2X', t^3Y')$, we obtain another Weierstrass equation $Y'^2 = (X' - t^{m-2}u)(X'^2 + t^{2n-4}h)$ over T that defines the same elliptic curve. Note that this Weierstrass equation has smaller discriminant, which is a contradiction. Another way to show this implication is by applying Tate's algorithm [58, IV. Tate's algorithm 9.4] to the Weierstrass equation $Y^2 = (X - t^m u)(X^2 + t^{2n}h^2)$. In this case, we reach to the last step of the algorithm, which shows that the equation that we started was not minimal; see Theorem 3.3.7. □

Proposition 3.3.10. *Let E/K be an elliptic curve. We assume that there exist $\lambda, a \in \mathfrak{m}$ such that $Y^2 = (X-\lambda)(X^2+a^2)$ is a minimal Weierstrass equation for E/K. Then E is of type I_n^*, for some $n \in \mathbb{N}$.*

Proof. In this case, we have that $a_2 = -\lambda, a_4 = a^2, a_6 = -\lambda a^2$ and that $b_2 = -4\lambda, b_4 = 2a^2, b_6 = -4\lambda a^2, b_8 = 4\lambda^2a^2 - a^4$. Hence

$$\Delta = -64a^2(\lambda^4 + 2\lambda^2a^2 + a^4).$$

We consider the polynomial $P(Z) = Z^3 - \lambda t^{-1}Z^2 + a^2t^{-2}Z - \lambda a^2t^{-3}$. Let s denote the discriminant of P. Then $s = -4a^2t^{-6}(\lambda^4 + 2\lambda^2a^2 + a^4)$. For the definition of the discriminant of a cubic equation; see [14, Pag. 612]. Note that $a_1 = a_3 = 0$, and hence $a_1, a_2 \in \mathfrak{m}, v(a_3), v(a_4) \geq 2$. Since $m + 2 \geq 3$, we have that $v(b_6) \geq 3$. Moreover $b_2 = -4\lambda \in \mathfrak{m}$. We observe that $\lambda^4 + 2\lambda^2a^2 + a^4 \neq 0$, because otherwise $\Delta = 0$, and the curve would be singular, which is not the case. By Theorem 3.3.9 we have that either $v(a) = 1$ or $v(\lambda) = 1$. We first treat the case where $v(a) = 1$. Let $m \in \mathbb{N}$ be such that $v(\lambda) = m$ with $m \geq 1$. If $m > 1$, then $\mathsf{Disc}(P) \in T^\times$, whereby E is of type I_0^*, by Theorem 3.3.6. Assume $m = 1$. In this case $v(\lambda^4 + 2\lambda^2a^2 + a^4) \geq 4$. If $v(\lambda^4 + 2\lambda^2a^2 + a^4) = 4$, then $s \in T^\times$, whereby E is of type I_0^*. If $v(\lambda^4 + 2\lambda^2a^2 + a^4) > 4$, then $v(s) > 0$, whereby E is of type I_n^*, where $n = v(\Delta) - 6$, by Theorem 3.3.6. We now consider the case where $v(\lambda) = 1$ and $v(a) > 1$. Let $d \in \mathbb{N}$ be such that $v(a) = d$. Since $v(\lambda^4 + 2\lambda^2a^2 + a^4) = 4$, we have that $v(s) = 2(d-1)$. Since $d > 1$, we have that $v(s) > 0$, whereby E is of type I_n^*, where $n = v(\Delta) - 6 = (2d+4) - 6 = 2(d-1)$. □

3.4 Construction of a regular model

Let F/K be a function field in one variable. A model of F/T can be obtained from a closed immersion of the unique smooth projective curve over K with function field F in some projective space; see [38, Example 10.1.4] and Theorem 3.3.3. Starting with suitable integral equations for the curve one obtains a starting fibered surface that one can desingularize in finitely many steps of normalizations and blowing-ups. In Theorem 3.4.2 we will construct the minimal regular model of an specific curve explicitly. In this case we will only need to blow up a closed point.

Let us first recall the blowing-up construction (in a closed point of a scheme). Given a scheme $\mathcal{C}$ and a closed point $P \in \mathcal{C}$, the *blowing-up* $\widetilde{\mathcal{C}}$ *of* $\mathcal{C}$ *at* P can be constructed in the following way:

1. Identify an affine open subscheme U of $\mathcal{C}$ containing P.
2. Construct the blowing-up $\widetilde{U}$ of U at P, together with the blowing-up morphism $\pi : \widetilde{U} \to U$, which defines the exceptional fiber $E = \pi^{-1}(P)$, and is otherwise an isomorphism from $\widetilde{U} \setminus E$ to $U \setminus \{P\}$.
3. Use the blowing-up morphism $\widetilde{U} \to U$ to glue $\mathcal{C} \setminus \{P\}$ with $\widetilde{U} \setminus E \simeq U \setminus \{P\}$ in order to obtain $\widetilde{\mathcal{C}}$ and the blowing up morphism $\widetilde{\mathcal{C}} \to \mathcal{C}$.

See [26, Pag. 28] for a more geometric description of the blowing-up. This process is well-defined, and it does not depend on the choice of the affine neighbourhood U of P. Moreover, the blowing up morphism $\widetilde{\mathcal{C}} \to \mathcal{C}$ is projective; see [38, Lemma 8.1.2]. In particular, if $\mathcal{C}$ is a projective fibered surface over T, then so is $\widetilde{\mathcal{C}}$. Now we only need to discuss how $\widetilde{U} \to U$ is constructed. Let $U = \mathrm{Spec}(A)$ and $\mathfrak{p} \subset A$ be the maximal ideal that defines P. By definition, $\widetilde{U} = \mathrm{Proj}(B)$ for the graded ring

$$B = \oplus_{d \in \mathbb{N}} \mathfrak{p}^d.$$

Since $A = \mathfrak{p}^0$ is the subalgebra of degree zero and $\mathrm{Proj}(A) = \mathrm{Spec}(A)$, we thus have $\widetilde{U} \to U$ given by the (trivially) graded inclusion of A in B. When A is Noetherian and, say, $\mathfrak{p} = (x_0, \ldots, x_n)$ we consider the surjective graded homomorphism

$$A[Z_0, \ldots, Z_n] \to B$$

given by $Z_i \mapsto x_i \in \mathfrak{p}^1$. Let $\mathcal{J}$ denote its kernel. Then

$$\widetilde{U} = \mathrm{Proj}\left(A[Z_0, \ldots, Z_n]/\mathcal{J}\right).$$

The ideal $\mathcal{J}$ contains the ideal $(Z_i x_j - Z_j x_i)_{0 \le i,j \le n}$. The blowing-up $\widetilde{U}$ can be decomposed into $n+1$ affine charts, where the i-th chart is described by the ideal

$$\mathcal{J}_i := \{Q \in A[S_1, \ldots, S_n] \mid \exists d \ge 0;\ x_i^d Q \in (x_j - S_j x_i)_{1 \le j \le n}\}$$

inside of the open affine part given by the homogeneous localization in Z_i, that is, inside of the

polynomial ring in n variables

$$A[S_0, \ldots, S_n],$$

where $S_j := \frac{Z_j}{Z_i}$ for $1 \leq j \leq n$. In particular $S_i = 1$. Hence, the corresponding affine chart is given by the scheme $\operatorname{Spec}\left(A\left[\frac{x_j}{x_j}\right]_{0\leq j\leq n}\right)$ inside of the localization A_{x_i}. See [38, Lemma 8.1.2] for details. In our case, A will always be a integral domain, hence any localization and thus also any affine chart of the blowing-up will be a subring of the field of fractions of A. The following lemma will help us to show that the affine charts of the blowing-up in Theorem 3.4.2 are normal.

Lemma 3.4.1. *Let A be a regular domain such that $2 \in A^\times$. Let K be the fraction field of A. Let $x \in A$ and let $F = K(\sqrt{x})$. Then $A(\sqrt{x})$ is normal.*

Proof. We first show that, if A is a unique factorization domain, then $A(\sqrt{x})$ is the integral closure of A in F. Let $\alpha = \frac{a}{c} + \frac{b}{c}\sqrt{x} \in F$, for some $a, b, c \in A$. Assume that α is integral over A. We claim that $c \mid a$ and $c \mid b$. Let $Tr_{F/K}$ and $N_{F/K}$ be the trace and norm from F to K, respectively. Since $\alpha^2 - Tr_{F/K}(\alpha)\alpha + N_{F/K}(\alpha) = 0$ and since A is integrally closed, we have $Tr_{F/K}(\alpha) \in A$ and $N_{F/K}(\alpha) \in A$. Since $Tr_{F/K}(\alpha) = \frac{2a}{c}$ we obtain that $c \mid a$. Moreover, since $N_{F/K}(\alpha) = (\frac{a}{c})^2 - x(\frac{b}{c})^2 \in A$, we thus have $c^2 \mid xb^2$, and hence $c^2 \mid b^2$ because x is square-free. Finally, since A is a unique factorization domain, we obtain that $c \mid b$. Therefore $\alpha \in A(\sqrt{x})$.

Now we assume that A is a regular domain. Set $B = A(\sqrt{x})$. Let $\mathfrak{p} \in B$ be a prime ideal. We claim that $B_\mathfrak{p}$ is normal. Let $\mathfrak{q} = A \cap \mathfrak{p}$. We have $A_\mathfrak{q} \subseteq B_\mathfrak{q} \subseteq B_\mathfrak{p}$. One can check easily that $B_\mathfrak{q} = A_\mathfrak{q}(\sqrt{x})$. It was shown in [2, Theorem 5] that $A_\mathfrak{q}$ is a unique factorization domain because $A_\mathfrak{q}$ is regular. Hence by the above $B_\mathfrak{q}$ is normal. On the other hand, one can argue as in the proof of Theorem 1.1.5 that $B_\mathfrak{p} = (B_\mathfrak{q})_{\mathfrak{p}B_\mathfrak{q}}$. Now, since the localization of $B_\mathfrak{q}$ at any prime ideal is normal, we have that $B_\mathfrak{p}$ is normal. Therefore B is normal. □

As shown in [39], the Kodeira-Néron reduction type of a curve of genus one over K that is not an elliptic curve over K is essentially the same (up to a constant factor on the multiplicities of the irreducible components of the special fiber) as the one of its Jacobian (which is an elliptic curve over K and a Galois-twist of the original curve of genus one). With Tate's algorithm we have a tool to find the minimal regular model of an elliptic curve. But for genus one curves we do not have such an algorithm. We construct by hand the minimal regular model of a genus one curve which is not an elliptic curve.

Proposition 3.4.2. *Let t be a uniformizer of T. Let F be the function field of the curve*

$$Y^2 = -(X^2 + 1)(X^2 + t^2).$$

Then F has genus one and is of reduction type I_2.

Proof. First we note that $g(F/K) = 1$, by Theorem 1.3.7. Considering the above curve as a curve in $\mathbb{P}^2_K$ given by the homogenization of the given equation using the Jacobian criterion, one can check that the point $[0 : 1 : 0]$ on the curve is singular. Thus, we first construct the nonsingular

curve C over K whose function field is F. This curve is constructed by glueing the affine curve $C_0 : Y^2 = f(X)$ with $C_1 : V^2 = g(U)$, where $f = -(X^2+1)(X^2+t^2)$ and $g = -(t^2U^2+1)(1+U^2)$ on $D(X) \simeq D(U)$ (here $D(X)$ and $D(U)$ are the principal Zariski open subsets of C given by the polynomials $X \in K[X,Y]$ and $U \in K[U,V]$ respectively). These two open are glued via the map $C_0 \to C_1$, given by $(X,Y) \mapsto (\frac{1}{X}, \frac{Y}{X^2})$ and its inverse $C_1 \to C_0$, given by $(U,V) \mapsto (\frac{1}{U}, \frac{V}{U^2})$; see [57, Example II.2.5.1, Proposition II.2.5.2]. Thus, the scheme $\mathcal{C}$ is given by the union of the two affine schemes

$$\mathcal{W}^0 = \mathsf{Spec}(T[X,Y]/(Y^2 - f(X))), \quad \mathcal{W}^1 = \mathsf{Spec}(T[U,V]/(V^2 - g(U)))$$

is a model of C/T. Since the special fiber of $\mathcal{W}^1$ is the smooth conic $V^2+U^2+1 = 0$, we have that $\mathcal{W}^1$ is regular by [38, Proposition 4.3.36]. Thus, we observe that any singular point of $\mathcal{C}$ is necessarily contained as a closed point in the special fiber of $\mathcal{W}^0$. We write x, y for the residues of X, Y in $T[X,Y]/(Y^2 - f(X))$. Using the Jacobian criterion, we can check that the special fiber $\mathcal{W}^0_k$ has a singularity at (x,y), which corresponds to the maximal ideal $\mathfrak{p} = (x,y,t) \in \mathcal{W}^0$ under the closed immersion $\mathcal{W}^0_k \to \mathcal{W}^0$. Since $Y^2 - f(X) \in \mathfrak{p}^2$, we have that $\mathcal{W}^0$ is not regular at $\mathfrak{p}$, by [38, Corollary 4.2.12]. We blow up $\mathcal{W}^0$ at $\mathfrak{p}$. The blowing-up $\widetilde{\mathcal{W}^0}$ can be covered by three affine charts, given by the following rings: The **first affine chart** U_1 is given by spectrum of the integral domain

$$A_1 = T[x, y, \frac{x}{t}, \frac{y}{t}] = T[\frac{x}{t}, \frac{y}{t}] = T[x', y'],$$

where the algebraic dependencies between $x' = \dfrac{x}{t}$ and $y' = \dfrac{y}{t}$, are described by the prime ideal in the polynomial ring $T[X', Y']$ generated by

$$Y'^2 + (t^2X'^2 + 1)(X'^2 + 1).$$

In particular, $T[x', y']$ is a normal domain by Theorem 3.4.1. The **second affine chart** U_2 is given by the spectrum of the integral domain

$$A_2 := T[x, y, \frac{t}{x}, \frac{y}{x}] = T[\frac{t}{x}, x, \frac{y}{x}] = T[z, x, y'],$$

where the algebraic dependencies between $z = \dfrac{t}{x}, x$ and $y' = \dfrac{y}{x}$, are described by the prime ideal in the polynomial ring $T[Z, X, Y']$ generated by

$$t - ZX \quad \text{and} \quad Y'^2 + (X^2+1)(1+Z^2).$$

We observe that $T[z,x] \simeq T[X][\frac{t}{X}]$ is a normal domain, in fact, it is a regular domain by [38, Theorem 8.1.19], since one can identify as an affine part of a blowing up of the regular domain $T[X]$ at the maximal ideal (t, X). As $T[z,x,y']$ is the integral closure of $T[X][\frac{t}{X}]$ in $K(X)\left(\sqrt{-(X^2+1)(1+\frac{t^2}{X^2})}\right)$ by Theorem 3.4.1, we have that it is a normal domain, as well. The **third affine chart** U_3 is given by the spectrum of the integral domain

$$A_3 := T[y, \frac{x}{y}, \frac{t}{y}] = T[y, x'', z''],$$

where the algebraic dependencies between $z'' = \dfrac{t}{y}, x'' = \dfrac{x}{y}$ and y, are described by the prime ideal

in the polynomial ring $T[X'', Y, Z'']$ generated by

$$t - Z''Y \quad \text{and} \quad 1 + (Y^2X''^2 + 1)(X''^2 + Z''^2).$$

Instead of proving that U_3 is normal, as we did for the previous charts, we will show that $U_3 \subseteq U_2 \cup U_3$, which allows us to dispense of the third chart. We first observe that $U_1 \cap U_3 = \mathsf{Spec}(T[\frac{t}{y}, \frac{x}{y}][\frac{y}{t}]) = D(\frac{t}{y}) = D(z'')$ and $U_2 \cap U_3 = \mathsf{Spec}(T[\frac{t}{y}, \frac{x}{y}][\frac{y}{x}]) = D(\frac{x}{y}) = D(x'')$. On the other hand, since $1 + (y^2x''^2 + 1)(x''^2 + z''^2) = 0$, we have $1 \in (x'', z'')$, whereby $V(x'', z'') = \varnothing$. Therefore $U_3 \subseteq U_1 \cup U_2$.

We observe that the special fiber in the first affine chart U_1 is defined by the smooth conic $Y'^2 + X'^2 + 1 = 0$, whereby U_1 is a regular affine chart of $\widetilde{\mathcal{C}}$. Let $i = \sqrt{-1}$. We now show that $\widetilde{\mathcal{C}}_k$ has at most two singular points over $k(i)$, which appear in the second chart and in the third chart of $\widetilde{\mathcal{C}}$. The special fiber in the second affine chart

$$A_2 = T[Z, X, Y']/(t - ZX, Y'^2 + (X^2 + 1)(1 + Z^2))$$

is defined by $k[Z, X, Y']/(ZX, Y'^2 + (X^2 + 1)(1 + Z^2))$, that is, for $Z = 0$, we have the irreducible component $Y^2 + 1 + X^2 = 0$, and for $X = 0$, we have the irreducible component $Y'^2 + Z^2 + 1 = 0$, which are smooth affine conics, and the latter corresponds to the exceptional fiber of the blowing-up. The only singularities in the special fiber are situated at $X = Z = 0$ and $Y'^2 + 1 = 0$, that is, either the maximal ideal $(X, Z, Y'^2 + 1)$ if -1 is not a square in k, or the maximal ideals $(X, Z, Y' \pm i)$, which corresponds to the maximal ideals $(t, X, Z, Y' \pm i)$ of $A_2(\sqrt{-1})$. We claim that the localization of $A_2(\sqrt{-1})$ at the maximal ideal $\mathfrak{q} = (t, X, Z, Y' + i)$ is regular. Observe that $Y' - i \notin (t, X, Z, Y' + i)$, which implies that $(t, X, Z, Y' + i) = (t, X, Z, Y'^2 + 1)$ in the localization of $A_2(\sqrt{-1})$ at $\mathfrak{q}$. Moreover, since $t = ZX$ and

$$Y^2 + 1 = -(Z^2 + X^2 + Z^2X^2),$$

we obtain that $\mathfrak{q}$ is generated by X and Z in the localization, showing that $A_2(\sqrt{-1})_{\mathfrak{q}}$ is a regular local ring. Hence the second affine chart is regular.

Therefore the blowing-up is regular. We observe that $\widetilde{\mathcal{C}}_k$ is a normal crossing divisor on $\widetilde{\mathcal{C}}$; see Theorem 3.2.12. That means that the special fiber $\widetilde{\mathcal{C}}_k$ is composed by two smooth curves Γ_1 and Γ_2 intersecting transversally at two points, which means that $\Gamma_1 \cdot \Gamma_2 = 2$ by [38, Proposition 9.1.8, (b)]. Moreover, by [38, Proposition 9.1.21] we have that $\Gamma_1^2 = \Gamma_2^2 = -2$, whereby $\widetilde{\mathcal{C}}$ is the minimal regular model of C/K as it contains no exceptional divisor, by Theorem 3.2.10. Therefore C is of type I_2. □

Chapter 4

The Kaplansky radical of a function field

Let K be a field of characteristic different from 2.. We denote by $\mathcal{V}(K)$ the set of all $\mathbb{Z}$-valuations on K. In this chapter, we study the Kaplansky radical $R(K)$ introduced in Section 2.4 and the finiteness of the quotient group $R(K)/K^{\times 2}$. It was pointed out by K. Becher and D. Leep that in certain fields satisfying a local-global principle for quadratic forms, the Kaplansky radical describes the failure of the local-global principle of quadratic forms in dimension 2; see Theorem 4.1.4. Concretely, the authors showed in [6, Proposition 3.2] that, if for every 3-dimensional anisotropic quadratic form φ over K there exists a valuation $v \in \mathcal{V}(K)$ such that φ stays anisotropic over the corresponding completion K^v, then

$$R(K) = K^\times \cap \bigcap_{v \in \mathcal{V}(K)} (K^v)^{\times 2}.$$

In Section 4.1 we study the group of local squares $\mathcal{L}(K) = K^\times \cap \bigcap_{v\in\mathcal{V}(K)}(K^v)^{\times 2}$ and its relation with $R(K)$ in more general situations.

In Section 4.2 we focus on hyperelliptic function fields F/K. In this case, we show in Theorem 4.2.4 that $\mathcal{L}(F)$ is contained in the group generated by a square-free polynomial f over K such that $F = K(X)(\sqrt{f})$, whenever K is euclidean or quadratically closed. Moreover, we show that these two groups are equal when $K = \mathbb{C}$, which allows us to show in Theorem 4.2.6 that the order of $\mathcal{L}(F)/F^{\times 2}$ is equal to 2^{2g} where g is the genus of F/K. In contrast, we show in Theorem 4.2.13 that $R(F)$ is contained in the group generated by f whenever K is neither euclidean nor quadratically closed. This implies in particular that the order of the quotient group $R(F)/F^{\times 2}$ is finite and bounded in terms of the genus of F/K.

