Fibrations by singular curves of arithmetic genus three in characteristic two

Cesar Hilario

A Dissertation
Presented to the Post-graduate
Program in Mathematics
at Instituto de Matemática Pura e Aplicada
in Candidacy for the Degree
of Doctor of Philosophy

Advisor: Karl-Otto Stöhr

March 2022

Abstract

The classical Bertini theorem on the smoothness of general fibres holds in characteristic zero, but fails in positive characteristic. In this thesis we investigate the geometry of a class of counterexamples, namely fibrations by singular curves of arithmetic genus three in characteristic two, from the perspective of function field theory. Given a fibration by singular curves, our strategy consists in looking at its generic fibre. By exploiting the deep connection between these generic fibres and the theory of non-conservative function fields, we construct and classify large families of counterexamples. Our study also reveals that very interesting geometric phenomena arise from them.

Resumo

O teorema clássico de Bertini sobre a não singularidade de fibras gerais vale em característica zero, mas é falso em característica positiva. Nesta tese investigamos a geometria de uma classe de contraexemplos, a saber, as fibrações por curvas singulares de gênero aritmético três em característica dois, do ponto de vista da teoria dos corpos de funções algébricas. Dada uma fibração por curvas singulares, nossa estratégia consiste em olhar para sua fibra genérica. Utilizando a profunda conexão entre essas fibras genéricas e a teoria dos corpos de funções não conservativos, construímos e classificamos uma grande família de contraexemplos. Nosso estudo também revela que deles surgem fenômenos geométricos muito interessantes.

To the memory of my mother

Acknowledgements

First of all, I would like to thank my advisor Karl-Otto Stöhr. I am deeply grateful to him for his unmatched patience and wisdom in holding my hand and guiding me through the difficult process of becoming a researcher. What I learned from him can hardly be overstated. His permanent disposition to discuss mathematics with me, his enlightening answers, his generosity in sharing ideas and perspectives on mathematics and life, his thorough feedback on my drafts, were all tremendously helpful. This thesis would not have been written without his support.

I am grateful to the many professors at IMPA from whom I learned beautiful mathematics and who shared their knowledge and experience with me, chiefly Carolina Araujo, Oliver Lorscheid, Eduardo Esteves, Misha Belolipetsky and Jorge Vitório Pereira. A warm and heartfelt thank you goes to Carolina, not only for sharing her particular philosophy on mathematics, with pictures helping keep a geometric sight in all the algebra, but also for her crucial assistance during my thesis defense, at a moment when I feared that everything was going wrong.

I thank Rodrigo Salomão, João Pedro dos Santos and Ethan Cotterill for kindly agreeing to join my thesis defense committee. I am particularly grateful to Rodrigo for the several discussions we had and for answering my questions, to João Pedro for his very detailed reading of my manuscript, and to Ethan for his suggestions and questions about my work.

I express my gratitude to professors Claudio Landim and Roberto Imbuzeiro for the help and advice I received from them when I came to IMPA.

The many friends I made during my time at IMPA prevented my life from becoming monotonous and made it more pleasant. I would like to thank Zoraida Fernandez, Jennifer Loria, Diego Salazar and Diego Navarro. Equally, I am warmly grateful to my algebraic geometry mates, Alex Agudelo, Hernán Iriarte, Cristian González, Enzo Aljovin and João Paulo, with whom I learned algebraic geometry side by side as a student. I express my thanks also to my other algebraic geometry friends, Roberto Villaflor, Valdir Pereira, Manoel Jarra, Xia Xiao, Eduardo Alves, Eduardo Santos, Crislaine Kuster and Luíze D'Urso, from whom I learned so much. A special thank you goes to Xia Xiao, my companion during the covid lockdown in Brazil back in 2020. Another special thank you goes to Wodson Mendson, for being my office mate during my last summer at IMPA (at a time where both of us were preparing to defend our theses), and for always being willing to play an antichess game.

Staying in a new country for so long may be hard, but the effect can be weakened if there are fellow countrymen willing to help. I am hugely grateful to my Peruvian friends at IMPA: Raúl Chávez, Enrique Chávez, Aracelli Medrano, Juan Paucar, Fernando Manrique, Braulio Calagua, Juan Carlos Rojas, Piere Rodriguez, Dan Agüero, Victor Perez, and Nelson Castro. I especially thank Andrés Chirre for his great assistance during my first months in Rio, for the funny moments we spent together, and for the countless times we stayed up late working at IMPA and ended up walking to Jardim Botânico because there were no buses whatsoever. I equally thank Jesús Ramos for his camaraderie and his constant disposition to answer and discuss any mathematical question I had in mind. An enormous thank you goes to Rubén Lizarbe, my flat mate, for his enthusiasm and eagerness to help, for the many conversations we had, and for unveiling the fascinating world of cinema to me.

I extend my gratitude to my Brazilian family, Isabel and Ana, for so warmly welcoming me in their apartment.

I am grateful to my teachers at UNI/IMCA back in Peru, particularly Hugo Castillo and the members of the optimization group: Orestes Bueno, Yboon Garcia and John Cotrina. Likewise, I am greatly indebted to professor Johel Beltran from PUCP for his encouragement and assistance when I moved to Brazil.

I express a warm gratitude to the staff at IMPA for all their help, and the *divisão de ensino* in particular for simplifying administrative matters so much, making life way easier for students. I thank Josenildo, Andrea and Kenia for the assistance I received from them on countless occasions. I express my thanks also to the people in the library and the restaurant for making IMPA a very pleasant place to work.

I thank CNPq and CAPES for financial support.

Most of all, I am grateful to my wonderful family for their patience and tenderness, for the several abnormal New Year's Eves they had to pass because of me (I usually traveled to Rio on the very first days of January), and for having endured our separation for so long. I especially thank my father, the strongest and most vigorous person I know, and my mother, the angel who keeps taking care of me even after a thirteen-year absence.

Contents

Chapter 1

Introduction

In Differential Topology there is a very classical result known as Sard's lemma. It states that the set of critical values of a smooth map $T \to B$ of differentiable manifolds is *small* in the sense that it has zero Lebesgue measure in B. Its analogue, the quite well-known *Bertini-Sard theorem* or *Bertini's theorem* (see [Sha13, Theorem 2.27]), tells that essentially the same happens in algebraic geometry. But with some exceptions. In fact, the theorem holds in characteristic zero, but counterexamples exist when the characteristic is positive.

The failure of a theorem leads naturally to the classification of its exceptions. The goal of this thesis is to study the geometry of a certain family of counterexamples to Bertini's theorem. As it will become clear in the next chapters, very rich geometric phenomena arise from them, a unique feature that does not occur in characteristic zero.

1.1 Failure of Bertini's theorem

In his 1882 paper [Ber82], Eugenio Bertini introduced the two fundamental theorems that now bear his name. The first one, Bertini's theorem on variable singular points, is a statement about singular points of members of a pencil of hypersurfaces in an algebraic variety. The second one, Bertini's theorem on reducible linear systems, is about the irreducibility of a general member of a linear system of hypersurfaces. Nowadays, the two theorems are among the ones most used in algebraic geometry.

The theorem we are interested in is Bertini's theorem on variable singular points. In its modern version, it states the same as Sard's lemma but in the context of algebraic geometry: in characteristic zero almost all fibres of a dominant morphism $\phi : T \to B$ of irreducible smooth algebraic varieties over an algebraically closed field k are smooth. It can be hoped that a similar statement holds in positive characteristic, but this is not the case as Zariski [Zar44] observed in 1944. This means that in positive characteristic there exist fibrations of smooth varieties with every fibre singular. The most familiar examples of such objects are the quasi-elliptic fibrations that arise in the classification of smooth surfaces by Bombieri and Mumford [BM76] in characteristic 2 and 3 (see also [Lan79]).

The failure of Bertini's theorem is one of many *pathologies* that occur in positive characteristic, among which are included the failure of Kodaira's vanishing theorem [Ray78] and of Hodge symmetry [Ser58, Prop. 16]. Understanding why this pathological behaviour occurs usually entails a detailed study of the counterexamples. In the case of Bertini's theorem, there are far too many of them that it is virtually impossible to study them all at a time. So we are forced to work under some "reasonable" hypotheses. Therefore, in this thesis we shall always assume that the *general fibre* of our fibration $\phi : T \to B$ is an irreducible complete algebraic curve over the constant field k, that is, almost every fibre is a curve with the aforementioned properties.

From the point of view of Grothendieck's scheme theory, our assumptions mean that the *generic fibre*[1] of $\phi : T \to B$, that is, the generic fibre

$$C := \mathcal{T} \times_{\mathcal{B}} \operatorname{Spec} k(B)$$

of the morphism of schemes $\mathcal{T} \to \mathcal{B}$ associated to $\phi : T \to B$, is a geometrically integral regular complete curve over the (not necessarily algebraically closed) field $k(B)$.[2] The importance of this generic fibre relies on the following fact: any two fibrations $T \to B$ and $T' \to B$ over the same base B are *birationally equivalent*, i.e., there exists a birational map $T \dashrightarrow T'$ making the diagram

$$\begin{tikzcd} T \arrow[rr, dashed] \arrow[dr] & & T' \arrow[dl] \\ & B & \end{tikzcd}$$

commute, if and only if their generic fibres C and C' are isomorphic over the base field $k(B)$. Thus every fibration $\phi : T \to B$ is uniquely determined (birationally) by (the isomorphism class of) its generic fibre C, and so this establishes a one-to-one correspondence between the set of fibrations up to birational equivalence and the set of curves up to isomorphism

$$\left\{ \begin{array}{c} \text{fibrations} \\ \phi : T \to B \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{curves } C \\ \text{over } k(B) \end{array} \right\}.$$

Therefore, it is equivalent to classify fibrations up to birational equivalence and curves (or *function fields*, as we will see in a moment) up to isomorphism.

Since our interest lies in the failure of Bertini's theorem, a natural question arises: what can we say about the generic fibre C of a fibration $\phi : T \to B$ for which Bertini's theorem fails? To answer this question we consider the *geometric generic fibre*

$$\overline{C} := C \otimes_{k(B)} \overline{k(B)}$$

of $\phi : T \to B$, which is an integral complete curve over the algebraically closed field $\overline{k(B)}$. The key point for us is that the curve $\overline{C}$ can be viewed as the general fibre of $\phi : T \to B$, that is, most of the fibres will look like $\overline{C}$ and in fact will inherit many of their properties from $\overline{C}$. In particular, if $g := p_a(\overline{C})$ and $\overline{g} := p_g(\overline{C})$ are the arithmetic and geometric genera of $\overline{C}$, then $\phi : T \to B$ will be a fibration by curves of arithmetic genus g and geometric genus $\overline{g}$. It follows that a fibration $\phi : T \to B$ provides a counterexample to Bertini's theorem if and only if its geometric generic fibre $\overline{C}$ is a singular curve over $\overline{k(B)}$, or equivalently, if its generic fibre C is *non-smooth* over $k(B)$. Therefore, a fibration

[1] We emphasize the difference between our use of the words *general* and *generic*. By the general fibre of $\phi : T \to B$ we mean "almost every fibre of ϕ". (Example: the general fibre of ϕ is reduced = almost every fibre of ϕ is reduced.) On the other hand, the generic fibre of ϕ is the generic fibre, in the sense of scheme theory, of the morphism of schemes $\mathcal{T} \to \mathcal{B}$ associated to $\phi : T \to B$. Thus the general fibre of ϕ is an algebraic curve over the algebraically closed ground field k, whereas the generic fibre of ϕ is a scheme over the spectrum of $k(B)$, the function field of B.

[2] More precisely, C is a geometrically integral regular complete one-dimensional scheme of finite type over $\operatorname{Spec} k(B)$.

$\phi : T \to B$ for which Bertini's theorem fails is characterized by the rather peculiar property that its generic fibre C is a *regular but non-smooth* algebraic curve over the field $k(B)$.

Interestingly, the non-smoothness of the generic fibre can be investigated from the perspective of function field theory. Indeed, since the generic fibre C is completely determined by its function field $F|K := k(T)|k(B)$, the above one-to-one correspondence can be extended to

$$\left\{ \begin{array}{c} \text{fibrations} \\ \phi : T \to B \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{curves } C \\ \text{over } k(B) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{function fields} \\ F|k(B) \end{array} \right\}, \tag{1.1}$$

where fibrations are taken up to birational equivalence, and curves and function fields up to isomorphism. Now, since the geometric generic fibre $\overline{C} = C \otimes_K \overline{K}$ is singular precisely when the non-negative integer $g - \overline{g} = p_a(\overline{C}) - p_g(\overline{C})$ is positive, the non-smoothness of the generic fibre C is characterized by the strict inequality $\overline{g} < g$. Because $g = p_a(C)$ coincides with the genus of the function field $F|K := K(C)|K$ of C (recall that C is regular) and $\overline{g}$ coincides with the genus of the extended function field $F \otimes_K \overline{K}|\overline{K} = \overline{K}(\overline{C})|\overline{K}$, the inequality $\overline{g} < g$ means that the genus of $F|K$ drops on extending its base field from K to $\overline{K}$, or equivalently, that $F|K$ is a *non-conservative* function field. Accordingly, under the one-to-one correspondence (1.1) a fibration for which Bertini's theorem fails corresponds to a non-smooth curve, which in turn corresponds to a non-conservative function field

$$\left\{ \begin{array}{c} \text{fibrations by} \\ \textit{singular} \text{ curves} \\ \phi : T \to B \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{non-smooth} \text{ curves} \\ C \text{ over } k(B) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{non-conservative} \\ \text{function fields } F|k(B) \end{array} \right\}.$$

More precisely, a fibration $\phi : T \to B$ by singular curves of arithmetic genus g and geometric genus $\overline{g}$ (with $\overline{g} < g$) corresponds to a non-conservative function field $F|K$ whose genus g drops to $\overline{g}$ on extending its base from K to $\overline{K}$. Consequently, the theory of function fields provides a natural setting in which to analyze the failure of Bertini's theorem: a given fibration by singular curves $\phi : T \to B$ can be studied by looking at the (non-conservative) function field of its generic fibre.

We finish this first section by remarking that a function field $F|K$ may be non-conservative only if its base field K is imperfect (see page 15). In particular, non-conservative function fields can only occur in positive characteristic, which in our setting means that Bertini's theorem can only fail in positive characteristic.

1.2 What this thesis is about

By a theorem of Tate (see [Tat52], or [Sch09] for a more modern interpretation), the drop in genus $g - \overline{g}$ is a multiple of $\frac{p-1}{2}$, where $p > 0$ is the characteristic of the ground field. It follows that a fibration by singular curves of arithmetic genus g in characteristic $p > 0$ may exist only if $p \leq 2g + 1$. This puts an upper bound on the characteristic p for a fixed genus g. Cases $g = 1$ and $g = 2$ were already settled by Queen [Que71], Borges Neto [BN79], Stöhr and Simarra Cañate [SCS16]. A birational classification of the case $g = 3$ was started by Stöhr [Stö04, Stö07] in characteristic $p = 5, 7$ and then continued by Salomão [Sal11, Sal14] in characteristic $p = 3$; but nothing was known in characteristic $p = 2$.[3] In this thesis we study the case $g = 3$, $p = 2$.

[3] As a matter of fact, in many problems in number theory the case of characteristic 2 is exceptional and much more difficult to handle. Sometimes it requires new ideas or methods.

In Chapter 2 we present a rather detailed description of the relationship between fibrations by curves and their generic fibres (Section 2.1) that was already outlined in the previous section, putting emphasis on the fact that these generic fibres can be investigated from the point of view of the theory of algebraic function fields in one variable. Algebraic function fields are very classical objects that were studied since the late nineteenth century [DW82, HL02]. Roughly speaking, a function field can be viewed as the field of rational functions of an algebraic curve, and in fact the theory of algebraic function fields provides an intrinsic way to study algebraic curves, independently from their ambient spaces. General results in the theory were developed by many mathematicians including E. Artin, H. Hasse, F. K. Schmidt, A. Weil and, from a more geometric point of view, by the geometers of the Italian school [Sev08]. The first book in modern treatment was written by Chevalley [Che51].

The function fields that are relevant to us are the so-called *non-conservative* function fields, of which we give a brief account in Section 2.2. These are function fields $F|K$ whose genera drop on extending their base fields from K to $\overline{K}$. The term *conservative* was coined by Artin [Art67, p. 291] in an attempt to single out a class of function fields "which is in some sense reasonable".[4] Several results on non-conservative function fields and their singular primes were developed by Stichtenoth, Bedoya, Stöhr [Stö88, Sti78, BS87], and others. These function fields will play a prominent role in this thesis (see Chapter 3) because they are precisely the function fields of the generic fibres of the fibrations for which Bertini's theorem fails. In this way, much information of a fibration by singular curves can be obtained by looking at the (non-conservative) function field of its generic fibre.

Chapter 3 is the technical heart of the thesis. It is written in the setting of function field theory. In it we characterize and classify large families of non-conservative function fields $F|K$ in characteristic $p = 2$, whose genus $g = 3$ drops to $\overline{g} = 0$ on extending their base fields from K to the algebraic closure $\overline{K}$. Each of these function fields has a unique singular prime, and unlike the situation in characteristics $p = 3, 5, 7$ [Stö04, Stö07, Sal11], the genus g_1 of the extended function field $K^{1/2} \otimes_K F|K^{1/2}$ can differ from $\overline{g}$.[5] This may happen because the number $\frac{p-1}{2}$ takes its smallest value when $p = 2$ and so the obstruction for the genus drop that appears in Tate's theorem (see the beginning of this section) is less restrictive. In any case, the two possible values of g_1, namely 0 and 1, let us divide the discussion accordingly. The first family of function fields ($g_1 = 0$) is characterized by Theorem 3.4, while the second family ($g_1 = 1$) is characterized by Theorems 3.7 and 3.9. We then obtain criteria that let us decide when any two of these function fields are isomorphic (see Theorems 3.5, 3.8 and 3.10). Looking at the invariants of the only singular prime that appears in each function field (e.g., degrees, ramification/inertia indices, singularity degrees) one can realize that there is a considerable variety of examples (see Table 1.1), which will entail very rich geometric phenomena when translated to the setting of fibrations.

A common feature of the function fields in Chapter 3 is the *non-decomposedness* (see Section 2.3) of their only singular primes. Non-decomposed primes do not always occur, but it is nice to work with them because there exists a method to compute their singularity

[4]The adjective "reasonable" may come from the fact that non-conservative function fields occur only in positive characteristic.

[5]A function field $F|K$ can be seen as a one-dimensional regular scheme C over $\operatorname{Spec} K$, whose closed points are the primes of $F|K$. With this in mind, the extended function field $K^{1/2} \otimes_K F|K^{1/2}$ can be seen as the normalization of the base extension $C \otimes_K K^{1/2}$.

Invariants	First function field	Second function field	Third function field
$\deg \mathfrak{p}$	2	4	2 or 4
$\deg \mathfrak{p}_1$	1	2	2
$\deg \mathfrak{p}_2$	1	1	2
$\deg \mathfrak{p}_3$	1	1	1
$e_{\mathfrak{p}\mid\mathfrak{p}_1}$	1	1	2 or 1
$e_{\mathfrak{p}_1\mid\mathfrak{p}_2}$	2	1	2
$e_{\mathfrak{p}_2\mid\mathfrak{p}_3}$	2	2	1
$\delta(\mathfrak{p})$	3	3	3
$\delta(\mathfrak{p}_1)$	0	1	1
$\delta(\mathfrak{p}_2)$	0	0	0

Table 1.1: Comparison between the invariants of the only singular prime $\mathfrak{p}$ of three function fields. The first, second and third function fields correspond to Theorem 3.4 (i), Theorem 3.7 (i) and Theorem 3.9 (i) respectively. Even though the invariants on the left will be defined formally in Section 2.2, the table should serve to illustrate how diverse the properties of our function fields can be.

degrees (see the discussion following Proposition 2.11), which in general is a very hard task. From a more geometric point of view, the fact that the function field associated to a fibration has a unique singular prime that is non-decomposed means that almost every fibre has a unique singular point.

In Chapter 4 we apply the results of Chapter 3 to obtain results about curves and fibrations by curves. Let C be a geometrically integral regular complete curve over a field K of characteristic $p > 0$. Let g, g_1 and $\overline{g}$ denote the arithmetic genera of C, the normalization of $C \otimes_K K^{1/p}$ and the normalization of $C \otimes_K \overline{K}$, respectively. Recall that $g \geq g_1 \geq \overline{g}$, and that C is non-smooth precisely when $g > \overline{g}$. Theorem 4.1 characterizes a family of regular but non-smooth curves with $g = 3$ and $g_1 = 0$.

Theorem (Theorem 4.1)**.** *A geometrically integral regular complete curve C over a field K of characteristic $p = 2$ has genera $g = 3$, $g_1 = 0$ and admits a unique non-smooth non-decomposed point, if and only if, it is isomorphic to one of the following projective curves defined over K.*

(i) *The intersection of the surface*

$$\left\{(u_0 : u_1 : u_2 : u_3 : u_4 : v) \;\middle|\; \operatorname{rank}\begin{pmatrix} u_1 & u_2 & u_3 & u_4 \\ u_0 & u_1 & u_2 & u_3 \end{pmatrix} < 2\right\} \subseteq \mathbb{P}^5$$

and the hypersurface cut out by the equation

$$v^2 = a_0u_0^2 + u_0u_1 + a_2u_1^2 + a_4u_2^2 + a_6u_3^2 + a_8u_4^2,$$

where $a_0, a_2, a_4, a_6 \in K$ and $a_8 \in K \setminus K^2$.

(ii) *The intersection of the threefold*

$$\left\{(u_0 : u_1 : u_2 : u_3 : u_4 : v) \;\middle|\; \operatorname{rank}\begin{pmatrix} u_1 & u_2 & u_4 \\ u_0 & u_1 & u_3 \end{pmatrix} < 2\right\} \subseteq \mathbb{P}^5$$

and the three hypersurfaces cut out by the equations

$$u_0u_3 = v^2 + b_2u_1^2 + b_3u_1u_2 + b_4u_2^2,$$
$$u_3^2 = a_0u_0^2 + u_0u_1 + a_2u_1^2,$$
$$u_4^2 = a_0u_1^2 + u_1u_2 + a_2u_2^2,$$

where $b_i \in K$, $a_2 \in K \setminus K^2$ and $a_0 \in K$ are constants satisfying one of the following relations

- $b_4^{1/2} \notin K(a_2^{1/2})$;
- $b_2 = b_4 = 0$ *and* $b_3 \neq 0$.

We remark that the curves in the theorem are hyperelliptic, because of the hypothesis $g_1 = 0$. Non-hyperelliptic curves of genera $g = 3$ and $\overline{g} = 0$ are completely characterized by Theorem 4.2, where we note that the non-decomposedness condition is no longer an assumption, but has become a consequence of the "non-hyperellipticness" of C.

Theorem (Theorem 4.2)**.** *A geometrically integral regular complete curve C over a field K of characteristic $p = 2$ is non-hyperelliptic and has genera $g = 3$ and $\overline{g} = 0$, if and only if, it is isomorphic to one of the following plane projective quartics.*

(i) $Y^4 + a_0Z^4 + XZ^3 + a_2X^2Z^2 + a_4X^4 = 0$, *where* $a_0, a_2 \in K$ *and* $a_4 \in K \setminus K^2$.

(ii) $c_0(A_2^2X^4 + Z^4) + (B_1(Y^2 + XZ) + c_1X^2)(A_2X^2 + Z^2) + B_1^2c_1^2(Y^4 + X^2Z^2) = 0$, *where* $c_0, c_1, A_2, B_1 \in K$ *are constants satisfying the conditions* $B_1, c_1 \neq 0$ *and* $A_2 \notin K^2$.

(iii) $aY^4 + (m_1^2 + an_0^2)Z^4 + m_1X^2Y^2 + (a + m_1n_0)X^2Z^2 + m_1X^3Z + m_1^2cX^4 = 0$, *where* $a, c, m_1, n_0 \in K$ *are constants satisfying the conditions* $m_1 \neq 0$ *and* $a \notin K^2$.

(iv) $Y^4 + a_0Z^4 + XZ^3 + aXZ + (a_2 + a^2a_0)X^4 = 0$, *where* $a_0, a_2 \in K$ *and* $a \in K \setminus K^2$.

(v) $aY^4 + n_1Y^2Z^2 + n_1^2cZ^4 + n_1XZ^3 + aX^2Z^2 + n_1a_2X^2Y^2 + n_1a_2X^3Z + (ca_2^2 + 1)n_1^2X^4 = 0$, *where* $a, c, a_2, n_1 \in K$ *are constants satisfying the conditions* $a, a_2 \notin K^2$ *and* $n_1 \neq 0$.

Each of these curves has a unique non-smooth point, which is non-decomposed.

Also in Chapter 4, we obtain several fibrations by singular curves of arithmetic genus $g = 3$ and geometric genus $\overline{g} = 0$ out of the curves in the above theorems (see Theorems 4.5 and 4.6). Recall that k represents an algebraically closed field of characteristic 2, which will serve as the ground field of our fibrations. The basic idea to construct a fibration from a given curve is to take its constants as parameters, so that the resulting family of curves is fibered over them. For instance, if we want to use the curve in the first item of the above theorem then we consider the fourfold

$$T \subseteq \mathbb{P}^2(k) \times \mathbb{A}^3(k)$$

defined by the equation

$$Y^4 + T_1Z^4 + XZ^3 + T_2X^2Z^2 + T_3X^4 = 0,$$

where X, Y, Z stand for the homogeneous coordinate functions of $\mathbb{P}^2(k)$ and T_1, T_2, T_3 stand for the affine coordinate functions of $\mathbb{A}^3(k)$, and we project

$$\phi : T \longrightarrow \mathbb{A}^3(k)$$

onto the second component. (This fibration will be analyzed in detail in Example 2.1.) As discussed in the previous section, the curve C will become the generic fibre of the fibration, and the extended curve $\overline{C}$ will become its general fibre, so in particular most of the fibres will be curves of arithmetic genus $g = 3$ and geometric genus $\overline{g} = 0$.

Interestingly, or fortunately, the total spaces of the fibrations constructed in Section 4.2 are all smooth, a nice feature that most of the time does not occur. Admittedly, the total space of a fibration that is obtained from a regular but non-smooth curve typically has singularities, which in some cases may cause difficulties. Note, however, that it is possible to reduce the dimension of the bases of our fibrations (by setting some constants to be zero, e.g., in the above example $a_0 = a_2 = 0$, so that $T \subseteq \mathbb{P}^2 \times \mathbb{A}^1$ and $\phi : T \to \mathbb{A}^1$), and when we do so the total spaces may acquire singularities. This phenomenon is studied in Section 4.3, where we analyze the geometry of two fibrations over $\mathbb{P}^1$ by plane projective rational quartics of arithmetic genus 3, whose total spaces have singularities. In the pencils of curves in this section, all but one of the fibres have interesting properties, namely they are rational non-hyperelliptic plane projective quartics of arithmetic genus 3. In both cases the *bad fibre*, that is, the fibre whose behaviour differs from those of the remaining ones, is reduced. Because each fibration is essentially a singular surface fibered over the projective line, the theory of (relatively) minimal models comes into place. Motivated by the work of Kodaira and Néron [Kod63, Nér64] on the classification of special fibres of minimal fibrations by elliptic curves, we construct the minimal proper regular models of both fibrations, determine the structure of their bad fibres and study the geometry of the total spaces (see Theorems 4.7, 4.8, 4.9 and 4.10).

The last chapter completes the picture of the material presented in the previous ones, by providing examples of fibrations whose general fibre has arithmetic genus $g = 3$ and positive geometric genus $\overline{g}$. Indeed, in Chapters 3 and 4 the emphasis was placed mainly on the case $\overline{g} = 0$ with the corresponding function field having a unique (non-decomposed) singular prime. In the first section we build a fibration by singular curves of arithmetic genus $g = 3$ and geometric genus $\overline{g} = 1$. This means that the normalizations of the fibres are elliptic curves and hence that we may compute their j-invariants. Unexpectedly, the equation of the fibration is quite simple, and one can see in addition an interesting phenomenon: the j-invariant associated to the fibre does not remain constant but varies in accordance with the value of the point in the base. In the second section we present a one-dimensional fibration by curves of arithmetic genus $g = 3$ and geometric genus $\overline{g} = 2$, whose equation is also rather simple.

Finally, in the last section of the thesis we present examples of function fields of genera $g = 3$, $\overline{g} = 0$ with several singular primes. (Recall that most of the function fields in Chapter 3 have a unique singular prime.) By the genus drop formula (see (2.4)), it may be possible that a function field with $g = 3$, $\overline{g} = 0$ has two or three singular primes, and we verify that the two cases can occur. More than that, when the function field has two singular primes, one of singularity degree 1 and the other of singularity degree 2, we show that the singular prime of singularity degree 2 can be decomposed for one family of examples, and non-decomposed for another.

Chapter 2

Preliminaries

In this chapter we recall some concepts and results that will be needed later in this thesis. One of our goals is to show how the theory of function fields can be used to analyze the failure of Bertini's theorem. This is done in Section 2.1, which is somehow an expanded version of the technical part in Section 1.1.

In Section 2.2 we give a brief account of the theory of non-conservative function fields. Since they are directly related to the fibrations for which Bertini's theorem fails, these function fields are one of the central objects in this thesis, and a whole chapter (Chapter 3) will be dedicated to their examination. In Section 2.3 we study a special class of primes in function fields, called *non-decomposed*, that will appear naturally in Chapter 3. We will see that the computation of their singularity degrees, which is a very hard task for arbitrary primes, can be performed by means of the algorithm developed in [BS87].

We will focus mainly on the parts of the theory that will be more relevant for our purposes.

2.1 Fibrations by curves versus function fields

This section is mainly based on [SCS16, Section 1].

Let k be a fixed algebraically closed field of characteristic p. Let $\phi : T \to B$ be a dominant morphism of irreducible smooth algebraic varietes over k. Adopting a more geometric language, we may think of ϕ as a *fibration* with *total space* T and *base space* B. By identifying the rational functions on the base B with the rational functions on the total space T that are constant on each fibre, we can view $k(B)$ as a subfield of $k(T)$.

We are interested in the situation where $\phi : T \to B$ is a fibration by curves, i.e., almost all fibres are algebraic curves. By the theorem on the dimension of fibres (see [Sha13, Theorem 2.27]) this means that $\dim T = \dim B + 1$, and so that the field $k(T)$ has transcendence degree 1 over the field $k(B)$. We assume that the dominant morphism $\phi : T \to B$ is proper, so in particular it is surjective and its fibres are complete. We assume as well that almost all fibres of $\phi : T \to B$ are integral, which by a theorem of Matsusaka [Mat50] means that $k(B)$ is algebraically closed in $k(T)$ and that the field extension $k(T)|k(B)$ is separable. The field $k(T)$ of the total space T is therefore a finitely generated separable field extension of transcendence degree 1 over the field $k(B)$ of the base B. That is, the field extension $k(T)|k(B)$ is a *one-dimensional separable function field*.

From the point of view of Grothendieck's scheme theory, the function field $k(T)|k(B)$

is the field of the generic fibre[1]

$$C := \mathcal{T} \times_{\mathcal{B}} \operatorname{Spec} k(B)$$

of the morphism of schemes $\Phi : \mathcal{T} \to \mathcal{B}$ associated to $\phi : T \to B$, where $\mathcal{T}$ and $\mathcal{B}$ are the schemes whose points correspond bijectively to the closed irreducible subsets of T and B respectively. As we will see in the next paragraph, the generic fibre C is a geometrically integral regular complete algebraic curve over (the spectrum of) $k(B)$.[2] It encapsulates much of the geometry of the fibration $\phi : T \to B$, as should be clear from the following fact: any two fibrations $T \to B$ and $T' \to B$ over the same base B are birationally equivalent, i.e., there exists a birational map $T \dashrightarrow T'$ such that the diagram

$$\begin{tikzcd} T \arrow[rr, dashed] \arrow[dr] & & T' \arrow[dl] \\ & B & \end{tikzcd}$$

commutes, if and only if the corresponding curves C and C' are isomorphic over $k(B)$. This sets up a one-to-one correspondence between the set of fibrations $\phi : T \to B$ up to birational equivalence and the set of curves C over $k(B)$ up to isomorphism

$$\left\{ \begin{array}{c} \text{fibrations} \\ \phi : T \to B \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{curves } C \\ \text{over } k(B) \end{array} \right\}.$$

Now we take a closer look at the generic fibre C of the fibration $\phi : T \to B$. It is complete, since ϕ is assumed to be proper and so must be Φ, and its points correspond bijectively to the closed irreducible subsets of T whose images are dense in B (in fact equal to B by the properness of ϕ). Since almost every fibre of $\phi : T \to B$ has dimension 1 the same must happen with its generic fibre. Thus C has dimension 1 and its closed points, which are exactly its non-generic points, correspond bijectively to the *horizontal prime divisors* of the fibration $\phi : T \to B$, that is, to the prime divisors of T whose images are equal to B

$$\left\{ \begin{array}{c} \text{horizontal prime} \\ \text{divisors of } \phi : T \to B \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{closed points} \\ \text{of } C \end{array} \right\}. \tag{2.1}$$

A local computation in affine charts shows that this correspondence preserves local rings; in other words, if the closed point $c \in C$ corresponds to the horizontal prime divisor $H \subseteq T$, then the local ring of C at c is isomorphic to the local ring of T along H, i.e.,

$$\mathcal{O}_{C,c} \cong \mathcal{O}_{T,H}. \tag{2.2}$$

As T is smooth and therefore regular in codimension 1 (the localization of a regular local ring at a prime ideal is regular [Ser00, p. 79, Prop. 23]), this implies that the local rings of the generic fibre C are regular, and hence that C is a regular scheme. Clearly, the isomorphism (2.2) also implies that C is integral. Because the function field $k(T)|k(B)$ is separable the tensor product $k(T) \otimes_{k(B)} \overline{k(B)}$ is a field, and so we deduce that C is in

[1] See footnote 1 on page 2 about our use of the words *general* and *generic*.

[2] To be more precise, C is a geometrically integral regular complete one-dimensional scheme of finite type over (the spectrum of) $k(B)$.

fact geometrically integral (see [Liu02, p. 90, Remark 2.9]). Thus C is a geometrically integral regular complete algebraic curve over (the spectrum of) $k(B)$.

In view of the correspondence between the classes of fibrations $\phi : T \to B$ and the curves C, we may ask for the kind of curves C that correspond to the fibrations ϕ for which Bertini's theorem fails. That is, given such a fibration, what properties should its generic fibre have? Since the non-smooth locus of the fibration $\phi : T \to B$, i.e., the union of the non-smooth loci of the fibres, is closed in T, it is clear that Bertini's theorem fails for ϕ if and only if there exists a horizontal prime divisor contained in the non-smooth locus of ϕ. These prime divisors, whose points are singularities of the fibres to which they belong, are called the *moving singularities of the fibration* $\phi : T \to B$. Considering the bijection (2.1), they correspond to the closed points of C that are *non-smooth*, as will be seen in the next paragraph.

Recall that a point $c \in C$ is *smooth* if the semilocal ring $\mathcal{O}_{C,c} \otimes_{k(B)} \overline{k(B)}$ is regular, or equivalently, if the points of the *geometric generic fibre*

$$\overline{C} := C \otimes_{k(B)} \overline{k(B)} = (\mathcal{T} \times_{\mathcal{B}} \operatorname{Spec} k(B)) \times_{\operatorname{Spec} k(B)} \operatorname{Spec} \overline{k(B)}$$

that lie over c are regular, i.e., all of them are non-singular points of the integral curve $\overline{C}$ defined over the algebraically closed field $\overline{k(B)}$. Let $c \in C$ be a closed point and let $H \subseteq T$ be the corresponding horizontal prime divisor. Since the non-smooth locus of the morphism $\Phi : \mathcal{T} \to \mathcal{B}$ is closed in $\mathcal{T}$ (see [Liu02, p. 224, Corollary 2.12]), and since the non-smooth locus of the original fibration $\phi : T \to B$ is closed in T, it follows that H is a moving singularity if and only if its generic point is contained in the non-smooth locus of Φ, that is, if and only if c is a non-smooth point of the generic fibre C. Thus the bijection (2.1) restricts to

$$\left\{ \begin{array}{c} \text{moving singularities} \\ \text{of } \phi : T \to B \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{non-smooth closed} \\ \text{points of } C \end{array} \right\},$$

and consequently

$$\begin{array}{c} \text{Bertini's theorem} \\ \text{fails for } \phi \end{array} \quad \Leftrightarrow \quad \begin{array}{c} \phi \text{ admits} \\ \text{moving singularities} \end{array} \quad \Leftrightarrow \quad \begin{array}{c} \text{the curve } C \\ \text{is non-smooth.} \end{array}$$

Since the generic fibre C associated to a fibration $\phi : T \to B$ is a geometrically integral regular complete one-dimensional scheme of finite type over (the spectrum of) $k(B)$, it coincides with the *regular complete model* $\mathcal{R}_{k(T)|k(B)}$ of the separable one-dimensional function field $k(T)|k(B)$, i.e.,

$$C = \mathcal{T} \times_{\mathcal{B}} \operatorname{Spec} k(B) = \mathcal{R}_{k(T)|k(B)}$$

(see [GD67, II, Prop. 7.4.18, Rem. 7.4.19]). The closed points of $\mathcal{R}_{k(T)|k(B)}$ are precisely the primes $\mathfrak{p}$ of the function field $k(T)|k(B)$, and their local rings are the corresponding valuation rings $\mathcal{O}_{\mathfrak{p}}$. A prime $\mathfrak{p}$ of $k(T)|k(B)$ is non-smooth as a point of C if and only if the semilocal ring $\mathcal{O}_{\mathfrak{p}} \otimes_{k(B)} \overline{k(B)}$ is non-regular, i.e., if and only if $\mathcal{O}_{\mathfrak{p}} \otimes_{k(B)} \overline{k(B)}$ is not integrally closed in $k(T) \otimes_{k(B)} \overline{k(B)}$, that is, if and only if $\mathfrak{p}$ is a *singular* prime of $k(T)|k(B)$. We thus get the following correspondence

$$\begin{array}{ccccc} \left\{ \begin{array}{c} \text{horizontal prime} \\ \text{divisors of } \phi : T \to B \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{closed points} \\ \text{of } C \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{primes of} \\ k(T)|k(B) \end{array} \right\} \\ \cup\!| & & \cup\!| & & \cup\!| \\ \left\{ \begin{array}{c} \text{moving singularities} \\ \text{of } \phi : T \to B \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{non-smooth closed} \\ \text{points of } C \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{singular primes} \\ \text{of } k(T)|k(B) \end{array} \right\}. \end{array}$$

In particular, a fibration $\phi : T \to B$ admits moving singularities if and only if the curve C is non-smooth, and this happens if and only if the function field $k(T)|k(B)$ is *non-conservative*.[3] A fibration by singular curves $\phi : T \to B$ is therefore characterized by the rather peculiar property that its generic fibre C is a *regular but non-smooth curve* over $k(B)$.

Let us take a look at an example. We note that the fibration in the example has been built from Theorem 4.2 (i).

Example 2.1. Suppose that the algebraically closed field k has characteristic 2. Consider the smooth fourfold

$$T \subseteq \mathbb{P}^2 \times \mathbb{A}^3$$

cut out by the polynomial equation

$$Y^4 + T_1Z^4 + XZ^3 + T_2X^2Z^2 + T_3X^4 = 0,$$

where X, Y, Z represent the homogeneus coordinates of $\mathbb{P}^2$ and T_1, T_2, T_3 represent the affine coordinates of $\mathbb{A}^3$. The second projection

$$\phi : T \longrightarrow \mathbb{A}^3$$

is a proper map ($\mathbb{P}^2$ is projective) and it yields a fibration by plane projective curves. The fibre over the point $t = (t_1, t_2, t_3)$ of the base $\mathbb{A}^3$ can be identified with the plane projective quartic

$$T_t : Y^4 + t_1Z^4 + XZ^3 + t_2X^2Z^2 + t_3X^4 = 0,$$

which by the Jacobian criterion has a unique singular point at $(1 : t_3^{1/4} : 0)$. Thus there is just one moving singularity

$$V(Z, Y^4 + T_3X^4) \subseteq \mathbb{P}^2 \times \mathbb{A}^3,$$

which cuts on every fibre its only singular point. It can be verified that the curves T_t are rational of arithmetic genus 3. The field of rational functions of the base is $k(\mathbb{A}^3) = k(t_1, t_2, t_3)$, where by an abuse of notation we let t_i denote the coordinate functions of $\mathbb{A}^3$. The field of rational functions of the total space is $k(T) = k(t_1, t_2, t_3, x, y)$, where the functions x and y satisfy the relation

$$y^4 + t_1 + x + t_2x^2 + t_3x^4 = 0.$$

The function field $k(T)|k(\mathbb{A}^3) = k(\mathbb{A}^3)(x, y)|k(\mathbb{A}^3)$ of the fibration has genus 3 and the generic fibre C is a plane projective quartic curve over $k(B)$ whose equation is obtained by homogenizing the above polynomial relation with respect to x and y, i.e.,

$$Y^4 + t_1Z^4 + XZ^3 + t_2X^2Z^2 + t_3X^4 = 0.$$

The geometric generic fibre $\overline{C} = C \otimes_{k(B)} \overline{k(B)}$ is the plane projective quartic defined by the above equation, but now over the algebraically closed field $\overline{k(B)}$. Even though the curve $\overline{C}$ and the curves T_t are defined over different algebraically closed fields, we

[3]Non-conservative function fields will be studied in detail in Section 2.2. A function field $F|K$ is non-conservative if its genus drops on extending its base field K to the algebraic closure $\overline{K}$. Equivalently, $F|K$ is non-conservative if at least one of its primes is singular.

can see from their equations that they are very similar and that in fact they share many properties. For instance, the curve $\overline{C}$ has arithmetic genus 3 and geometric genus 0, and so do the fibres T_t; the curve $\overline{C}$ has a unique singular point, and so do the fibres C_t; and so on. From the point of view of function field theory (see Section 2.2), the moving singularity of the fibration $\phi : T \to \mathbb{A}^3$ corresponds to the pole of the function $x \in k(T)$, that is, to the only prime $\mathfrak{p}$ of $k(T)|k(B)$ such that $v_\mathfrak{p}(x) < 0$.

As should be clear from the previous paragraphs, a lot of information on a given fibration $\phi : T \to B$ is encoded in its generic fibre C. However, the geometric generic fibre $\overline{C} = C \otimes_{k(B)} \overline{k(B)}$, which is a complete integral algebraic curve over the algebraically closed field $\overline{k(B)}$, reflects the properties of the fibres in a more precise manner than C. (For instance, this was the case in Example 2.1.) In fact, most of the fibres will look like $\overline{C}$, which means that many of their properties will be inherited from $\overline{C}$. Hence the geometric generic fibre $\overline{C}$ can be viewed as the *general fibre* of the fibration.

Let g denote the arithmetic genus of the generic fibre C, which coincides with the genus of its function field $k(T)|k(B)$ because C is regular. Let $\overline{g}$ denote the geometric genus of the geometric generic fibre $\overline{C}$, i.e., the genus of its normalization, which coincides with the genus of the extended function field $k(T) \otimes_{k(B)} \overline{k(B)}|\overline{k(B)}$. Since the arithmetic genus of a curve is invariant under base field extensions, we deduce that g coincides with the arithmetic genus of $\overline{C}$. Thus $\overline{C}$, and almost every fibre of $\phi : T \to B$, has arithmetic genus g and geometric genus $\overline{g}$. Since we know from Hironaka's genus formula [Hir57] that the non-negative integer $g-\overline{g}$ is equal to the number of singular points of $\overline{C}$ counted according to their singularity degrees,[4] the fibration $\phi : T \to B$ admits moving singularities if and only if its geometric generic fibre $\overline{C}$ is a singular curve, i.e., if and only if $\overline{g} < g$, in which case $\phi : T \to B$ will be a fibration by singular curves of arithmetic genus g and geometric genus $\overline{g}$.

Curves and function fields

As we saw above, the generic fibre associated to a fibration $\phi : T \to B$ is a geometrically integral regular complete curve over the (not necessarily algebraically closed) field $k(B)$, which encapsulates many properties of ϕ. Curves satisfying these properties are therefore relevant, and hence it might be useful to look at them from a fibration-free point of view.

So let C be a geometrically integral regular complete curve over a field K of characteristic p.[5] Let $F := K(C)$ be its function field. By our assumptions on C, the field extension $F|K$ is a one-dimensional separable extension of transcendence degree 1 such that K is algebraically closed in F. Thus $F|K$ is a one-dimensional separable function field. Because of the properties the curve C has, it is in fact the regular complete model of $F|K$, that is,

$$C = \mathcal{R}_{F|K}.$$

The closed points of $\mathcal{R}_{F|K}$ correspond bijectively to the primes $\mathfrak{p}$ of the function field $F|K$, and its local rings are the corresponding valuation rings $\mathcal{O}_\mathfrak{p}$.

[4] The *singularity degree* (also known as *δ-invariant*) of a point P on a curve C' over an algebraically closed field k' is defined as $\delta_P = \dim_{k'}(\widetilde{\mathcal{O}_{C',P}}/\mathcal{O}_{C',P})$. This number measures how singular a point is. For instance, a point P is singular if and only if $\delta_P > 0$.

[5] To keep a geometric perspective, the field K should be thought of as the field of rational functions $k(B)$ of the base B of the corresponding fibration $T \to B$, and the field F as the field $k(T)$ of the total space T.