In Section 4.3 we study the case of function fields in one variable F/K of genus zero. In Theorem 4.3.1 we show that F is radical-free whenever K is neither euclidean nor quadratically closed. This extends [6, Proposition 3.4], where the same was shown under the assumption that F/K is rational.

In Section 4.4 we consider arbitrary function fields F/K in one variable, but under the additional assumption that the field K is complete with respect to a $\mathbb{Z}$-valuation. We will show that $|R(F)/F^{\times 2}| \leq 2^g$; see Theorem 4.4.3. The proof is based on a description of the Kaplansky radical in terms of the topology of the reduction graph of a curve due to D. Harbater, J. Hartmann and D.

Krashen; see [25, Theorem 9.6]. Finally, for any $g \in \mathbb{N}$ we construct a hyperelliptic function field of genus g such that $|R(F)/F^{\times 2}| = 2^g$; see Theorem 4.4.6. This shows the optimality of the previous bound.

4.1 Local squares

Let K be a field of characteristic different from 2. We recall that the Kaplansky radical of K was defined in Section 2.4 as

$$R(K) = \bigcap_{a \in K^\times} D_K\langle 1, -a\rangle.$$

In this section we inquire the relation between the group of local squares of K and $R(K)$.

We denote by $\mathcal{V}(K)$ the set of all $\mathbb{Z}$-valuations on K. Given $V \subseteq \mathcal{V}(K)$, we set

$$\mathcal{L}(V, K) = K^\times \cap \bigcap_{v \in V} (K^v)^{\times 2}.$$

We also set $\mathcal{L}(K) = \mathcal{L}(\mathcal{V}(K), K)$. Note that $\mathcal{L}(K)$ is a subgroup of $K^\times$ which we call the *group of local squares of* K. Clearly

$$K^{\times 2} \subseteq \mathcal{L}(V, K) \subseteq K^\times$$

for every subset $V \subseteq \mathcal{V}(K)$.

Example 4.1.1. Let K be a *global field*, i.e. a finite extension of $\mathbb{Q}$ or a function field in one variable over $\mathbb{F}_p$, for some prime number p (different from 2, since we assume that $\mathsf{char}(K) \neq 2$). It is a consequence of [46, Global Square Theorem 65:15] that $\mathcal{L}(K) = K^{\times 2}$. By the following proposition, it follows that $R(K) = K^{\times 2}$.

Proposition 4.1.2 (Becher-Leep)**.** *Let $V \subseteq \mathcal{V}(K)$ be a subset of nondyadic valuations whose residue fields are not quadratically closed. Then the following hold:*

(1) $R(K) \subseteq \mathcal{L}(V, K)$.

(2) If $\mathcal{L}(V, K) = K^{\times 2}$, *then* $R(K) = K^{\times 2}$.

(3) If for every 3-dimensional anisotropic quadratic form φ over K there exists $v \in V$ such that φ stays anisotropic over K^v, then $R(K) = \mathcal{L}(V, K)$.

Proof. See [6, Proposition 3.2]. □

Let v be a complete $\mathbb{Z}$-valuation on K. Let F/K be a function field in one variable. We recall that $\mathcal{V}(F/v)$ is the set of *v-divisorial* valuations on F. We have the following consequence of the local-global principle Theorem 2.1.10. We set

$$\mathcal{L}(\mathcal{V}(F/v), F)) = \mathcal{L}(v, F).$$

Proposition 4.1.3. *Assume that K carries a complete nondyadic $\mathbb{Z}$-valuation v. Let F/K be a function field in one variable. Then*

$$R(F) = \mathcal{L}(v, F).$$

Proof. Note that, since for any $w \in \mathcal{L}(v, F)$, either κ_w/K is a finite extension or κ_w/κ_v is a function field in one variable, κ_w is not quadratically closed. Thus, by Theorem 2.1.10 and by Theorem 4.1.2 (3), we have $R(F) = \mathcal{L}(v, F)$. □

The failure of the above local-global principle is given by the group of local squares, or equivalently by the Kaplansky radical, as follows.

Corollary 4.1.4. *Let v be a complete nondyadic $\mathbb{Z}$-valuation on K. Let F/K be a function field in one variable. Let φ be a regular quadratic form over F that is hyperbolic over F^w for every $w \in \mathcal{V}(v, F)$. Then there exists $c \in R(F)$ such that $[\varphi] = [\langle 1, -c\rangle]$ in WF.*

Proof. We may assume without loss of generality that φ is anisotropic over F, by [35, II. Proposition 1.4]. By Theorem 2.1.10 φ has dimension 0 or 2. In the case of dimension 0, choose $c = 1$. Otherwise, let $a, b \in F^\times$ such that $\varphi = \langle a, b\rangle$. Assume that φ is hyperbolic over F^w for every $w \in \mathcal{V}(v, F)$. Then $\langle a, b, -1\rangle$ is isotropic over F^w for every $w \in V$, and by Theorem 2.1.10 we obtain that $\langle a, b, -1\rangle$ is isotropic over F, whereby $1 \in D_F\langle a, b\rangle$. It follows from Theorem 2.1.1 that $\langle a, b\rangle \simeq \langle 1, ab\rangle$. Let $c = -ab$. Then $c \in (F^w)^{\times 2}$ for every $w \in V$, i.e. $c \in \mathcal{L}(v, F)$, whereby $c \in R(F)$ by Theorem 4.1.3. □

In [11, Appendix. 6] the authors gave the following example showing that their local-global principle does not extend to forms of dimension 2.

Example 4.1.5. Let p be an odd prime, and let $f = X(X-1)(X-p) \in \mathbb{Q}_p[X]$. Set $F = \mathbb{Q}_p(X)(\sqrt{f})$. It was shown in [11, Appendix. 6] that $X - 1 \in (F^v)^{\times 2}$ for every $v \in \mathcal{V}(F/v)$ and that $X - 1 \notin F^{\times 2}$. In particular $X - 1 \in (F^v)^{\times 2}$ for all $v \in \mathcal{V}(F/v)$. Then $X - 1$ represents a non-trivial class in $\mathcal{L}(v, F)/F^{\times 2}$, and thus in $R(F)/F^{\times 2}$, by Theorem 4.1.3. We will show in Theorem 4.4.5 that $X - 1$ represents the unique non-trivial class in $R(F)/F^{\times 2}$, whereby $R(F) = F^{\times 2} \cup (X - 1)F^{\times 2}$.

4.2 Hyperelliptic function fields

Let K be a field of characteristic different from 2. In this section, we study the group of local squares and the Kaplansky radical in hyperelliptic function fields F/K, and we bound the quotient group $R(F)/F^{\times 2}$ in terms of its genus.

For a field extension E/K, we denote by $\mathcal{V}(E/K)$ the set of all $\mathbb{Z}$-valuations on E which are trivial on K, and we set $\mathcal{L}(E/K) = \mathcal{L}(\mathcal{V}(E/K), E)$. We recall that $\mathcal{P}_K$ is the set of all monic irreducible polynomials over K and $\mathcal{P}'_K = \mathcal{P}_K \cup \{\infty\}$. Furthermore, $\mathcal{V}(K(X)/K) = \{v_p \mid p \in \mathcal{P}'_K\}$, by Theorem 1.3.2.

Lemma 4.2.1. *Let $f \in K[X]$ be square-free. We set $F = K(X)(\sqrt{f})$. Let $N : F \to K(X)$ be the norm map of $F/K(X)$. Let $x \in F^\times$. If $x \in \mathcal{L}(F/K)$, then $w(N(x)) \in 2\mathbb{Z}$ for every $w \in \mathcal{V}(K(X)/K)$.*

Proof. Let σ be the non-trivial $K(X)$-automorphism of F. Let $x \in \mathcal{L}(F/K)$, let $p \in \mathcal{P}_K$ and let w_p be an extension of the p-adic valuation v_p to F. Assume first that p does not divide f in $K[X]$. Then $v_p(f) = 0$, hence $w_p, w_p \circ w_p \in \mathcal{V}(F)$ because w_p/v_p and $w_p \circ \sigma/v_p$ are unramified by Theorem 1.1.21. Then $w_p(N(x)) = w_p(x\sigma(x)) = w_p(x) + w_p \circ \sigma(x) \in 2\mathbb{Z}$, whence $v_p(N(x)) = w_p(N(X)) \in 2\mathbb{Z}$. Assume now that p divides f. Since f is square-free we have that $v_p(f) = 1$, and it follows by Theorem 1.1.21 that w_p is the unique extension of v_p to F and that $2w_p \in \mathcal{V}(F)$. By [17, Remark 3.2.17] we have that $w_p(x) = \frac{1}{2}v_p(N(x))$ and hence $v_p(N(x)) = 2w_p(x) \in 2\mathbb{Z}$ because $x \in \mathcal{L}(F/K)$. Therefore $v_p(K(X)) \in 2\mathbb{Z}$ for all $p \in \mathcal{P}_K$. Let $g, h \in \mathcal{P}_K$ such that $N(x)) = g/h$. Then every irreducible factor of g and h has even multiplicity, whereby $v_\infty(N(x)) \in 2\mathbb{Z}$. The statement follows since $\mathcal{V}(K(X)/K) = \{v_p \mid p \in \mathcal{P}'_K\}$. □

Let $f \in K[X]$ be a square-free polynomial. The set

$$\mathsf{Supp}(f) = \{q \in \mathcal{P}_K \mid v_q(f) \neq 0\}$$

is called the *support of* f. Set $F = K(X)(\sqrt{f})$. We denote by $\langle \mathsf{Supp}(f) \rangle$ the multiplicative subgroup of $F^\times$ generated by the elements of $\mathsf{Supp}(f)$.

Proposition 4.2.2. *Let $f \in K[X]$ be a nonconstant square-free polynomial. Set $F = K(X)(\sqrt{f})$. Let $q_1, \dots, q_n \in \mathcal{P}_K, \alpha \in K^\times$ be such that $f = \alpha \cdot q_1 \cdots q_n$. Then $\langle \mathsf{Supp}(f) \rangle \cdot F^{\times 2}$ is a subgroup of $F^\times$ generated by $\alpha, q_1, \dots, q_n$ and $F^{\times 2}$. Furthermore*

$$|\langle \mathsf{Supp}(f) \rangle \cdot F^{\times 2}/F^{\times 2}| = \begin{cases} 2^{n-1} & \text{if } \alpha \in K^{\times 2}, \\ 2^n & \text{if } \alpha \notin K^{\times 2}. \end{cases}$$

Proof. This is an easy consequence of the fact that the only non trivial square-class of a field that becomes the trivial square-class in a quadratic extension is the square-class of the discriminant of the extension. □

Lemma 4.2.3. *Let $f \in K[X]$ be a square-free polynomial. Set $F = K(X)(\sqrt{f})$. Let $N : F \to K(X)$ be the norm map of $F/K(X)$. Then*

$$\mathcal{L}(F/K) \cap N^{-1}(K(X)^{\times 2}) \subseteq \langle \mathsf{Supp}(f) \rangle \cdot F^{\times 2}.$$

Proof. Let $E = K(X)$. Let $G = \mathcal{L}(F/K) \cap N^{-1}(E^{\times 2})$. We first show that

$$G \subseteq \bigcup_{a \in K^\times} a \cdot \langle \mathsf{Supp}(f) \rangle \cdot F^{\times 2}.$$

Let $x \in G$. Since $N(x) \in E^{\times 2}$, it follows by [35, VII. 5.10] that $x \in E^\times F^{\times 2}$. We write $x = a \cdot p \cdot h^2$, for some $a \in K^\times$, $h \in F^\times$ and where $p \in K[X]$ is a monic square-free polynomial. We have to show that $\mathsf{Supp}(p) \subseteq \mathsf{Supp}(f)$. Let $q \in \mathsf{Supp}(p)$, and let w be an extension of v_q to F. Suppose $q \notin \mathsf{Supp}(f)$.

Then w/v_q is unramified by Theorem 1.1.21. Hence $w \in \mathcal{V}(F/K)$. But $w(x) = w(ap) = v_q(p) = 1$, which contradicts the fact that $x \in \mathcal{L}(F/K)$. Hence $\mathsf{Supp}(p) \subseteq \mathsf{Supp}(f)$, which proves the claim.

We now show that $G \subseteq \langle \mathsf{Supp}(f)\rangle \cdot F^{\times 2}$. Suppose that there exists $x \in G$ such that $x \notin \langle \mathsf{Supp}(f)\rangle \cdot F^{\times 2}$. In particular, $x \in a \cdot \langle \mathsf{Supp}(f)\rangle \cdot F^{\times 2}$, for some $a \in K^\times \setminus \langle \mathsf{Supp}(f)\rangle \cdot F^{\times 2}$. Let $c \in K^\times$ be such that $f = cf'$, for some monic square-free polynomial f' in $K[X]$. Then $\langle \mathsf{Supp}(f)\rangle \cdot F^{\times 2} \cap K^\times = K^{\times 2} \cup cK^{\times 2}$, since $c \in f'F^{\times 2}$ and K is relatively algebraically closed in F. In particular $a \notin K^\times \cup cK^{\times 2}$. Since $F^{\times 2} \subseteq \mathcal{L}(F/K)$, without loss of generality, we may assume that $x = aq$, for some monic $q \in K[X]$ dividing f. Let $d = \deg q$. Let v be an extension of v_∞ to F.

a) Assume that $\deg f$ is even. Then v/v_∞ is an unramified extension with $\kappa_v = K(\sqrt{c})$, by Theorem 1.1.21. In particular, $a \notin \kappa_v^{\times 2}$. Since $x \in (F^v)^{\times 2}$, we obtain that

$$-d = v(X^d) = v(X^d(aq/X^d)) = v(x) \in 2\mathbb{Z}.$$

Since $1/X$ is a uniformizer of v and $aq/X^d \in \mathcal{O}_v^\times$, with residue $a \in \kappa_v^\times = K(\sqrt{c})^\times$, we have a contradiction by Theorem 1.1.16.

b) Assume that $\deg f$ is odd. Then $\Gamma_v = \frac{1}{2}\mathbb{Z}$ and $\kappa_v = K$, by Theorem 1.1.21. In particular $a/c \notin \kappa_v^{\times 2}$. Let $v' = 2v$. Then $v'(y) = v_\infty(N(y))$, by [17, Remark 3.2.17]. Let $n \in \mathbb{N}$ be such that $2n + 1 = \deg f$. Then $v'(\sqrt{f}/X^n) = 1$. Writing $x = (X^n/\sqrt{f})^{-2d}u$, where $u = aqX^{2nd}/f^d$, we have that $u \in \mathcal{O}_v^\times$ and $\overline{u} = a/c \in \kappa_v$. This contradicts Theorem 1.1.16.

We conclude that $G \subseteq \langle \mathsf{Supp}(f)\rangle \cdot F^{\times 2}$. □

Proposition 4.2.4. *Assume that K is either quadratically closed or euclidean. Let $f \in K[X]$ be a square-free polynomial. Set $F = K(X)(\sqrt{f})$. Then*

$$\mathcal{L}(F) \subseteq \langle \mathsf{Supp}(f)\rangle \cdot F^{\times 2}.$$

Proof. Note that $\mathcal{V}(F/K) \subseteq \mathcal{V}(F)$ and therefore we have $\mathcal{L}(F) \subseteq \mathcal{L}(F/K)$. Let $E = K(X)$. Let $x \in \mathcal{L}(F)$. Let $N : F \to E$ be the norm map of F/E. We claim that $N(x) \in E^{\times 2}$. Since $x \in \mathcal{L}(F/K)$, it follows by Theorem 4.2.1 that $v_p(N(x)) \in 2\mathbb{Z}$ for all $p \in \mathcal{P}_K$. Hence $N(x) \in K^\times \cdot E^{\times 2}$. Since $K^\times = K^{\times 2} \cup -K^{\times 2}$ we obtain that $N(x) \in E^{\times 2} \cup -E^{\times 2}$. If K is quadratically closed, $-1 \in K^{\times 2}$, and then $N(x) \in E^{\times 2}$. Suppose that K is euclidean. For the sake of a contradiction we assume that $N(x) \in -E^{\times 2}$. We write $x = a + b\sqrt{f}$, with $a, b \in E$, and let $x' = a - b\sqrt{f}$. Since $a^2 - b^2 f = N(x) \in -E^{\times 2}$, we thus have $f \in \mathsf{S}_2(E)$. Let $p = X$, and let w be an extension of v_p to F. Since $\kappa_{v_p} = K$ is real, $v_p(f) \in 2\mathbb{Z}$ by Theorem 2.2.9. Hence there exists $u \in \mathcal{O}_{v_p}^\times \cap \mathsf{S}_2(E)$ such that $\kappa_w = K(\sqrt{\overline{u}})$. But $\overline{u} = u(0) \in \mathsf{S}_2(K) = K^{\times 2}$ which implies that $\kappa_w = K$. On the other hand, since $x, x' \in (F^w)^{\times 2}$ and thus $N(x) \in (F^w)^{\times 2}$, we have that $-1 \in (F^w)^{\times 2}$, thus $-1 \in \kappa_w^{\times 2}$. This contradicts the fact that K is real. Hence $N(x) \in E^{\times 2}$. This shows that $\mathcal{L}(F) \subseteq \mathcal{L}(F/K) \cap N^{-1}(E^{\times 2})$. The statement follows from Theorem 4.2.3. □

In the following, we apply the above theory of local squares in the particular case of hyperelliptic function fields over $\mathbb{R}$ and over $\mathbb{C}$.

Lemma 4.2.5. *Let $g \in \mathbb{N}$. Let $F/\mathbb{C}$ be a hyperelliptic function field of genus g. Then there exists a square-free polynomial $f \in \mathbb{C}[X]$ of degree $2g+1$ such that $F = \mathbb{C}(X)(\sqrt{f})$.*

Proof. By Theorem 1.3.6 there exists a square-free polynomial $p \in \mathbb{C}[X]$ of degree $2g+1$ or $2g+2$ such that $F = \mathbb{C}(X)(\sqrt{p})$. Assume that $\deg p = 2g+2$. We write $p = a(X-\alpha_1)\cdots(X-\alpha_{2g+2})$, for certain $a \in \mathbb{C}^\times$ and $\alpha_1, \ldots, \alpha_{2g+2} \in \mathbb{C}$. Since $\mathbb{C}$ is quadratically closed, we may assume that $a = 1$, and by applying the change of variable $X' = X - \alpha_1$, we may assume also that $\alpha_1 = 0$. Then $p = X(X-\alpha_2)\cdots(X-\alpha_{2g+2})$. Letting $X = Z^{-1}$, we obtain that F is isomorphic to $\mathbb{C}(Z)(\sqrt{h(Z)})$, where $h(Z) = (1-\alpha_2 Z)\cdots(1-\alpha_{2g+2}Z)\left(\frac{1}{Z^{g+1}}\right)^2$. By considering the polynomial $f = (1-\alpha_2 Z)\cdots(1-\alpha_{2g+2}Z)$ we obtain the equality. □

For a field F, we set $\overline{\mathcal{L}}(F) = \mathcal{L}(F)/F^{\times 2}$.

Proposition 4.2.6. *Let $g \in \mathbb{N}$. Let $F/\mathbb{C}$ be a hyperelliptic function field of genus g. Then*

$$|\overline{\mathcal{L}}(F)| = 2^{2g}.$$

In particular, if $g > 0$, then $F^{\times 2} \subsetneqq \mathcal{L}(F) \subsetneqq R(F) = F^\times$.