The above reasoning establishes a one-to-one correspondence

$$\left\{ \begin{array}{c} \text{geometrically integral regular} \\ \text{complete curves } C \text{ over } K \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{one-dimensional separable} \\ \text{function fields } F|K \end{array} \right\},$$

which is defined by associating to any curve C its function field $K(C)|K$, and to any function field $F|K$ its regular complete model $\mathcal{R}_{F|K}$. Since C is regular, its arithmetic genus g coincides with the genus of the corresponding function field $F|K$. The base extension

$$\overline{C} := C \otimes_K \overline{K} = C \times_{\operatorname{Spec} K} \operatorname{Spec} \overline{K}$$

is an integral complete algebraic curve defined over the algebraically closed field $\overline{K}$. It has arithmetic genus g (the arithmetic genus of a curve remains invariant under base field extensions) and its function field is equal to the extended function field

$$\overline{K}{\cdot}F|\overline{K} := \overline{K} \otimes_K F|\overline{K}.$$

The geometric genus $\overline{g}$ of $\overline{C}$, i.e., the genus of its normalization, is then equal to the genus of the function field $\overline{K}{\cdot}F|\overline{K}$. A prime $\mathfrak{p}$ of $F|K$ is non-smooth as an element of C if and only if the semilocal ring $\mathcal{O}_p \otimes_K \overline{K}$ is not integral in $\overline{K}{\cdot}F$, i.e., if and only if it is a *singular* prime of $F|K$. Thus a curve C is non-smooth if and only if its corresponding function field $F|K$ is *non-conservative*,[6] and this happens if and only if the extended curve $\overline{C}$ is singular, that is, $\overline{g} < g$. Since the genus of a function field is preserved under separable base field extensions (see page 15), the drop in genus can only occur when K is imperfect, and so this happens only when the characteristic p of K is positive.

Back to fibrations

As follows from the previous pages, the theory of algebraic function fields provides a natural setting in which to analyze the failure of Bertini's theorem. Essentially, classifying fibrations with moving singularities (those for which Bertini's theorem fails) is equivalent to classifying geometrically integral regular complete curves C defined over some (non-algebraically closed) field K, and this is equivalent to classifying non-conservative function fields $F|K$ with an imperfect base field K.

By a theorem of Tate [Tat52], a fibration by singular curves of arithmetic genus g in characteristic $p > 0$ may exist only if $p \leq 2g + 1$. This gives an upper bound on the characteristic p for a fixed genus g. Cases $g = 1$ and $g = 2$ were already settled by Queen [Que71], Borges Neto [BN79], Stöhr and Simarra Cañate [SCS16]. A birational classification of the case $g = 3$ was started by Stöhr [Stö04, Stö07] in characteristic $p = 5, 7$ and then continued by Salomão [Sal11, Sal14] in characteristic $p = 3$; but nothing was known in characteristic $p = 2$. In the next chapter we begin a classification of the case $g = 3$, $p = 2$.

2.2 Non-conservative function fields

Let $F|K$ be a one-dimensional separable function field of genus g in characteristic p. Since $F|K$ is separable, there exists a function $y \in F \setminus K$ that forms a separating transcendence

[6] See footnote 3 on page 11.

base of F over K, i.e., such that the finite field extension $F|K(y)$ is separable. Such a function is called a *separating variable* of $F|K$.

Given a prime $\mathfrak{p}$ of $F|K$ we use the following notation

$$\begin{aligned} v_\mathfrak{p} &: \text{discrete valuation associated to } \mathfrak{p},\\ \mathcal{O}_\mathfrak{p} &: \text{discrete valuation ring associated to } \mathfrak{p},\\ \mathfrak{m}_\mathfrak{p} &: \text{maximal ideal of } \mathcal{O}_\mathfrak{p},\\ K_\mathfrak{p} &: \text{residue field of } \mathfrak{p}, \text{ i.e., } \mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}. \end{aligned}$$

The *degree* of $\mathfrak{p}$, denoted $\deg \mathfrak{p}$, is defined as the degree of the finite field extension $K_\mathfrak{p}|K$. Primes of degree 1 are called *rational*.

Let K' be an algebraic extension of the base field K. The base extension $K'{\cdot}F|K' := K' \otimes_K F|K'$ is then a one-dimensional separable function field. As will follow from Rosenlicht's genus drop formula (2.4) and equation (2.3), the genus g' of $K'{\cdot}F|K'$ is smaller than or equal to the genus g of $F|K$, i.e., $g \geq g'$, and so one says that *the genus of a function field can only decrease when we extend its base.*

For each prime $\mathfrak{p}$ of $F|K$ there are only finitely many primes $\mathfrak{p}'_1, \ldots, \mathfrak{p}'_r$ of $K'{\cdot}F|K'$ that lie over $\mathfrak{p}$, i.e., such that their local rings $\mathcal{O}_{\mathfrak{p}'_i}$ dominate the local ring $\mathcal{O}_\mathfrak{p}$ of $\mathfrak{p}$. Then the integral closure of the extended semilocal ring $K'{\cdot}\mathcal{O}_\mathfrak{p} := K' \otimes_K \mathcal{O}_\mathfrak{p}$ in its field of fractions $K'{\cdot}F$ is equal to

$$\widetilde{K'{\cdot}\mathcal{O}_\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}'_1} \cap \cdots \cap \mathcal{O}_{\mathfrak{p}'_r}.$$

The dimension of the K'-vector space $\widetilde{K'{\cdot}\mathcal{O}_\mathfrak{p}}/K'{\cdot}\mathcal{O}_\mathfrak{p}$ is referred to as the K'-*singularity degree* of $\mathfrak{p}$. If $K' = \overline{K}$, then we simply speak of the *singularity degree* of $\mathfrak{p}$, and we denote it by $\delta(\mathfrak{p})$. The K'-singularity degree of a prime $\mathfrak{p}$ is finite (see [Ros52, p. 172]) and it may increase as K' gets larger. To be more precise, let K'' be an algebraic extension of K' and consider the extended function field $K''{\cdot}F|K''$. Then the natural homomorphism

$$\widetilde{K''{\cdot}\mathcal{O}_\mathfrak{p}} = \bigcap \widetilde{K''{\cdot}\mathcal{O}_{\mathfrak{p}'_i}} \longrightarrow \bigoplus \widetilde{K''{\cdot}\mathcal{O}_{\mathfrak{p}'_i}}/K''{\cdot}\mathcal{O}_{\mathfrak{p}'_i}$$

has kernel $K''{\cdot}\widetilde{K'{\cdot}\mathcal{O}_\mathfrak{p}}$ and is surjective, as follows from the approximation theorem and the fact that each conductor $\big(K''{\cdot}\mathcal{O}_{\mathfrak{p}'_i} : \widetilde{K''{\cdot}\mathcal{O}_{\mathfrak{p}'_i}}\big)$ is a nonzero ideal of the semilocal ring $\widetilde{K''{\cdot}\mathcal{O}_{\mathfrak{p}'_i}}$. This means that

$$\begin{aligned} \dim_{K''} \widetilde{K''{\cdot}\mathcal{O}_\mathfrak{p}}/K''{\cdot}\mathcal{O}_\mathfrak{p} &= \dim_{K''} K''{\cdot}\widetilde{K'{\cdot}\mathcal{O}_\mathfrak{p}}/K''{\cdot}\mathcal{O}_\mathfrak{p} + \sum \dim_{K''} \widetilde{K''{\cdot}\mathcal{O}_{\mathfrak{p}'_i}}/K''{\cdot}\mathcal{O}_{\mathfrak{p}'_i}\\ &= \dim_{K''} K'' \otimes_{K'} \widetilde{K'{\cdot}\mathcal{O}_\mathfrak{p}}/K'' \otimes_{K'} K'{\cdot}\mathcal{O}_\mathfrak{p} + \sum \dim_{K''} \widetilde{K''{\cdot}\mathcal{O}_{\mathfrak{p}'_i}}/K''{\cdot}\mathcal{O}_{\mathfrak{p}'_i}\\ &= \dim_{K'} \widetilde{K'{\cdot}\mathcal{O}_\mathfrak{p}}/K'{\cdot}\mathcal{O}_\mathfrak{p} + \sum \dim_{K''} \widetilde{K''{\cdot}\mathcal{O}_{\mathfrak{p}'_i}}/K''{\cdot}\mathcal{O}_{\mathfrak{p}'_i}. \end{aligned} \tag{2.3}$$

Put into words, the above equality asserts that the difference between the K''-singularity degree and the K'-singularity degree of $\mathfrak{p}$ is equal to the sum of the K''-singularity degrees of the primes $\mathfrak{p}'_i$ of $K'F|K'$ lying over $\mathfrak{p}$.

If the field extension $K'|K$ is separable, then it can be shown that the domains $K'{\cdot}\mathcal{O}_\mathfrak{p}$ are integrally closed in $K'{\cdot}F$, which means that every prime of $F|K$ has K'-singularity degree zero. This fact together with equation (2.3) implies that singularity degrees are *preserved* by separable base field extensions, that is, the singularity degree of a prime equals the sum of the singularity degrees of the primes lying over it, provided that the base field extension one considers is separable.

A prime $\mathfrak{p}$ is called *singular* if its singularity degree is positive, i.e., $\delta(\mathfrak{p}) > 0$. By Rosenlicht's genus drop formula (see [Ros52, Theorem 11]), the genus $\overline{g}$ of the extended function field $\overline{K}F|\overline{K}$ is related to the singularity degrees of the primes of $F|K$ in the following way

$$\overline{g} = g - \sum \delta(\mathfrak{p}), \tag{2.4}$$

where $\mathfrak{p}$ runs through the primes of $F|K$. The function field $F|K$ is called *conservative* if the genus drop is zero, i.e., if $\overline{g} = g$, and *non-conservative* otherwise, i.e., if $\overline{g} < g$. Clearly, $F|K$ is non-conservative if and only if at least one of its primes is singular.

One can verify easily that the above genus drop formula holds for arbitrary algebraic base field extensions: if g' is the genus of the extended function field $K'F|K'$, then the genus drop $g - g'$ equals the sum of the K'-singularity degrees of the primes of $F|K$. As a result, the genus of a function field remains invariant under separable base field extensions, i.e., $g' = g$ if $K'|K$ is separable. Thus every function field $F|K$ whose base field K is perfect is conservative. In particular, non-conservative function fields can only occur in positive characteristic.

Example 2.2. Assume that $p > 2$. Consider the function field $F|K = K(x,y)|K$ defined by the polynomial equation

$$y^2 = x^p + c, \quad \text{where } c \in K \setminus K^p.$$

This function field is non-conservative and has genera $g = \frac{p-1}{2}$ and $\overline{g} = 0$. The zero of y, i.e., the prime $\mathfrak{p}$ such that $y \in \mathfrak{m}_\mathfrak{p}$, is the only singular prime of $F|K$.

Since non-conservative function fields are our main object of study in this section, from now we shall assume that the characteristic p of $F|K$ is positive.

For each non-negative integer n we consider the function field $F_n|K := K{\cdot}F^{p^n}|K$ of genus g_n, which is uniquely determined by the property that the extension $F|F_n$ is purely inseparable of degree p^n. This function field is called the *n-th Frobenius pullback* of $F|K$. Note that a function $y \in F$ is a separating variable of $F|K$ if and only if $y \notin F_1$. In particular, if y is a separating variable of $F|K$ then y^{p^n} is a separating variable of $F_n|K$ for every n.

Given a prime $\mathfrak{p}$, we let $\mathfrak{p}_n$ denote its restriction to $F_n|K$. Since the extension $K^{1/p^n}|K$ is purely inseparable, so is the extension $K^{1/p^n}{\cdot}F|F$, and hence there is only one prime of $K^{1/p^n}{\cdot}F|K^{1/p^n}$, say $\mathfrak{p}^{(n)}$, lying over $\mathfrak{p}$. The n-th Frobenius map $z \mapsto z^{p^n}$ defines an isomorphism between the function fields $K^{1/p^n}{\cdot}F|K^{1/p^n}$ and $F_n|K$ under which the primes $\mathfrak{p}^{(n)}$ and $\mathfrak{p}_n$ correspond. This embeds the finite purely inseparable base field extensions of $F|K$ inside $F|K$, and so we can study them by looking just at $F|K$. By the fundamental equality, the following identity holds

$$e_{\mathfrak{p}|\mathfrak{p}_n} \cdot f_{\mathfrak{p}|\mathfrak{p}_n} = p^n \text{ for every } n,$$

where $e_{\mathfrak{p}|\mathfrak{p}_n}$ and $f_{\mathfrak{p}|\mathfrak{p}_n} := [K_\mathfrak{p} : K_{\mathfrak{p}_n}]$ are the ramification and inertia indices of $\mathfrak{p}|\mathfrak{p}_n$ respectively. In particular, if $n = 1$ then $\mathfrak{p}$ is unramified over F_1, i.e., $e_{\mathfrak{p}|\mathfrak{p}_1} = 1$, if and only if it is inertial over F_1, i.e., $f_{\mathfrak{p}|\mathfrak{p}_1} = p$.

By a theorem of Stichtenoth (see [Sti78, Satz 2 (ii)]), the residue field $K_\mathfrak{p}$ of a prime $\mathfrak{p}$ is separable over the base field K if and only if $\mathfrak{p}$ is non-singular and ramified over F_1, i.e., $K_\mathfrak{p} = K_{\mathfrak{p}_1}$. By the same theorem (see [Sti78, Satz 2 (i)]), if the extension $K_\mathfrak{p}|K$ is not simple then $\mathfrak{p}$ is singular. Thus we can write in a schematic way

$$K_\mathfrak{p}|K \text{ separable} \quad \Rightarrow \quad \mathfrak{p} \text{ non-singular} \quad \Rightarrow \quad K_\mathfrak{p}|K \text{ simple}.$$

In particular, rational primes are non-singular.

As follows from [Stö88, Corollary 2.5], the singularity degrees of a prime $\mathfrak{p}$ and its extensions $\mathfrak{p}^{(1)}$ and $\mathfrak{p}^{(2)}$ are related by the following formula

$$\delta(\mathfrak{p}) - \delta(\mathfrak{p}^{(1)}) = p\big(\delta(\mathfrak{p}^{(1)}) - \delta(\mathfrak{p}^{(2)})\big) + \frac{p-1}{2} \cdot m \cdot \deg \mathfrak{p}^{(1)}, \tag{2.5}$$

where m is a non-negative integer. The $K^{1/p}$-singularity degree $\delta(\mathfrak{p}) - \delta\big(\mathfrak{p}^{(1)}\big)$ of $\mathfrak{p}$ divided by p is then larger than the $K^{1/p}$-singularity degree $\delta\big(\mathfrak{p}^{(1)}\big) - \delta\big(\mathfrak{p}^{(2)}\big)$ of its extension $\mathfrak{p}^{(1)}$. Since the singularity degree $\delta(\mathfrak{p})$ of a prime $\mathfrak{p}$ is equal to the sum of the $K^{1/p}$-singularity degrees of $\mathfrak{p}, \mathfrak{p}^{(1)}, \mathfrak{p}^{(2)}, \ldots$, this implies that

$$\mathfrak{p} \text{ is a singular prime if and only if it is } K^{1/p}\text{-singular, i.e., if } \delta(\mathfrak{p}) > \delta\big(\mathfrak{p}^{(1)}\big)$$

(see also [Stö88, Corollary 3.2]). A straightforward consequence is Kimura's theorem [Kim69], a remarkable result which says that

$$F|K \text{ is non-conservative if and only if } g > g_1,$$

i.e., the genus of a non-conservative function field $F|K$ already drops on extending its base K to $K^{1/p}$. As a result, the sequence of genera

$$g \geq g_1 \geq g_2 \geq \cdots$$

of $F|K$ decreases strictly until it stabilizes at $\overline{g}$, that is, there exists an integer $n \geq 0$ such that $g > g_1 > \cdots > g_n$ and $g_n = g_{n+1} = \cdots = \overline{g}$. In particular, the function fields $K^{1/p^n}F|K^{1/p^n} \cong F_n|K$ are conservative, and hence all their primes are non-singular.

The drop in genus that occurs when extending the base K of $F|K$ is not arbitrary. Indeed, the first genus drop $g - g_1$ (and hence every genus drop $g_n - g_{n+1}$) is always a multiple of $(p-1)/2$. To see this it suffices to verify that the $K^{1/p}$-singularity degree of a prime $\mathfrak{p}$ is a multiple of $(p-1)/2$, which is a consequence of the following two observations: 1) the $K^{1/p}$-singularity degree of the extended prime $\mathfrak{p}^{(n)}$ vanishes for n large enough; 2) by (2.5), the difference between the $K^{1/p}$-singularity degrees of the primes $\mathfrak{p}^{(n)}$ and $\mathfrak{p}^{(n+1)}$ is a multiple of $(p-1)/2$ for every n. Thus the global genus drop $g - \overline{g}$ is also a multiple of $(p-1)/2$. This result, first proved by Tate [Tat52], has an important consequence: if $F|K$ is non-conservative, then

$$p \leq 2g + 1.$$

This gives an upper bound on the characteristic p of a non-conservative function field in terms of its genus g.

Non-conservative function fields of genus 1 were classified by Queen [Que71], and of genus 2 by Borges Neto [BN79], Stöhr and Simarra Cañate [SCS16]. The case of genus $g = 3$ in characteristics $p = 3, 5, 7$ was studied by Salomão [Sal11, Sal14] and Stöhr [Stö04, Stö07], but nothing was known in characteristic $p = 2$. In the next chapter we shall begin a classification of the case $g = 3$, $p = 2$.

Computing the singularity degree of a prime

In practice, it is rather hard to compute the singularity degree of a given prime. However, in some cases we can take advantage of the algorithm developed by Bedoya and Stöhr in [BS87]. We recall it in a form that is suitable for our purposes.

Theorem 2.3 ([BS87, Theorem 2.3]). *Let $\mathfrak{p}$ be a prime of a function field $F|K$ such that its restriction $\mathfrak{p}_n$ to $F_n|K$ is rational for some integer $n \geq 0$. Then*

$$\delta(\mathfrak{p}) = p \cdot \delta(\mathfrak{p}_1) + \frac{p-1}{2} \cdot v_{\mathfrak{p}_n}(dz^{p^n}),$$

where $z \in F$ is any function such that $\mathcal{O}_\mathfrak{p} = \mathcal{O}_{\mathfrak{p}_1}[z]$.

Let $\mathfrak{p}$ be a prime whose restriction $\mathfrak{p}_n$ is rational for some $n \geq 0$. Then every restricted prime $\mathfrak{p}_m$ ($0 \leq m \leq n$) satisfies the hypothesis of Theorem 2.3, and since $\mathfrak{p}_n$ has singularity degree 0 we can apply the theorem to compute successively the singularity degrees of $\mathfrak{p}_{n-1}, \mathfrak{p}_{n-2}, \dots, \mathfrak{p}_1, \mathfrak{p}$. This yields a useful algorithm to compute the singularity degree of the prime $\mathfrak{p}$.

Remark 2.4. In [BS87] it is always assumed that the base field K is separably closed, i.e., that every algebraic extension of K is inseparable. Nevertheless, the results in the paper hold under weaker hypotheses. More precisely, the separability assumption on K is used only to guarantee that for every prime $\mathfrak{p}$ there is an integer $n \geq 0$ such that $\mathfrak{p}_n$ is rational (see [BS87, Lemma 2.1]). The existence of such an n is in fact the *crucial condition* needed in order for everything to work in the paper. This is the reason why we have dropped the separability assumption on K in Theorem 2.3.

We point out that the original statement of the theorem, as written in [BS87], is given in terms of some integers $c_\mathfrak{p}$, called *conductors*, that satisfy the identity $c_\mathfrak{p} = 2\delta(\mathfrak{p})$. Several other results in [BS87] are also given in terms of them.

The following proposition and theorem, also taken from [BS87], will be useful to us in many situations.

Proposition 2.5 ([BS87, Proposition 4.1]). *Let $\mathfrak{p}$ be a prime of a function field $F|K$ such that its restriction $\mathfrak{p}_1$ to $F_1|K$ is rational. Let $x \in F$ be a local parameter at $\mathfrak{p}_1$, so that for every separating variable y of $F|K$ we can write $y^p \in F_1$ as a Laurent series in x with coefficients in K*

$$y^p = \sum_{i=\gamma}^{\infty} a_i x^i.$$

Define $\mu := \min\{\, i \mid a_i \neq 0,\ i \not\equiv 0 \bmod p \,\}$. Then $\mathfrak{p}$ is non-rational if and only if there is an integer τ smaller than μ such that $a_\tau \notin K^p$. If τ is minimal with this property then $K_\mathfrak{p} = K(a_\tau^{1/p})$ and

$$\delta(\mathfrak{p}) = \frac{(p-1)(\mu - \tau - 1)}{2}.$$

Theorem 2.6 ([BS87, Theorem 2.7]). *Let $\mathfrak{p}$ be a prime of a function field $F|K$ such that its restriction $\mathfrak{p}_n$ to $F_n|K$ is rational for some integer $n \geq 0$. If y is a separating variable of $F|K$, then the orders of the differentials dy and dy^{p^n} of $F|K$ and $F_n|K$ at $\mathfrak{p}$ and $\mathfrak{p}_n$ respectively are related by*

$$v_\mathfrak{p}(dy) = \frac{2\delta(\mathfrak{p}) + v_{\mathfrak{p}_n}(dy^{p^n})}{\deg \mathfrak{p}}.$$

2.3 Non-decomposed primes

We say that a prime $\mathfrak{p}$ of a separable function field $F|K$ is *non-decomposed* if there is only one prime of $\overline{K}F|\overline{K}$ lying over $\mathfrak{p}$. Equivalently, there is only one prime of $FL|L$ above $\mathfrak{p}$, where L denotes the separable closure of K.

Example 2.7. Rational primes are non-decomposed. Indeed, we shall prove that if a prime $\mathfrak{p}$ is rational and L is an algebraic extension of K, then there is a unique prime $\mathfrak{q}$ of $LF|L$ lying over $\mathfrak{p}$. When $L|K$ is finite, the uniqueness of $\mathfrak{q}$ follows from the fundamental inequality because $f_{\mathfrak{q}|\mathfrak{p}} = [L_{\mathfrak{q}} : K_{\mathfrak{p}}] = [L_{\mathfrak{q}} : K] \geq [L : K] = [LF : F]$. In the general case, if $\mathfrak{q}_1 \neq \mathfrak{q}_2$ are two primes of $LF|L$ lying over $\mathfrak{p}$, then there is a function $z \in LF$ with $v_{\mathfrak{q}_1}(z) \neq v_{\mathfrak{q}_2}(z)$ and a finite subextension $K'|K$ of $L|K$ such that $z \in K'F$. The restrictions of $\mathfrak{q}_1$ and $\mathfrak{q}_2$ to $K'F$ are therefore different. But since both lie over $\mathfrak{p}$, they must coincide by the proof of the finite case, a contradiction.

For an example of a prime that is decomposed we refer the reader to Proposition 5.1. In general, it may be difficult to decide whether a given prime is non-decomposed. We provide a sufficient criterion for a given singular prime to be non-decomposed.

Proposition 2.8. *Let r denote the number of primes of $\overline{K}F|\overline{K}$ lying over $\mathfrak{p}$. Then r divides the singularity degree $\delta(\mathfrak{p}_n)$ of $\mathfrak{p}_n$ for each nonnegative integer n.*

Proof. Let L be the separable closure of K. As $\overline{K}F|LF$ is a purely inseparable extension, each prime of $LF|L$ has exactly one extension to $\overline{K}F|\overline{K}$, and so the integer r is also equal to the number of primes of $LF|L$ lying over $\mathfrak{p}$.

Since separable base field extensions preserve singularity degrees (see page 14), the singularity degree of $\mathfrak{p}$ equals the sum of the singularity degrees of the primes of $LF|L$ lying over $\mathfrak{p}$. But these primes are conjugated because $L|K$ is normal, and hence their singularity degrees coincide. This proves that r is a divisor of $\delta(\mathfrak{p})$. $\square$

Corollary 2.9. *If the integers $\delta(\mathfrak{p}_n)$ are coprime, then $\mathfrak{p}$ is non-decomposed.*

The importance of non-decomposed primes relies on the following two results.

Proposition 2.10. *Every non-singular non-decomposed prime that is ramified over F_1 is rational.*

Proof. Let $\mathfrak{p}$ be a non-singular non-decomposed prime that is ramified over F_1. Since the extension $K_{\mathfrak{p}}|K$ is separable by [Sti78, Satz 2 (ii)], the normal closure L' of $K_{\mathfrak{p}}$ is a finite Galois extension of K. Therefore, the degree of $\mathfrak{p}$ is equal to the number of primes of $L'F|L'$ lying over $\mathfrak{p}$ counted according to their degrees. But there is only one such prime ($\mathfrak{p}$ is non-decomposed), which is rational as $K_{\mathfrak{p}} \subseteq L'$. Thus $\mathfrak{p}$ is rational as desired. $\square$

Note that the proposition gives a partial answer to the problem of deciding whether a given non-singular prime is rational.

Proposition 2.11. *If $\mathfrak{p}$ is a non-singular non-decomposed prime, then $K_{\mathfrak{p}}|K$ is a purely inseparable extension, say of degree p^m, and the restricted prime $\mathfrak{p}_m$ is rational.*

Proof. By [Sti78, Satz 2 (ii)] we know that $K_{\mathfrak{p}} = K_{\mathfrak{p}_1}$ if and only if $K_{\mathfrak{p}}|K$ is separable. Therefore, by an inductive argument we can find an integer $m \geq 0$ such that the field extensions $K_{\mathfrak{p}}|K_{\mathfrak{p}_m}$ and $K_{\mathfrak{p}_m}|K$ are purely inseparable and separable respectively. Since the prime $\mathfrak{p}_m$ is rational by Proposition 2.10, the result follows. $\square$

As an immediate consequence of the proposition, we deduce that if $\mathfrak{p}$ is a singular non-decomposed prime, then its singularity degree $\delta(\mathfrak{p})$ can be computed by means of the algorithm developed by Bedoya and Stöhr [BS87]. Indeed, to see this it is enough to show that the restricted prime $\mathfrak{p}_n$ is rational for some integer n (see Theorem 2.3 and the discussion that follows), and since we already know that $\mathfrak{p}_n$ is non-singular for n large enough, a straightforward application of the proposition yields the desired result.

Since in the next chapter we shall be dealing with non-conservative function fields of genus $g = 3$, now we establish a result concerning singular primes of singularity degree at most 3.

Proposition 2.12. *Let $F|K$ be a function field in characteristic $p = 2$, and let $\mathfrak{p}$ be a singular prime of singularity degree $\delta(\mathfrak{p}) \leq 3$. Then*

$$\delta(\mathfrak{p}_1) \begin{cases} \leq 1, & \text{if } \delta(\mathfrak{p}) = 3, \\ = 0, & \text{if } \delta(\mathfrak{p}) \leq 2. \end{cases}$$

Assume in addition that $\mathfrak{p}$ is non-decomposed.

(i) *If $\delta(\mathfrak{p}) = 3$ and $\delta(\mathfrak{p}_1) = 1$ then $\mathfrak{p}_3$ is rational.*

(ii) *If $\delta(\mathfrak{p}) = 3$ and $\delta(\mathfrak{p}_1) = 0$ then $\mathfrak{p}_2$ is rational.*

(iii) *If $\delta(\mathfrak{p}) = 2$ then $\mathfrak{p}_3$ is rational.*

(iv) *If $\delta(\mathfrak{p}) = 1$ then $\mathfrak{p}_2$ is rational.*

Note that by Corollary 2.9 the non-decomposedness assumption is not necessary in items (i) and (iv). In the proof of the proposition we shall use the following fact: a prime $\mathfrak{p}$ is singular if and only if $\delta(\mathfrak{p}) - \delta(\mathfrak{p}_1) > 0$ (see page 16).

Proof. The proof will follow from the formula

$$\delta(\mathfrak{p}) - \delta(\mathfrak{p}_1) = 2(\delta(\mathfrak{p}_1) - \delta(\mathfrak{p}_2)) + \frac{1}{2} \cdot m \cdot \deg \mathfrak{p}_1, \tag{2.6}$$

where $m \geq 0$ is an integer (see equation (2.5)). Indeed, if $\delta(\mathfrak{p}) = 3$ and $\delta(\mathfrak{p}) - \delta(\mathfrak{p}_1) > 0$ is equal to 1, then $\delta(\mathfrak{p}_1) - \delta(\mathfrak{p}_2) = 0$ and so $\mathfrak{p}_1$ is non-singular, a contradiction. And if $\mathfrak{p}_1$ is singular then $\delta(\mathfrak{p}_1) - \delta(\mathfrak{p}_2) > 0$ and so $\delta(\mathfrak{p}) > 2$.

We now prove the second part of the proposition.

(i) Since $\delta(\mathfrak{p}_2) = 0$, equation (2.6) gives $2 = m \deg \mathfrak{p}_2$. Since $\deg \mathfrak{p}_2$ is the degree of the field extension $K_{\mathfrak{p}_2}|K$, we conclude from Proposition 2.11 that $\mathfrak{p}_3$ is rational.

(ii) The formula (2.6) gives $6 = m \deg \mathfrak{p}_1$. Then Proposition 2.11 implies that $\mathfrak{p}_2$ is rational.

(iii) The formula (2.6) gives $4 = m \deg \mathfrak{p}_1$. Then Proposition 2.11 implies that $\mathfrak{p}_3$ is rational.

(iv) This follows from the proof of (i). □

Corollary 2.13. *Let $F|K$ be a function field of genus $g = 3$ in characteristic $p = 2$, and assume that it is geometrically rational, that is, $\overline{g} = 0$. Then its Frobenius pullback $F_1|K$ has genus $g_1 \leq 1$. Moreover, if $F|K$ admits at least two singular primes then $g_1 = 0$.*

Chapter 3

Non-conservative function fields of genus 3 in characteristic 2

This chapter is devoted to the investigation of non-conservative function fields of genus $g = 3$ in characteristic $p = 2$. As such, it is written in the language of function field theory, and the notation and terminology introduced in Sections 2.2 and 2.3 will be freely used. To keep a geometric perspective one can think of a function field $F|K$ as a one-dimensional scheme over $\operatorname{Spec} K$ whose closed points are precisely the primes $\mathfrak{p}$ of $F|K$ and whose local rings are the corresponding valuation rings $\mathcal{O}_\mathfrak{p}$ (see Section 2.1). Our interest in non-conservative function fields comes from the fact that they are precisely the function fields of the generic fibers of the fibrations for which Bertini's theorem fails (see Section 2.1). Consequently, it is hoped that an in-depth examination of the former will yield very valuable information about the latter (see Chapter 4).

Let $F|K$ be a non-conservative one-dimensional separable function field of genus $g = 3$ in characteristic $p = 2$. Given a prime $\mathfrak{p}$ of $F|K$ we use the following notation, which was already introduced in Section 2.2

$$\begin{aligned} v_\mathfrak{p} &: \text{discrete valuation associated to } \mathfrak{p}, \\ \mathcal{O}_\mathfrak{p} &: \text{discrete valuation ring associated to } \mathfrak{p}, \\ \mathfrak{m}_\mathfrak{p} &: \text{maximal ideal of } \mathcal{O}_\mathfrak{p}, \\ K_\mathfrak{p} &: \text{residue field of } \mathfrak{p}, \text{ i.e., } \mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}. \end{aligned}$$

By Rosenlicht's genus drop formula (2.4), we know that the genus $\overline{g}$ of the extended function field $\overline{K}F|\overline{K}$ can take three values, namely 0, 1 and 2. The following examples show that each of these cases can actually occur.

Example 3.1 ($g = 3$ and $\overline{g} = 0$)**.** Consider the function field $F|K = K(x,y)|K$ in characteristic 2 given by the equation

$$y^4 = x^3 + a,$$

where $a \in K \setminus K^2$. We claim that $F|K$ has genera

$$g = 3 \quad \text{and} \quad \overline{g} = 0,$$

and that is has a unique singular prime of singularity degree 3. Indeed, we note that the Frobenius pullbacks of $F|K$ are given by

$$\begin{aligned} F_1|K &= K(x,y^2), \\ F_2|K &= K(x,y^4) = K(x)|K, \end{aligned}$$

so in particular the genus g_2 of the rational function field $F_2|K$ is zero, whence $\overline{g}$ is zero too. We show that the zero $\mathfrak{p}$ of x, that is, the only prime $\mathfrak{p}$ such that $v_{\mathfrak{p}}(x) > 0$, is a singular prime of singularity degree 3. To this end, we observe that its restriction $\mathfrak{p}_2$ is a rational prime of $F_2|K = K(x)|K$ with local parameter x, and so that we can compute its singularity degree $\delta(\mathfrak{p})$ by applying the algorithm developed in [BS87] (see Theorem 2.3 and the discussion that follows). Now, since the value $y^2(\mathfrak{p}) = a^{1/2}$ of the function $y^2 \in F_1$ at $\mathfrak{p}$ does not lie in $K_{\mathfrak{p}_2} = K$, the prime $\mathfrak{p}_1$ of $F_1|K$ is inertial over F_2 with residue field $K_{\mathfrak{p}} = K(y^2(\mathfrak{p}))$, and hence we see from Theorem 2.3 that

$$\delta(\mathfrak{p}_1) = 2\delta(\mathfrak{p}_2) + \frac{1}{2} \cdot v_{\mathfrak{p}_2}(d(y^2)^2) = \frac{1}{2} \cdot v_{\mathfrak{p}_2}(x^2 dx) = 1.$$

Similarly, since the value $y(\mathfrak{p}) = a^{1/4}$ of the function $y \in F$ at $\mathfrak{p}$ does not lie in $K_{\mathfrak{p}_1} = K(a^{1/2})$ the prime $\mathfrak{p}$ of $F|K$ is inertial over F_1 with residue field $K_{\mathfrak{p}} = K(y(\mathfrak{p}))$, hence we deduce from Theorem 2.3 that $\mathfrak{p}$ has singularity degree

$$\delta(\mathfrak{p}) = 2\delta(\mathfrak{p}_1) + \frac{1}{2} \cdot v_{\mathfrak{p}_2}(dy^4) = 2 \cdot 1 + 1 = 3.$$

As follows from the genus drop formula (2.4), to conclude that $F|K$ has genus $g = 3$ it remains to verify that there are no singular primes other than $\mathfrak{p}$. To see this we introduce the functions $\breve{x} := x^{-1}$ and $\breve{y} := yx^{-1}$, which satisfy the polynomial relation

$$\breve{y}^4 = \breve{x} + a\breve{x}^4,$$

and we note that $\breve{x}$ has a pole at $\mathfrak{p}$. Since the center $(\breve{x}(\mathfrak{q}), \breve{y}(\mathfrak{q}))$ of every singular prime $\mathfrak{q} \neq \mathfrak{p}$ of $F|K$ is necessarily a singular point of the plane curve defined by the above equation (see [Sal11, Corollary 4.5]), it follows from the Jacobian criterion that no such singular prime exist. Thus $F|K$ has genus $g = 3$, as claimed.

Remark. The method employed to analyze Example 3.1 is a prototype of the procedure we will follow to find singular primes and to compute their singularity degrees in the proofs of the theorems in this chapter.

Example 3.2 ($g = 3$ and $\overline{g} = 1$)**.** Let $F|K = K(x, y)|K$ be the function field in characteristic 2 defined by the equation

$$y^4 + (a + b)y^2 + ab = x^3,$$

where $a, b \in K \setminus K^2$ are two distinct constants. We claim that $F|K$ has genera $g = 3$ and $\overline{g} = 1$, and furthermore that it has two singular primes, each of singularity degree 1.

Indeed, since the first Frobenius pullback $F_1|K = K(x, y^2)|K$ is defined by the polynomial equation in y^2 and x

$$(y^2)^2 + (a + b)y^2 + ab = x^3, \tag{3.1}$$

it is an elliptic function field with discriminant $\Delta = (a + b)^4 \neq 0$, which means that both $F_1|K$ and its extension $\overline{K}F_1|\overline{K}$ have genus 1. [1] Equivalently, $g_1 = g_2 = \cdots = \overline{g} = 1$.

[1]Another way to see this in the language of Section 2.1: since the curve C associated to $F_1|K$ is the plane projective curve over K that in affine coordinates is given by $Y^2 + (a + b)Y + (a + b) = X^3$, the condition $\Delta \neq 0$ means that the extended curve $\overline{C}$, which is defined by the same equation but over $\overline{K}$, is a (smooth) elliptic curve. In other words, C is smooth and has genera $g = \overline{g} = 1$.

By the Jacobian criterion (see [Sal11, Corollary 4.5]), every singular prime $\mathfrak{p}$ of $F|K$ is necessarily a zero of x, i.e., $x(\mathfrak{p}) = 0$, and furthermore $y(\mathfrak{p}) \in \{a^{1/2}, b^{1/2}\}$. We shall see that there are exactly two zeros of x, and that both of them have singularity degree 1. This will then imply that $F|K$ has genus $g = 3$.

Let $\mathfrak{p}$ be a prime such that $x(\mathfrak{p}) = 0$. Then the above equation implies that the value $y^2(\mathfrak{p})$ of the function $y^2 \in F_1$ at $\mathfrak{p}$ belongs to $\{a, b\}$. Since y^2 is a root of the separable polynomial $T^2 + (a + b)T + ab + x^3 \in K(x)[T]$, there is a $K(x)$-automorphism σ of $F_1 = K(x, y^2)$ mapping y^2 to $y^2 + a + b$, and therefore if, say $y^2(\mathfrak{p}) = a$, then there will be another prime $\mathfrak{q}$ with the property that $v_{\mathfrak{q}_1} = v_{\mathfrak{p}_1} \circ \sigma$, i.e., such that $x(\mathfrak{q}) = 0$ and $y^2(\mathfrak{q}) = b$. By the fundamental inequality, this shows that there are exactly two (rational) primes of $F_1|K$ lying over the only rational prime of $K(x)|K$ whose local parameter is the function x. So we conclude that there are two primes $\mathfrak{p}$ and $\mathfrak{q}$ satisfying the properties $x(\mathfrak{p}) = y(\mathfrak{p}) = 0$, $y(\mathfrak{p}) = a^{1/2}$, $y(\mathfrak{q}) = b^{1/2}$, and such that their restrictions $\mathfrak{p}_1$ and $\mathfrak{q}_1$ are rational primes of $F_1|K$ with local parameter x. Thus we can compute their singularity degrees by using the algorithm developed in [BS87].

It remains to prove that both primes $\mathfrak{p}$ and $\mathfrak{q}$ have singularity degree 1. Indeed, as $y(\mathfrak{p}) = a^{1/2}$ does not belong to K the prime $\mathfrak{p}$ is inertial over F_1 with residue field $K_{\mathfrak{p}} = K(y(\mathfrak{p}))$, and hence $\delta(\mathfrak{p}) = \frac{1}{2} v_{\mathfrak{p}_1}(dy^2)$ by Theorem 2.3. Since by differentiating equation (3.1) we obtain $(a + b)dy^2 = x^2 dx$, we conclude that $\mathfrak{p}$ has singularity degree $\delta(\mathfrak{p}) = 1$, as desired. One sees similarly that $\delta(\mathfrak{q}) = 1$.

Example 3.3 ($g = 3$ and $\overline{g} = 2$)**.** The function field $F|K = K(x, y)|K$ given by the polynomial relation

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

where $a \in K \setminus K^2$, has genera $g = 3$ and $\overline{g} = 2$ and a unique singular prime of singularity degree 1 (see Section 5.2). More generally, it can be proved that any function field $F|K = K(x, y)|K$ defined by

$$y^3 = (x^2 + a)(x + b)(x + c),$$

where $a \in K \setminus K^2$ and $b, c \in K$ are distinct, has the same genera $g = 3$, $\overline{g} = 2$.

The examples suggests the existence of a great variety of examples. And one of the objectives of this thesis is to show that this is actually the case. In fact, we can use the genus drop formula (2.4) to divide cases $\overline{g} = 0$ and $\overline{g} = 1$ into subcases depending on the number of singular primes that appear. The resulting division can be seen in Table 3.1. Surprisingly, *all* of these possibilities can occur, as follows from the previous examples and Chapter 5.

$\overline{g}$	Number of singular primes	Singularity degrees
0	1	3
	2	1 and 2
	3	1
1	1	2
	2	1
2	1	1

Table 3.1: Possibilities for singular primes and their singularity degrees

This is a special phenomenon taking place only in characteristic 2. For in characteristic 3 the situation is quite different and not every possibility can occur (cf. [Sal11, Table 1]), while in characteristics 5 and 7 there can only be one singular prime of singularity degree 2 and 3 respectively (see [Stö07, Stö04]). As a result, due to the abundance of examples in characteristic 2, it may be hard to obtain a full characterization, let alone a classification.

In this chapter we shall focus our attention on a special class of non-conservative function fields of genus $g = 3$, those which are *geometrically rational*, that is $\overline{g} = 0$, and which have a unique singular prime. We know from Corollary 2.13 that in this situation the genus g_1 of the Frobenius pullback $F_1|K$ can take two values, namely 0 and 1. So our study of $F|K$ can be naturally divided into two major parts, in accordance with the value of g_1.

3.1 Function fields of genus $g = 3$ and $g_1 = 0$

In this section we specialize the discussion to the case where $g = 3$, $g_1 = 0$ and $p = 2$.

So let $F|K$ be a one-dimensional separable function field of genus $g = 3$ in characteristic 2, whose first Frobenius pullback $F_1|K$ has genus $g_1 = 0$. For simplicity, we shall assume that $F|K$ has a unique singular prime $\mathfrak{p}$ and, furthermore, that $\mathfrak{p}$ is non-decomposed.

By the genus drop formula (2.4), the prime $\mathfrak{p}$ has singularity degree $\delta(\mathfrak{p}) = 3$. By Proposition 2.12, its restriction $\mathfrak{p}_2$ to the second Frobenius pullback $F_2|K$ is then rational, thus making available the algorithm developed in [BS87] (see Theorem 2.3 and the discussion that follows). In obtaining our results, we shall exploit this algorithm together with the requirement $\delta(\mathfrak{p}) = 3$.

We remark that, in general, the assumptions on the prime $\mathfrak{p}$ need not be fullfilled. That is, $\mathfrak{p}$ may not be non-decomposed and, what is more, $\mathfrak{p}$ may not be unique, i.e., there can be more than one singular prime (see Proposition 5.1).

Theorem 3.4. *A one-dimensional separable function field $F|K$ in characteristic $p = 2$ has genera $g = 3$, $g_1 = 0$, $\overline{g} = 0$ and admits a unique singular prime that is non-decomposed, if and only if it can be put into one of the following normal forms*

(i) $y^2 = a_0 + x + a_2x^2 + a_4x^4 + a_6x^6 + a_8x^8$, *where* $a_0, a_2, a_4, a_6 \in K$ *and* $a_8 \in K \setminus K^2$.

(ii) $z^2 = a_0+x+a_2x^2$ *and* $y^2 = b_2x^2+b_3x^3+b_4x^4+z$, *where the constants* $a_0, b_2, b_3, b_4 \in K$ *and* $a_2 \in K \setminus K^2$ *satisfy one of the following relations*

  (a) $b_4^{1/2} \notin K(a_2^{1/2})$;

  (b) $b_2 = b_4 = 0$ *and* $b_3 \neq 0$.

In both cases, the function x has a pole at the singular prime $\mathfrak{p}$ of $F|K$. Moreover, item (i) *occurs if and only if the restricted prime $\mathfrak{p}_1$ of $F_1|K$ is rational.*

In item (ii)*, the prime $\mathfrak{p}$ is inertial (respectively ramified) over F_1 in case* (a) *(respectively in case* (b)*).*

The proof of the theorem will consist in finding some necessary conditions the function field $F|K$ should satisfy (i.e., the normal form), and then proving that they are in fact sufficient (i.e., that any function field defined by the normal form has the desired properties). This will be carried out by showing that $F_n|K$ is rational for some n, and this will then let us study the primes of $F|K$ as the extensions of the primes of $F_n|K$, which are well-known.

Proof. Let $F|K$ be a function field as in the statement of the theorem and let $\mathfrak{p}$ be its only singular prime. Our study of $F|K$ will be divided into two parts, in accordance with the rationality of the restricted prime $\mathfrak{p}_1$ of $F_1|K$. In fact, item (i) will correspond to the case where $\mathfrak{p}_1$ is rational, while item (ii) will correspond to the case where $\mathfrak{p}_1$ is non-rational.

Because the prime $\mathfrak{p}_2$ of $F_2|K$ is rational, we know that $\mathfrak{p}_1$ is non-rational if and only if it is unramified over F_2, or equivalently, it has degree $\deg \mathfrak{p}_1 = 2$. And since $\mathfrak{p}$ is not rational, we also know that $\mathfrak{p}_1$ is rational if and only if $\mathfrak{p}$ is unramified over F_1 and has degree $\deg \mathfrak{p} = 2$.

Assume first that the prime $\mathfrak{p}_1$ is rational, i.e., that $\mathfrak{p}$ is unramified over F_1 and has degree $\deg \mathfrak{p} = 2$. Since the function field $F_1|K$ has genus $g_1 = 0$ and $\mathfrak{p}_1$ is rational, we have that $F_1|K$ is a rational function field, say $F_1|K = K(x)|K$ with $v_{\mathfrak{p}_1}(x) = -1$. It then follows from Riemann's theorem that $\dim H^0(\mathfrak{p}_1^n) = n + 1$, that is,

$$H^0(\mathfrak{p}_1^n) = K \oplus Kx \oplus \cdots \oplus Kx^n \quad \text{for all } n \geq 0. \tag{3.2}$$

Similarly, since the function field $F|K$ has genus $g = 3$ and $\mathfrak{p}$ has degree 2 we have

$$\dim H^0(\mathfrak{p}^n) = 2n - 2 \quad \text{for all } n \geq 3.$$

Thus $\dim H^0(\mathfrak{p}^4) = 6 > \dim H^0(\mathfrak{p}_1^4) = 5$, and so we can find a function $y \in F$ such that

$$H^0(\mathfrak{p}^4) = H^0(\mathfrak{p}_1^4) \oplus Ky = K \oplus Kx \oplus Kx^2 \oplus Kx^3 \oplus Kx^4 \oplus Ky, \tag{3.3}$$

which does not lie in $F_1 = K(x)$ because $F_1 \cap H^0(\mathfrak{p}^4) = H^0(\mathfrak{p}_1^4)$. This means in particular that y is a separating variable of $F|K$, or equivalently $F = F_1(y) = K(x, y)$. And since its square y^2 belongs to $F_1 \cap H^0(\mathfrak{p}^8) = H^0(\mathfrak{p}_1^8)$, there must exist constants $a_i \in K$ such that

$$y^2 = a_0 + a_1 x + \cdots + a_7 x^7 + a_8 x^8.$$

Note that one of the constants a_1, a_3, a_5, a_7 must be non-zero, for the function y is a separating variable and hence x is separable over $K(y)$. Now, in the notation of Proposition 2.5, the fact that $\mathfrak{p}$ is unramified over $F_1 = K(x)$ with singularity degree $\delta(\mathfrak{p}) = 3$, means that the parameters τ, μ satisfy the relation $\mu - \tau - 1 = 6$, i.e., $a_1 \neq 0$, $a_3 = a_5 = a_7 = 0$ and $a_8 \notin K^2$, in which case we may normalize $a_1 = 1$ by substituting x with $a_1 x$ and y with $a_1 y$, respectively. We thus obtain the following normal form of $F|K$

$$y^2 = a_0 + x + a_2 x^2 + a_4 x^4 + a_6 x^6 + a_8 x^8, \quad \text{where } a_8 \notin K^2.$$

We observe that, conversely, this normal form already guarantees that the pole $\mathfrak{p}$ of x is the only singular prime of $F|K$, and, moreover, that $F|K$ has genus $g = 3$. More precisely, since a singular prime satisfies necessarily the Jacobian criterion (see [Sal11, Cor. 4.5, Cor. 4.6]), any function field $F|K = K(x, y)|K$ given by the above relation has at most one singular prime, namely the pole of x, which by the previous considerations is unramified over $F_1 = K(x)$ and has singularity degree 3; this implies in particular that $F|K$ has genera $g = 3$, $g_1 = 0$.