Proof. By Theorem 4.2.5 we may assume that $F = \mathbb{C}(X)(\sqrt{f})$, for some square-free polynomial $f \in \mathbb{C}[X]$ with $\deg f = 2g+1$. Let $E = \mathbb{C}(X)$, and let $q \in \mathsf{Supp}(f)$. We claim that $q \in \mathcal{L}(F)$. Let $w \in \mathcal{V}(F)$. Note that, since $\kappa_w = \mathbb{C}$, we have that $q \in (F^w)^{\times 2}$ if and only if $w(q) \in 2\mathbb{Z}$, by Theorem 1.1.16. We have that $w|_{\mathbb{C}}$ is trivial, by Theorem 1.1.17. Hence $w|_E$ is equivalent to v_p, for some $p \in \mathcal{P}'_{\mathbb{C}}$, by Theorem 1.3.2. If $p \neq q$ and $p \neq \infty$, then $w(q) = 0$, whereby $q \in (F^w)^{\times 2}$. If $p = q$ or $p = \infty$, then $\Gamma_{w|_E} = 2\mathbb{Z}$, by Theorem 1.1.21. Hence $w(q) \in 2\mathbb{Z}$, whereby $q \in (F^w)^{\times 2}$. Since $q \in \mathsf{Supp}(f)$ was arbitrarily chosen, we obtain that $\mathsf{Supp}(f) \subseteq \mathcal{L}(F)$, which implies that $\langle \mathsf{Supp}(f)\rangle \cdot F^{\times 2} \subseteq \mathcal{L}(F)$. The converse inclusion follows by Theorem 4.2.4. Hence $\overline{\mathcal{L}}(F) = \langle \mathsf{Supp}(f)\rangle \cdot F^{\times 2}/F^{\times 2}$. Since any $2g$ of the $2g+1$ linear factors of f form a $\mathbb{Z}/2\mathbb{Z}$-basis of $\overline{\mathcal{L}}(F)$, by Theorem 4.2.2, we obtain that $|\overline{\mathcal{L}}(F)| = 2^{2g}$. If $g > 0$, any $q \in \mathsf{Supp}(f)$ is such that $q \notin F^{\times 2}$, which implies that $F^{\times 2} \subsetneqq \mathcal{L}(F)$. Moreover, by Theorem 2.4.2(5), we have $R(F) = F^\times$. Moreover, any $p \in \mathcal{P}_{\mathbb{C}} \setminus \mathsf{Supp}(f)$ is such that $p \notin \mathcal{L}(F)$. Hence $\mathcal{L}(F) \subsetneqq R(F)$. □

There is a geometric way to obtain Theorem 4.2.6. Let F/K be a function field in one variable and let $\mathcal{E}(F)$ be the group of elements $x \in F^\times$ such that $v(x) \in 2\mathbb{Z}$ for all $v \in \mathcal{V}(F/K)$. We denote the 2-torsion part of the divisor class group by $\mathsf{Cl}(F)[2]$.

Proposition 4.2.7. *Let F/K be a function field in one variable. Then $\mathsf{Cl}(F)[2]$ is isomorphic to $\mathcal{E}(F)/K^\times F^{\times 2}$.*

Proof. We define $\varphi : \mathcal{E}(F) \to \mathsf{Cl}(F)[2]$ as the group homomorphism given by $x \mapsto [\frac{1}{2}(x)]$. Then φ is surjective, because for $[D] \in \mathsf{Cl}(F)[2]$, we have $2D = (x)$ for some $x \in F^\times$, whence $\varphi(x) = [D]$. We claim that $\ker(\varphi) = K^\times F^{\times 2}$. Note that for $x \in K^\times$, we have $x \in \ker(\varphi)$ if and only if $\frac{1}{2}(x) = (y)$ for some $y \in F^\times$. Let $x \in \ker(\varphi)$ and let $y \in F^\times$ be such $\frac{1}{2}(x) = (y)$. Then $(x) = (y^2)$, that is, $(xy^{-2}) = 0$

in $\mathsf{Div}(F)$, which by [59,], means that $xy^{-2} \in K^\times$. Therefore $x \in \ker(\varphi)$ if and only if $x \in K^\times F^{\times 2}$. This shows that $\ker(\varphi) = K^\times F^{\times 2}$. Therefore $\mathsf{Cl}(F)[2]$ is isomorphic to $\mathcal{E}(F)/K^\times F^{\times 2}$. □

Proposition 4.2.8. *Let $g \in \mathbb{N}$. Let $F/\mathbb{C}$ be a function field in one variable of genus g. Then $|\overline{\mathcal{L}}(F)| = 2^{2g}$.*

Proof. By Theorem 1.1.17 we have $\mathcal{V}(F) = \mathcal{V}(F/K)$. Hence $\mathcal{L}(F) = \mathcal{L}(F/\mathbb{C})$, whereby $\mathcal{E}(F)/\mathbb{C}^\times F^{\times 2} = \overline{\mathcal{L}}(F)$. Hence $\overline{\mathcal{L}}(F)$ is isomorphic to $\mathsf{Cl}(F)[2]$, by Theorem 4.2.7. It follows by [58, III. Corollary 2.7] that $|\overline{\mathcal{L}}(F)| = 2^{2g}$. □

Proposition 4.2.9. *Let $f \in \mathbb{R}[X]$ be a square-free polynomial. Set $F = \mathbb{R}(X)(\sqrt{f})$. Then all the monic irreducible quadratic factors of f lie in $\mathcal{L}(F)$.*

Proof. Set $E = \mathbb{R}(X)$. Let q be the product of all monic irreducible quadratic factors of f. Consider $z \in \mathsf{Supp}(q)$. We claim that $z \in \mathcal{L}(F)$. Let $w \in \mathcal{V}(F)$. Since $w|_{\mathbb{R}}$ is trivial, by Theorem 1.1.17, we have that $w|_E$ is equivalent to v_p for some $p \in \mathcal{P}'_{\mathbb{R}}$, by Theorem 1.3.2. If $p = \infty$, then $z \in (F^w)^{\times 2}$. Assume $p \neq z$ and $p \neq \infty$. In this case $w(z) = 0$. If p is quadratic, then $\kappa_w = \mathbb{C}$, and thus $z \in (F^w)^{\times 2}$, by Theorem 1.1.16. We observe that $q \in \mathsf{S}_2(E)$; see Theorem 2.2.5 (5). Hence $z \in \mathsf{S}_2(E)$, because $z \in \mathsf{Supp}(q)$. If p is linear, then $\overline{z} = z(b) \in \mathsf{S}_2(\mathbb{R}) \subseteq \mathbb{R}^{\times 2} \subseteq \kappa_w^{\times 2}$, where $b \in \mathbb{R}$ is the root of p. Thus $z \in (F^w)^{\times 2}$, by Theorem 1.1.16. Assume now that $p = z$. In this case $\kappa_w = \kappa_{v_p} = \mathbb{C}$. Since $\Gamma_{w|_E} = 2\mathbb{Z}$, because w/v_p is ramified, we have $w(z) \in 2\mathbb{Z}$, whereby $z \in (F^w)^{\times 2}$, by Theorem 1.1.16. □

Proposition 4.2.10. *Let $a_1, a_2, a_3 \in \mathbb{R}$ be such that $a_1 < a_3 < a_3$. Let $q \in \mathbb{R}[X]$ be a monic polynomial without roots in $\mathbb{R}$. For $1 \leq i \leq 3$, let $p_i = X - a_i$. We set $F = \mathbb{R}(X)(\sqrt{p_1p_2p_3q})$. Then*

$$\mathcal{L}(F) = \langle \mathsf{Supp}(q) \rangle \cdot F^{\times 2} \cup p_1 \langle \mathsf{Supp}(q) \rangle \cdot F^{\times 2}.$$

Proof. We first observe that it follows by Theorem 4.2.9 and by Theorem 4.2.4 that $\langle \mathsf{Supp}(q) \rangle \cdot F^{\times 2} \subseteq \mathcal{L}(F) \subseteq \langle \mathsf{Supp}(p_1p_2p_3q) \rangle \cdot F^{\times 2}$. We claim that $p_2, p_3, p_1p_2, p_1p_3 \notin \mathcal{L}(F)$. Let $b \in \mathbb{R}$ be such that $a_1 < b < a_2 < a_3$, and let w be an extension of v_{X-b} to F, where v_{X-b} is the $(X-b)$-adic valuation on $\mathbb{R}(X)$. Then $\kappa_w = \mathbb{R}$, $p_2(b) < 0, p_3(b) < 0, p_1(b)p_2(b) < 0$ and $p_1(b)p_3(b) < 0$, which implies that $\overline{p_2}, \overline{p_3}, \overline{p_1p_2}, \overline{p_1p_3} \notin \kappa_w^{\times 2}$, whereby $p_2, p_3, p_1p_2, p_1p_3 \notin (F^w)^{\times 2}$, by Theorem 1.1.16. Hence $p_2, p_3, p_1p_2, p_1p_3 \notin \mathcal{L}(F)$ and therefore

$$\mathcal{L}(F) \subseteq \langle \mathsf{Supp}(q) \rangle \cdot F^{\times 2} \cup p_1 \langle \mathsf{Supp}(q) \rangle \cdot F^{\times 2},$$

by Theorem 4.2.2. Now, we claim that $p_1 \in \mathcal{L}(F)$. Let $w \in \mathcal{V}(F)$. Since $w|_{\mathbb{R}}$ is trivial, by Theorem 1.1.17, we have that $w|_{\mathbb{R}(X)}$ is equivalent to v_p for some $p \in \mathcal{P}'_{\mathbb{R}}$, by Theorem 1.3.2. Clearly, if either $p = \infty$ or p is quadratic, then $p_1 \in (F^w)^{\times 2}$. Thus, we may assume that there exists some $b \in \mathbb{R}$ such that $p = X - b$. If $b < a_1$, then $\kappa_w = \mathbb{R}\left(\sqrt{p_1(b)p_2(b)p_3(b)q(b)}\right) = \mathbb{C}$. Hence $p_1 \in (F^w)^{\times 2}$, by Theorem 1.1.16. Assume $b = a_1$. In this case, we have that $w(p_2p_3) = 0$ and $p_2(b)p_3(b) > 0$, whereby $p_2p_3q \in (F^w)^{\times 2}$, by Theorem 1.1.16. Since $p_1 = p_2p_3qh^2$, for some $h \in F^\times$, we obtain that $p_1 \in (F^w)^{\times 2}$. In the case where $a_1 < b$, we have $p_1(b) > 0$, and hence $p_1 \in (F^w)^{\times 2}$, by Theorem 1.1.16. Therefore $p_1 \in \mathcal{L}(F)$. This shows that $\mathcal{L}(F) = \langle \mathsf{Supp}(q) \rangle \cdot F^{\times 2} \cup p_1 \langle \mathsf{Supp}(q) \rangle \cdot F^{\times 2}$. □

In the following, we describe two propositions that can be found in [6], which we will use in Theorem 4.2.13 to bound the Kaplansky radical of hyperelliptic function fields when the base field is neither euclidean nor quadratically closed.

Proposition 4.2.11. *Let L/K be a finite field extension and let $N : L^\times \to K^\times$ be the norm map. Then $N(R(L)) \subseteq R(K)$.*

Proof. See [6, Proposition 4.1]. □

Proposition 4.2.12. *Let $F = K(X)$. Then $\mathcal{L}(F/K) = F^{\times 2}$. Moreover, if $K(\sqrt{-1})$ is not quadratically closed, then F is radical-free.*

Proof. See [6, Proposition 3.4].

□

Lemma 4.2.13. *Assume that K is neither euclidean nor quadratically closed. Let $f \in K[X]$ be a square-free polynomial. Set $F = K(X)(\sqrt{f})$. Then*

$$R(F) \subseteq \langle \mathsf{Supp}(f) \rangle \cdot F^{\times 2}.$$

Proof. By the assumption on K, either $|K^\times/K^{\times 2}| \geq 4$ or K is a nonreal field with $|K^\times/K^{\times 2}| = 2$. Consider $v \in \mathcal{V}(F/K)$. By Theorem 1.3.2, κ_v/K is a finite field extension. If κ_v were quadratically closed, it would follow by [35, VIII. Corollary 5.11] that K is quadratically closed or K is euclidean, in contradiction to the hypothesis. Hence κ_v is not quadratically closed. In view of Theorem 4.1.2, this argument implies that $R(F) \subseteq \mathcal{L}(F/K)$. Let $N : F \to K(X)$ be the norm map of $F/K(X)$. Since $K(\sqrt{-1})$ is not quadratically closed, it follows by Theorem 4.2.11 and by Theorem 4.2.12 that $N(R(F)) \subseteq R(K(X)) = K(X)^{\times 2}$. Therefore $R(F) \subseteq \mathcal{L}(F/K) \cap N^{-1}(K(X)^{\times 2})$. Hence, by Theorem 4.2.3 we conclude that $R(F) \subseteq \langle \mathsf{Supp}(f) \rangle \cdot F^{\times 2}$. □

For a field F, we set $\overline{R}(F) = R(F)/F^{\times 2}$.

Theorem 4.2.14. *Let $g \in \mathbb{N}$. Assume that K is neither euclidean nor quadratically closed. Let F/K be a hyperelliptic function field of genus g. Then $|\overline{R}(F)| \leq 2^{2g+2}$.*

Proof. By Theorem 1.3.6 there exists $f \in K[X]$ square-free such that $F = K(X)(\sqrt{f})$. Moreover, it follows by Theorem 4.2.13 that $R(F) \subseteq \langle \mathsf{Supp}(f) \rangle \cdot F^{\times 2}$, which implies that $|\overline{R}(F)| \leq |\langle \mathsf{Supp}(f) \rangle \cdot F^{\times 2}/F^{\times 2}|$. Now, since the maximum possible number of irreducible factors of f is $2g + 2$, we have that $|\overline{R}(F)| \leq 2^{2g+2}$, by Theorem 4.2.2. □

4.3 Function fields of conics

We assume in this section that K is a perfect field of characteristic different from 2. For a function field in one variable F/K, where K is hereditarily euclidean or hereditarily quadratically closed, we have $R(F) = \mathsf{S}_2(F)$; see Theorem 2.4.3. If furthermore F is real, we have that

$$F^{\times 2} \subsetneqq R(F) = \mathsf{S}_2(F) \subsetneqq F^{\times}.$$

In contrast, under the assumption that K is neither euclidean nor quadratically closed, we show in Theorem 4.3.1 that any function field in one variable of genus zero F/K is radical-free.

Theorem 4.3.1. *Let K be a field which is neither euclidean nor quadratically closed. Let F/K be a regular function field of genus zero. Then F is radical-free.*

Proof. By the hypothesis, $K(\sqrt{-1})$ is not quadratically closed. If F/K is a rational function field, then the result follows by [6, Proposition 3.4]. Assume now that F/K is not rational. Since F/K is regular, it follows by Theorem 1.3.4 that $F = K(X)(\sqrt{a_1X^2 + a_2})$, for some $a_1, a_2 \in K^{\times}$. By Theorem 2.1.3 and Theorem 2.1.4 we may consider the following two cases:

(a) We assume that K is pythagorean and $a_1 = a_2 = -1$. It follows by Theorem 4.2.13 that $R(F) \subseteq F^{\times 2} \cup -F^{\times 2}$. Clearly $-1 \notin K^{\times 2}$, because otherwise F/K would be rational. Since K is not euclidean and in particular not hereditarily euclidean, we have $p(F) \geq 3$, by [9, Theorem 4.7]. In particular $D_F\langle 1, 1\rangle \subsetneqq F^{\times}$, whereby $-1 \notin R(F)$. Therefore $R(F) = F^{\times 2}$.

(b) Assume $a_1a_2 \notin K^{\times 2}$. Since $F = K(X)\left(\sqrt{a_1(X^2 + a_2a_1^{-1})}\right)$ and $F \cong K(X)\left(\sqrt{a_2(X^2 + a_1a_2^{-1})}\right)$, it follows by Theorem 4.2.13 that $R(F) \subseteq F^{\times 2} \cup a_iF^{\times 2}$, for $i = 1, 2$. Since K is algebraically closed in F, we have $a_1a_2 \notin F^{\times 2}$, and hence $(F^{\times 2} \cup a_1F^{\times 2}) \cap (F^{\times 2} \cup a_2F^{\times 2}) = F^{\times 2}$.

Therefore F is radical-free. □

Theorem 4.3.1 and Theorem 2.4.3 suggest the following question.

Question 4.3.2. Assume that K is euclidean or quadratically closed but neither hereditarily euclidean nor hereditarily quadratically closed. Let F/K be a function field in one variable of genus zero. Is F radical-free ?

4.4 Arithmetic function fields

We assume further that K is a field of characteristic different from 2. In this section, we focus on function fields F/K in the case where K is the fraction field of a discrete valuation ring. Given such a function field F/K, we study the order of the quotient group $\overline{R}(F)$ and its relation with the genus g of F/K. More precisely, we show that $|\overline{R}(F)| \leq 2^g$. Moreover, in Theorem 4.4.6, we construct for any $g \in \mathbb{N}$ a hyperelliptic function field F/K of genus g such that $|\overline{R}(F)| = 2^g$, which shows the optimality of the bound.

Lemma 4.4.1. *Assume that K carries a nondyadic $\mathbb{Z}$-valuation v. Let $a,b,c \in K^\times$ be such that $c = a^2 + b^2$. If $v(a) \neq v(b)$, then $c \in (K^v)^{\times 2}$.*

Proof. We assume without loss of generality that $v(a) > v(b)$. Then we have $c = b^2(1+(ab^{-1})^2)$ and $\overline{1+ab^{-1}} = \overline{1} \in \kappa_v^{\times 2}$. It follows by Theorem 1.1.16 that $(1+ab^{-1}) \in (K^v)^{\times 2}$. Therefore $c \in (K^v)^{\times 2}$. □

Let v be a $\mathbb{Z}$-valuation on K. Let F/K be a function field in one variable. We recall from Section 3.2 that for a regular model $\mathcal{C}$ of $F/\mathcal{O}_v$, we denote by $b(\mathcal{C})$ the Betti number of the graph $\mathcal{G}(\mathcal{C})$.

Theorem 4.4.2 (D. Harbater-J. Hartmann-D. Krashen)**.** *Let k be a field of characteristic different from 2. Let $F/k((t))$ be a function field in one variable. Let $\mathcal{C}$ be a regular model of $F/k[\![t]\!]$. Then*

$$|\overline{R}(F)| = 2^{b(\mathcal{C})}.$$

Proof. For a point $x \in \mathcal{C}_k$, we denote by F_x the field of fractions of the completion of the local ring $\mathcal{O}_{\mathcal{C},x}$ with respect to its maximal ideal. It follows by [25, Theorem 9.6] that the kernel of the natural local-global homomorphism of Witt groups $\varphi : WF \to \prod_{x\in\mathcal{C}_k} WF_x$ is isomorphic to the abelian 2-group $\mathsf{Hom}(\pi_1(\mathcal{G}(\mathcal{C})), \mathbb{Z}/2\mathbb{Z})$, where $\pi_1(\mathcal{G}(\mathcal{C}))$ is the fundamental group of $\mathcal{G}(\mathcal{C})$ as a topological space. It follows by [27, Proposition 1A.1 and Proposition 1A.2] that the group $\pi_1(\mathcal{G}(\mathcal{C}))$ is freely generated by $b(\mathcal{C})$ elements. Hence $\mathsf{Hom}(\pi_1(\mathcal{G}(\mathcal{C})), \mathbb{Z}/2\mathbb{Z})$ is isomorphic $(\mathbb{Z}/2\mathbb{Z})^{b(\mathcal{C})}$, whereby $\ker\varphi$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{b(\mathcal{C})}$. On the other hand, let $V = \mathcal{V}(v,F)$, and let $\varphi' : WF \to \prod_{v\in V} WF^v$ be the natural global-local homomorphism of Witt groups. It follows by [25, Proposition 9.10, (b)] that $\ker(\varphi') = \ker(\varphi)$. Moreover, it follows by Theorem 4.1.4 that every class in $\ker(\varphi')$ is represented by a 2-dimensional quadratic form $\langle 1, -c\rangle$ for some $c \in R(F)$. Note that by Theorem 4.1.3 we have that $\langle 1, -c\rangle \in \ker(\varphi')$ for all $c \in R(F)$. Moreover, if $\langle 1, -c\rangle$ is Witt equivalent to $\langle 1, -c'\rangle$, for some $c, c' \in R(F)$, then $c \in c'F^{\times 2}$. Thus, there exists a natural group isomorphism $\overline{R}(F) \to \ker(\varphi')$, by $c \mapsto \langle 1, -c\rangle$, which implies that $\ker(\varphi') = \overline{R}(F)$. Therefore $\overline{R}(F)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{b(\mathcal{C})}$, whereby $|\overline{R}(F)| = 2^{b(\mathcal{C})}$. □

Corollary 4.4.3. *Let $g \in \mathbb{N}$. Let k be a field of characteristic different from 2. Let $F/k((t))$ be a regular function field in one variable of genus g. Let $\mathcal{C}$ be a regular model over T with normal crossing. Assume that $H^0(\mathcal{C}_k, \mathcal{O}_{\mathcal{C}_k}) = k$ and that each irreducible component of $\mathcal{C}_k$ intersects at least two other irreducible components. Then*

$$|\overline{R}(F)| \leq 2^g.$$

Proof. The statement follows directly from Theorem 4.4.2 and from Theorem 3.2.9. □

Proposition 4.4.4. *Let k be a field such that $-1 \notin k^{\times 2}$. Let $T = k[\![t]\!]$. Let $b \in (t)$, $a \in T^\times$, and let $f = (X-a)(X^2+b^2) \in k((t))[X]$, and set $F = k((t))(X)(\sqrt{f})$. If $\overline{a} \in -k^{\times 2}$, then*

$$R(F) = F^{\times 2} \cup (X-a)F^{\times 2},$$

and in particular $|\overline{R}(F)| = 2$. If $\overline{a} \in k^{\times 2}$ and k is real, then F is radical-free.

Proof. Let $K = k((t))$. Assume first that $\overline{a} \in -k^{\times 2}$. Set $q = X^2 + b^2$. Consider an arbitrary $\mathbb{Z}$-valuation w on F. We claim that $q \in (F^w)^{\times 2}$ or $X - a \in (F^w)^{\times 2}$. If $w(X) \neq w(b)$ then $q \in (F^w)^{\times 2}$, by Theorem 4.4.1. We may thus assume $w(X) = w(b)$. Suppose first that $w(b) \neq 0$. Then $w|_K$ is non-trivial and thus equivalent to v. Since $(t) \subseteq \mathfrak{m}_w$ and $b \in (t)$, we obtain that $X \in \mathfrak{m}_w$. Hence $w(X-a) = 0$ and $\overline{X-a} = -\overline{a} \in \kappa_w^{\times 2}$, and therefore $X-a \in (F^w)^{\times 2}$ by Theorem 1.1.16. Set $E = K(X)$. Assume now $w(X) = w(b) = 0$. In particular $w|_K$ is trivial and thus $w|_E$ is equivalent to v_p for some $p \in \mathcal{P}'_K$, by Theorem 1.3.2. Clearly, if $p = \infty$ then $q \in (E^{v_p})^{\times 2}$ because q is monic and quadratic. If $p \in \mathcal{P}_K$, let $\beta \in \kappa_{v_p}$ be a root of p. We identify κ_{v_p} with $K(\beta)$. Let v' denote the extension of v to κ_{v_p}. Note that κ_{v_p} is complete with respect to v' by [46, Theorem 14:1]. We have $\overline{q} = q(\beta) = \beta^2 + b^2 \in \kappa_{v_p}$ and $\overline{X-a} = \beta - a \in \kappa_{v_p}$. If $v'(\beta) \neq v'(b)$, then $\overline{q} \in \kappa_{v_p}^{\times 2}$ by Theorem 4.4.1, whereby $q \in (F^w)^{\times 2}$. We may thus assume that $v'(\beta) = v'(b)$. Since $\mathfrak{m}_v \subseteq \mathfrak{m}_{v'}$, we have $v'(\beta) > 0$, whereby $\overline{\beta - a} = -\overline{a} \in \kappa_{v'}^{\times 2}$. Since v' is henselian, we have $\beta - a \in \kappa_{v_p}^{\times 2}$, whereby $X - a \in (E^{v_p})^{\times 2} \subseteq (F^w)^{\times 2}$ by Theorem 1.1.16.

Since $q \in (X-a)F^{\times 2}$, we obtain that $q \in (F^w)^{\times 2}$ for all $w \in \mathcal{V}(F)$. Hence $F^{\times 2} \cup (X-a)F^{\times 2} \subseteq \mathcal{L}(F)$, and $F^{\times 2} \cup (X-a)F^{\times 2} \subseteq R(F)$ by Theorem 4.1.3. Hence $2 \leq |\overline{R}(F)|$. Since q is irreducible over K, we obtain that $|\langle \mathsf{Supp}(f)\rangle \cdot F^{\times 2}/F^{\times 2}| = 2$. Then $|\overline{R}(F)| = 2$, by Theorem 4.2.13. In particular $R(F) = F^{\times 2} \cup (X-a)F^{\times 2}$.

Assume now that $\overline{a} \in k^{\times 2}$ and that k is real. By Theorem 4.2.13 we have that $R(F) \subseteq \langle \mathsf{Supp}(f)\rangle \cdot F^{\times 2}$. We claim that the above inclusion is proper. Let v' be the Gauss extension of v to $K(X)$ with respect to Xb^{-1}, and let w be an extension of v' to F. Set $Z = Xb^{-1}$. Since F is equal to $K(Z)\left(\sqrt{(bZ-a)(Z^2+1)}\right)$, we have that $\kappa_w = k(\overline{Z})\left(\sqrt{-(\overline{Z}^2+1)}\right)$. Note that $q = b^2(Z^2+1), X-a = bZ-a$ in $K[Z]$, and $Z^2+1, bZ-a \in \mathcal{O}_w^\times$. Since k is real, we have $s(\kappa_w) = 2$, hence $\overline{X-1} = -\overline{1} \notin \kappa_w^{\times 2}$ and $\overline{Z}^2 + 1 \notin \kappa_w^{\times 2}$. By Theorem 1.1.16 we have that $X - 1 \notin (F^w)^{\times 2}$ and that $q \notin (F^w)^{\times 2}$. Since w is a v-divisorial valuation on K, we have that neither $X - a$ is in $R(F)$ nor $X^2 + b^2$ is in $R(F)$, by Theorem 4.1.3. Therefore F is radical-free. □

The following describes an example of a function field of a elliptic curve over a complete dicretely valued field which is not radical-free and where the residue field of the valued base field has characteristic different from zero.

Example 4.4.5. Let $p \in \mathbb{N}$ be an odd prime, and let $f = X(X-1)(X-p) \in \mathbb{Q}_p[X]$. We set $F = \mathbb{Q}_p(X)(\sqrt{f})$. We know that $F^{\times 2} \cup (X-1)F^{\times 2} \subseteq R(F)$ by Theorem 4.1.5. Moreover, we know that $R(F) \subseteq F^{\times 2} \cup (X-1)F^{\times 2} \cup (X-p)F^{\times 2} \cup (X-1)(X-p)F^{\times 2}$ by Theorem 4.2.13 and by Theorem 4.2.2. We claim that the above inclusion is proper. It suffices to show that $X \notin \mathcal{L}(v, F)$. Let v be the Gauss extension of v_p to $\mathbb{Q}_p(X)$ with respect to X, and let w be an extension of v to F. Note that w is a v-divisorial valuation on F. Set $Z = \overline{X}$. Then we have that $\kappa_w = \mathbb{F}_p(Z)\left(\sqrt{Z-1}\right)$. Moreover $X \in \mathcal{O}_w^\times$. The only non-trivial square class of $\mathbb{F}_p(Z)$ that becomes trivial in the quadratic extension κ_w is the class of $Z-1$. Hence $Z \notin \kappa_w^{\times 2}$, whereby $X \notin (F^w)^{\times 2}$, by Theorem 1.1.16. Therefore $X \notin \mathcal{L}(F)$. Thus $X, (X-1)(X-p) \notin R(F)$ by Theorem 4.1.3 and we conclude that $R(F) = F^{\times 2} \cup (X-1)F^{\times 2}$.

The following proposition shows that the bound in Theorem 4.4.3 for the Kaplansky radical is optimal.

Theorem 4.4.6. *Let $g \in \mathbb{N}$. Let k be a field such that $-1 \notin k^{\times 2}$. Let $f = \prod_{i=1}^{g+1}(X^2 + t^{2i}) \in k((t))[X]$. Then $F = k((t))(X)(\sqrt{f})$ is a function field of genus g and*

$$R(F) = \langle X^2 + t^{2i} \mid 1 \leq i \leq g+1 \rangle \cdot F^{\times 2}.$$

In particular $|\overline{R}(F)| = 2^g$.

Proof. Let $K = k((t))$. For $1 \leq i \leq g+1$, let $q_i = X^2 + t^{2i}$. We claim that $q_1, \dots, q_{g+1} \in \mathcal{L}(F)$. Since f is monic, by Theorem 4.2.2, it is enough to show that g of the $g+1$ elements $q_1, \dots, q_{g+1}$ are in $\mathcal{L}(F)$. Let w be a $\mathbb{Z}$-valuation on F, and let v be the t-adic valuation on K. If $w(X) \neq w(t^i)$ for all $1 \leq i \leq g+1$, then $q_1, \dots, q_{g+1} \in (F^w)^{\times 2}$ by Theorem 4.4.1. We may therefore assume that $w(X) = w(t^s)$ for some $1 \leq s \leq g+1$. If $w(t^s) \neq 0$, then $w|_K$ is equivalent to a $\mathbb{Z}$-valuation on K, and since v is the unique $\mathbb{Z}$-valuation on K, by Theorem 1.1.20, we have that $w|_K$ is equivalent to v. Hence $w(X) \neq w(t^i)$ for all $i \neq s$, whereby $q_1, \dots, q_{s-1}, q_{s+1}, \dots, q_{g+1} \in (F^w)^{\times 2}$. Let $E = K(X)$. Assume now that $w(t^s) = 0$. In particular $w|_K$ is trivial and thus $w|_E$ is equivalent to v_p for some $p \in \mathcal{P}'_K$. Clearly, if $p = \infty$, then we have that $q_1, \dots, q_{g+1} \in (E^{v_p})^{\times 2}$, because every q_i is quadratic and monic. Assume now that $p \in \mathcal{P}_K$. Let $\beta \in \kappa_{v_p}$ be a root of p and let v' be an extension of v to κ_{v_p}. We identify κ_{v_p} with $K(\beta)$. Note that κ_{v_p} is complete with respect to v', by [46, Theorem 14:1], and thus v' is equivalent to a $\mathbb{Z}$-valuation. If $p \nmid f$, then $w(q_i) = 0$, and thus $\overline{q_i} = q_i(\beta) = \beta^2 + t^{2i}$ in κ_{v_p} for $1 \leq i \leq g+1$. Hence $q_i(\beta) \in \kappa_{v_p}^{\times 2}$ for all $i \in \{1, \dots, g\}$ such that $v'(\beta) \neq v'(t^i)$, by Theorem 4.4.1. If $p \mid q_j$ for some $j \in \{1, \dots, g+1\}$, then $\kappa_{v_p} = K(\sqrt{-1})$, thus $\overline{q_i} = q_i(\beta) = -t^{2j} + t^{2i} \in K(\sqrt{-1})^{\times 2}$ for all $i \neq j$. Since $(E^{v_p})^{\times 2} \subseteq (F^w)^{\times 2}$ we conclude the claim.

Hence $\langle \mathsf{Supp}(f) \rangle \cdot F^{\times 2} \subseteq \mathcal{L}(F)$, and whereby $2^g \leq |\overline{\mathcal{L}}(F)|$, by Theorem 4.2.2. It follows by Theorem 4.1.3 that $2^g \leq |\overline{R}(F)|$. Observe that $q_1, \dots, q_{g+1}$ are irreducible over K, because $-1 \notin \kappa_v^{\times 2}$. Then $|\langle \mathsf{Supp}(f) \rangle / F^{\times 2}| = 2^g$, by Theorem 4.2.2. Now the proof follows by Theorem 4.2.13. □

Chapter 5

Sums of squares in function fields over hereditarily pythagorean fields

In Section 5.1 we will begin by presenting the striking new result that, if K is hereditarily pythagorean, then there exists a uniform upper bound for the Pythagoras number of all finite extensions of $K(X)$, namey 5 is such a bound; see Theorem 5.1.7. This result was obtained towards the end of my doctoral studies in a collaboration with N. Daans, M. Zaninelli and my supervisors. Since the nature of this colaborative result is closely related to a main topic of my thesis, and grew out of discussions I initiated on this topic, I dediced to include a presentation of this result in my thesis, with the consent and support of all collaborators. A key ingredient to obtain the result is the fact that every hereditarily pythagorean field K admits a henselian valuation whose residue field has at most two field orderings. In the case where the residue field is uniquely ordered, we can show that the pythagoras number for any finite extension of $K(X)$ is bounded by 3.

Assume for the rest of the introduction that K is hereditarily pythagorean. For quadratic extensions $F = K(X)(\sqrt{f})$, for some $f \in [X]$ square-free, it was shown in [9, Theorem 3.10] that if f has only real roots, then the pythagoras number of F is equal to 2, and otherwise it is at most 4, and has finite second Pfister index $[\mathsf{S}_4(F) : \mathsf{S}_2(F)]$ bounded in terms of the square class numbers of the residue fields of the roots fields of the nonreal irreducible factors of f. In the case where K admits a henselian $\mathbb{Z}^n$-valuation with uniquely ordered residue field, this yields the finite bound $2^{n(g+1)}$ (see Theorem 5.3.4), for the aforementioned group, where g is the genus of F/K. Two questions arise naturally: does this bound extend to arbitrary finite extensions $F/K(X)$ and is it optimal? In the case of $n = 1$ and $g = 0, 1$ the optimality of above bound was known. In fact, it was shown in [9, Example 5.12] that the second Pfister index of the function field of the curve $Y^2 = -(X^2+1)(X^2+t^2)$ over $\mathbb{R}((t))$, is equal to 4, by proving that t, tX and X represent non-trivial classes in $\mathsf{S}_4(F)/\mathsf{S}_2(F)$. In Section 5.2 we show that the second Pfister index of F is finite for every finite extension $F/K(X)$; see Theorem 5.2.5. This generalizes [4, Theorem 6.11] where the special case $K_n = \mathbb{R}((t_1))\dots((t_n))$ was considered. In Section 5.3 we give an example of a hyperelliptic function field over K_n with second Pfister index $2^{n(g+1)}$, which shows that the bound is optimal.

It is a consequence of [16, Corollary 2.18] that for a real field with Pythagoras number 2 the Pythagoras number of any totally positive quadratic extension is also 2. In particular, the second

Pfister index of a totally positive quadratic extension $F/K(X)$, is trivial when K is hereditarily pythagorean; see [9, Corollary 4.10]. In Section 5.4 we generalize this triviality of the second Pfister index for some real quadratic twists of totally positive hyperelliptic function fields, but with the additional hypothesis that K admits a henselian $\mathbb{Z}^n$-valuation whose residue field is uniquely ordered. There is further evidence that the second Pfister index of any real hyperelliptic function field F/K is strictly smaller than the general optimal bound $2^{n(g+1)}$.

For example, S. Tikhonov and V.I. Yanchevskiĭ showed in [62, Theorem 3] that a real function field of genus zero over a hereditarily pythagorean field has Pythagoras number 2, that is, its second Pfister index is trivial. On the other hand, the function field F of the nonreal conic $Y^2+X^2+1=0$ over K has second Pfister index equal to 2^n, in the case where K admits a henselian $\mathbb{Z}^n$-valuation whose residue field is uniquely ordered. This motivates the following question: If a function field in one variable of genus $g \in \mathbb{N}$ has second Pfister index $2^{n(g+1)}$, does this imply that the field is nonreal? We show in Theorem 5.4.5, using arithmetic geometry, that this question has an affirmative answer in the case where $n = 1$, and we describe in that case all the (necessarily nonreal) hyperelliptic function fields of genus g with second Pfister index 2^{g+1}; see Theorem 5.4.4.

In [61] it was shown that the Pythagoras number of a real hyperelliptic function field over $\mathbb{R}((t))$ of good reduction is equal to 2, or equivalently, its second Pfister index is trivial. Furthermore, the authors realized that the condition that the function field is of good reduction cannot be removed from the hypothesis due to the following example: Let F be the function field of the elliptic curve $Y^2 = (tX-1)(X^2+1)$ over $\mathbb{R}((t))$, which has bad reduction with respect to $\mathbb{R}[[t]]$. Note that $tx = \left(\frac{YX}{X^2+1}\right)^2 + \left(\frac{Y}{X^2+1}\right)^2 + 1^2$. However, it was shown in [61, Example 3.8] that in fact tX is not a sum of two squares in F. This implies that $p(F) > 2$, i.e. the second Pfister index is non-trivial. Thus, it is a natural question to relate the second Pfister index with the reduction type in the case of bad reduction. In Section 5.5 we treat the second Pfister index in the elliptic case and study one example of a non-elliptic curve of genus one, leaving the case of an arbitrary curve of genus one for future research.

5.1 A uniform bound on the Pythagoras number

Let v be a complete rank-one valuation on K, and let F/K be a function field in one variable. We recall that $\mathcal{M}(F/v)$ is the set of valuations w on F of rank one such that $w|_K$ is trivial or $w|_K = v$.

The following statements Theorem 5.1.2, Theorem 5.1.3 and Theorem 5.1.5 are variations of [4, Lemma 6.3, Theorem 6.7, Theorem 6.8] respectively, to the case where v has rank one but is not necessarily discrete.

Lemma 5.1.1. *Let K be a perfect field. Let L/K be an algebraic extension. Then*

$$p'(L) \leq p(K(X)).$$

Proof. If the extension L/K is finite, then the result follows from [4, Lemma 6.3]. Assume that

L/K is algebraic. If $p(K(X)) = \infty$, then the inequality is trivially satisfied. Assume $p(K(X)) < \infty$. Let $r = p(K(X))$, and let $\sigma \in \mathsf{S}_{r+1}(L)$. Let $x_0, \dots, x_r \in L$ be such that $\sigma = x_0^2 + \cdots + x_r^2$, and let $K' = K(x_0, \dots, x_r)$. Hence K'/K is finite. Then $p(K') \leq r$, by [4, Lemma 6.3], and since $K' \subseteq L$, we have that $\sigma \in \mathsf{S}_r(L)$ because $\mathsf{S}_r(K') \subseteq \mathsf{S}_r(L)$. Therefore $p(L) \leq r$. □

Lemma 5.1.2. *Let K be a field and v a nondyadic henselian valuation of rank one with perfect residue field. Let F/K be a function field in one variable. Let $w \in \mathcal{M}(F/v)$ be such that $w|_K$ is trivial. Then $p'(\kappa_w) \leq p(\kappa_v(X))$.*

Proof. Since $w|_K$ is trivial, we have that κ_w/K is a finite extension. Let v' be an extension of v to κ_w. Then v' is henselian. Since κ_v is perfect, by the Primitive Element Theorem, we can chose an element $\theta \in \kappa_{v'}$ such that $\kappa_{v'} = \kappa_v[\theta]$. Hence $\kappa_{v'}$ is the residue field of the q-adic $\mathbb{Z}$-valuation on $\kappa_v(X)$, where q is the minimal polynomial of θ over κ_v. It follows by Theorem 2.2.11 and Theorem 5.1.1 that $p(\kappa_w) \leq p'(\kappa_{v'}) \leq p(\kappa_v(X))$. If κ_w is real, then $p'(\kappa_w) = p(\kappa_w) \leq p(\kappa_v(X))$. If w is nonreal, then $s(\kappa_w) = s(\kappa_{v'})$, by Theorem 2.2.8, because v' is a henselian nondyadic valuation on κ_w. Hence $p'(\kappa_w) = p'(\kappa_{v'}) \leq p(\kappa_v(X))$. □

Theorem 5.1.3. *Let K be a field carrying a nondyadic complete valuation v of rank one. Let F/K be a function field in one variable. Then*

$$p(F) \leq \sup\{p'(\kappa_w) \mid w \in \mathcal{M}(F/v)\} \leq p(F) + 1.$$

Proof. Let $m \geq 2$. By applying Theorem 2.1.11 to the regular quadratic form $m \times \langle 1 \rangle \perp \langle -a \rangle$, for any $a \in F^\times$, we obtain that

$$\mathsf{S}_m(F) = F^\times \cap \Big(\bigcap_{w \in \mathcal{M}(F/v)} \mathsf{S}_m(F^w) \Big).$$

Hence

$$\begin{aligned} p(F) &\leq \inf\{m \geq 2 \mid \mathsf{S}_m(F) = \mathsf{S}_{m+1}(F)\} \\ &\leq \inf\{m \geq 2 \mid \mathsf{S}_m(F^w) = \mathsf{S}_{m+1}(F^w) \text{ for all } w \in \mathcal{M}(F/v)\} \\ &= \sup\{p(F^w) \mid w \in \mathcal{M}(F/v)\}. \end{aligned}$$

It follows by Theorem 2.2.11 that $p(F) \leq \sup\{p'(\kappa_w) \mid w \in \mathcal{M}(F/v)\}$. Now let $w \in \mathcal{M}(F/v)$. If w is real, then $p(F^w) = p(\kappa_w) \leq p(F)$, by Theorem 2.2.11. If w is nonreal, then we have that $p(F^w) \leq p'(\kappa_w) = s(\kappa_w) + 1 \leq p(F) + 1$ by Theorem 2.2.11 and by Theorem 2.2.8. □

Proposition 5.1.4. *Let K be a field and v a henselian valuation of rank one on K. Let F/K be a regular function field in one variable. Let E be the compositum of F and K^v over K. Then, for any integer $k \geq 2$, we have*

$$F^\times \cap \mathsf{S}_k(E) = \mathsf{S}_k(F).$$

In particular $p(F) \leq p(E)$ and $s(F) = s(E)$.