We next treat the second part of the proof. That is, we assume that $\mathfrak{p}_1$ is non-rational, which means that $\mathfrak{p}_1$ is unramified over F_2 and has degree 2. Let $e \in \{1, 2\}$ denote the ramification index of $\mathfrak{p}$ over F_1.

Since the function field $F_2|K$ has genus $g_2 = 0$ and its prime $\mathfrak{p}_2$ is rational, it is in fact a rational function field, say $F_2|K = K(x)|K$ with $v_{\mathfrak{p}_2}(x) = -1$. Then it follows from Riemann's theorem that $\dim H^0(\mathfrak{p}_2^n) = n + 1$, that is,

$$H^0(\mathfrak{p}_2^n) = K \oplus Kx \oplus \cdots \oplus Kx^n \quad \text{for all } n \geq 0. \tag{3.4}$$

Analogously, since the function field $F_1|K$ has genus $g_1 = 0$ and $\mathfrak{p}_1$ has degree 2 we have

$$\dim H^0(\mathfrak{p}_1^n) = 2n + 1 \quad \text{for all } n \geq 0.$$

And since $F|K$ has genus $g = 3$ we also have

$$\dim H^0(\mathfrak{p}^n) = \begin{cases} 4n - 2 & \text{for all } n \geq 2, \quad \text{if } e = 1, \\ 2n - 2 & \text{for all } n \geq 3, \quad \text{if } e = 2. \end{cases}$$

As in the previous part of the proof, these data will enable us to study the function fields $F_1|K$ and $F|K$. We will do this first for $F_1|K$, and then for $F|K$.

As $\dim H^0(\mathfrak{p}_1) = 3 > \dim H^0(\mathfrak{p}_2) = 2$ we can choose a function $z \in F$ such that

$$H^0(\mathfrak{p}_1) = H^0(\mathfrak{p}_2) \oplus Kz = K \oplus Kx \oplus Kz, \tag{3.5}$$

which does not belong to $F_2 = K(x)$ because $F_2 \cap H^0(\mathfrak{p}_1) = H^0(\mathfrak{p}_2)$. This means that z is a separating variable of $F_1|K$, or equivalently $F_1 = F_2(z) = K(x, z)$. Since z^2 lies in $F_2 \cap H^0(\mathfrak{p}_1^2) = H^0(\mathfrak{p}_2^2) = K \oplus Kx \oplus Kx^2$ there are constants $a_0, a_1, a_2 \in K$ such that

$$z^2 = a_0 + a_1 x + a_2 x^2.$$

Because z is a separating variable of $F_1|K$ and therefore x is separable over $K(z)$, the constant a_1 must be non-zero, and so we may normalize $a_1 = 1$ by substituting x with $a_1 x$ and z with $a_1 z$. By Proposition 2.5, the fact that $\mathfrak{p}_1$ is non-rational means that $a_2 \notin K^2$, thus yielding the following normal form of $F_1|K$

$$z^2 = a_0 + x + a_2 x^2, \quad \text{where } a_2 \notin K^2.$$

We observe that this normal form already ensures, by the Jacobian criterion, that every prime of $F_1|K$ is non-singular, i.e., $F_1|K$ has genus $g_1 = 0$, and that the pole $\mathfrak{p}_1$ of x is non-rational (see Proposition 2.5).

We now look at the function field $F|K$. As $\dim H^0(\mathfrak{p}^{2e}) = 6 > \dim H^0(\mathfrak{p}_1^2) = 5$, there is a function y such that

$$H^0(\mathfrak{p}^{2e}) = H^0(\mathfrak{p}_1^2) \oplus Ky = K \oplus Kx \oplus Kx^2 \oplus Kz \oplus Kxz \oplus Ky, \tag{3.6}$$

which lies outside $F_1 = K(x, z)$ because $F_1 \cap H^0(\mathfrak{p}^{2e}) = H^0(\mathfrak{p}_1^2)$. This means in particular that y is a separating variable of $F|K$, that is, $F = F_1(y) = K(x, z, y)$. And since y^2 belongs to $H^0(\mathfrak{p}^{4e}) \cap F_1 = H^0(\mathfrak{p}_1^4) = K \oplus Kx \oplus Kx^2 \oplus Kx^3 \oplus Kx^4 \oplus Kz \oplus Kxz \oplus Kx^2 z \oplus Kx^3 z$, there exist constants $b_i, c_i \in K$ such that

$$y^2 = b_0 + b_1 x + b_2 x^2 + b_3 x^3 + b_4 x^4 + (c_0 + c_1 x + c_2 x^2 + c_3 x^3) z.$$

Observe that at least one of the c_i must be non-zero, for y^2 will be a separating variable of $F_1|K$ and therefore $y^2 \notin F_2 = K(x)$.

We want to rephrase the fact that $\mathfrak{p}$ has singularity degree $\delta(\mathfrak{p}) = 3$ in terms of equations on the constants a_i, b_i, c_i. To do this we introduce the functions $\breve{x} := x^{-1}$, $\breve{z} := zx^{-1}$ and $\breve{y} := yx^{-2}$. Note that $\breve{x}$ is a local parameter at both $\mathfrak{p}_1$ and $\mathfrak{p}_2$, and that $\breve{y}$ and $\breve{z}$ satisfy the equations

$$\begin{aligned}
&\breve{z}^2 = a_2 + \breve{x} + a_0\breve{x}^2,\\
&\breve{y}^2 = b_4 + b_3\breve{x} + b_2\breve{x}^2 + b_1\breve{x}^3 + b_0\breve{x}^4 + (c_3 + c_2\breve{x} + c_1\breve{x}^2 + c_0\breve{x}^3)\breve{z}.
\end{aligned}$$

In particular,

$$\begin{aligned}
&\breve{z}(\mathfrak{p})^2 = a_2 \notin K^2,\\
&\breve{y}(\mathfrak{p})^2 = b_4 + c_3\breve{z}(\mathfrak{p}).
\end{aligned}$$

Now there are two cases we must consider: $\breve{y}(\mathfrak{p}) \notin K_{\mathfrak{p}_1}$ and $\breve{y}(\mathfrak{p}) \in K_{\mathfrak{p}_1}$. The first case will correspond to (a) in the statement of the theorem, while the second case will correspond to (b).

Assume first that $\breve{y}(\mathfrak{p}) \notin K_{\mathfrak{p}_1} = K(\breve{z}(\mathfrak{p}))$, so that $\mathfrak{p}$ is inertial over F_1. By Theorem 2.3, the fact that $\mathfrak{p}$ has singularity degree 3 means that the order of

$$d\breve{y}^4 = (c_3^2 + c_2^2\breve{x}^2 + c_1^2\breve{x}^4 + c_0^2\breve{x}^6)d\breve{x}$$

at $\mathfrak{p}_2$ is equal to 6, that is, $c_3 = c_2 = c_1 = 0$ and $c_0 \neq 0$. Substituting $\breve{x}$, $\breve{z}$ and $\breve{y}$ with $c_0^{-2}\breve{x}$, $c_0^{-1}\breve{z}$ and $c_0^{-3}\breve{y}$ respectively, we may normalize $c_0 = 1$. Thus, replacing $\breve{z}$ with $\breve{z} + b_1 + b_0\breve{x}$ we get the following normal form of $F|K$

$$\begin{aligned}
&z^2 = a_0 + x + a_2x^2, &&\text{where } a_2 \notin K^2,\\
&y^2 = b_2x^2 + b_3x^3 + b_4x^4 + z, &&\text{where } b_4 \notin K^2(a_2).
\end{aligned}$$

We note that, conversely, this normal form guarantees that our function field has the desired properties. Indeed, the relation $y^4 = b_2^2x^4 + b_3^2x^6 + b_4^2x^8 + a_0 + x + a_2x^2$ implies by the Jacobian criterion that any function field $F|K = K(x, z, y)|K$ defined by the above normal form has at most one singular prime, namely the pole $\mathfrak{p}$ of x, which is unramified over $F_2 = K(x)$ and has residue fields $K_\mathfrak{p} = K(a_2^{1/2}, b_4^{1/2})$ and $K_{\mathfrak{p}_1} = K(a_2^{1/2})$; furthermore, it follows from the previous considerations that $\mathfrak{p}$ has singularity degree 3, and therefore that $F|K$ has genus $g = 3$.

Now we examine the second case $\breve{y}(\mathfrak{p}) \in K_{\mathfrak{p}_1} = K(\breve{z}(\mathfrak{p}))$, say $\breve{y}(\mathfrak{p}) = \alpha + \beta\breve{z}(\mathfrak{p})$. Substracting $\alpha + \beta\breve{z}$ from $\breve{y}$ we may assume $\breve{y}(\mathfrak{p}) = 0$, i.e., $b_4 = c_3 = 0$ since $a_2 \notin K^2$.

We claim that $b_3 + c_2\breve{z}(\mathfrak{p}) = 0$ cannot happen. Indeed, assuming the contrary we have $b_3 = c_2 = 0$ as $a_2 \notin K^2$, and so yx lies in $H^0(\mathfrak{p}^{2e})$. Thus we can replace y with $\frac{y}{x}$. Equivalently, we can replace $\breve{y}$ with $\breve{x}\breve{y}$, so that

$$\breve{y}^2 = b_2 + b_1\breve{x} + b_0\breve{x}^2 + (c_1 + c_0\breve{x})\breve{z},$$

where $c_1 + c_0\breve{x} \neq 0$, as we pointed out before. If $\breve{y}(\mathfrak{p}) \notin K_{\mathfrak{p}_1} = K(\breve{z}(\mathfrak{p}))$, then $\mathfrak{p}$ is inertial over F_1 and $\delta(\mathfrak{p}) = 3$ must be equal to $\frac{1}{2}v_{\mathfrak{p}_2}(d\breve{y}^4) = \frac{1}{2}v_{\mathfrak{p}_2}(c_1^2 + c_0^2\breve{x}^2)$ by Theorem 2.3, a contradiction. In the opposite case $\breve{y}(\mathfrak{p}) \in K(\breve{z}(\mathfrak{p}))$ we may normalize $\breve{y}(\mathfrak{p}) = 0$ by substracting from $\breve{y}$ an element of $K + K\breve{z}$, i.e., $b_2 = c_1 = 0$ as $a_2 \notin K^2$, hence we conclude that $\mathfrak{p}$ is ramified over F_1 with local parameter $\breve{y}$ as $v_{\mathfrak{p}_2}(d\breve{y}^4) = 2 < 4$, and therefore $\delta(\mathfrak{p}) = 3$ is equal to $\frac{1}{2}v_{\mathfrak{p}_2}(d\breve{y}^4) = 1$ by Theorem 2.3, a contradiction. This proves the claim.

As $b_3+c_2\breve{z}(\mathfrak{p})$ is non-zero and therefore $v_{\mathfrak{p}}(b_3+c_2\breve{z})=0$, the prime $\mathfrak{p}$ is clearly ramified over F_1 with local parameter $\breve{y}$, hence the condition $\delta(\mathfrak{p})=3$ means that $v_{\mathfrak{p}_2}(d\breve{y}^4)=6$ by Theorem 2.3, that is, $c_2=c_1=0$ and $c_0\neq 0$. As in the preceding case, we may then normalize $c_0=1$ and $b_1=b_0=0$. Replacing x and z with $x+b_2b_3^{-1}$ and $z+b_2^2b_3^{-1}x$ respectively, we may also normalize $b_2=0$. So this yields the following normal form of $F|K$

$$\begin{aligned} z^2 &= a_0+x+a_2x^2, && \text{where } a_2\notin K^2,\\ y^2 &= b_3x^3+z, && \text{where } b_3\neq 0. \end{aligned}$$

Since $y^4=b_3^2x^6+a_0+x+a_2x^2$, this normal form guarantees that the pole $\mathfrak{p}$ of x is the only singular prime of $F|K$ (by the Jacobian criterion), and therefore that $F|K$ has genus $g=3$; moreover, it can also be seen from the normal form that $\mathfrak{p}$ is ramified over F_1 and that $\mathfrak{p}_1$ is unramified over F_2, thus completing the proof of the theorem. □

Theorem 3.4 characterizes the function fields we are interested in. The following result lets us decide when any two of them are isomorphic over (the spectrum of) K.

Theorem 3.5. *No function field from item* (i) *in Theorem 3.4 is isomorphic to a function field from item* (ii). *Moreover,*

(i) *two function fields $F|K$ and $F'|K$ from item* (i) *with parameters a_0,a_2,a_4,a_6,a_8 and a_0',a_2',a_4',a_6',a_8' are isomorphic if and only if there exist constants $c_0,c_1,c_2,c_3,c_4,t,b\in K$ with $t\neq 0$ such that*

$$\begin{aligned} t^{-2}a_0' &= a_0+c_0^2+c_1^2b^2+c_2^2b^4+c_3^2b^6+c_4^2b^8+b^8a_8+b^6a_6+b^4a_4+b^2a_2+b,\\ t^2a_2' &= a_2+c_1^2+c_3^2b^4+b^4a_6,\\ t^6a_4' &= a_4+c_2^2+c_3^2b^2+b^2a_6,\\ t^{10}a_6' &= a_6+c_3^2,\\ t^{14}a_8' &= a_8+c_4^2. \end{aligned}$$

(ii) *two function fields $F|K$ and $F'|K$ from item* (ii) *with parameters a_0,a_2,b_2,b_3,b_4 and a_0',a_2',b_2',b_3',b_4' are isomorphic if and only if there exist constants $r_0,t,t_0,t_1,t_2,t_3,t_4\in K$ with $t\neq 0$ such that*

$$\begin{aligned} t^{14}b_4' &= b_4+t_2^2+t_4^2a_2,\\ t^{10}b_3' &= b_3+t_4^2,\\ t^6b_2' &= b_2+r_0t_4^2+r_0b_3+t_1^2+t_3^2a_2+t_4^2a_0,\\ t^4a_2' &= a_2+r_0^4t_4^4+r_0^4b_3^2+t_3^4,\\ t^{-4}a_0' &= a_0+r_0^8t_2^4+r_0^8t_4^4a_2^2+r_0^8b_4^2+r_0^6t_4^4+r_0^6b_3^2+r_0^4t_1^4+r_0^4t_3^4a_2^2\\ &\quad +r_0^4t_4^4a_0^2+r_0^4b_2^2+r_0^2t_3^4+r_0^2a_2+r_0+t_0^4+t_3^4a_0^2. \end{aligned}$$

Proof. It is clear that a function field from item (i) is not isomorphic to any function field from item (ii).

(i) Let $F|K=K(x,y)$ and $F'|K=K(x',y')|K$ be two function fields as in (i), with parameters a_0,a_2,a_4,a_6,a_8 and a_0',a_2',a_4',a_6',a_8'. Assume there is a K-isomorphism $\sigma:F'\to F$. Because $F_1=K(x)$ and $F_1'=K(x')$ are the only subfields of F and F' such that $F|F_1$ and $F'|F_1'$ are purely inseparable of degree 2, they must be preserved under σ, i.e., σ restricts to an isomorphism $F_1' \xrightarrow{\sim} F_1$. Moreover, the only singular prime $\mathfrak{p}'$ of $F'|K$ must be mapped by σ into the only singular prime $\mathfrak{p}$ of $F|K$, that is, $\mathfrak{p}' = \mathfrak{p} \circ \sigma$, and hence $\mathfrak{p}_1' = \mathfrak{p}_1 \circ \sigma$ as both $\mathfrak{p}'|\mathfrak{p}_1$ and $\mathfrak{p}|\mathfrak{p}_1'$ are unramified. Thus σ restricts to isomorphisms

$$H^0(\mathfrak{p}'^n) \xrightarrow{\sim} H^0(\mathfrak{p}^n), \qquad H^0(\mathfrak{p}_1'^n) \xrightarrow{\sim} H^0(\mathfrak{p}_1^n), \quad \text{for all } n \geq 0.$$

It then follows from (3.2) and (3.3) that the images $\sigma(x')$ and $\sigma(y')$ of x' and y' lie in $H^0(\mathfrak{p}_1)\backslash K$ and $H^0(\mathfrak{p}^4)\backslash H^0(\mathfrak{p}_1^4)$ respectively; equivalently, there are constants $a, b, t, c_0, c_1, c_2, c_3, c_4$ in K with $a, t \neq 0$ such that

$$\begin{aligned}
\sigma(x') &= ax + bt^2, \\
\sigma(y') &= t(c_0 + c_1x + c_2x^2 + c_3x^3 + c_4x^4 + y)
\end{aligned}$$

By applying σ to the equation $y'^2 = a_0' + x' + a_2'x'^2 + a_4'x'^4 + a_6'x'^6 + a_8'x'^8$ and replacing $y^2 = a_0 + x + a_2x^2 + a_4x^4 + a_6x^6 + a_8x^8$ we get a system of six equations involving the constants a, b, c_i, c, a_i, a_i'. We can eliminate a, since one of these equations is $a = t^2$. The remaining five equations are exactly those stated in item (i).

Conversely, if the constants $c_0, c_1, c_2, c_3, c_4, c, b \in K$ with $c \neq 0$ satisfy these relations, then the substitutions

$$x' \mapsto t^2(x + b), \qquad y' \mapsto t(c_0 + c_1x + c_2x^2 + c_3x^3 + c_4x^4 + y)$$

define a K-isomorphism $F' \to F$.

(ii) Let $F|K = K(x, z, y)$ and $F'|K = K(x', z', y')|K$ be two function fields as in (ii), with parameters a_0, a_2, b_2, b_3, b_4 and $a_0', a_2', b_2', b_3', b_4'$. Suppose there exists a K-isomorphism $\sigma : F' \xrightarrow{\sim} F$. Since σ preserves the only singular primes of $F|K$ and $F'|K$ we have $v_{\mathfrak{p}'} = v_{\mathfrak{p}} \circ \sigma$, hence $v_{\mathfrak{p}_1'} = v_{\mathfrak{p}_1} \circ \sigma$ and $v_{\mathfrak{p}_2'} = v_{\mathfrak{p}_2} \circ \sigma$, as the associated ramification indices must coincide. In particular, σ induces isomorphisms $H^0(\mathfrak{p}'^n) \xrightarrow{\sim} H^0(\mathfrak{p}^n)$, $H^0(\mathfrak{p}_1'^n) \xrightarrow{\sim} H^0(\mathfrak{p}_1^n)$ and $H^0(\mathfrak{p}_2'^n) \xrightarrow{\sim} H^0(\mathfrak{p}_2^n)$. Thus we see from (3.4), (3.5) and (3.6) that there exist constants $r, s, t, r_i, s_i, t_i \in K$ with $r, s, t \neq 0$ such that

$$\begin{aligned}
\sigma(x') &= t^4r_0 + rx, \\
\sigma(z') &= t^2s_0 + t^2s_1x + sz, \\
\sigma(y') &= t(t_0 + t_1x + t_2x^2 + t_3z + t_4xz + y).
\end{aligned}$$

By applying σ to the equations $z'^2 = a_0' + x' + a_2'x'^2$ and $y'^2 = z' + b_2'x'^2 + b_3'x'^3 + b_4'x'^4$, and by replacing $z^2 = a_0 + x + a_2x^2$ and $y^2 = z + b_2x^2 + b_3x^3 + b_4x^4$ we obtain a system of nine equations

$$\begin{aligned}
0 &= r^4b_4' + t^2t_2^2 + t^2t_4^2a_2 + t^2b_4, \\
0 &= r^3b_3' + t^2t_4^2 + t^2b_3, \\
0 &= r^2b_2' + t^4r^2r_0b_3' + t^2t_1^2 + t^2t_3^2a_2 + t^2t_4^2a_0 + t^2b_2, \\
0 &= r^2a_2' + t^4s_1^2 + s^2a_2, \\
0 &= a_0' + t^8r_0^2a_2' + t^4r_0 + t^4s_0^2 + s^2a_0, \\
0 &= r + s^2, \\
0 &= s + t^2, \\
0 &= t^2s_0 + t^{16}r_0^4b_4' + t^{12}r_0^3b_3' + t^8r_0^2b_2' + t^2t_0^2 + t^2t_3^2a_0, \\
0 &= t^2s_1 + t^8rr_0^2b_3' + t^2t_3^2.
\end{aligned}$$

We can view the first five equations as a system of equations with coefficients in K and indeterminates in F'. We can clearly resolve it, since $r \neq 0$. That is, we obtain the parameters a'_i, b'_i of the function field $F'|K$ explicitly in terms of the parameters a_i, b_i of the function field $F|K$ and the constants r_0, r, s_i, s, t_i, t of the automorphism σ. By eliminating r, s, s_0, s_1, we obtain the relations in the statement of the theorem.

Conversely, if the constants $r_0, t, t_0, t_1, t_2, t_3, t_4 \in K$ satisfy these relations and $t \neq 0$, then the substitutions

$$x' \mapsto t^4(r_0 + x), \qquad z' \mapsto t^2(s_0 + s_1 x + z), \qquad y' \mapsto t(t_0 + t_1 x + t_2 x^2 + t_3 z + t_4 xz + y),$$

where $s_0 := r_0^4 t_2^2 + r_0^4 t_4^2 a_2 + r_0^4 b_4 + r_0^2 t_1^2 + r_0^2 t_3^2 a_2 + r_0^2 t_4^2 a_0 + r_0^2 b_2 + t_0^2 + t_3^2 a_0$ and $s_1 := r_0^2 t_4^2 + r_0^2 b_3 + t_3^2$, define a K-isomorphism $F' \to F$. $\square$

We can specialize Theorem 3.5 to subcase (b) of Theorem 3.4 (ii).