Proof. Let $k \geq 2$. Let $\sigma \in F^\times \cap \mathsf{S}_k(E)$. Let $\varphi = k \times \langle 1 \rangle \perp \langle -\sigma \rangle$. Since φ is isotropic over E, so it is over F, by Theorem 1.3.11 and hence $\sigma \in \mathsf{S}_k(F)$. Therefore $F^\times \cap \mathsf{S}_k(E) = \mathsf{S}_k(F)$ by Theorem 2.1.2. Having this for all $k \geq 2$, we obtain that $p(F) \leq p(E)$ because $p(E) > 1$, by [4, Corollary 4.8]. We claim that $s(F) = s(E)$. Since E is an extension of F, we have $s(E) \leq s(F)$. Assume $s(E) = s < \infty$. Let $\varphi = (s+1) \times \langle 1 \rangle$. Since φ is isotropic over E, it follows from Theorem 1.3.11 that φ is isotropic over F, whereby $s(F) = s(E)$. □

For a field K, we define

$$\widetilde{p}(K) = \sup\{p'(F) \mid F/K \text{ function field in one variable}\} \in \mathbb{N} \cup \{\infty\}.$$

Theorem 5.1.5. *Let K be a field and v a real henselian rank-one valuation. Then $\tilde{p}(K) \leq \tilde{p}(\kappa_v)$.*

Proof. Let $(K^v, \hat{v})$ be the completion of (K, v). We claim that $\tilde{p}(K^v) \leq \tilde{p}(\kappa_v)$. Let E/K^v be a function field in one variable. We need to show that $p'(E) \leq p'(L)$ for some function field in one variable L/κ_v. By Theorem 5.1.3 there exists a valuation $w \in \mathcal{M}(E/\hat{v})$ such that either $p'(\kappa_w) = p(E)$ or $p'(\kappa_w) = p(E) + 1$. We consider the following cases:

a) Assume that $p'(E) \neq p(E) = p'(\kappa_w)$. Then E is nonreal with $s(E) = p(E) = s(\kappa_w) + 1$. Since $s(\kappa_w)$ and $s(E)$ are both powers of two, by Theorem 2.2.2, we obtain that $s(E) = 2$ and $s(\kappa_w) = 1$. Therefore $p'(E) = 3$. Then, for $L = \kappa_v(X)(\sqrt{-(X^2+1)})$ we have $p'(L) = s(L) + 1 = 3 = p'(E)$.

b) Assume that $p'(E) = p(E) = p'(\kappa_w)$. If $w|_K$ is trivial, then it follows by Theorem 5.1.2 that $p'(\kappa_w) \leq p(\kappa_v(X))$, and we choose $L = \kappa_v(X)$. Assume now that $\mathcal{O}_w \cap K = \mathcal{O}_v$. If κ_w/κ_v is a function field in one variable, we may choose $L = \kappa_w$. If κ_w/κ_v is an algebraic extension, it follows by Theorem 5.1.1 that $p'(\kappa_w) \leq p(\kappa_v(X))$, whereby $p'(E) = p(E) \leq p'(L)$, for $L = \kappa_v(X)$.

c) Assume that $p'(E) \neq p(E) = p'(\kappa_w) - 1$. Then E is nonreal and such that $p(E) = s(E) = s(\kappa_w)$. If $w|_K$ is trivial, it follows by Theorem 5.1.2 that

$$p'(E) = s(E) + 1 \leq p(E) + 1 = p'(\kappa_w) \leq p(\kappa_v(X)),$$

and we may choose $L = \kappa_v(X)$. Assume now that $\mathcal{O}_w \cap K = \mathcal{O}_v$. If κ_w/κ_v is a function field in one variable, then since $p(E) = s(\kappa_w) \leq p(\kappa_w)$, we have $p'(E) \leq p'(\kappa_w)$, and we may choose $L = \kappa_w$. If κ_w/κ_v is an algebraic extension, it follows by Theorem 5.1.1 that $p(E) + 1 = s(\kappa_w) + 1 \leq p(\kappa_v(X))$, and we may choose $L = \kappa_v(X)$.

d) Assume that $p'(E) = p(E) = p'(\kappa_w) - 1$. If $w|_K$ is trivial, it follows by Theorem 5.1.2 that $p'(E) = p(E) = p'(\kappa_w) - 1 \leq p(\kappa_v(X))$, and we may choose $L = \kappa_v(X)$. Assume now that $\mathcal{O}_w \cap K = \mathcal{O}_v$. If κ_w/κ_v is a function field in one variable, then we have that

$$p(E) = p'(\kappa_w) - 1 < p'(\kappa_w),$$

whereby $p'(E) \leq p'(\kappa_w)$ and we may choose $L = \kappa_w$. If κ_w/κ_v is an algebraic extension, it follows from Theorem 5.1.1 that $p'(\kappa_w) \leq p(\kappa_v(X))$, whereby $p'(E) = p(E) \leq p(\kappa_v(X))$, and we may choose $L = \kappa_v(X)$.

Hence, so far we have shown that $\tilde{p}(K^v) \leq \tilde{p}(\kappa_v)$. Let now F/K be a regular function field in one variable, and let E be the compositum of F and K^v over K. Then E/K^v is a function field in one variable and by Theorem 5.1.4 we have $p'(F) \leq p'(E)$. Hence we have $\tilde{p}(K) \leq \tilde{p}(K^v) \leq \tilde{p}(\kappa_v)$. □

Theorem 5.1.6. *Let K be a field and v a real henselian valuation on K. Then $\tilde{p}(K) \leq \tilde{p}(\kappa_v)$.*

Proof. First, we assume that v is a valuation with $\mathsf{rk}(v) = n < \infty$, and we show the statement by induction on n. If $n = 0$, then v is the trivial valuation on K, and hence $K = \kappa_v$, whereby the statement is trivial. Assume $n > 0$. By Theorem 1.1.6, there exists a rank-one coarsening v_1 of v Let $\overline{v}$ be the residual valuation of v with respect to v_1. Recall that $\overline{v}$ and v_1 are real henselian valuations on κ_{v_1} and K, of rank $n-1$ and rank 1, respectively, by Theorem 1.1.18,Theorem 1.1.11 and Theorem 2.2.8. Then $\tilde{p}(\kappa_{v_1}) \leq \tilde{p}(\kappa_{\overline{v}})$ by the induction hypothesis, and $\tilde{p}(K) \leq \tilde{p}(\kappa_{v_1})$, by Theorem 5.1.5. Since $\kappa_v = \kappa_{\overline{v}}$, by Theorem 1.1.9, we conclude that $\tilde{p}(K) \leq \tilde{p}(\kappa_{v_1}) \leq \tilde{p}(\kappa_{\overline{v}}) = \tilde{p}(\kappa_v)$.

Consider now of arbitrary rank. If $\tilde{p}(\kappa_v) = \infty$, then the inequality is satisfied trivially. Assume now that $\tilde{p}(\kappa_v) < \infty$. Let $p = \tilde{p}(\kappa_v)$, and let F/K be a function field in one variable. Let $f \in \mathsf{S}_{p+1}(F)$. Let $g \in K[X,Y]$ be an irreducible polynomial such that $F = K[X,Y]/(g)$, and let $f_0, \dots, f_p \in K[X,Y]$ be such that $f = \overline{f}_0^2 + \cdots + \overline{f}_p^2$. Let K_0 be the smallest subfield of K containing all the coefficients of $f_0, \dots, f_p, g$. Hence K_0 is a finitely generated extension of $\mathbb{Q}$ and thus $v_0 = v|_{K_0}$ has finite rank by Theorem 1.1.23. It follows by Theorem 1.1.25 that there exists an intermediate extension $K_0 \subseteq K' \subseteq K$ such that $v' = v|_{K'}$ is a henselian valuation on K' of finite rank and such that $\kappa_{v'} = \kappa_v$. Let $F' = K'[X,Y]/(g)$. Hence $f \in \mathsf{S}_{p+1}(F')$ and F'/K' is a function field in one variable. Therefore $p'(F') \leq p$, by the above case, and then $f \in \mathsf{S}_p(F') \subseteq \mathsf{S}_p(F)$.

We conclude that $p(F) \leq p$. Note that if F' is nonreal, since $F' \subseteq F$, we have $p'(F) = s(F) + 1 \leq s(F') + 1 = p'(F') \leq p$. We conclude that $p'(F) \leq p$, in every case. This shows that $\tilde{p}(K) \leq \tilde{p}(\kappa_v)$. □

Theorem 5.1.7. *Let K be a hereditarily pythagorean field. Let F/K be a function field in one variable. Then $p(F) \leq 5$. Moreover, if K admits a henselian valuation whose residue field is hereditarily euclidean, then $p(F) \leq 3$.*

Proof. It follows by Theorem 2.3.5 that there exists a henselian valuation v on K such that κ_v is hereditarily pythagorean and admits at most two orderings. We first observe that κ_v is uniquely ordered if and only if it is hereditarily euclidean, by Theorem 2.3.12. Assume that κ_v is hereditarily euclidean. Let E/κ_v be a function field in one variable. Then $p(E) \leq 2$, by Theorem 2.4.3. Assume that E is nonreal. By Theorem 2.2.3 we have that $s(E) \leq p(E)$, whereby $p'(E) \leq 3$. This implies that $\tilde{p}(\kappa_v) \leq 3$. Therefore $p(F) \leq 3$ for every function field in one variable F/K, by Theorem 5.1.6.

Assume that κ_v has exactly two orderings, and let E/κ_v be a function field in one variable. Then $p(E) \leq 4$, by Theorem 2.3.9. If E is nonreal, since $s(E) \leq p(E)$, we have that $p'(E) \leq 5$. This implies that $\tilde{p}(\kappa_v) \leq 5$. Therefore $p(F) \leq 5$ by Theorem 5.1.6. □

Corollary 5.1.8. *Let K be a hereditarily pythagorean field. Let $F = K(X,Y)$, the field of rational functions in two variables over K. Then $p(F) \leq 2^3 = 8$.*

Proof. Let $K' = K(X)$ be the rational function field in one variable X over K. Thus $F = K'(Y)$. Since $p(L) < 2^3$ for all finite extensions L/K' by Theorem 5.1.7, it follows by Theorem 2.3.10 that $p(F) \leq 8$. □

The above leaves the question open:

Question 5.1.9. Let K be a hereditarily pythagorean field. Let $F = K(X,Y,Z)$, the rational function field in 3 variables. Is $p(F) < \infty$?

5.2 Finiteness of the second Pfister index

For a valued field (K,v), a function field in one variable F/K, and $r \in \mathbb{N}$, we define

$$\mathcal{X}^r(F/v) = \{\mathcal{O} \in \Omega^*(F/v) \mid 2^r \leq s(\kappa_{\mathcal{O}}) < \infty\},$$

and

$$\mathcal{E}^r(F/v) = \{x \in F^\times \mid x \in \mathcal{O}^\times F^{\times 2} \text{ for all } \mathcal{O} \in \mathcal{X}^r(F/v)\},$$

where $\Omega^*(F/v)$ is defined in Section 1.4.

Lemma 5.2.1. *Let K be a field and $v \in V(K)$. Let F/K be a function field in one variable. Let $\mathcal{O} \in \Omega_1^*(F/v)$. Let $a \in F^\times$ and $r \in \mathbb{N}$. If $a \in \mathcal{E}^r(F/v) \cap \mathcal{O}^\times$, then $\overline{a} \in \mathcal{E}^r(\kappa_{\mathcal{O}}/\overline{v})$, where $\overline{v}$ is the residual valuation of v modulo $v_{\mathcal{O}}|_K$.*

Proof. Let $v_1 = v_{\mathcal{O}}|_K$. It follows by Theorem 1.4.1 and Theorem 1.4.2 that v_1 is equivalent to a $\mathbb{Z}$-valuation. Let $\overline{v}$ be the residual valuation of v modulo v_1. Let $\mathcal{O}' \in \mathcal{X}^r(\kappa_{\mathcal{O}}/\overline{v})$. Let $a \in \mathcal{E}^r(F/v) \cap \mathcal{O}^\times$. We need to show that $\overline{a} \in \mathcal{O}'\kappa_{\mathcal{O}}^{\times 2}$. Let $v' = v_{\mathcal{O}'}|_{\kappa_{v_1}}$. Let w be a composition of $v_{\mathcal{O}}$ with $v_{\mathcal{O}'}$, and let ν be a composition of v_1 with v'. Since $\kappa_{\mathcal{O}'} = \kappa_w$ and $\kappa_{v'} = \kappa_\nu$ by Theorem 1.1.12, we have that κ_w/κ_ν is a function field in one variable with $2^r \leq s(\kappa_w) < \infty$ and $\mathcal{O}_v \subseteq \mathcal{O}_{w|_K} = \mathcal{O}_\nu$, that is $\mathcal{O}_w \in \mathcal{X}^r(F/v)$. Then $a \in \mathcal{O}_w^\times F^{\times 2} \cap \mathcal{O}^\times$, because $a \in \mathcal{E}^r(F/v)$, which implies that $\overline{a} \in \mathcal{O}'^\times \kappa_{\mathcal{O}}^{\times 2}$ by Theorem 1.1.13. □

Lemma 5.2.2. *Let $r \in \mathbb{N}$. Let K be a field carrying a real henselian valuation v such that $\tilde{p}(\kappa_v) \leq 2^r$. Then $p(K(X)) \leq 2^r$. Moreover, let K'/K be a finite extension. Then $p(K') < 2^r$, and $s(K') \leq 2^{r-1}$ if K' is nonreal.*

Proof. We have $p(K(X)) \leq \tilde{p}(K) \leq \tilde{p}(\kappa_v)$, by Theorem 5.1.6. This implies that $p(K(X)) \leq 2^r$. The rest follows directly by Theorem 2.3.10. □

We recall that for a rank-one valuation v on a field K, the valued field $(K^v, \hat{v})$ is the completion of (K, v).

Lemma 5.2.3. *Let $r \in \mathbb{N}$. Let K be a field and v a real henselian valuation in $V(K)$ such that $\tilde{p}(\kappa_v) \leq 2^r$. Let v_1 be a rank-one coarsening of v. Let $\overline{v}$ be the residual valuation of v modulo v_1. Let v' be a composition of $\hat{v}_1$ with $\overline{v}$. Let F/K be a regular function field in one variable. Let E be the compositum of F and K^{v_1} over K. Then*

$$\mathsf{S}(F) \cap \mathcal{E}^r(F/v) \subseteq \mathsf{S}(E) \cap \mathcal{E}^r(E/v').$$

Proof. Let $\mathcal{O} \in \mathcal{X}^r(E/v')$. Let $\mathcal{O}_F = \mathcal{O} \cap F$ and $\mathcal{O}_K = \mathcal{O} \cap K$. We claim that $\mathcal{O}_F \in \mathcal{X}^r(F/v)$ or $\kappa_{\mathcal{O}_F}$ is real. By definition we have that $\mathcal{O}_{v'} \subseteq \mathcal{O} \cap K^{v_1}$, and since v is henselian, we have that $\mathcal{O} \cap K^{v_1} \subseteq \mathcal{O}_{\hat{v}_1} \subseteq K^{v_1}$, Theorem 1.1.20. Hence $\mathcal{O}_v \subseteq \mathcal{O}_K \subseteq \mathcal{O}_{v_1} \subseteq K$. We denote by ν the residual valuation of v modulo $v_{\mathcal{O}_K}$. We recall that ν is a henselian valuation on $\kappa_{\mathcal{O}_K}$ such that $\kappa_\nu = \kappa_v$, by Theorem 1.1.18. Since $\tilde{p}(\kappa_v) \leq 2^r$, it follows from Theorem 2.3.10 that $s(L) \leq 2^{r-1}$ for every finite nonreal extension L/κ_v. Let $L'/\kappa_{\mathcal{O}_K}$ be a finite nonreal extension. Since ν is henselian, any extension of ν to L' is again henselian, and by Theorem 2.2.8 we obtain that $s(L') \leq 2^{r-1}$. Since $\kappa_{\mathcal{O}_F} \subseteq \kappa_{\mathcal{O}}$, we have that $s(\kappa_{\mathcal{O}_F}) \geq s(\kappa_{\mathcal{O}}) \geq 2^r$ and hence the extension $\kappa_{\mathcal{O}_F}/\kappa_{\mathcal{O}_K}$ cannot be algebraic. Hence $\kappa_{\mathcal{O}_F}/\kappa_{\mathcal{O}_K}$ is transcendental. If $\kappa_{\mathcal{O}_F}$ is nonreal, since $s(\kappa_{\mathcal{O}_F}) \geq 2^r$, then $2^r < p(\kappa_{\mathcal{O}_F})$, by Theorem 2.2.10, because $v_{\mathcal{O}|_F}$ is equivalent to a valuation in $V(F)$, by Theorem 1.4.2. This implies that $\kappa_{\mathcal{O}_F}/\kappa_{\mathcal{O}_K}$ cannot be ruled, by Theorem 5.2.2, whenever $\kappa_{\mathcal{O}_F}$ is nonreal. Hence $\mathcal{O}_F \in \mathcal{X}^r(F/v)$ because $\mathcal{O}_v \subseteq \mathcal{O}_K$. We conclude that $s(\kappa_{\mathcal{O}_F}) \geq 2^r$.

Let $a \in \mathsf{S}(F) \cap \mathcal{E}^r(F/v)$. Hence $a \in \mathcal{O}_F^\times F^{\times 2}$ because $\mathcal{O}_F \in \mathcal{X}^r(F/v)$ or $\kappa_{\mathcal{O}_F}$ is real, and the latter follows by Theorem 2.2.9. Therefore $a \in \mathcal{O}_F^\times F^{\times 2} \subseteq \mathcal{O}^\times E^{\times 2}$. Since $\mathcal{O}$ was arbitrarily chosen, we conclude that $a \in \mathsf{S}(E) \cap \mathcal{E}^r(E/v')$. □

Proposition 5.2.4. *Let $r \in \mathbb{N}$. Let K be a field and v a real henselian valuation in $V(K)$ such that $\tilde{p}(\kappa_v) \leq 2^r$. Let F/K be a regular function field in one variable. Then*

$$\mathsf{S}(F) \cap \mathcal{E}_r(F/v) = \mathsf{S}_{2^r}(F).$$

Proof. It follows from Theorem 2.2.9 that $\mathsf{S}_{2^r}(F) \subseteq \mathsf{S}(F) \cap \mathcal{E}^r(F/v)$. Let $n = \mathsf{rk}(v)$. Let us now show by induction over n that $\mathsf{S}(F) \cap \mathcal{E}_r(F/v) \subseteq \mathsf{S}_{2^r}(F)$. For $n = 0$, it follows trivially from the assumption.

Let now $n > 0$. By Theorem 1.1.6, there exists a rank-one coarsening v_1 of v. Let v' be a composition of $\hat{v}_1$ with $\overline{v}$. It follows by Theorem 1.1.22 that v' is a henselian valuation of rank n on K^{v_1} such that $\kappa_v = \kappa_{v'}$ and $\mathcal{O}_{v'} \cap K = \mathcal{O}_v$.

Let E be the compositum of F and K^{v_1} over K. Let $\sigma \in \mathsf{S}(F) \cap \mathcal{E}^r(F/v)$. Then $\sigma \in \mathsf{S}(E) \cap \mathcal{E}^r(E/v')$, by Theorem 5.2.3. Let φ be the quadratic form $2^r \times \langle 1 \rangle \perp \langle -\sigma \rangle$ over F. We first show that φ is isotropic over E.

Let w be a rank one valuation on E. We claim that $p(E^w) \leq 2^r$. If $w|_{K^{v_1}}$ is trivial, then κ_w/K^{v_1} is

a finite field extension, and it follows that $p(E^w) \leq p'(\kappa_w)$, by Theorem 2.2.11 and that $p'(\kappa_w) \leq 2^r$ by Theorem 5.2.2. Let us assume now that $\mathcal{O}_w \cap K^{v_1} = \mathcal{O}_{\hat{v}_1}$ and $\kappa_w/\kappa_{\hat{v}_1}$ is algebraic. Since the residual valuation $\overline{v'}$ of v' modulo $\hat{v}_1$ is a henselian valuation on $\kappa_{\hat{v}_1}$ such that $\tilde{p}(\kappa_{\overline{v'}}) \leq 2^r$, it follows by Theorem 5.2.2 and by Theorem 5.1.1 that $p'(\kappa_w) \leq p(\kappa_{\hat{v}_1}(X)) \leq 2^r$. Since $p(E^w) \leq p'(\kappa_w) \leq 2^r$ by Theorem 5.1.1 and by Theorem 2.2.11, we have $p(E^w) \leq 2^r$. Therefore φ is isotropic over E^w in both cases.

Let us assume now that $\mathcal{O}_w \cap K^{v_1} = \mathcal{O}_{\hat{v}_1}$ and $\kappa_w/\kappa_{\hat{v}_1}$ is a function field in one variable. We claim that φ is isotropic over E^w. If $s(\kappa_w) \leq 2^{r-1}$, since $s(E^w) = s(\kappa_w)$ by Theorem 2.2.8, we have that φ is isotropic over E^w. Let $d \in \mathbb{N}, x_1, \dots, x_d \in F$ be such that $\sigma = x_1^2 + \cdots + x_d^2$. If κ_w is real, then $w(\sigma) = \min\{2w(x_1), \dots, 2w(x_d)\}$, by [4, Lemma 4.1]. If $2^r \leq s(\kappa_w) < \infty$, then $2^r < p(\kappa_w)$. Hence $\kappa_w/\kappa_{\hat{v}_1}$ cannot be ruled by Theorem 5.2.2, which implies that $\mathcal{O}_w \in \mathcal{X}^r(E/v')$. In any case $w(\sigma) \in 2\Gamma_w$, because $\sigma \in \mathcal{E}^r(E/v')$, and thus $w(\sigma) = 2w(y)$ for some $y \in E$. Let $\tau = \sigma y^{-2}$. Then $\overline{\tau} \in \mathsf{S}(\kappa_w)$ and, if $\varphi' = 2^r \times \langle 1 \rangle \perp \langle -\tau \rangle$ is isotropic over E^w, then φ is isotropic over E^w. By the induction hypothesis, we have that $\mathsf{S}_{2^r}(\kappa_w) = \mathsf{S}(\kappa_w) \cap \mathcal{E}^r(\kappa_w/\overline{v'})$. Since $\tau \in \mathcal{E}^r(E/v')$, it follows by Theorem 5.2.1 that $\overline{\tau} \in \mathcal{E}^r(\kappa_w/\overline{v'})$, and hence $\overline{\tau} \in \mathsf{S}_{2^r}(\kappa_w)$. Hence $\overline{\varphi'_r}$ is isotropic over κ_w, and then φ' is isotropic over E^w, by Theorem 2.2.7, whereby φ is isotropic over E^w.

By Theorem 2.1.11, φ is isotropic over E if and only if φ is isotropic over E^w for every rank one valuation w on E such that $w|_{K^{v_1}}$ is trivial or $\mathcal{O}_w \cap K^{v_1} = \mathcal{O}_{\hat{v}_1}$. If $\mathcal{O}_w \cap K^{v_1} = \mathcal{O}_{\hat{v}_1}$ then it follows byTheorem 1.4.1 that, either $\kappa_w/\kappa_{\hat{v}_1}$ is algebraic or $\kappa_w/\kappa_{\hat{v}_1}$ is a function field in one variable. By the above, in any case φ is isotropic over E, and it follows from Theorem 1.3.11 that φ is isotropic over F, whereby $\sigma \in \mathsf{S}_{2^r}(F)$. □

For a field K and $r \in \mathbb{N}$, we set $G_r(K) = \mathsf{S}(K)/\mathsf{S}_{2^r}(K)$.

Theorem 5.2.5. *Let $n, r \in \mathbb{N}$. Let K be a field carrying a real henselian $\mathbb{Z}^n$-valuation v such that $\tilde{p}(\kappa_v) \leq 2^r$. Let F/K be a function field in one variable. Then*

$$|G_r(F)| = 2^{|\mathcal{X}^r(F/v)|}.$$

In particular $|G_r(F)|$ is finite.

Proof. It follows by Theorem 1.4.6 that we may choose a finite and saturated set $W \subseteq \Omega(F)$ such that $\mathcal{X}^r(F/v) \subseteq W$, and it follows by Theorem 1.2.7 that we can choose a coherent subset $S' \subseteq V(F)$ such that $W = \{\mathcal{O}_w \mid w \in S'\}$. We consider $S = \{w \in S' \mid \mathcal{O}_w \in \mathcal{X}^r(F/v)\}$. Let $\Phi : S(F) \to \prod_{w \in S} \mathbb{Z}/2\mathbb{Z}$ be the map given by the composition of $\Phi_{S'}|_{\mathsf{S}(F)}$, where $\Phi_{S'} : F^\times \to \prod_{w \in S'} \mathbb{Z}$ is defined in Equation (1.1), and the natural surjective map

$$\prod_{w \in S'} \mathbb{Z} \to \prod_{w \in S} \mathbb{Z} \to \prod_{w \in S} \mathbb{Z}/2\mathbb{Z}.$$

We claim that Φ is a surjective group homomorphism with $\ker(\Phi) = \mathsf{S}_{2^r}(F)$.

First, we observe that Φ is a group homomorphism simply because valuations and projections are group homomorphisms. The inclusion $\mathsf{S}_{2^r}(F) \subseteq \ker(\Phi)$ follows directly from Theorem 5.2.4. Let

us show that $\ker(\Phi) \subseteq \mathsf{S}_{2^r}(F)$. Let $\sigma \in \ker(\Phi)$ and we assume that $\sigma \notin \mathsf{S}_{2^r}(F)$. By Theorem 5.2.4, $\sigma \notin \mathcal{O}^\times F^{\times 2}$, for some $\mathcal{O} \in \mathcal{X}^r(F/v)$. Let $w \in S$ be such that $\mathcal{O}_w = \mathcal{O}$, and let $a_1, \dots, a_{\mathsf{rk}(w)} \in \mathbb{Z}$ be such that $w(\sigma) = (a_1, \dots, a_{\mathsf{rk}(w)})$. Since $w(\sigma) \notin 2\mathbb{Z}$, there exists $d \leq \mathsf{rk}(w)$ such that $a_d \notin 2\mathbb{Z}$. Let $w' = \pi_d \circ w$. Since $w'(\sigma) \notin 2\mathbb{Z}$, the residue field $\kappa_{w'}$ cannot be real by [4, Lemma 4.1]. Let $\overline{w}$ be the residual valuation of w modulo w'. Then $2^r \leq s(\kappa_w) = s(\kappa_{\overline{w}}) \leq s(\kappa_{w'}) < \infty$, which implies that $\mathcal{O}_{w'} \in \mathcal{X}^r(F/v)$. Since S' is coherent, we obtain that $w' \in S'$, and since $\mathcal{O}_{w'} \in \mathcal{X}^r(F/v)$, we have $w' \in S$. But $\pi^1(w'(\sigma)) = a_d \notin 2\mathbb{Z}$, which contradicts the fact that $\sigma \in \ker(\Phi)$. This shows that $\ker(\Phi) = \mathsf{S}_{2^r}(F)$.

We show now that Φ is surjective. Let $(e_w)_{w\in S}$ be the canonical basis of $\prod_{w\in S} \mathbb{Z}/2\mathbb{Z}$ as a $\mathbb{Z}/2\mathbb{Z}$-module. Consider $w \in S$, and let $d = \mathsf{rk}(w)$. We claim that there exists $\sigma \in \mathsf{S}(F)$ with $\Phi(\sigma) = e_w$. Since $2^r \leq s(\kappa_w) < \infty$, there exists $f \in \mathfrak{m}_w$ and $x_1, \dots, x_m \in \mathcal{O}_w^\times$, for some $m \in \mathbb{N}$, such that $f = 1 + x_1^2 + \cdots + x_m^2$. Let $b = (1 - \frac{f}{2})^2 + x_1^2 + \cdots + x_m^2 = \frac{f^2}{4}$. Note that $w(b) = 2w(f) > e_1^d$, where e_1^d is the minimal positive element of $\mathbb{Z}^d$. For $\nu \in S$, we set $n_\nu = \mathsf{rk}(\nu)$, and we denote by $p_d^{n_\nu}$ the n_ν-tuple $(p_1, \dots, p_{n_\nu})$ such that $p_d = 1$ and $p_i = 0$ for all $i \neq d$. By Theorem 1.5.2, there exists $z \in F$ such that for all $\nu \in S$ we have that $\nu(z) = p_d^{n_\nu}$ if ν is a refinement of w and $\nu(z) < \min\{0, \nu(f)\}$ otherwise. Let $\sigma = (z - (1 - \frac{f}{2}))^2 + x_1^2 + \cdots + x_m^2$ in $\mathsf{S}(F)$. Let $\nu \in S$ be such that $\mathcal{O}_\nu$ is a refinement of $\mathcal{O}_w$. Since $\sigma = z(z - 2(1 - \frac{f}{2})) + b$ and $\nu(z) < \nu(b)$ we have that $\nu(\sigma) = \nu(z) = p_d^{n_\nu}$. Let $\nu \in S$ be such that $\mathcal{O}_\nu$ is not a refinement of $\mathcal{O}_w$. Since $\nu(z) < \min\{0, \nu(f)\}$, we have that $\nu(\sigma) = \nu(z(z - 2(1 - \frac{f}{2}))) = 2\nu(z)$. Thus $\pi^1(\nu(\sigma)) = 0$ if $\mathcal{O}_\nu$ is a proper refinement of $\mathcal{O}_w$ and $\pi^1(\nu(\sigma)) \in 2\mathbb{Z}$ otherwise, except when $\nu = w$. Moreover, by Theorem 1.2.2 we have that $w(\sigma) = (\pi^d \circ \nu)(\sigma) = p_d^d$, where $\nu \in S$ and $\mathcal{O}_\nu$ is a refinement of $\mathcal{O}_w$. Thus $\pi^1(w(\sigma)) = 1$, whence $\Phi(\sigma) = e_w$. Therefore Φ is surjective and $|G_r(F)| = 2^{|\mathcal{X}^r(F/v)|}$. □

Corollary 5.2.6. *Let $n \in \mathbb{N}$. Assume that K carries a henselian $\mathbb{Z}^n$-valuation v such that κ_v is hereditarily pythagorean. Let F/K be a function field in one variable. Then the following hold*

(1) If κ_v has one ordering, then $|G_1(F)| = 2^{|\mathcal{X}_1(F/v)|}$.

(2) If κ_v has two orderings, then $|G_2(F)| = 2^{|\mathcal{X}_2(F/v)|}$.

Proof. We assume first that κ_v has only one ordering. It follows by Theorem 2.3.12 that $p(E) \leq 2$ for all function fields in one variable E/κ_v. Applying Theorem 5.2.5 to case where $r = 1$, we obtain that $|G_1(F)| = 2^{|\mathcal{X}^1(F/v)|}$. Now assume that κ_v has exactly two ordering. Then $p(E) \leq 2^2 = 4$ for all function fields in one variable E/κ_v, by Theorem 2.3.9. Applying Theorem 5.2.5 to the case where $r = 2$, we obtain that $|G_2(F)| = 2^{|\mathcal{X}^2(F/v)|}|$. □

5.3 An effective optimal bound on the index in the hyperelliptic case

In this section, we will apply the valuation-theoric description of the order of $G_1(F)$ from the previous section in the case where F/K is a hyperelliptic function field, where K is a field carrying

a henselian $\mathbb{Z}^n$-valuation whose residue field is hereditarily euclidean, in order to give an effective bound in terms of n and of the genus g of F/K.

The following Lemma is a variation of [22, Proposition 1.2.8].

Lemma 5.3.1. *Let (K,v) be a valued field. Let $a_1,a_2 \in \mathcal{O}_v, b_1,b_2 \in \mathcal{O}_v \setminus \{0\}$ and let v_i be the Gauss extension of v to $K(X)$ with respect to $Y_i = \frac{X-a_i}{b_i}$, for $i = 1,2$. Then $v_1 = v_2$ if and only if $2v(a_1-a_2) \geq v(b_1b_2)$ and $v(b_1) = v(b_2)$.*

Proof. We note that $Y_2 = \dfrac{X-a_2}{b_2} = \dfrac{b_1Y_1 + (a_1-a_2)}{b_2}$. Let

$$M = \begin{pmatrix} b_1 & a_1-a_2 \\ 0 & b_2 \end{pmatrix}$$

By [22, Proposition 1.2.7] we have that $v_1 = v_2$ if and only if there exists some $c \in K^\times$ such that $c^{-1}M \in \mathbb{GL}_2(\mathcal{O}_v)$. Moreover, $c^{-1}M \in \mathbb{GL}_2(\mathcal{O}_v)$ if and only if $v(a_1-a_2) \geq v(c), v(b_1) \geq v(c), v(b_2) \geq v(c)$ and $2v(c) = v(b_1b_2)$. Such $c \in K^\times$ exists if and only if $2v(a_1-a_2) \geq v(b_1b_2)$ and $v(b_1) = v(b_2)$. □

Proposition 5.3.2. *Let $g \in \mathbb{N}$. Let (K,v) be a valued field with κ_v hereditarily pythagorean. Let $a_0,\dots,a_g \in \mathcal{O}_v$ and $b_0,\dots,b_g \in \mathcal{O}_v \setminus \{0\}$ be such that for every pair (i,j) with $i \neq j$ and $0 \leq i,j \leq g$ either $2v(a_i-a_j) < v(b_ib_j)$ or $v(b_i) \neq v(b_j)$. We set*

$$f(X) = -((X-a_0)^2 + b_0^2)\cdots((X-a_g)^2 + b_g^2).$$

Let $F = K(X)(\sqrt{f})$. Then there exists $g+1$ different unramified extensions w of v to F such that $1 < s(\kappa_w) < \infty$. Moreover, $\kappa_w \simeq \kappa_v(X)(\sqrt{-(X^2+1)})$ for every such extension w.

Proof. For $0 \leq i \leq g$, let $q_i = (X-a_i)^2 + b_i^2$ and $Y_i := b_i^{-1}(X-a_i)$, and let v_i be the Gauss extension of v to $K(X)$ with respect to Y_i. By Theorem 5.3.1, the hypothesis on $a_0,b_0,\dots,a_g,b_g$ implies that all the valuations $v_0,\dots,v_g$ are different. For $i \in \{0,\dots,g\}$, let w_i be an extension of v_i to F. We claim that κ_{w_i} is the function field of the conic $Y^2+X^2+1=0$ over κ_v. Without loss of generality, we consider $i=0$. Set

$$Z_j = \begin{cases} 1+Y_j^2 & \text{if } v_0(Y_j) \geq 0, \\ 1+Y_j^{-2} & \text{if } v_0(Y_j) < 0. \end{cases}$$

Note that, since κ_{v_0} is real, $Z_j \in \mathcal{O}_{v_0}^\times$ for all $0 \leq j \leq g$. Thus

$$\overline{Z_j} = \begin{cases} 1+\overline{Y_j}^2 & \text{if } v_0(Y_j) = 0, \\ \overline{1} & \text{otherwise .} \end{cases}$$

Let $1 \leq j \leq g$. We show that $\overline{Z_j} \in \kappa_{v_0}^{\times 2}$. If $v_0(Y_j) \neq 0$, then $\overline{Z_j} = \overline{1} \in \kappa_v^{\times 2}$. Assume $v_0(Y_j) = 0$. Then $\overline{Z_j} = \overline{1} + \overline{Y_j}^2$. It follows by [17, Corollary 2.2.2], that v_j is the unique extension of v to $K(X)$ such that the residue of $\overline{Y_j}$ on κ_{v_j} is transcendental over κ_v. Since $v_0 \neq v_j$, we have that $\overline{Y_j} \in \kappa_{v_0}^\times$ is algebraic over κ_v. Since $\kappa_{v_0} = \kappa_v(\overline{Y_0})$, we have that $\overline{Y_j} \in \kappa_v^\times$. Therefore $\overline{Z_j} \in \mathsf{S}_2(\kappa_v) = \kappa_v^{\times 2}$. Since j

was arbitrarily chosen, we obtain that $\overline{Z_j} \in \kappa_v^{\times 2}$ for every $1 \leq j \leq g$. Thus

$$\kappa_{w_0} = \kappa_v(\overline{Y_0})\left(\sqrt{-(\overline{Y_0}^2+1)\prod_{1=j}^{g}\overline{Z_j}}\right) = \kappa_v(\overline{Y_0})\left(\sqrt{-(\overline{Y_0}^2+1)}\right).$$

Since $\overline{Y_0}^2+1$ is irreducible over $\kappa_v[\overline{Y_0}]$, we obtain the first statement. Moreover, $\Gamma_{w_0} = \Gamma_{v_0}$ and w_0 is the unique extension of v_0 to F, by Theorem 1.1.21. Therefore, for all $w \in \{w_0, \dots, w_g\}$ we have $\kappa_w \simeq \kappa_v(X)(\sqrt{-(X^2+1)})$. □

For a field K, we set $G(K) = G_1(K)$.

Proposition 5.3.3. *Let K be a hereditarily pythagorean field. Let $f \in K[X]$ be square-free. Set $F = K(X)(\sqrt{f})$. Let $K_1, \dots, K_r$ denote the root fields of the distinct nonreal irreducible factors of f. Then*

$$|G(F)| \leq \prod_{i=1}^{r} |K_i^{\times}/K_i^{\times 2}|.$$

Proof. See [9, Theorem 3.10]. □

Proposition 5.3.4. *Let $n \in \mathbb{N}$. Let K be a field carrying a henselian $\mathbb{Z}^n$-valuation v with κ_v hereditarily euclidean. Let $f \in K[X]$ be a square-free polynomial. Set $F = K(X)(\sqrt{f})$. Then*

$$|G(F)| \leq 2^{n(g+1)},$$

where g is the genus of F/K.

Proof. Note that K is hereditarily pythagorean by Theorem 2.3.5. Let $K_1, \dots, K_r$ be the root fields of the distinct nonreal irreducible factors of f. By Theorem 5.3.3 we have that

$$|G(F)| \leq \prod_{i=1}^{r} |K_i^{\times}/K_i^{\times 2}|.$$

Consider $i \in \{1, \dots, r\}$. Note that, since K is hereditarily pythagorean, we have $-1 \in K_i^{\times 2}$. Since K_i/K is a finite extension, there exists a henselian $\mathbb{Z}^n$-valuation v_i on K_i such that $\mathcal{O}_{v_i} \cap K = \mathcal{O}_v$. Then $-1 \in \kappa_{v_i}^{\times 2}$. By Theorem 2.3.6 we have that $|K_i^{\times}/K_i^{\times 2}| = 2^n|\kappa_{v_i}^{\times}/\kappa_{v_i}^{\times 2}|$. By [35, VII. Theorem 7.15] we have that κ_{v_i} is quadratically closed, whence $|K_i^{\times}/K_i^{\times 2}| = 2^n$. Let $g \in \mathbb{N}$ be such that $\deg f = 2g+1$ or $2g+2$. Then $r \leq g+1$, hence $|G(F)| \leq 2^{n(g+1)}$. □

Remark 5.3.5. Under the assumption of Theorem 5.3.4, since f is a polynomial of $\deg 2g+1$ or $\deg 2g+2$, it follows that the unique situation where this bound can be optimal is when $f \in K[X]$ is a square-free polynomial of degree $2(g+1)$ and has $g+1$ nonreal irreducible factors.

We recall that $\pi_d : \mathbb{Z}^n \to \mathbb{Z}^d$ is the projection on the first d-components of $\mathbb{Z}^n$. Let (K, v) be a valued field, and let F/K be a function field in one variable. We set $\mathcal{X}(F/v) = \mathcal{X}^1(F/v)$.