Corollary 3.6. *Suppose that $F|K$ is a function field from Theorem 3.4* (ii)*, subcase* (b)*, with parameters a_0, a_2, b_3. Another such function field $F'|K$ with parameters a'_0, a'_2, b'_3 is isomorphic to $F|K$ if and only if there exist constants $t, t_0, t_1, t_3 \in K$ with $t \neq 0$ such that*

$$\begin{aligned}
t^{10} b'_3 &= b_3, \\
t^4 a'_2 &= a_2 + r_0^4 b_3^2 + t_3^4, \\
t^{-4} a'_0 &= a_0 + r_0^6 b_3^2 + r_0^4 t_1^4 + r_0^4 t_3^4 a_2^2 + r_0^2 t_3^4 + r_0^2 a_2 + r_0 + t_0^4 + t_3^4 a_0^2,
\end{aligned}$$

where $r_0 := b_3^{-1}(t_1^2 + t_3^2 a_2)$. In particular, the class $b_3 \mod (K^*)^{10}$ is an invariant of the function field $F|K$.

The proof of Theorem 3.5 lets us discuss the group $\mathrm{Aut}(F|K)$ of automorphisms of the function fields $F|K$ in Theorem 3.4. Suppose first that $F|K$ has a normal form as in Theorem 3.4 (i), with constants a_0, a_2, a_4, a_6, a_8. Then any automorphism of $F|K$ is given by the substitutions

$$x \mapsto t^2(x + b), \qquad y \mapsto t(c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4 + y),$$

where the constants $b, c_0, c_1, c_2, c_3, c_4 \in K$ and $t \in K \setminus \{0\}$ satisfy the relations

$$\begin{aligned}
t^{-2} a_0 &= a_0 + c_0^2 + c_1^2 b^2 + c_2^2 b^4 + c_3^2 b^6 + c_4^2 b^8 + b^8 a_8 + b^6 a_6 + b^4 a_4 + b^2 a_2 + b, \\
t^2 a_2 &= a_2 + c_1^2 + c_3^2 b^4 + b^4 a_6, \\
t^6 a_4 &= a_4 + c_2^2 + c_3^2 b^2 + b^2 a_6, \\
t^{10} a_6 &= a_6 + c_3^2, \\
t^{14} a_8 &= a_8 + c_4^2.
\end{aligned}$$

Note that $c_4 = 0$ since $a_8 \notin K^2$, and thus $t^7 = 1$. Therefore, the automorphisms of $F|K$ are given by the substitutions

$$x \mapsto t^2(x + b), \qquad y \mapsto t(c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4 + y),$$

where $t, b, c_0, c_1, c_2, c_3 \in K$, $t^7 = 1$ and

$$\begin{aligned}
t^{-2} a_0 &= a_0 + c_0^2 + c_1^2 b^2 + c_2^2 b^4 + c_3^2 b^6 + b^8 a_8 + b^6 a_6 + b^4 a_4 + b^2 a_2 + b, \\
t^2 a_2 &= a_2 + c_1^2 + c_3^2 b^4 + b^4 a_6, \\
t^{-1} a_4 &= a_4 + c_2^2 + c_3^2 b^2 + b^2 a_6, \\
t^3 a_6 &= a_6 + c_3^2.
\end{aligned}$$

Assume next that $F|K$ has a normal form as in item (ii), with constants a_0, a_2, b_2, b_3, b_4. An automorphism of $F|K$ is defined by the substitutions

$$x \mapsto t^4(r_0 + x), \qquad y \mapsto t(t_0 + t_1 x + t_2 x^2 + t_3 z + t_4 xz + y),$$

where the constants $r_0, t, t_0, t_1, t_2, t_3, t_4 \in K$ satisfy the conditions $t \neq 0$ and

$$\begin{aligned}
t^{14} b_4 &= b_4 + t_2^2 + t_4^2 a_2, \\
t^{10} b_3 &= b_3 + t_4^2, \\
t^6 b_2 &= b_2 + r_0 t_4^2 + r_0 b_3 + t_1^2 + t_3^2 a_2 + t_4^2 a_0, \\
t^4 a_2 &= a_2 + r_0^4 t_4^4 + r_0^4 b_3^2 + t_3^4, \\
t^{-4} a_0 &= a_0 + r_0^8 t_2^4 + r_0^8 t_4^4 a_2^2 + r_0^8 b_4^2 + r_0^6 t_4^4 + r_0^6 b_3^2 + r_0^4 t_1^4 + r_0^4 t_3^4 a_2^2, \\
&\quad + r_0^4 t_4^4 a_0^2 + r_0^4 b_2^2 + r_0^2 t_3^4 + r_0^2 a_2 + r_0 + t_0^4 + t_3^4 a_0^2.
\end{aligned}$$

Note that $t^4 + 1 = 0$ since $a_2 \notin K^2$, whence $t = 1$. Then $t_4 = 0$, $t_2 = 0$, $r_0 b_3 = t_1^2 + t_3^2 a_2$, $r_0^2 b_3 = t_3^2$ and $r_0^8 b_4^2 + r_0^6 b_3^2 + r_0^4 t_1^4 + r_0^4 t_3^4 a_2^2 + r_0^4 b_2^2 + r_0^2 t_3^4 + r_0^2 a_2 + r_0 + t_0^4 + t_3^4 a_0^2 = 0$. Thus the group $\mathrm{Aut}(F|K)$ of automorphisms of $F|K$ are given by the substitutions

$$x \mapsto r_0 + x, \qquad y \mapsto t_0 + t_1 x + t_3 z + y,$$

where the constants $r_0, t_0, t_1, t_3 \in K$ satisfy the requirements $r_0 b_3 = t_1^2 + t_3^2 a_2$, $r_0^2 b_3 = t_3^2$ and $t_0^4 = r_0^8 b_4^2 + r_0^4 b_2^2 + r_0^2 t_3^4 + r_0^2 a_2 + r_0 + t_3^4 a_0^2$.

To finish this discussion, let us consider some special subcases. If $b_3 \notin K^2$, then $\mathrm{Aut}(F|K)$ is trivial because $r_0 = 0$, and so $t_0 = t_1 = t_3 = 0$. If $b_2 = b_4 = 0$ and $b_3 \neq 0$, then $\mathrm{Aut}(F|K)$ is given by

$$x \mapsto r_0 + x, \qquad y \mapsto t_0 + t_1 x + t_3 z + y,$$

where the constants $r_0, t_0, t_1, t_3 \in K$ satisfy the conditions $r_0 = b_3^{-1}(t_1^2 + t_3^2 a_2)$, $r_0^2 b_3 = t_3^2$ and $t_0^4 = r_0^2 t_3^4 + r_0^2 a_2 + r_0 + t_3^4 a_0^2$.

3.2 Function fields of genus $g = 3$, $g_1 = 1$ and $\overline{g} = 0$

In this section we discuss the situation where $g = 3$, $g_1 = 1$, $\overline{g} = 0$, and $p = 2$.

Let $F|K$ be a one-dimensional separable function field of genus $g = 3$ in characteristic 2. Assume that $F|K$ is geometrically rational, i.e., $\overline{g} = 0$, and that its Frobenius pullback $F_1|K$ has genus $g_1 = 1$.

The setting here is quite similar to that of Section 3.1. That is to say, there is a unique singular prime, say $\mathfrak{p}$, and this singular prime is non-decomposed. However, here the uniqueness and non-decomposedness of $\mathfrak{p}$ will no longer be *assumptions* but genuine properties of the function field $F|K$ (see Corollaries 2.13 and 2.9).

Since the singular prime $\mathfrak{p}$ is non-decomposed and its restriction $\mathfrak{p}_1$ to $F_1|K$ has singularity degree $\delta(\mathfrak{p}_1) = 1$, the restricted prime $\mathfrak{p}_3$ of $F_3|K$ is rational (see Proposition 2.12). Thus the prime $\mathfrak{p}_2$ of $F_2|K$ is non-rational if and only if it is unramified over F_3, or equivalently, if it has degree $\deg \mathfrak{p}_2 = 2$.

We shall divide our study of $F|K$ into two parts, according to the rationality of $\mathfrak{p}_2$.

3.2.1 The case where $\mathfrak{p}_2$ is rational

Theorem 3.7. *A one-dimensional separable function field $F|K$ in characteristic $p = 2$ has genera $g = 3$, $g_1 = 1$, $\overline{g} = 0$ and the restriction $\mathfrak{p}_2$ of its only singular prime $\mathfrak{p}$ to $F_2|K$ is rational, if and only if, $F|K$ can be put into one of the following normal forms*

(i) $y^4 = a_0 + x + a_2x^2 + a_4x^4$, *where* $a_0, a_2 \in K$ *and* $a_4 \in K \setminus K^2$*;*

(ii) $z^2 = c(x)A(x)$ *and* $y^2 = c(x)(B(x) + z)$, *where the polynomials* $c(x)$, $A(x)$ *and* $B(x)$ *are given by*

$$\begin{aligned} c(x) &= c_0 + c_1x + x^2, \\ A(x) &= (c_0A_2 + c_1^{-1}) + c_1A_2x + A_2x^2, \\ B(x) &= B_0 + B_1x, \end{aligned}$$

and the constants $c_0, c_1, A_2, B_0, B_1 \in K$ *satisfy the conditions* $c_1 \neq 0$ *and* $A_2 \notin K^2$*.*

In both cases, the function x has a pole at the singular prime $\mathfrak{p}$ of $F|K$, which is unramified over $F_2 = K(x)$. Moreover, item (i) *occurs if and only if the divisor $\mathfrak{p}$ is canonical.*

As in the proof of Theorem 3.4, we will find the normal forms of $F|K$ and then show they guarantee that $F|K$ has the desired properties.

Proof. Let $F|K$ be a function field as in the statement of the theorem and let $\mathfrak{p}$ be its only singular prime. By assumption, we know that the prime $\mathfrak{p}_2$ of $F_2|K$ is rational. In particular, the prime $\mathfrak{p}_1$ has degree 2. Let $e \in \{1, 2\}$ denote the ramification index of $\mathfrak{p}$ over F_1.

Since the function field $F_2|K$ has genus $g_2 = 0$ and $\mathfrak{p}_2$ is rational, we see that $F_2|K$ is rational, say $F_2|K = K(x)|K$ with $v_{\mathfrak{p}_2}(x) = -1$. Then it follows from Riemann's theorem that $\dim H^0(\mathfrak{p}_2^n) = n + 1$, that is,

$$H^0(\mathfrak{p}_2^n) = K \oplus Kx \oplus \cdots \oplus Kx^n \quad \text{for all } n \geq 0. \tag{3.7}$$

Analogously, since the function field $F_1|K$ has genus $g_1 = 1$ and $\mathfrak{p}_1$ has degree 2 we deduce that

$$\dim H^0(\mathfrak{p}_1^n) = 2n \quad \text{for all } n \geq 1.$$

And since $F|K$ has genus $g = 3$ we also deduce that

$$\dim H^0(\mathfrak{p}^n) = \begin{cases} 4n - 2 & \text{for all } n \geq 2, \quad \text{if } e = 1, \\ 2n - 2 & \text{for all } n \geq 3, \quad \text{if } e = 2. \end{cases}$$

As $\dim H^0(\mathfrak{p}_1^2) = 4 > \dim H^0(\mathfrak{p}_2^2) = 3$, we can choose a function $z \in F$ such that

$$H^0(\mathfrak{p}_1^2) = H^0(\mathfrak{p}_2^2) \oplus Kz = K \oplus Kx \oplus Kx^2 \oplus Kz, \tag{3.8}$$

which lies outside $F_2 = K(x)$ because $F_2 \cap H^0(\mathfrak{p}_1^2) = H^0(\mathfrak{p}_2^2)$. This means that z is a separating variable of $F_1|K$, or equivalently, $F_1 = F_2(x) = K(x, z)$. Since z^2 belongs to $H^0(\mathfrak{p}_1^4) \cap F_2 = H^0(\mathfrak{p}_2^4) = K \oplus Kx \oplus Kx^2 \oplus Kx^3 \oplus Kx^4$, there exist constants a_i such that

$$z^2 = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4.$$

Notice that one of the constants a_1, a_3 must be non-zero, for the function x is separable over $K(z)$. Now, by Proposition 2.5, the fact that the prime $\mathfrak{p}_1$ is non-rational and has singularity degree $\delta(\mathfrak{p}_1) = 1$ means that $a_3 = 0$, $a_1 \neq 0$ and $a_4 \notin K^2$, in which case we may normalize $a_1 = 1$ by substituting x with $a_1 x$ and z with $a_1 z$, respectively. This yields the following normal form of $F_1|K$

$$z^2 = a_0 + x + a_2x^2 + a_4x^4, \quad \text{where } a_4 \notin K^2.$$

We stress that by the Jacobian criterion this normal form already ensures that the pole of x is the only singular prime of $F_1|K$, and therefore that $F_1|K$ has genus $g_1 = 1$.

In order to obtain a normal form of the function field $F|K$, we observe that the divisor $\mathfrak{p}^e$ has degree $4 = 2g - 2$ and that its space of global sections $H^0(\mathfrak{p}^e)$ contains the 2-dimensional vector space $H^0(\mathfrak{p}_1) = K \oplus Kx$. Since $g = 3$, this means that $\mathfrak{p}^e$ is canonical if and only if $H^0(\mathfrak{p}_1)$ is contained properly in $H^0(\mathfrak{p}^e)$. We shall examine each case separately.

(i) Assume first that the divisor $\mathfrak{p}^e$ is canonical. We can then pick a function y such that

$$H^0(\mathfrak{p}^e) = H^0(\mathfrak{p}_1) \oplus Ky = K \oplus Kx \oplus Ky,$$

which does not belong to F_1 because $F_1 \cap H^0(\mathfrak{p}^e) = H^0(\mathfrak{p}_1)$. This means that y is a separating variable of $F|K$, i.e., $F = F_1(y)$. It follows in particular that its square $z := y^2$ lies in $F_1 \cap H^0(\mathfrak{p}^{2e}) = H^0(\mathfrak{p}_1^2)$, but not in F_2, and hence not in $H^0(\mathfrak{p}_2^2)$, i.e.,

$$H^0(\mathfrak{p}_1^2) = H^0(\mathfrak{p}_2^2) \oplus Kz = K \oplus Kx \oplus Kx^2 \oplus Kz.$$

Therefore, by proceeding as we did when finding a normal form of $F_1|K$ we obtain the following normal form of $F|K$

$$y^4 = a_0 + x + a_2x^2 + a_4x^4, \quad \text{where } a_4 \notin K^2.$$

Since the residue fields of $\mathfrak{p}$ and $\mathfrak{p}_1$ are $K(a_4^{1/4})$ and $K(a_4^{1/2})$ respectively, one sees in particular that the prime $\mathfrak{p}$ is unramified over $F_1 = K(x, z)$, that is, $e = 1$.

We claim that this normal form ensures that our function field has the desired properties. Indeed, any function field $F|K = K(x, y)|K$ given by the above relation has at most one singular prime by the Jacobian criterion, namely the pole $\mathfrak{p}$ of x, which is unramified over $F_2 = K(x)$ and has residue fields $K_\mathfrak{p} = K(a_4^{1/4})$ and $K_{\mathfrak{p}_1} = K(a_4^{1/2})$. Moreover, $F|K$ must have genera $g = 3$, $g_1 = 1$, since $\mathfrak{p}_1$ and $\mathfrak{p}$ have singularity degrees $\delta(\mathfrak{p}_1) = \frac{1}{2}v_{\mathfrak{p}_2}\big(d\big(\frac{y^2}{x^2}\big)^2\big) = 1$ and $\delta(\mathfrak{p}) = 2\delta(\mathfrak{p}_1) + \frac{1}{2}v_{\mathfrak{p}_2}\big(d(\frac{y}{x})^4\big) = 3$ by Theorem 2.3. Finally, the function $y^4 = a_0 + x + a_2x^2 + a_4x^4$ clearly belongs to $H^0(\mathfrak{p}_2^4) \subseteq H^0(\mathfrak{p}^4)$ and hence $y \in H^0(\mathfrak{p})$, that is,

$$H^0(\mathfrak{p}) = K \oplus Kx \oplus Ky. \tag{3.9}$$

This shows that the divisor $\mathfrak{p}$ is canonical, thus completing the proof of the claim.

(ii) We now assume that $\mathfrak{p}^e$ is not canonical, that is, $H^0(\mathfrak{p}^e) = H^0(\mathfrak{p}_1) = K \oplus Kx$. We recall that $F_2 = K(x)$, $v_{\mathfrak{p}_2}(x) = -1$ and $F_1 = K(x, z)$, where

$$z^2 = a_0 + x + a_2x^2 + a_4x^4 \quad \text{and} \quad a_4 \notin K^2.$$

As $\dim H^0(\mathfrak{p}^{2e}) = 6 > \dim H^0(\mathfrak{p}_1^2) = 4$ there is an element $y \in H^0(\mathfrak{p}^{2e}) \setminus H^0(\mathfrak{p}_1^2)$, which does not belong to F_1 because $F_1 \cap H^0(\mathfrak{p}^{2e}) = H^0(\mathfrak{p}_1^2)$. In particular, y is a separating variable of $F|K$, or equivalently $F = F_1(y) = K(x, z, y)$. And since y^2 lies in $H^0(\mathfrak{p}^{4e}) \cap F_1 = H^0(\mathfrak{p}_1^4)$, there exist constants b_i and c_i such that

$$y^2 = b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4 + (c_0 + c_1x + c_2x^2)z.$$

As in the proof of Theorem 3.4 we observe that $c_0+c_1x+c_2x^2 \neq 0$, since y^2 is a separating variable of $F_1|K$ and hence $y^2 \notin F_2 = K(x)$.

In order to study the singular prime $\mathfrak{p}$ we introduce the functions $\breve{x} := x^{-1}$, $\breve{z} := zx^{-2}$ and $\breve{y} := yx^{-2}$. Note that $\breve{x}$ is a local parameter at both $\mathfrak{p}_1$ and $\mathfrak{p}_2$, and that $\breve{z}$ and $\breve{y}$ satisfy the relations

$$\begin{aligned}
\breve{z}^2 &= a_4 + a_2\breve{x}^2 + \breve{x}^3 + a_0\breve{x}^4, \\
\breve{y}^2 &= b_4 + b_3\breve{x} + b_2\breve{x}^2 + b_1\breve{x}^3 + b_0\breve{x}^4 + (c_2 + c_1\breve{x} + c_0\breve{x}^2)\breve{z}.
\end{aligned}$$

In particular,

$$\begin{aligned}
\breve{z}(\mathfrak{p})^2 &= a_4 \notin K^2, \\
\breve{y}(\mathfrak{p})^2 &= b_4 + c_2\breve{z}(\mathfrak{p}).
\end{aligned}$$

We claim that $\breve{y}(\mathfrak{p})$ does not belong to $K_{\mathfrak{p}_1} = K(\breve{z}(\mathfrak{p}))$. Indeed, assuming the contrary, say $\breve{y}(\mathfrak{p}) = \alpha + \beta\breve{z}(\mathfrak{p})$, by substracting $\alpha + \beta\breve{z}$ from $\breve{y}$ we may suppose that $\breve{y}(\mathfrak{p}) = 0$, i.e., $b_4 = c_2 = 0$ as $a_4 \notin K^2$. If $b_3 + c_1\breve{z}(\mathfrak{p}) \neq 0$, then $v_{\mathfrak{p}}(b_3 + c_1\breve{z}) = 0$ and $\mathfrak{p}$ is clearly ramified over F_1 with local parameter $\breve{y}$, hence $\delta(\mathfrak{p}) = 3$ must be equal to $2\delta(\mathfrak{p}_1) + \frac{1}{2}v_{\mathfrak{p}_2}(d\breve{y}^4) = 2 + \frac{1}{2}v_{\mathfrak{p}_2}(c_1^2\breve{x}^4 + c_0^2\breve{x}^6)$ by Theorem 2.3, a contradiction. In the opposite case we have $b_3 = c_1 = 0$ as $a_4 \notin K^2$, whence $y^2 = b_0 + b_1x + b_2x^2 + c_0z$ belongs to $H^0(\mathfrak{p}_1^2) \subseteq H^0(\mathfrak{p}^{2e})$ and therefore $y \in H^0(\mathfrak{p}^e) \setminus H^0(\mathfrak{p}_1)$, which is in contradiction to $\mathfrak{p}^e$ not being canonical. This proves the claim.

Now we can rephrase the fact that $\mathfrak{p}$ has singularity degree $\delta(\mathfrak{p}) = 3$ in terms of equations on the constants a_i, b_i, c_i. Indeed, by Theorem 2.3 the condition $\delta(\mathfrak{p}) = 3$ means that $v_{\mathfrak{p}_2}(d\breve{y}^4) = 2$, i.e., $c_2 \neq 0$, in which case we may normalize $c_2 = 1$ by substituting x, y, z with c_2^2x, c_2^3y, c_2z respectively. This yields the following normal form of $F|K$

$$\begin{aligned}
z^2 &= a(x) = a_0 + x + a_2x^2 + a_4x^4, \\
y^2 &= b(x) + c(x)z = b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4 + (c_0 + c_1x + x^2)z,
\end{aligned}$$

where $a_4 \notin K^2$. Since the residue fields of $\mathfrak{p}$ and $\mathfrak{p}_1$ are $K(b_4^{1/2} + a_4^{1/4})$ and $K(a_4^{1/2})$ respectively, one sees in particular that the prime $\mathfrak{p}$ is unramified over $F_1 = K(x, z)$, that is, $e = 1$.

We emphasize that this is not yet the normal form we search for. Indeed, we have only analyzed the condition $\delta(\mathfrak{p}) = 3$, and it remains to study the requirement that $F|K$ has genus 3. More precisely, the above equations ensure that in any function field $F|K = K(x, z, y)|K$ defined by them, the pole $\mathfrak{p}$ of x is unramified over $F_2 = K(x)$ and has the desired singularity degrees, i.e., $\delta(\mathfrak{p}_1) = 1$ and $\delta(\mathfrak{p}) = 3$, but we don't know whether they ensure that $F|K$ has genus 3 (though we know already that $F_1|K$ has genus $g_1 = 1$).

By the Jacobian criterion and the genus drop formula (2.4), the fact that $F|K$ has genus $g = 3$ means that the zeros of the function $\frac{dy^4}{dx} = c_0^2 + c_1^2x^2 + x^4$ are non-singular primes, i.e., the zeros of

$$c(x) = c_0 + c_1x + x^2$$

are non-singular primes. We therefore need to transform this condition into equations on the constants a_i, b_i, c_i.

We claim that $c_1 \neq 0$. Indeed, we will verify that the vanishing of c_1 leads to a contradiction. Suppose initially that the root $r := c_0^{1/2}$ of the polynomial $c(x)$ belongs to K. By our hypothesis, the zero $\mathfrak{q}$ of the function $x+r$ is a non-singular prime, i.e., $\delta(\mathfrak{q}) = 0$. Replacing x with $x+r$ we may assume that $c_0 = 0$, i.e., that x is a local parameter at the rational prime $\mathfrak{q}_2$ of $F_2|K = K(x)|K$. As is clear from Proposition 2.5, this implies that the prime $\mathfrak{q}_1$ is rational (and ramified over F_2) if and only if $z(\mathfrak{q}) = a_0^{1/2}$ belongs to K. It follows in particular that $K_{\mathfrak{q}_1} = K(z(\mathfrak{q}))$, and therefore $y(\mathfrak{q})$ lies necessarily in $K(z(\mathfrak{q}))$ by Theorem 2.3, for $\delta(\mathfrak{q}) = 0$ and $\frac{1}{2}v_{\mathfrak{q}_2}(dy^4) = 2$ are different. Substracting from y an element of $K + Kz$ we may then normalize $y(\mathfrak{q}) = 0$, i.e., $b_0 = 0$.