Lemma 5.3.6. *Let $n \in \mathbb{N}$ Assume that K is a field carrying a henselian $\mathbb{Z}^n$-valuation with hereditarily euclidean residue field. Let F/K be a regular function field of genus zero. Then*

$$|G(F)| = \begin{cases} 2^n & \text{if } F \text{ is nonreal,} \\ 1 & \text{if } F \text{ is real.} \end{cases}$$

Proof. We assume that F is nonreal. Then $F = K(X)(\sqrt{\alpha \cdot q})$, where q is a monic irreducible quadratic polynomial over K, by Theorem 1.3.4. Then $q(X) = (X-a)^2 + b^2$, for some $a, b \in K$, by Theorem 2.3.11. Moreover $\alpha \in -K^{\times 2}$, because F is nonreal. Replacing $X' = X - a$, we have that F is isomorphic to $K(X)(\sqrt{-(X^2+1)})$. We prove that statement by induction on n. For $n = 0$, it follows from Theorem 2.3.13 that $G(F)$ is trivial. Let $n \geq 1$. Let $v_1 = \pi_1 \circ v$. Let w' be the Gauss extension of v_1 to $K(X)$ with respect to X and let w be an extension of w' to F. Since κ_{v_1} is real, the polynomial $X^2 + 1$ is irreducible over κ_{v_1}. Then we have $\kappa_w = \kappa_{v_1}(\overline{X})\left(\sqrt{-(\overline{X}^2+1)}\right)$, and $\mathcal{O}_w \in \mathcal{X}(F/v) \cap \Omega_1(F)$. It follows from [5, Corollary 3.6] that $\mathcal{O}_w$ is the unique valuation ring in $\mathcal{X}(F/v) \cap \Omega_1(F)$, and hence every $\mathcal{O} \in \mathcal{X}(F/v)$ is a refinement of $\mathcal{O}_w$, by Theorem 1.1.12. Let $\overline{v}$ be the residual valuation of v modulo v_1. Thus $|\mathcal{X}(F/v)| = 1 + |\{\mathcal{O} \in \Omega(\kappa_w) \mid \mathcal{O} \in \mathcal{X}(\kappa_w/\overline{v})\}|$, whereby $|G(F)| = 2|G(\kappa_w)|$, by Theorem 5.2.5. Note that $\overline{v}$ is a henselian $\mathbb{Z}^{n-1}$-valuation on κ_{v_1} with hereditarily euclidean residue field. Thus, by the induction hypothesis $|G(\kappa_w)| = 2^{n-1}$. Therefore $|G(F)| = 2^n$.

If F is real, then $p(F) = 2$ by [62, Theorem 3], whereby $|G(F)| = 1$. □

Corollary 5.3.7. *Let $n, g \in \mathbb{N}$. Assume that K carries a henselian $\mathbb{Z}^n$-valuation v with hereditarily euclidean residue field. Let $v_1 = \pi_1 \circ v$. Let $a_0, \dots, a_g \in \mathcal{O}_{v_1}$ and $b_0, \dots, b_g \in \mathcal{O}_{v_1} \setminus \{0\}$ be such that for every pair (i, j) with $i \neq j$ and $0 \leq i, j \leq g$ either $2v_1(a_i - a_j) < v_1(b_i b_j)$ or $v_1(b_i) \neq v_1(b_j)$. We set*

$$f(X) = -((X-a_0)^2 + b_0^2) \cdots ((X-a_g)^2 + b_g^2).$$

Let $F = K(X)(\sqrt{f})$. Then

$$|G(F)| = 2^{n(g+1)}.$$

Proof. It follows by Theorem 5.3.2 that there exist $g+1$ extensions $w_0, \dots, w_g$ of v_1 such that $\mathcal{O}_{w_i} \in \mathcal{X}(F/v) \cap \Omega_1(F)$. It follows by Theorem 1.4.5 that $|\mathcal{X}(F/v) \cap \Omega_1(F)| = g+1$ and that $\mathcal{X}(F/v) \cap \Omega_1(F) = \Omega_1^*(F/v)$. Hence, any $\mathcal{O} \in \mathcal{X}(F/v) \setminus \Omega_1(F)$ is a refinement of $\mathcal{O}_{w_i}$, for some $0 \leq i \leq g$, by Theorem 1.4.4. Then

$$|\mathcal{X}(F/v)| = g + 1 + \sum_{i=0}^{g} |\mathcal{X}(\kappa_{w_i}/\overline{v})|,$$

where $\overline{v}$ is the residual valuation of v modulo $\pi_1 \circ v$. Thus $|G(F)| = 2^{g+1} \prod_{i=0}^{g} |G(\kappa_{w_i})|$ by Theorem 5.2.5. Note that $\overline{v}$ is a henselian $\mathbb{Z}^{n-1}$-valuation on κ_{v_1} such that $\kappa_{\overline{v}}$ is hereditarily euclidean. Since for every $i \in \{0, \dots, g\}$ the residue field κ_{w_i} is the function field of the conic $Y^2 + X^2 + 1 = 0$ over κ_{v_1}, we obtain that $|G(\kappa_{w_i})| = 2^{n-1}$, by Theorem 5.3.6, whereby $|G(F)| = 2^{n(g+1)}$. □

Example 5.3.8. Let $n, g \in \mathbb{N}$. Assume that K is a field carrying a henselian $\mathbb{Z}^n$-valuation v with hereditarily euclidean residue field. Let $v_1 = \pi_1 \circ v$. Let $t \in K$ be such that $v_1(t) = 1$, and let $f = -\prod_{i=0}^{g}(X^2 + t^{2i}) \in K[X]$. We set $F = K(X)(\sqrt{f})$. Then

$$|G(F)| = 2^{n(g+1)}.$$

This follows directly by Theorem 5.3.7, because $v_1(t^i) \neq v_1(t^j)$ for $0 \leq i, j \leq g$.

5.4 The index in the real hyperelliptic case

Let K be a hereditarily pythagorean field. Let $f \in K[X]$ be a monic square-free polynomial with only nonreal roots. We set $F = K(X)(\sqrt{f})$. By Theorem 2.3.11 we have that $f = h_1^2 + h_2^2$, for some $h_1, h_2 \in K[X]$, hence $F/K(X)$ is a totally positive quadratic extension and by [9, Corollary 4.10] we have that $p(F) = 2$. Asumming that f is not necessarily monic and F is real, we ask whether $p(F) = 2$. Under certain conditions on K, we show in Theorem 5.4.2 that this is the case.

Let $g \in \mathbb{N}$. Let $F/\mathbb{R}((t))$ be a function field in one variable of genus g. It is a consequence of Theorem 1.4.5 and Theorem 5.2.6 that $|G(F)| \leq 2^{g+1}$. Assuming that $|G(F)| = 2^{g+1}$, we show that F/K is nonreal. Furthermore, we describe in Theorem 5.4.4 all the hyperelliptic function fields that reach this upper bound.

Proposition 5.4.1. *Let $g \in \mathbb{N}$. Assume that K carries a henselian $\mathbb{Z}$-valuation v with κ_v hereditarily pythagorean. Let $f \in K[X]$ be a square-free polynomial of degree $2g+2$ with all roots in $K(\sqrt{-1}) \setminus K$. Set $F = K(X)(\sqrt{f})$. Let w be a residually transcendental extension of v to F. Assume that F is real. Then one of the following conditions holds:*

(a) κ_w is nonreal with $s(\kappa_w) = 1$.

(b) κ_w/κ_v is ruled.

(c) $\kappa_w = \kappa_v(X)(\sqrt{h})$ is a real field with $h \in \kappa_v[X]$ a square-free polynomial with all roots in $\kappa_v(\sqrt{-1}) \setminus \kappa_v$.

Proof. By Theorem 2.3.11 and by Theorem 1.3.8 we may choose irreducible polynomials $q_i = (X - a_i)^2 + b_i^2$ with $a_i, b_i \in \mathcal{O}_v$, and $\alpha \in K^\times$ such that $f = \alpha \cdot q_0 \cdots q_g$. Since F is real, $\alpha \notin -K^{\times 2}$. We set $Y_i = (X - a_i)b_i^{-1}$.

Let w be a residually transcendental extension of v to F and let $w_0 = w|_{K(X)}$. As $[F : K(X)] = 2$ we have that $[\kappa_w : \kappa_{w_0}] \leq 2$. Let ℓ be the relative algebraic closure of κ_v in κ_w. If ℓ is nonreal, since κ_v is a hereditarily pythagorean, we have that $-1 \in \kappa_w^{\times 2}$ (case (a)).

Thus we assume now that ℓ is real. If $\kappa_w = \kappa_{w_0}$, since w is a residually transcendental extension of v, by Theorem 1.4.3 we have that $\kappa_w = \kappa_{w_0} = \ell(\overline{T})$, for some $T \in \mathcal{O}_{w_0}^\times$ with $\overline{T}$ transcendental over κ_v (case (b)). Now assume that $[\kappa_w : \kappa_{w_0}] = 2$ and ℓ is real. Then $\Gamma_w = \Gamma_{w_0}$. Let $f' = q_0 \cdots q_g$.

Since $f \in F^{\times 2}$, we have that $w_0(f) \in 2\Gamma_{w_0}$ and since $f' \in \mathsf{S}_2(K(X))$ we have $w_0(f') \in 2\Gamma_{w_0}$, by Theorem 2.2.9. Hence $w_0(\alpha) \in 2\Gamma_{w_0}$. Consider $i \in \{0, \dots, g\}$. Set

$$Z_i = \begin{cases} 1 + Y_i^2 & \text{if } w(Y_i) \geq 0, \\ 1 + Y_i^{-2} & \text{if } w(Y_i) < 0. \end{cases}$$

Note that, since ℓ is real, $Z_i \in \mathcal{O}_w^\times$ for all $0 \leq i \leq g$. Thus

$$\overline{Z_i} = \begin{cases} 1 + \overline{Y_i}^2 & \text{if } w(Y_i) = 0, \\ \overline{1} & \text{otherwise .} \end{cases}$$

Let us first assume that $v(\alpha) \notin 2\mathbb{Z}$. This implies that w_0 is a ramified extension of v. Hence $\overline{Y}_i$ is algebraic over κ_v for all $i \in \{0, \dots, g\}$, because otherwise w_0 must be a Gauss extension of v with respect to some Y_i, which would contradict the ramification. Since ℓ is pythagorean, we have $\overline{Z_i} \in \ell^{\times 2} \subseteq \kappa_w^{\times 2}$ because ℓ is the relative algebraic closure of κ_v in κ_w. By Theorem 1.1.21 we have that $\kappa_w = \kappa_{w_0}(\sqrt{\overline{u}})$, for any $u \in \alpha f' K(X)^{\times 2}$ with $w_0(u) = 0$. Since $\prod_{i=0}^g \overline{Z_i} \in \kappa_{w_0}^{\times 2}$, we have that $\kappa_w = \kappa_{w_0}\left(\sqrt{\overline{\alpha h^2}}\right)$ for any $h \in K(X)^\times$ such that $w_0(\alpha h^2) = 0$. Let $K' = K(\sqrt{\alpha})$. Let w_0' be an extension of w_0 to $K'(X)$ and let $v' = w_0'|_{K'}$. We have that $\kappa_{w_0'} = \kappa_{w_0}\left(\sqrt{\overline{\alpha h^2}}\right)$, because $K'(X) = K(X)(\sqrt{\alpha})$ and $w_0(\alpha h^2)$. Furthermore, w_0' is a residually transcendental extension of v' to $K'(X)$. Therefore κ_w/κ_v is ruled, by Theorem 1.4.3 (case (b)).

Let us assume now that $v(\alpha) \in 2\mathbb{Z}$. Let J be the set of indices $i \in \{0, \dots, g\}$ such that $w(Y_i) = 0$ and $\overline{Y}_i$ is transcendental over κ_v. Assume first that $J = \varnothing$. Then $\overline{Z_i} \in \kappa_w$ is algebraic over ℓ for all $0 \leq i \leq g$, and since ℓ is pythagorean, we have that $\kappa_w = \kappa_{w_0}(\sqrt{\alpha})$. Therefore κ_w/κ_v is ruled (case (b)). Now we assume that $J \neq \varnothing$. Without loss of generality we put $J = \{0, \dots, s\}$, for some $s \leq g$. For $i \in J$, let v_i be the Gauss extension of v to $K(X)$ with respect to Y_i. By Theorem 1.1.24 we have that $w_0 = v_0 = \cdots = v_s$, $\kappa_{w_0} = \kappa_v(\overline{Y_0})$ and $\Gamma_{w_0} = \mathbb{Z}$. Thus $w_0(\alpha) \in 2\mathbb{Z}$, and we may consider some $\beta \in \mathcal{O}_v^\times$ such that $\alpha \in \beta K^{\times 2}$. Let $j \in J$. We have $Y_j^2 + 1 \in \mathcal{O}_{w_0}^\times$. We set $c_j = b_0 b_j^{-1}, d_j = (a_0 - a_j) b_j^{-1}$. Since $Y_j = c_i Y_0 + d_j$, we have $Y_j^2 + 1 = c_j^2 Y_0^2 + 2c_j d_j Y_0 + d_j^2 + 1$, and hence $f \in h(Y_0) \cdot K^{\times 2}$, where

$$h(Y_0) = \beta(Y_0^2 + 1) \cdots (c_s^2 Y_0^2 + 2d_s c_s Y_0 + d_s^2 + 1) \prod_{i=s+1}^{g} Z_i.$$

Therefore $F = K(Y_0)(\sqrt{h(Y_0)})$. Since v is henselian and $\beta \notin -K^{\times 2}$, we have $\overline{\beta} \notin -\kappa_v^{\times 2}$. Finally, since $h \in \mathcal{O}_{w_0}^\times$, we have that $h \in f K(Y_0)^{\times 2} \cap \mathcal{O}_{w_0}^\times$, and we can conclude that $\kappa_w = \kappa_v(\overline{Y_0})\left(\sqrt{\overline{h}(\overline{Y_0})}\right)$ is a real field, where $\overline{h} \in \kappa_v[\overline{Y_0}]$ is a polynomial with all roots in $\kappa_v(\sqrt{-1}) \setminus \kappa_v$ by Theorem 1.1.21 (case (c)). □

The following states the triviality of the sum-of-two squares index for all real quadratic twists of totally positive hyperelliptic function fields.

Corollary 5.4.2. *Let n be a positive integer. Assume that K carries a henselian $\mathbb{Z}^n$-valuation v such that κ_v is hereditarily euclidean. Let $f \in K[X]$ be a nonconstant square-free polynomial with all roots in $K(\sqrt{-1}) \setminus K$. We set $F = K(X)(\sqrt{f})$. Assume that F is real. Then $p(F) = 2$.*

Proof. We prove the statement by induction on n. Note that by Theorem 5.2.6 we have that $p(F) = 2$ if and only if $\mathcal{X}(F/v)$ is empty. Assume $n = 1$. Let w be a residually transcendental extension of v. It follows by Theorem 5.4.2 that either $s(\kappa_w) = 1$ or κ_w is real. Hence $\mathcal{X}(F/v) =$ and $p(F) = 2$. Assume now that $n > 1$. We show that $\mathcal{X}(F/v)$ is empty. Let $v_1 = \pi_1 \circ v$. Let $\overline{v}$ be the residual valuation of v modulo v_1. Then $\overline{v}$ is a henselian $\mathbb{Z}^{n-1}$-valuation on κ_{v_1} such that $\kappa_v = \kappa_{\overline{v}}$. It follows by induction hypothesis and by Theorem 5.4.1 that all the residually transcendental extensions w of v_1 to F satisfy $p'(\kappa_w) = 2$. If we had some $\mathcal{O} \in \mathcal{X}(F/v)$, then we would obtain that the residue field of the rank-one coarsening $\mathcal{O}'$ of $\mathcal{O}$ would have $p'(\kappa_{\mathcal{O}'}) > 2$ by Theorem 2.2.10, which is a contradiction. Therefore $\mathcal{X}(F/v) = \varnothing$, whereby $p(F) = 2$ by Theorem 5.2.5. □

Note that, if $f \in K[X]$ is assumed to be monic in Theorem 5.4.2, then $F/K(X)$ is a totally positive quadratic extension.

Theorem 5.4.3. *Let $g \in \mathbb{N}$. Assume that K carries a henselian $\mathbb{Z}$-valuation v with hereditarily euclidean residue field. Let F/K be a hyperelliptic function field of genus g. Let $f \in K[X]$ be a square-free polynomial such that $F = K(X)(\sqrt{f})$. If $|G(F)| = 2^{g+1}$, then*

$$f(X) = -\prod_{i=0}^{g}((X - a_i)^2 + b_i^2),$$

for certain $a_0, b_0 \ldots, a_g, b_g \in \mathcal{O}_v$ such that for every pair (i, j) with $i \neq j$ and $0 \leq i, j \leq g$, we have that either $v(b_i) \neq v(b_j)$ or $2v(a_i - a_j) < v(b_i b_j)$.

Proof. It follows by Theorem 5.3.4 and by Theorem 2.3.11 that we may choose irreducible polynomials $q_i = (X - a_i)^2 + b_i^2$, with $a_i, b_i \in \mathcal{O}_v$, and $\alpha \in K^\times$ such that $f = \alpha \cdot q_0 \cdots q_g$. For $i \in \{0, \ldots, g\}$ let $Y_i := b_i^{-1}(X - a_i)$. If $\alpha \notin -K^{\times 2}$, then $p(F) = 2$, by Theorem 5.4.2. Therefore, under the assumption that $|G(F)| = 2^{g+1}$, we have that $\alpha \in -K^{\times 2}$. Let $w \in \mathcal{X}(F/v)$. We claim that $w_0 := w|_{K(X)}$ is the Gauss extension of v to $K(X)$ with respect to Y_i, for some $i \in \{0, \ldots, g\}$. Since w_0 is a residually transcendental extension of v to $K(X)$, by Theorem 1.4.3 we have that $\kappa_{w'} = \ell(\overline{Y})$, for some $Y \in \mathcal{O}_{w'}^\times$ and some finite extension ℓ/κ_v. Since κ_v is pythagorean, ℓ is real, because otherwise ℓ would contain $\sqrt{-1}$ by Theorem 2.3.4. Since $s(\kappa_w) < \infty$, it follows that $[\kappa_w : \kappa_{w_0}] = 2$, which implies that $\Gamma_w = \Gamma_{w'}$ and that w is the unique extension of w' to F, by Theorem 1.1.21. Set

$$Z_i = \begin{cases} 1 + Y_i^2 & \text{if } w(Y_i) \geq 0, \\ 1 + Y_i^{-2} & \text{if } w(Y_i) < 0. \end{cases}$$

Note that, since ℓ is real, $Z_i \in \mathcal{O}_w^\times$ for all $0 \leq i \leq g$. Thus

$$\overline{Z_i} = \begin{cases} 1 + \overline{Y_i}^2 & \text{if } w(Y_i) = 0, \\ \overline{1} & \text{otherwise .} \end{cases}$$

For $i \in \{0, \ldots, g\}$ such that $w(Y_i) = 0$, we assume that $\overline{Y}_i \in \kappa_{w'}^\times$ is algebraic over κ_v. Hence $\overline{Z_i} \in \ell^{\times 2} \subseteq \kappa_{w'}^{\times 2}$, whereby

$$\kappa_w = \ell(\overline{Y})\left(\sqrt{-\prod_{i=0}^{g}\overline{Z_i}}\right) = \ell(\sqrt{-1})(\overline{Y}),$$

which is a contradiction. Thus w' is the Gauss extension of v to $K(X)$ with respect to Y_i, for some $\{0,\dots,g\}$. Therefore $\mathfrak{X}(F/v) = \{w_0,\dots,w_g\}$, where w_i is the unique extension to F, of the Gauss extension v_i of v to $K(X)$ with respect to Y_i, for $0 \le i \le g$. Since $|\mathfrak{X}(F/v)| = 1$, it follows that $v_0,\dots,v_g$ are different. Hence, by Theorem 5.3.1 we obtain the conditions on the coefficients $a_i, b_i \in \mathcal{O}_v$. □

Corollary 5.4.4. *Let $g \in \mathbb{N}$. Assume that K carries a henselian $\mathbb{Z}$-valuation v with hereditarily euclidean residue field. Let F/K be a hyperelliptic function field of genus g. Let $f \in K[X]$ be a square-free polynomial such that $F = K(X)(\sqrt{f})$. Then the following statements are equivalent:*

(1) $|G(F)| = 2^{g+1}$.

(2) $|\mathfrak{X}(F/v)| = g+1$.

(3) $f(X) = -\prod_{i=0}^{g}((X-a_i)^2 + b_i^2)$, *for certain* $a_0, b_0 \dots, a_g, b_g \in \mathcal{O}_v$ *such that for every pair* (i,j) *with* $i \neq j$ *and* $0 \le i,j \le g$, *we have that either* $v(b_i) \neq v(b_j)$ *or* $2v(a_i - a_j) < v(b_i b_j)$.

Proof. (1) ⇔ (2) : By Theorem 5.2.5. (2) ⇒ (3) : By Theorem 5.4.3. (3) ⇒ (2) is given by Theorem 5.3.2. □

The previous corollary can be extended to non-hyperelliptic function fields in one variable using geometric methods, as a consequence of [3, Theorem 5.3].

Proposition 5.4.5. *Let $g \in \mathbb{N}$. Let $F/\mathbb{R}((t))$ be a regular function field in one variable of genus g. If F is real, then $|G(F)| \le 2^g$.*

Proof. Let $K = \mathbb{R}((t))$, and let v the $\mathbb{Z}$-valuation corresponding to $\mathbb{R}[[t]]$. By Theorem 5.2.6 we have $|G(F)| = 2^{|\mathfrak{X}(F/v)|}$, and since $\mathfrak{X}(F/v) \subseteq \Omega_1^*(F/v)$, it follows by Theorem 1.4.5 that $|G(F)| \le 2^{g+1}$. Suppose that $|G(F)| = 2^{g+1}$. Then $|\mathfrak{X}(F/v)| = g+1$. We observe that any $\mathbb{Z}$-valuation corresponding to a valuation ring in $\mathfrak{X}(F/v)$ is a nonruled residually transcendental extension of v. By Theorem 3.1.3, we can consider a regular model $\mathcal{C}$ of $F/\mathbb{R}[[t]]$. It is a consequence of [3, Theorem 5.3] that there is no $\mathbb{R}$-rational point on the special fiber $\mathcal{C}_{\mathbb{R}}$. However, the existence of a K'-rational point on $\mathcal{C}_K$ for some finite real extension K'/K, would imply the existence of a $\mathbb{R}$-rational point in $\mathcal{C}_{\mathbb{R}}$, by Theorem 3.2.14. Therefore $\mathcal{C}_K$ admits no K'-rational point for any real extension K' of K, and it is well known (see for example [20, Proposition 2.3]) that this implies that F is nonreal. In particular, since $p(F) = 3$ by Theorem 5.1.7, it follows by Theorem 2.2.11 that $s(F) = 2$. □

5.5 The index by reduction type in the elliptic case

Let T be a discrete valuation ring with maximal ideal $\mathfrak{m}$, hereditarily pythagorean residue field k and fraction field K. Let v be a $\mathbb{Z}$-valuation on K corresponding to T. Let $\bar{k}$ be an algebraic closure of k.

In this section, we show that an elliptic curve E/K whose function field has Pythagoras number 3 is of reduction type I_{2n}, for some $n \in \mathbb{N}$, whenever k is hereditarily euclidean. For this, we will use the arithmetic geometry studied in Chapter 3 to describe the valuation-theoric invariant $\mathfrak{X}(F/v)$ in terms of irreducible components of the special fiber of the minimal regular model of F/T.

Theorem 5.5.1. *Let T be a henselian discrete valuation ring with fraction field K and hereditarily euclidean residue field k. Let F/K be an elliptic function field. The following are equivalent.*

(1) $p(F) = 3$.

(2) There exist $\lambda \in T^\times, a \in \mathfrak{m}$ with $\overline{\lambda} \in k^{\times 2}$ such that F is isomorphic to the function field of the curve $Y^2 = (X - \lambda)(X^2 + a^2)$ over K.

Moreover, if one of the above conditions is satisfied, then F/T is of reduction type I_{2n}, for some $n \in \mathbb{N}$.

Proof. We first note that $p(F) = 2$ or $p(F) = 3$, by Theorem 5.1.7. We assume that $p(F) = 3$. By the definition of an elliptic function field, there exists $f \in K[X]$ of degree 3 such that $F = K(X)(\sqrt{f})$. By Theorem 1.3.8 we can assume that f is monic and is defined over T. Since K is hereditarily pythagorean and $p(F) > 2$, f has a nonreal irreducible factor by [9, Theorem 3.10]. Hence, $f = (X - c) \cdot q$, where $c \in T$ and $q \in T[X]$ is an irreducible monic quadratic polynomial. Hence $q = (X - b)^2 + a^2$, for some $a, b \in T$, by Theorem 2.3.11. Changing variables, we can assume that F is the function field of $Y^2 = (X - \lambda)(X^2 + a^2)$ with $\lambda, a \in T$. By [57, VII. Proposition 1.3, (d)], one can apply a change of variable a finite number of times to obtain a minimal Weierstrass equation. Thus, without loss of generality we assume that the latter equation is minimal. Let v be the $\mathbb{Z}$-valuation corresponding to T. By Theorem 3.3.9 we have that either $\lambda, a \in T^\times$ or $\lambda \in T^\times, a \in \mathfrak{m}$ or $\lambda \in \mathfrak{m}, v(a) = 1$ or $v(\lambda) = 1, a \in \mathfrak{m}$. Since $p(F) = 3$, $G(F)$ is non-trivial, so $\mathfrak{X}(F/v)$ is non-empty, by Theorem 5.2.6. We show that $\lambda \in T^\times$ and $a \in \mathfrak{m}$. Assume $a \in T^\times$. Then E has good reduction (see Theorem 3.3.3), and by Theorem 3.3.4 the unique valuation extension T' of T to F with nonruled residue field corresponds to the elliptic curve $Y^2 = (X - \overline{\lambda})(X^2 + \overline{a}^2)$ over k, that is, the residue field of T' is a real function field in one variable over k, which implies that $\mathfrak{X}(F/v)$ is empty, contradiction. We assume now that $a, \lambda \in \mathfrak{m}$. Since the equation is minimal, it follows by Theorem 3.3.10 that E/K is of reduction type I_n^*, for some $n \in \mathbb{N}$. Since every valuation ring in $\mathfrak{X}(F/v)$ is a nonruled residually transcendental extension of T to F, we obtain by that $\mathfrak{X}(F/v)$ is empty, by Theorem 3.3.5, and we get a contradiction for the same reason as before. Hence $\lambda \in T^\times$ and $a \in \mathfrak{m}$.

Now we claim that $\overline{\lambda} \in k^{\times 2}$. By the sake of a contradiction, we assume that there exists $c \in k^\times$ such that $\overline{\lambda} = -c^2$. Let $\mathcal{W} \subseteq \mathbb{P}^2_T$ be the model of E/T given by its homogenization, that is,

$$\mathcal{W} = \mathsf{Proj}(T[X, Y, Z]/ZY^2 - (X - \lambda Z)(X^2 + aZ^2)).$$

Then the special fiber $\mathcal{W}_k$ is the curve $ZY^2 = (X - \overline{\lambda}Z)X^2$. Using the Jacobian criterion, one can check that the point $p = [0 : 0 : 1]$ on $\mathcal{W}_k$ is singular. Let $\pi : \Gamma \to \mathcal{W}_k$ be the normalization of

$\mathcal{W}_k$ (see [38, Definition 4.1.19] for the definition of the normalization morphism). Then Γ is the curve $U^2 = S - \overline{\lambda}$ over k, and $\pi^{-1}(p)$ is made up of the two k-rational points $(c,0)$ and $(-c,0)$, that is E has split multiplicative reduction (see [38, Definition 10.2.2] and [38, Lemma 10.2.1] for the definition of split and non-split multiplicative reduction). Let $\mathcal{C}$ be the minimal regular model of E/T. It follows by [58, Tate's algorithm 9.4, Step 2] that every irreducible component of $\mathcal{C}_k$ is isomorphic to $\mathbb{P}^1_k$. This implies, by Theorem 3.3.4, that every residually transcendental extension of v to F is ruled, whereby $\mathcal{X}(F/v)$ is empty, contradiction. We conclude that $\overline{\lambda} \in k^{\times 2}$.

On the other hand, we assume that there exist $\lambda \in T^\times, a \in \mathfrak{m}$ such that F is the function field of $Y^2 = (X-\lambda)(X^2+a^2)$ with $\overline{\lambda} \in k^{\times 2}$. Then $F = K(X)(\sqrt{(X-\lambda)(X^2+a^2)})$. Let v' be the Gauss extension of v to $K(X)$ with respect to X/a, and let w be an extension of v' to F. Hence we have $\kappa_w = k(Z)(\sqrt{-(Z^2+1)})$, where $Z = \overline{X/a}$. Therefore $\mathcal{O}_w \in \mathcal{X}(F/v)$, whereby $\mathcal{X}(F/v)$ is non-empty, and hence $p(F) = 3$.

Finally, if one of the above conditions is satisfied, then F is of reduction type I_{2n}, for some $n \in \mathbb{N}$, by Theorem 3.3.8. □

Example 5.5.2. Let $K = \mathbb{R}((t))$, and let v be the $\mathbb{Z}$-valuation on K corresponding to $\mathbb{R}[[t]]$. We consider $f = -(X^2+1)(X^2+t^2) \in K[X]$. Set $F = K(X)(\sqrt{f})$. It was shown in [9, Example 5.12], using methods from the theory of quadratic forms, that $|G(F)| = 4$. On the other hand, let $\mathcal{C}$ be the minimal regular model $F/\mathbb{R}[[t]]$. It is shown in Theorem 3.4.2 that $\mathcal{C}_\mathbb{R}$ consists of two irreducible components that are each isomorphic to the conic $Y^2 + X^2 + Z^2 = 0$ and that F is reduction type I_2. This implies that $|\mathcal{X}(F/v)| = 2$, and therefore $|G(F)| = 2^2 = 4$, by Theorem 5.2.6.

It is shown in [39] that the reduction type of a genus one curve (non necessarilly elliptic) is the reduction type of its Jacobian. Thus, we can say that a curve of genus one has reduction type as the notations in the case of elliptic curves, that is, as Theorem 3.3.1. In addition, the Theorem 5.5.2 describes an example of a genus one curve which is not elliptic and whose function field has Pythagoras number 3, and second Pfister index 4. Thus, it is natural to wonder the following.

Question 5.5.3. Let $X/\mathbb{R}((t))$ be an integral curve of genus one, and let F its function field. If $p(F) = 3$, does this imply that X is of reduction type I_{2n}, for some $n \in \mathbb{N}$?

About the Kaplansky radical in elliptic curves, the following result follows from Theorem 5.5.1.

Corollary 5.5.4. *Let $F/\mathbb{R}((t))$ be an elliptic function field. Set $L = F(\sqrt{-1})$. If $p(F) = 3$, then F is radical-free and*

$$|\overline{R}(L)| = 2.$$

Proof. Since $p(F) = 3$, it follows by Theorem 5.5.1 that there exist $\lambda \in \mathbb{R}[[t]]^\times$ with $\lambda \in \mathbb{R}^{\times 2}$ and $a \in (t)$ such that F is isomorphic to the function field of the curve $Y^2 = (X-\lambda)(X^2+a^2)$. Then F is radical-free by Theorem 4.4.4. Let $\mathcal{C}$ be the minimal regular model of $F/\mathbb{R}[[t]]$, and $\mathcal{C}' = \mathcal{C} \times_{\mathbb{R}[[t]]} \mathbb{C}[[t]]$. By Theorem 5.5.1 F is of reduction type I_{2n}, for some $n \in \mathbb{N}$, which implies that $b(\mathcal{C}') = 1$. Therefore $|\overline{R}(L)| = 2$, by Theorem 4.4.2. □

It is natural to wonder whether Theorem 5.5.4 can be generalized to any function field in one variable.

Question 5.5.5. Let $F/\mathbb{R}((t))$ be a function field in one variable. Does $p(F) = 3$ imply that F is radical-free and $F(\sqrt{-1})$ is not radical-free ?

Bibliographic References

[1] S. Anscombe, P. Dittmann, A. Fehm. *Approximation theorems for spaces of localities.* Mathematische Zeitschrift, **296**:1471-1499, 2020.

[2] M. Auslander, D.A. Buchsbaum. *Unique factorization in regular local rings.* Proc. Nat. Acad. Sci. U.S.A. **45** (1959), 733–734.

[3] K.J. Becher, D. Grimm. *nonsplit conics in the reduction of an arithmetic curve.* https://arxiv.org/abs/2005.11855.

[4] K.J. Becher, D. Grimm, J. Van Geel. *Sums of squares in algebraic function fields over a complete discretely valued field.* Pacific J. of Math **267** (2014), 257–276.

[5] K.J. Becher, P. Gupta. *Ruled residue theorem for function fields of conics.* Journal of Pure and Applied Algebra **225** (2021), 106638.

[6] K.J. Becher, D.B. Leep. *The kaplansky radical of a quadratic field extension.* Journal of Pure and Applied Algebra **218** (2014), 1577–1582.

[7] K.J. Becher. *On the number of square Classes of a field of finite level.* Documenta Mathematica, Extra volume, Quadratic forms LSU (2001): 65-84.

[8] E. Becker. *Hereditarily pythagorean fields and orderings of higher level.* Monografias de Matemática Vol. 29. Instituto de matematica pura e aplicada, Rio de Janeiro (1978).

[9] K.J. Becher, J. Van Geel. *Sums of squares in function fields of hyperelliptic curves.* Mathemastische Zeitschrift, **261** (4): 829 - 844, 2009.

[10] L. Bröcker. *Characterization of fans and hereditarily pythagorean fields.* Math. Z. **152**, (1976), 149-163.

[11] J.-L. Colliot-Thélène, R. Parimala, V. Suresh. *Patching and local-global principles for homogeneous spaces over function fields of p-adic curves.* Comment. Math. Helv. (2012), no. 87, 1011–1033.

[12] C.M. Cordes. *Kaplansky's radical and quadratic forms over nonreal fields.* Acta arith. **28** (1975) 253-261.

[13] N. Daans, P. Dittmann, A. Fehm. *Existencial rank and essential dimension of diophantine sets.* https://arxiv.org/abs/2102.06941.

[14] D.S. Dummitt, R.M. Foote. *Abstract Algebra.* 3rd edition, Jhon Wiley & Sons, Inc (2004).

[15] R. Elman, N. Karpenko, A. Merkurjev. *The Algebraic and Geometric Theory of Quadratic Forms.* AMS, 2008.

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

[17] A.J. Engler, A. Prestel. *Valued fields.* Springer-Verlag, 2005.

[18] R. Elman, A.R. Wadsworth. *Hereditarily quadratically closed fields.* J. Algebra **111**, 475-482 (1987).

[19] P. Gille, T. Szamuely. *Central Simple Algebras and Galois Cohomology.* Cambridge University Press, Cambridge, 2006.

[20] D. Grimm. *Lower bounds for Pythagoras numbers of function fields.* Comment. Math. Helv. **90** (2015), no. 2, pp. 365–375.

[21] D. Grimm. *On an isotropy criterion for quadratic forms over function fields of curves over non-dyadic complete discrete valuation rings.* Banach Center Publications. **108** (2016), 95-103.

[22] P. Gupta. *Local-global principles for quadratic forms and strong linkage.* Phd Thesis. Universiteit Antwerpen. https://doc.anet.be/docman/docman.phtml?file=.irua.21c9b2.156147.pdf.

[23] D. Harbater, J. Hartmann. *Patching over fields.* Israel J. Math. **176** (2010), 61-107.

[24] D. Harbater, J. Hartmann, D. Krashen. *Applications of patching to quadratic forms and central simple algebras.* Inventiones Mathematicae **178** (2009), 231-269.

[25] D. Harbater, J. Hartmann, D. Krashen. *Local-global principles for torsors over arithmetic curves.* American Journal of Mathematics **137** (2015), 1559– 1612.

[26] R. Hartshorne. *Algebraic geometry.* vol. 52, Springer-Verlag, New york-Berling, 1977.

[27] A. Hatcher. *Algebraic topology.* Cambridge univ. Press, Cambridge, 2000.

[28] P. Hill, J. Mott. *Embedding theorems and generalized discrete ordered abelian groups.* Trans. Amer. Math. Soc. **175**, 283-297.

[29] D.W. Hoffmann. Pythagoras numbers of fields. J. Amer. Math. Soc. **12** (1999), 839–848.

[30] N. Jacobson. *Lectures in Abstract Algebra, III. Theory of Fields and Galois Theory.* Springer-Verlag, Berlin.

[31] I. Kaplansky. *Fröhlich'slocalquadraticforms.* J. Reine Angew. Math. 239–240 (1969) 74–77.

[32] H. Koch. *Number theory: Algebraic numbers and functions.* Graduate Studies in Mathematics, 2000.

[33] F.-V. Kuhlmann. *The algebra and model theory of valued fields.* J. Reine Angew. Math. **719** (2016), 1–43.

[34] M. Kula. *Fields with non-trivial Kaplansky's radical and finite square class number.* Acta Arith. **38** (1980/1981) 411-418.

[35] T.Y. Lam. *Introduction to quadratic forms over fields.* American Mathematical Society, 2005.

[36] T. Y. Lam. *The algebraic theory of quadratic forms.* W. A. Benjamin, Inc., Reading, Mass., 1973. Mathematics Lecture Note Series.

[37] S. Lang. *Algebra.* third ed., Graduate texts in mathematics, Springer-Verlag, 2002.

[38] Q. Liu. *Algebraic Geometry and Arithmetic curves.* Oxford Graduate Texts in Mathematics, Oxford University Press, Oxford, 2002.

[39] Q. Liu, D. Lorenzini, M. Raynaud. *Néron models, Lie algebras, and reduction of curves of genus one.* Invent. Math. **157**(3), 455-518 (2004).

[40] V. Mehmeti. *Patching over Berkovich curves and quadratic forms.* Compos. Math., **155**(12):2399–2438, 2019.

[41] A. S. Merkurjev, A. A. Suslin. *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 46 (1982), no. 5, 1011-1046, 1135-1136.

[42] A. Néron. *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux.* Publ. Math. IHES **21** (1964), 361-482.

[43] J. Neukirch, A. Schmidt, K. Wingberg. *Cohomology of Number Fields.* Sec. Ed., corr.sec. print. Springer, 2008.

[44] J. Ohm. *Simple transcendental extensions of value fields.* J. Math. Kyoto Univ. **22** (1982), 201-221.

[45] J. Ohm. *The ruled residue theorem for simple transcendental extensions of valued fields.* Proceedings of the American Mathematical Society **89** (1983), no. 1, 16–18.

[46] T. O'Meara. *Introduction to Quadratic Forms.* Springer, 2000.

[47] D. Orlov, A. Vishik, V. Voevodsky. *An exact sequence for K_*^M with applications to quadratic forms.* In: Ann. of Math. **165** (1 2007), pp. 1–13.

[48] A. Pfister. *Quadratic forms with applications to algebraic geometry and topology.* London Mathematical Society Lecture Note Series 217, Cambridge University Press, 1995.

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

[50] M. Raynaud. *Spécialisation du foncteur de Picard.* Publ. Math. IHES **38** (1970), 27–76.

[51] P. Ribenboim. *Le théorème d' approximation pour les valuations de krull.* Math. Z. **68**, 1-18 (1957).

[52] P. Ribenboim. *The theory of classical valuations.* Springer-Verlag, New york, 1999.

[53] R. Scognamillo, U. Zannier. *Introductory Notes on Valuation Rings and Function Fields in One Variable.* Springer, 2014.

[54] J.-P. Serre. *Galois cohomology.* Corrected reprint of the 1997 English edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, ISBN 3-540-42192-0, Translated from the French by Patrick Ion and revised by the author. MR1867431 (2002i:12004).

[55] J.-P. Serre. *Local fields.* Graduate texts in mathematics, vol. 67, Springer New York, 1979.

[56] R.Y. Sharp. *The dimension of the tensor product of two field extensions.* Bull. London Math. Soc., **9** (1977) 42-48.

[57] J. Silverman. *The Arithmetic of Elliptic Curves.* Grad. Texts math., **106**, Springer, New york-Heidelberg-Berlin, 1986.

[58] J. Silverman. *Advanced topics in the Arithmetic of Elliptic curves.* Grad. Texts Math., **106**, Springer, New-York-Heidelberg-Berlin, 1994.

[59] H. Stichtenoth. *Algebraic function fields and codes.* 2nd. ed. Graduate texts in Mathematics **254**. Berlin; Springer. xiii, 355 p., 2009.

[60] J. Tate. *Algorithm for determining the type of a singular fiber in an elliptic pencil.* In modular Functions of One Variable IV, Lect. Notes in Math. **476**, B.J. Birch and W. Kuyk, eds., Springer-Verlag, Berlin, 1975, 33-52.

[61] S. V. Tikhonov, J. Van Geel, V.I. Yanchevskiĭ. *Pythagoras numbers of function fields of hyperelliptic curves with good reduction.* Manuscripta Math. **119**, 305-322 (2006).

[62] S. V. Tikhonov, V. I. Yanchevskiĭ. *Pythagoras number of function fields of conics over hereditarily pythagorean fields.* Dokl. Nats. Akad. Nauk Belarusi **47**, 5-8 (2003).

[63] G.D. Villa. *Topics in the Theory of Algebraic Function Fields.* Birkhäuser 2006.

[64] V. Voevodsky. *Motivic cohomology with $\mathbb{Z}/2$-coefficients.* In: Publ. Math. IHES **98** (2003), pp. 59–104.

[65] S. Warner. *Topological fields.* Mathematics studies **157**, North Holland, Amsterdam (1989).

[66] E. Witt. *Zerlegung reeller algebraischer Funktionen in Quadrate. Schiefkörper über reellem Funktionenkörper.* J. Reine Angew. math **171** (1934), 4-11.