When $\mathfrak{q}_1$ is not rational, i.e., $z(\mathfrak{q}) = a_0^{1/2} \notin K$, one has $b_1 = 0$ (otherwise $\mathfrak{q}$ is ramified over F_1 with local parameter y and $\delta(\mathfrak{q}) = \frac{1}{2}v_{\mathfrak{q}}(dy^4) = 2$), and therefore the function $\left(\frac{y}{x}\right)^2 = b_2 + b_3x + b_4x^2 + z$ belongs to $H^0(\mathfrak{p}_1^2) \subseteq H^0(\mathfrak{p}^2)$, i.e., $\frac{y}{x} \in H^0(\mathfrak{p}) \setminus H^0(\mathfrak{p}_1)$, a contradiction because $\mathfrak{p}$ is not canonical by assumption. Hence $\mathfrak{q}_1$ is rational, that is, $a_0^{1/2} \in K$. By substracting $a_0^{1/2}$ from z we can then suppose that $a_0 = 0$, and so that z is a local parameter at $\mathfrak{q}_1$. From the relation $z^2 = x + a_2x^2 + a_4x^4$ we obtain x as a power series in z

$$x = z^2 + a_2z^4 + (a_4 + a_2^3)z^8 + \big(a_4a_2^4 + a_2(a_4^2 + a_2^6)\big)z^{16} + \cdots,$$

and hence y^2 as a power series in z

$$y^2 = b_1z^2 + (b_1a_2 + b_2)z^4 + z^5 + \cdots.$$

Since $\delta(\mathfrak{q}) = 0$, it follows from Proposition 2.5 that $b_1 \in K^2$, and then by replacing y with $y + b_1^{1/2}z$ we may normalize $b_1 = 0$. As before, this implies the contradiction $\frac{y}{x} \in H^0(\mathfrak{p}) \setminus H^0(\mathfrak{p}_1)$, so we conclude that the root $c_0^{1/2}$ of the polynomial $c(x)$ does not belong to K.

Let $\mathfrak{q}$ denote the zero of the function $\tau := c(x) = c_0 + x^2 \in F$. By assumption, we know that $\mathfrak{q}$ is a non-singular prime, i.e., $\delta(\mathfrak{q}) = 0$. Moreover, it is clear that τ is a local parameter at the rational prime $\mathfrak{q}_3$ of $F_3|K = K(\tau)|K$, and that $\mathfrak{q}_2$ is unramified over F_3. Since $z(\mathfrak{q}) \notin K_{\mathfrak{q}_2} = K(x(\mathfrak{q}))$ as $a(c_0^{1/2}) \notin K$ and $K^2(c_0) \subseteq K$, the prime $\mathfrak{q}_1$ is unramified over F_2. Now, if $y(\mathfrak{q}) \notin K_{\mathfrak{q}_1} = K(x(\mathfrak{q}), z(\mathfrak{q}))$, then $\mathfrak{q}$ is inertial over F_1 and $\delta(\mathfrak{q}) = \frac{1}{2}v_{\mathfrak{q}_3}(dy^8) = \frac{1}{2}v_{\mathfrak{q}_3}(\tau^4dz^4) = 2$ by Theorem 2.3, a contradiction. In the opposite case, say $w(\mathfrak{q}) = 0$ for some w in $y + K + Kx + Kz + Kxz$, the prime $\mathfrak{q}$ is ramified over F_1 with local parameter w because

$$v_{\mathfrak{q}_3}(dw^8) = v_{\mathfrak{q}_3}(dy^8) = v_{\mathfrak{q}_3}(\tau^4dz^4) = 4 < 8,$$

and therefore $\delta(\mathfrak{q}) = \frac{1}{2}v_{\mathfrak{q}_3}(dw^8) = 2$, a contradiction. This shows that c_1 is necessarily non-zero.

We now proceed to translate the condition $g = 3$ in terms of the roots of the quadratic polynomial

$$c(x) = c_0 + c_1x + x^2.$$

For simplicity, we initially suppose that K is separably closed, so that both the roots of $c(x)$ belong to K. Let $r \in K$ be one of these roots and let $\mathfrak{q}$ be the zero of the function $x + r$. We wish to see when $\mathfrak{q}$ is non-singular, i.e., when $\delta(\mathfrak{q}) = 0$ occurs. We claim that in fact $\delta(\mathfrak{q}) = 0$ if and only if $z(\mathfrak{q}), y(\mathfrak{q}) \in K$. Since $x(\mathfrak{q}) = r \in K$, to see this one may suppose $x(\mathfrak{q}) = 0$, that is, $c_0 = 0$ and x is a local parameter at the rational prime $\mathfrak{q}_2$ of $F_2|K = K(x)|K$. Since

$$v_{\mathfrak{q}_2}(dy^4) = v_{\mathfrak{q}_2}(c_1^2 x^2 + x^4) = 2,$$

one sees from Theorem 2.3 that $y(\mathfrak{q}) \in K_{\mathfrak{q}_1}$ whenever $\delta(\mathfrak{q}) = 0$. Assuming that $z(\mathfrak{q}) \notin K$, the prime $\mathfrak{q}_1$ is unramified over F_2 with residue field $K_{\mathfrak{q}_1} = K(z(\mathfrak{q}))$, and if we suppose $\delta(\mathfrak{q}) = 0$ then $y(\mathfrak{q}) \in K_{\mathfrak{q}_1}$ means that we may normalize $y(\mathfrak{q}) = 0$, so that $\mathfrak{q}$ is ramified over F_1 with local parameter y because

$$v_{\mathfrak{q}_2}(dy^4) = 2 < 4,$$

and therefore $\delta(\mathfrak{q}) = \frac{1}{2} v_{\mathfrak{q}_2}(dy^4) = 1$, a contradiction. Thus the condition $\delta(\mathfrak{q}) = 0$ implies that $z(\mathfrak{q}) \in K$. So in order to prove the claim we may assume that $z(\mathfrak{q}) = 0$, i.e., $a_0 = 0$, in which case $\mathfrak{q}_1$ is ramified (and therefore rational) over F_2 with local parameter z. Since $v_{\mathfrak{q}_1}(dy^2) = v_{\mathfrak{q}_1}((c_1 x + x^2)dz) = 2$ as $dx = dz^2 = 0$ in $F_1|K$, it follows from Proposition 2.5 that $\delta(\mathfrak{q}) = 0$ if and only if $y(\mathfrak{q}) \in K$, thus proving the claim.

Therefore, when K is separably closed the following holds

$$g = 3 \text{ if and only if } a(r), a(s), b(r), b(s) \in K^2,$$

where $r, s \in K$ denote the roots of the quadratic polynomial $c(x)$. We thus conclude that in the general case, i.e., when K is not separably closed, one has

$$g = 3 \text{ if and only if } a(r), a(s), b(r), b(s) \in L^2,$$

where L denotes the separable closure of K and $r, s \in L$ denote the roots of $c(x)$.

We note that at this point that we can normalize $b_4 = 0$ by replacing z with $z + b_4 x^2$, and that the above conditions hold true also with the new normal form. Since these conditions are given in terms of $a(r)$, $a(s)$, $b(r)$ and $b(s)$, it is not evident how to obtain new normalizations out of them. Therefore, we need to rewrite them in a suitable manner, and we will achieve this by using symmetric polynomials. To this end put

$$q := c_1 = r + s \in K, \qquad t := c_0 = rs \in K.$$

Clearly, the four symmetric polynomial expressions

$$\begin{aligned}
a(r) + a(s) &= q + a_2 q^2 + a_4 q^4, \\
r^2 a(r) + s^2 a(s) &= a_0 q^2 + (q^3 + qt) + a_2 q^4 + a_4 (q^6 + q^2 t^2), \\
b(r) + b(s) &= b_1 q + b_2 q^2 + b_3 (q^3 + qt), \\
r^2 b(r) + s^2 b(s) &= b_0 q^2 + b_1 (q^3 + qt) + b_2 q^4 + b_3 (q^5 + t(q^3 + qt)),
\end{aligned}$$

lie in $L^2 \cap K = K^2$, say they can be written as α^2, β^2, θ^2, γ^2 respectively. Since $q \neq 0$ we can perform four normalizations along the following steps: substitute z with $z + \frac{\alpha}{q} x$, so that $a(r) + a(s) = 0$; replace z with $z + \frac{\beta}{q}$, so that $r^2 a(r) + s^2 a(s) = 0$; substitute y with $y + \frac{\theta}{q} x$, so that $b(r) + b(s) = 0$; replace y with $y + \frac{\gamma}{q}$, so that $r^2 b(r) + s^2 b(s) = 0$. Thus

$$a(r) + a(s) = r^2 a(r) + s^2 a(s) = b(r) + b(s) = r^2 b(r) + s^2 b(s) = 0,$$

i.e., $a(r) = a(s) = b(r) = b(s) = 0$, which means that $c(x)$ divides both $a(x)$ and $b(x)$. We have therefore obtained a normal form for $F|K$ as in item (ii) in the statement of the theorem.

To complete the proof of the theorem we must verify that the equations of the normal form guarantee that any function field $F|K = K(x,z,y)|K$ given by them has the desired properties. By the preceding discussion we know that the pole $\mathfrak{p}$ of x satisfies the required conditions, and that $F|K$ has genera $g = 3$, $g_1 = 1$, $\overline{g} = 0$. Thus the only requirement one still has to verify is the fact that the divisor $\mathfrak{p}^e = \mathfrak{p}$ is not canonical, i.e., that $H^0(\mathfrak{p}) = K \oplus Kx$.

To do this we will find the space of global sections $H^0(\mathfrak{p}^2)$ of the divisor $\mathfrak{p}^2$. Since the 6-dimensional vector space $H^0(\mathfrak{p}^2)$ contains the 4-dimensional vector space $H^0(\mathfrak{p}_1^2)$ and the function y, we must construct a sixth element $u \in H^0(\mathfrak{p}^2)$ such that

$$H^0(\mathfrak{p}^2) = K \oplus Kx \oplus Kx^2 \oplus Kz \oplus Ky \oplus Ku. \tag{3.10}$$

We claim that $u := \frac{yz}{c(x)}$ has the desired property. Indeed, since $u^2 = A(x)(B(x)+z)$ lies in

$$H^0(\mathfrak{p}_1^4) = K \oplus Kx \oplus Kx^2 \oplus Kx^3 \oplus Kx^4 \oplus Kz \oplus Kxz \oplus Kx^2z$$

and hence in $H^0(\mathfrak{p}^4)$, it is clear that $u \in H^0(\mathfrak{p}^2)$. Moreover, the functions $1, x, x^2, z, y, u$ are linearly independent over K because their squares $1, x^2, x^4, c(x)A(x), c(x)(B(x)+z), A(x)(B(x)+z)$ are so.

We finally show that $H^0(\mathfrak{p}) = K \oplus Kx$. Indeed, we must prove that each element h of $H^0(\mathfrak{p})$ lies in $K \oplus Kx$. Since $H^0(\mathfrak{p})$ is contained in $H^0(\mathfrak{p}^2)$, we may write $h = \alpha + \beta x + \theta x^2 + \gamma z + \xi y + \zeta y$, so that

$$h^2 = \alpha^2 + \beta^2x^2 + \theta^2x^4 + \gamma^2c(x)A(x) + \xi^2c(x)(B(x)+z) + \zeta^2A(x)(B(x)+z)$$

lies in $F_1 \cap H^0(\mathfrak{p}^2) = H^0(\mathfrak{p}_1^2) = K \oplus Kx \oplus Kx^2 \oplus Kz$. Looking at the coefficient of x^2z gives $\xi^2 + \zeta^2A_2 = 0$, whence $\xi = \zeta = 0$ as $A_2 \notin K^2$. Similarly, since the coefficient $\theta^2 + \gamma^2A_2$ of x^4 is zero, we conclude that $\theta = \gamma = 0$, that is, $h \in K \oplus Kx$. □

Having obtained normal forms for those function fields whose singular primes $\mathfrak{p}$ have the property that $\mathfrak{p}_2$ is rational, we give criteria to decide when any two of them are isomorphic over K.

Theorem 3.8. *No function field from item* (i) *in Theorem 3.7 is isomorphic to a function field from item* (ii). *Moreover,*

(i) *two function fields $F|K$ and $F'|K$ from item* (i) *with parameters a_0, a_2, a_4 and a_0', a_2', a_4' are isomorphic if and only if there exist constants $b, c_0, c_1, t \in K$ with $t \neq 0$ such that*

$$\begin{aligned} t^4a_2' &= a_2, \\ t^{12}a_4' &= a_4 + c_1^4, \\ t^{-4}a_0' &= a_0 + b^2a_2 + b^4a_4 + c_0^4 + c_1^4b^4 + b; \end{aligned}$$

(ii) *two function fields $F|K$ and $F'|K$ from item* (ii) *with parameters c_0, c_1, A_2, B_0, B_1 and $c_0', c_1', A_2', B_0', B_1'$ are isomorphic if and only if there exist constants $r_0, t_2, t_3, t_4, t_5 \in K$ with $(t_4, t_5) \neq (0,0)$ such that*

$$\begin{aligned} t^6A_2' &= A_2 + s_2^2, \\ c_1' &= t^2c_1, \\ t^{-3}c_0' &= r_0^2t + r_0tc_1 + t_5^2c_1^{-1} + tc_0, \\ tB_1' &= B_1, \\ B_0' &= (r_0B_1 + B_0)t + c_1^{-1}(t_4t_5 + t_3^2), \end{aligned}$$

where $t := t_4^2 + t_5^2A_2 \neq 0$ and $s_2 := t^{-1}(t_2^2 + t_3^2A_2)$.

We note that the non-vanishing of $t = t_4^2 + t_5^2 A_2$ in item (ii) is equivalent to the non-vanishing of the pair (t_4, t_5), since $A_2 \notin K^2$.

Before proving the theorem we list some of its consequences. If $F|K$ is a function field from Theorem 3.7, item (i), with parameters a_0, a_2, a_4, then the class $a_2 \mod (K^*)^4$ is an invariant of $F|K$.

Suppose now that $F|K$ is a function field as in item (ii), with constants c_0, c_1, A_2, B_0, B_1. Then the class $c_1 \mod (K^*)^2$ is an invariant of the function field $F|K$. One could say as well that $B_1 \mod K^*$ is another such invariant; that is, the vanishing of B_1 is invariant under isomorphisms.

If $B_1 \neq 0$ then we can normalize $B_0 = 0$, and therefore the constant r_0 may be eliminated.

If K is separably closed then $c_0 = 0$ may be normalized. But here we cannot eliminate r_0 since there exist two values of r_0 in K satisfying $r_0^2 + c_1 r_0 + t^{-1} c_1^{-1} t_5^2 = 0$, namely if r_0' is one such value, the other one is $r_0' + c_1$.

Proof of Theorem 3.8. (i) Let $F|K$ and $F'|K$ be two function fields as in (i), with parameters a_0, a_2, a_4 and a_0', a_2', a_4', and assume there is a K-isomorphism $\sigma : F' \xrightarrow{\sim} F$. Since this isomorphism preserves the only singular primes of $F'|K$ and $F|K$, that is, $v_{\mathfrak{p}'} = v_{\mathfrak{p}} \circ \sigma$, $v_{\mathfrak{p}_1'} = v_{\mathfrak{p}_1} \circ \sigma$ and $v_{\mathfrak{p}_2'} = v_{\mathfrak{p}_2} \circ \sigma$, it induces isomorphisms $H^0(\mathfrak{p}'^n) \xrightarrow{\sim} H^0(\mathfrak{p}^n)$, $H^0(\mathfrak{p}_1'^n) \xrightarrow{\sim} H^0(\mathfrak{p}_1^n)$, $H^0(\mathfrak{p}_2'^n) \xrightarrow{\sim} H^0(\mathfrak{p}_2^n)$. Thus it follows from (3.7) and (3.9) that there are constants $a, b, c_i, t \in K$ with $a, t \neq 0$ such that

$$\begin{aligned} \sigma(x') &= bt^4 + ax, \\ \sigma(y') &= t(c_0 + c_1 x + y). \end{aligned}$$

Applying σ to the equality $y'^4 = a_0' + x' + a_2' x'^2 + a_4' x'^4$ and replacing $y^4 = a_0 + x + a_2 x^2 + a_4 x^4$ we get a system of four equations involving the constantst r_i, s_i, a_i, a_i'. Since one of these equations is $a = t^4$ we can eliminate a, thus obtaining the system of three equations stated in the theorem.

Conversely, if the constants $b, c_0, c_1, t \in K$ satisfy these three equations and $t \neq 0$, then the substitutions

$$x' \mapsto t^4(b + x), \quad y' \mapsto t(c_0 + c_1 x + y)$$

define a K-isomorphism $F' \to F$.

(ii) Let $F|K$ and $F'|K$ be two function fields as in (ii), with parameters c_0, c_1, A_2, B_0, B_1 and $c_0', c_1', A_2', B_0', B_1'$. Suppose there is a K-isomorphism $\sigma : F' \xrightarrow{\sim} F$. Since σ must preserve the only singular primes of $F|K$ and $F'|K$, i.e., $v_{\mathfrak{p}'} = v_{\mathfrak{p}} \circ \sigma$, $v_{\mathfrak{p}_1'} = v_{\mathfrak{p}_1} \circ \sigma$ and $v_{\mathfrak{p}_2'} = v_{\mathfrak{p}_2} \circ \sigma$, it induces isomorphisms $H^0(\mathfrak{p}'^n) \xrightarrow{\sim} H^0(\mathfrak{p}^n)$, $H^0(\mathfrak{p}_1'^n) \xrightarrow{\sim} H^0(\mathfrak{p}_1^n)$ and $H^0(\mathfrak{p}_2'^n) \xrightarrow{\sim} H^0(\mathfrak{p}_2^n)$. From (3.7), (3.8) and (3.10) we obtain constants r_i, s_i, t_i, t in K with $r_1, t \neq 0$ such that

$$\begin{aligned} \sigma(x') &= r_1(r_0 + x), \\ \sigma(z') &= t(s_0 + s_1 x + s_2 x^2 + z), \\ \sigma(y') &= t^2(t_0 + t_1 x + t_2 x^2 + t_3 z + t_4 y + t_5 u). \end{aligned}$$

Note that $(t_4, t_5) \neq (0, 0)$ necessarily. Applying σ to the equations

$$z'^2 = c'(x')A'(x') \quad \text{and} \quad y'^2 = c'(x')\big(B'(x') + z'\big),$$

and using the relations $z^2 = c(x)A(x)$, $y^2 = c(x)(B(x)+z)$, $u^2 = A(x)(B(x)+z)$ we get a system of twelve equations

$$\begin{aligned}
0 &= r_1^4 A_2' + s_2^2 t^2 + t^2 A_2,\\
0 &= r_1 t c_1' + t_4^2 t^4 c_1 + t_5^2 t^4 c_1 A_2,\\
0 &= t c_0' + r_0^2 r_1^2 t + r_0 r_1 t c_1' + t_4^2 t^4 c_0 + t_5^2 t^4 c_0 A_2 + t_5^2 t^4 c_1^{-1},\\
0 &= r_1^3 B_1' + r_1^2 s_1 t + r_1 s_2 t c_1' + t_4^2 t^4 B_1 + t_5^2 t^4 A_2 B_1,\\
0 &= r_1^2 B_0' + r_0^2 r_1^2 s_2 t + r_0 r_1^3 B_1' + r_0 r_1 s_2 t c_1' + r_1^2 s_0 t + r_1^2 c_1' B_1'\\
&\quad + r_1 s_1 t c_1' + t_1^2 t^4 + t_3^2 t^4 c_1^2 A_2 + t_3^2 t^4 c_1^{-1} + t_4^2 t^4 c_1 B_1 + t_4^2 t^4 B_0\\
&\quad + t_5^2 t^4 c_1 A_2 B_1 + t_5^2 t^4 A_2 B_0 + s_2 t c_0',\\
0 &= r_1 + t^2,\\
0 &= r_1^2 t + t_4^2 t^4 + t_5^2 t^4 A_2,\\
0 &= r_1^2 c_1'^2 A_2' + r_1^2 c_1'^{-1} + s_1^2 t^2 + t^2 c_1^2 A_2 + t^2 c_1^{-1},\\
0 &= r_0^3 r_1^3 B_1' + r_0^2 r_1^2 s_0 t + r_0^2 r_1^2 c_1' B_1' + r_0^2 r_1^2 B_0'\\
&\quad + r_0 r_1 s_0 t c_1' + r_0 r_1 c_0' B_1' + r_0 r_1 c_1' B_0' + t_0^2 t^4 + t_3^2 t^4 c_0^2 A_2 + t_3^2 t^4 c_0 c_1^{-1}\\
&\quad + t_4^2 t^4 c_0 B_0 + t_5^2 t^4 c_0 A_2 B_0 + t_5^2 t^4 c_1^{-1} B_0 + s_0 t c_0' + c_0' B_0',\\
0 &= r_0^4 r_1^4 A_2' + r_0^2 r_1^2 c_1'^2 A_2' + r_0^2 r_1^2 c_1'^{-1} + r_0 r_1 + s_0^2 t^2 + t^2 c_0^2 A_2 + t^2 c_0 c_1^{-1} + c_0'^2 A_2' + c_0' c_1'^{-1},\\
0 &= r_0^2 r_1^3 B_1' + r_0^2 r_1^2 s_1 t + r_0 r_1 s_1 t c_1' + r_1 s_0 t c_1' + r_1 c_0' B_1' + r_1 c_1' B_0' + t_3^2 t^4\\
&\quad + t_4^2 t^4 c_0 B_1 + t_4^2 t^4 c_1 B_0 + t_5^2 t^4 c_0 A_2 B_1 + t_5^2 t^4 c_1 A_2 B_0 + t_5^2 t^4 c_1^{-1} B_1 + s_1 t c_0',\\
0 &= r_1^2 s_2 t + t_2^2 t^4 + t_3^2 t^4 A_2.
\end{aligned}$$

We view the first five equations as a system of equations with coefficients in K and indeterminates in F'. We can clearly resolve it, since $r_1, t \neq 0$. That is, we obtain $A_2', B_2', c_1', c_0', B_1'$ explicitly in terms of the constants c_i, A_i, B_i of the function field $F|K$ and the constants r_i, s_i, t_i of the automorphism σ.

The sixth and seventh equations tell us that r_1 and t may be eliminated. Cancelling out the powers of $t_4^2 + t_5^2 A_2 \neq 0$ appearing in the eighth and ninth equations gives $s_1 = s_2 c_1$ and $t_1 = t_2 c_1$, that is, we can eliminate s_1 and t_1 too. Now it is clear from the last three equations that the constants s_0, t_0 and s_2 can also be eliminated. The system we search for consists of the five equations that remain.

Conversely, if there are constants $r_0, t_2, t_3, t_4, t_5 \in K$ with $(t_4, t_5) \neq (0,0)$ satisfying the five equations stated in (ii), then the substitutions

$$x' \mapsto t^2(r_0 + x), \quad z' \mapsto t(s_0 + s_2 c_1 x + s_2 x^2 + z), \quad y' \mapsto t^2(t_0 + t_2 c_1 x + t_2 x^2 + t_3 z + t_4 y + t_5 u),$$

where $t := t_4^2 + t_5^2 A_2 \neq 0$, $s_2 := t^{-1}(t_2^2 + t_3^2 A_2)$, $s_0 := s_2 c_0 + t^{-1} c_1^{-1} t_5 (t_4 + t_5 s_2)$ and $t_0 := t_2 c_0 + t^{-1} c_1^{-1} t_5 (t_2 t_5 + t_3 t_4)$, define a K-isomorphism $F' \to F$. □

The proof of Theorem 3.8 lets us discuss the group of automorphisms of the function fields in Theorem 3.7. So assume initially that $F|K$ is given as in item (i) with constants a_0, a_2, a_4. An automorphism of $F|K$ is defined by the substitutions

$$x \mapsto t^4(b + x), \qquad y \mapsto t(c_0 + c_1 x + y),$$

where the constants $b, c_0, c_1 \in K$ and $t \in K \setminus \{0\}$ satisfy the relations

$$\begin{aligned}
t^4 a_2 &= a_2,\\
t^{12} a_4 &= a_4 + c_1^4,\\
t^{-4} a_0 &= a_0 + b^2 a_2 + b^4 a_4 + c_0^4 + c_1^4 b^4 + b.
\end{aligned}$$

Observe that $c_1 = 0$ since $a_4 \notin K^2$, and hence $t^3 = 1$. Therefore, the automorphisms of $F|K$ are given by the substitutions

$$x \mapsto t(b + x), \qquad y \mapsto t(c_0 + y),$$

where $b, c_0, t \in K$, $t^3 = 1$ and

$$\begin{aligned} ta_2 &= a_2, \\ t^{-1}a_0 &= a_0 + b^2 a_2 + b^4 a_4 + c_0^4 + b. \end{aligned}$$

If $a_2 \neq 0$ then one has $t = 1$, and so $t = 1$ together with $b^2 a_2 + b^4 a_4 + c_0^4 + b = 0$ are the only relations the constants b, c_0, t must satisfy.

Suppose next that $F|K$ is a function field as in item (ii), with parameters c_0, c_1, A_2, B_0, B_2. The automorphisms of $F|K$ are given by the substitutions of the form

$$x \mapsto t^2(r_0 + x), \qquad y \mapsto t^2(t_0 + t_2 c_1 x + t_2 x^2 + t_3 z + t_4 y + t_5 u),$$

where r_0, t_2, t_3, t_4, t_5 are constants in K and $t_0 := t_2 c_0 + t^{-1} c_1^{-1} t_5(t_2 t_5 + t_3 t_4)$; these constants must satisfy the conditions $(t_4, t_5) \neq (0, 0)$ and

$$\begin{aligned} t^6 A_2 &= s_2^2 + A_2, \\ c_1 &= t^2 c_1, \\ t^{-3} c_0 &= r_0^2 t + r_0 t c_1 + t_5^2 c_1^{-1} + t c_0, \\ t B_1 &= B_1, \\ B_0 &= (r_0 B_1 + B_0) t + c_1^{-1}(t_4 t_5 + t_3^2), \end{aligned}$$

where $t := t_4^2 + t_5^2 A_2 \neq 0$ and $s_2 := t^{-1}(t_2^2 + t_3^2 A_2)$. Note that $t = 1$ since $c_1 \neq 0$, and so $t_4 = 1$, $t_5 = 0$ because $A_2 \notin K^2$. One sees similarly that $t_2 = t_3 = 0$, and hence $r_0^2 + r_0 c_1 = r_0 B_1 = 0$. Thus the group $\mathrm{Aut}(F|K)$ of automorphisms of $F|K$ are given by the substitutions

$$x \mapsto r_0 + x, \qquad y \mapsto y,$$

where the constant $r_0 \in K$ satisfies the condition $r_0^2 + r_0 c_1 = r_0 B_1 = 0$. If $B_1 \neq 0$, then $\mathrm{Aut}(F|K)$ is trivial. And if $B_1 = 0$, then $\mathrm{Aut}(F|K)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

3.2.2 The case where $\mathfrak{p}_2$ is non-rational

Let $F|K$ be a one-dimensional separable function field of genera $g = 3$, $g_1 = 1$, $\overline{g} = 0$ in characteristic 2.

Recall that $F|K$ has a unique singular prime $\mathfrak{p}$ of singularity degree $\delta(\mathfrak{p}) = 3$. Recall also that $\mathfrak{p}$ is non-decomposed, and that its restriction $\mathfrak{p}_3$ to $F_3|K$ is a rational prime.

In this section we analyse the situation where $\mathfrak{p}_2$ is not rational.

Theorem 3.9. *A one-dimensional separable function field $F|K$ in characteristic $p = 2$ has genera $g = 3$, $g_1 = 1$, $\overline{g} = 0$ and the restriction $\mathfrak{p}_2$ of its only singular prime $\mathfrak{p}$ to $F_2|K$ is non-rational, if and only if, $F|K$ can be put into one of the following normal forms*

(i) $z^2 = ax^2 + x + c, \qquad a \notin K^2,$
$w^2 = z,$
$y^2 = m_1 x + m_0 + n_0 z + w;$

(ii) $z^2 = ax^2 + x, \qquad a \notin K^2,$
$w^2 = a_2x^2 + a_0 + z,$
$y^2 = xw;$

(iii) $z^2 = ax^2 + x + c, \qquad a \notin K^2,$
$w^2 = a_2z^2 + z, \qquad a_2 \notin K^2,$
$y^2 = (n_0 + n_1x + w)z,$

where $a, c, a_i, m_i, n_i \in K$ are constants.

In each case, the function x has a pole at the singular prime $\mathfrak{p}$ of $F|K$. Moreover, item (i) *occurs if and only if the divisor $\mathfrak{p}^e$ is canonical, where e denotes the ramification index of $\mathfrak{p}$ over F_1.*

Proof. Let $F|K$ be a function field as in the statement of the theorem, and let $\mathfrak{p}$ be its only singular prime. By assumption, the prime $\mathfrak{p}_2$ of $F_2|K$ is not rational, so that $\deg \mathfrak{p}_2 = 2$. Let e and e_1 denote the ramification indices of $\mathfrak{p}$ and $\mathfrak{p}_1$ over F_1 and F_2 respectively.

Since the function field $F_3|K$ has genus $g_3 = 0$ and its prime $\mathfrak{p}_3$ is rational, it is a rational function field, say $F_3|K = K(x)|K$ with $v_{\mathfrak{p}_3}(x) = -1$. It then follows from Riemann's theorem that $\dim H^0(\mathfrak{p}_3^n) = n + 1$, that is,

$$H^0(\mathfrak{p}_3^n) = K \oplus Kx \oplus \cdots \oplus Kx^n \quad \text{for all } n \geq 0. \tag{3.11}$$

Analogously, since the function field $F_2|K$ has genus $g_2 = 0$ and $\mathfrak{p}_2$ has degree 2 we have

$$\dim H^0(\mathfrak{p}_2^n) = 2n + 1 \quad \text{for all } n \geq 0.$$

Similarly, since $F_1|K$ has genus $g_1 = 1$ we also have

$$\dim H^0(\mathfrak{p}_1^n) = \begin{cases} 4n & \text{for all } n \geq 1, \quad \text{if } e_1 = 1, \\ 2n & \text{for all } n \geq 1, \quad \text{if } e_1 = 2. \end{cases}$$

And since $F|K$ has genus $g = 3$ one has

$$\dim H^0(\mathfrak{p}^n) = \begin{cases} 8n - 2 & \text{for all } n \geq 1, \quad \text{if } e_1e = 1, \\ 4n - 2 & \text{for all } n \geq 2, \quad \text{if } e_1e = 2, \\ 2n - 2 & \text{for all } n \geq 3, \quad \text{if } e_1e = 4. \end{cases}$$

As $\dim H^0(\mathfrak{p}_2) = 3 > \dim H^0(\mathfrak{p}_3) = 2$, we can find a function $z \in F$ such that

$$H^0(\mathfrak{p}_2) = H^0(\mathfrak{p}_3) \oplus Kz = K \oplus Kx \oplus Kz, \tag{3.12}$$

which does not belong to $F_3 = K(x)$ because $F_3 \cap H^0(\mathfrak{p}_2) = H^0(\mathfrak{p}_3)$. This means in particular that z is a separating variable of $F_2|K$, or equivalently $F_2 = F_3(z) = K(x, z)$. Since z^2 lies in $H^0(\mathfrak{p}_2^2) \cap F_2 = H^0(\mathfrak{p}_3)$, there exist constants $a, b, c \in K$ such that

$$z^2 = ax^2 + bx + c.$$

Because the function z is separable over $F_3 = K(x)$ the constant b must be non-zero, hence we can normalize $b = 1$ by replacing x with bx and z with bz. By Proposition 2.5, the fact that $\mathfrak{p}_2$ is non-rational means that $a \notin K^2$, thus yielding the following normal form of $F_2|K$

$$z^2 = ax^2 + x + c, \qquad a \notin K^2.$$

We observe that this normal form already guarantees that every prime of $F_2|K$ is non-singular (by the Jacobian criterion), i.e., $F_2|K$ has genus 0, and that its prime $\mathfrak{p}_2$ is non-rational (see Proposition 2.5).

As $\dim H^0(\mathfrak{p}_1^{e_1}) = 4 > \dim H^0(\mathfrak{p}_2) = 3$ there is a function $w \in F$ such that

$$H^0(\mathfrak{p}_1^{e_1}) = H^0(\mathfrak{p}_2) \oplus Kw = K \oplus Kx \oplus Kz \oplus Kw, \tag{3.13}$$

which lies outside $F_2 = K(x, z)$ because $F_2 \cap H^0(\mathfrak{p}_1^{e_1}) = H^0(\mathfrak{p}_2)$. In particular, w is a separating variable of $F_1|K$, or in other words $F_1 = F_2(z) = K(x, z, w)$. And because w^2 belongs to $H^0(\mathfrak{p}_1^{2e_1}) \cap F_2 = H^0(\mathfrak{p}_2^2) = K \oplus Kx \oplus Kx^2 \oplus Kz \oplus Kxz$, there are constants a_i and c_i such that

$$w^2 = a_2x^2 + a_1x + a_0 + (c_1x + c_0)z.$$

Observe that one of the c_i must be non-zero, since w^2 is a separating variable of $F_2|K$ and therefore $w^2 \notin F_3 = K(x)$.

We want to rephrase the fact that $\mathfrak{p}_1$ has singularity degree $\delta(\mathfrak{p}_1) = 1$ in terms of equations on the constants a_i, c_i, a, c. To do this we introduce the functions $\breve{x} := x^{-1}$, $\breve{z} := zx^{-1}$ and $\breve{w} := wx^{-1}$. Note that $\breve{x}$ is a local parameter at both $\mathfrak{p}_2$ and $\mathfrak{p}_3$, and that $\breve{z}$ and $\breve{w}$ satisfy the relations

$$\begin{aligned}\breve{z}^2 &= a + \breve{x} + c\breve{x}^2,\\ \breve{w}^2 &= a_2 + a_1\breve{x} + a_0\breve{x}^2 + (c_1 + c_0\breve{x})\breve{z}.\end{aligned}$$

In particular,

$$\begin{aligned}\breve{z}(\mathfrak{p})^2 &= a \notin K^2,\\ \breve{w}(\mathfrak{p})^2 &= a_2 + c_1\breve{z}(\mathfrak{p}).\end{aligned}$$

We claim that the condition $\delta(\mathfrak{p}_1) = 1$ means that $c_1 = 0$ and $c_0 \neq 0$. Indeed, when $\breve{w}(\mathfrak{p}) \notin K_{\mathfrak{p}_2} = K(\breve{z}(\mathfrak{p}))$ it suffices to observe that $\mathfrak{p}_1$ is inertial over F_2 and $\delta(\mathfrak{p}_1) = \frac{1}{2}v_{\mathfrak{p}_3}(d\breve{w}^4) = \frac{1}{2}v_{\mathfrak{p}_3}(c_1^2 + c_0^2\breve{x}^2)$, by Theorem 2.3. In the opposite case $\breve{w}(\mathfrak{p}) \in K(\breve{z}(\mathfrak{p}))$, say $f(\mathfrak{p}) = 0$ for some f in $\breve{w} + K + K\breve{z}$, we have $c_1 = 0$ (and therefore $c_0 \neq 0$) since $\breve{z}(\mathfrak{p}) \notin K$, hence the prime $\mathfrak{p}_1$ is ramified over F_2 with local parameter f because

$$v_{\mathfrak{p}_3}(df^4) = v_{\mathfrak{p}_3}(d\breve{w}^4) = v_{\mathfrak{p}_3}(c_0^2\breve{x}^2) = 2 < 4,$$

and therefore $\delta(\mathfrak{p}_1) = \frac{1}{2}v_{\mathfrak{p}_3}(df^4) = 1$, thus proving our claim.

Substituting x, z, w with c_0^2x, c_0z, c_0w we can normalize $c_0 = 1$ and we obtain the following normal form of $F_1|K$

$$\begin{aligned}z^2 &= ax^2 + x + c, &\qquad a \notin K^2,\\ w^2 &= a_2x^2 + a_1x + a_0 + z.\end{aligned}$$

Since $w^4 = (c + a_0) + x + (a + a_1^2)x^2 + a_2^4x^4$, it follows from the Jacobian criterion that $\mathfrak{p}_1$ is the only singular prime of $F_1|K$, and therefore this normal form guarantees that $F_1|K$ has genus $g_1 = 1$.

Note that the above paragraph implies that the prime $\mathfrak{p}_1$ is ramified over F_2 if and only if $\breve{w}(\mathfrak{p}) = a_2^{1/2}$ lies in $K_{\mathfrak{p}_2} = K(a^{1/2})$. In particular, $\mathfrak{p}_1$ has residue field $K_{\mathfrak{p}_1} = K(a^{1/2}, a_2^{1/2}) = K(\breve{z}(\mathfrak{p}), \breve{w}(\mathfrak{p}))$.

Remark. Further normalizations can be made at this point: replacing z with $z+a_0+a_1x$ yields $a_1=a_0=0$; and if in addition $\mathfrak{p}_1$ is ramified over F_2 then one may normalize $a_2=0$ by substracting from w an element of $Kx+Kz$. However, keeping the coefficients a_i unnormalized will be useful later in the proof, as it will allow for more flexibility when normalizing the functions w and z.

Having obtained a normal form for $F_1|K$, we now proceed to analyse the function field $F|K$. Since $\dim H^0(\mathfrak{p}^{ee_1})=6>\dim H^0(\mathfrak{p}_1^{e_1})=4$, we can pick a function y in $H^0(\mathfrak{p}^{ee_1})\setminus H^0(\mathfrak{p}_1^{e_1})$. This function does not belong to $F_1=K(x,z,w)$ because $H^0(\mathfrak{p}^{ee_1})\cap F_1=H^0(\mathfrak{p}_1^{e_1})$, and so it is a separating variable of $F|K$, i.e., $F=F_1(y)$. Since its square y^2 lies in $H^0(\mathfrak{p}^{2ee_1})\cap F_1=H^0(\mathfrak{p}_1^{2e_1})=K\oplus Kx\oplus Kx^2\oplus Kz\oplus Kxz\oplus Kw\oplus Kxw\oplus Kzw$, there exist constants m_i,n_i,p_i such that

$$y^2=m_2x^2+m_1x+m_0+(n_1x+n_0)z+(p_1x+p_0+p_2z)w.$$

One notes as before that one of the p_i's must be non-zero, since y^2 is a separating variable of $F_1|K$, i.e., $y^2\notin F_2=K(x,z)$.

In order to study the singular prime $\mathfrak{p}$ of $F|K$ we introduce the function $\breve{y}:=yx^{-1}$, which must satisfy the following relation

$$\breve{y}^2=m_2+m_1\breve{x}+m_0\breve{x}^2+(n_1+n_0\breve{x})\breve{z}+(p_1+p_0\breve{x}+p_2\breve{z})\breve{w}.$$

In particular,

$$\breve{y}(\mathfrak{p})^2=m_2+n_1\breve{z}(\mathfrak{p})+(p_1+p_2\breve{z}(\mathfrak{p}))\breve{w}(\mathfrak{p}).$$

Now we divide the discussion into two major parts, depending on the value of $p_1^2+p_2^2a$. As we will see in a moment, item (i) will correspond to the case $p_1^2+p_2^2a=0$, while items (ii) and (iii) will correspond to the case $p_1^2+p_2^2a\neq 0$.

Suppose first that $p_1^2+p_2^2a=0$. Since $a\notin K^2$, this means that $p_1=p_2=0$. Then $p_0\neq 0$ and so we may normalize $p_0=1$ by substituting $\breve{x}$, $\breve{z}$, $\breve{w}$, $\breve{y}$ with $p_0^{-4}\breve{x}$, $p_0^{-2}\breve{z}$, $p_0^{-1}\breve{w}$, $p_0^{-2}\breve{y}$ respectively. Since $v_{\mathfrak{p}_3}(d\breve{y}^8)=v_{\mathfrak{p}_3}(\breve{x}^4d\breve{w}^4)=6$, it is clear that the value $\breve{y}(\mathfrak{p})$ of $\breve{y}$ lies necessarily in $K_{\mathfrak{p}_1}=K(\breve{z}(\mathfrak{p}),\breve{w}(\mathfrak{p}))$, for otherwise $\mathfrak{p}$ is inertial over F_1 and $\delta(\mathfrak{p})=2\cdot 1+\frac{1}{2}v_{\mathfrak{p}_3}(d\breve{y}^8)=5$, a contradiction. Thus $f(\mathfrak{p})=0$ for some f in $\breve{y}+K+K\breve{z}+K\breve{w}+K\breve{z}\breve{w}$, so it follows from

$$v_{\mathfrak{p}_3}(df^8)=v_{\mathfrak{p}_3}(d\breve{y}^8)=6<8$$

that the prime $\mathfrak{p}_1$ must be ramified over F_2, i.e., $e_1=2$, for otherwise $\mathfrak{p}$ is ramified over F_1 with local parameter f and therefore $\delta(\mathfrak{p})=2\cdot 1+\frac{1}{2}v_{\mathfrak{p}_3}(df^8)=5$, a contradiction. Substracting from $\breve{w}$ an element of $K+K\breve{z}$ we may assume $\breve{w}(\mathfrak{p})=0$, i.e., $a_2=0$, and by substracting from $\breve{z}$ an element of $K+K\breve{x}$ we may normalize $a_1=a_0=0$. Since $K_{\mathfrak{p}_1}=K(\breve{z}(\mathfrak{p}))$, by substracting from $\breve{y}$ an element of $K+K\breve{z}$ we may suppose $\breve{y}(\mathfrak{p})=0$, that is, $m_2=n_1=0$ as $a\notin K^2$. We have thus obtained a normal form as in item (i).

We claim that this normal form already guarantees that the prime $\mathfrak{p}$ has singularity degree 3 and that the function field $F|K$ has genus 3. Indeed, since $y^8=(n_0^4c^2+c+m_0^4)+x+(n_0^4+a)x^2+(m_1^4+n_0^4a^2)x^4$ it follows from the Jacobian criterion that there are no singular primes other than $\mathfrak{p}$. Now, dividing $\breve{y}^8$ by a power of the local parameter $\breve{w}$ at $\mathfrak{p}_1$ we obtain

$$\left(\frac{\breve{y}}{\breve{w}}\right)^8=\frac{(m_1^4+n_0^4a^2)\breve{x}^4+(n_0^4+a)\breve{x}^6+\breve{x}^7+(n_0^4c^2+c+m_0^4)\breve{x}^8}{a^2\breve{x}^4+\breve{x}^6+c^2\breve{x}^8}=\varepsilon_0+\varepsilon_2\breve{x}^2+a^{-2}\breve{x}^3+\cdots,$$

where $\varepsilon_0 := n_0^4 + a^{-2}m_1^4$ and $\varepsilon_2 := a^{-2}\varepsilon_0$. If $\frac{\breve{y}}{\breve{w}}(\mathfrak{p}) \notin K_{\mathfrak{p}_1} = K(\breve{z}(\mathfrak{p}))$, then $\mathfrak{p}$ is inertial over F_1 and $\delta(\mathfrak{p}) = 2 \cdot 1 + \frac{1}{2}v_{\mathfrak{p}_3}\big(d(\frac{\breve{y}}{\breve{w}})^8\big) = 3$. In the opposite case, say $f(\mathfrak{p}) = 0$ for some f in $\frac{\breve{y}}{\breve{w}} + K + K\breve{z}$, we have

$$f^8 = \varepsilon_2 \breve{x}^2 + a^{-2}\breve{x}^3 + \cdots ,$$

so we see that $\mathfrak{p}$ is ramified over F_1 with local parameter f, and therefore $\delta(\mathfrak{p}) = 2 \cdot 1 + \frac{1}{2}v_{\mathfrak{p}_3}(df^8) = 3$. This proves our claim.

We next treat the second part of the discussion, that is, we assume $p_1^2 + p_2^2 a \neq 0$. We immediately observe that

$$d\breve{y}^8 = \big((p_1^4 + p_2^4 a^2)\breve{x}^2 + p_2^4\breve{x}^4 + (p_0^4 + p_2^4 c^2)\breve{x}^6\big)d\breve{x},$$

and therefore $v_{\mathfrak{p}_3}(d\breve{y}^8) = 2$, which by Theorem 2.3 implies that $\delta(\mathfrak{p}) = 2 \cdot 1 + 1 = 3$ whenever $\breve{y}(\mathfrak{p})$ lies outside $K_{\mathfrak{p}_1} = K(\breve{z}(\mathfrak{p}), \breve{w}(\mathfrak{p}))$. If this does not happen, say $f(\mathfrak{p}) = 0$ for some f in $\breve{y} + K + K\breve{z} + K\breve{w} + K\breve{z}\breve{w}$, then the prime $\mathfrak{p}$ must be ramified over $\mathfrak{p}_1$ with local parameter f since

$$v_{\mathfrak{p}_3}(df^8) = v_{\mathfrak{p}_3}(d\breve{y}^8) = 2 < 4,$$

and hence $\delta(\mathfrak{p}) = 2{\cdot}1 + \frac{1}{2}v_{\mathfrak{p}_3}(df^8) = 3$. We have thus verified that under the assumption $p_1^2 + p_2^2 a \neq 0$ the requirement $\delta(\mathfrak{p}) = 3$ holds already. So it remains to study the requirement that $F|K$ has genus $g = 3$.

By the Jacobian criterion and the genus drop formula, the fact that $F|K$ has genus 3 means that the zeros of $\frac{dy^8}{dx} = (p_0^4 + p_2^4 c^2) + p_2^4 x^2 + (p_1^4 + p_2^4 a^2)x^4$ are non-singular primes, that is, the zeros of

$$\alpha(x) := (p_0^2 + p_2^2 c) + p_2^2 x + (p_1^2 + p_2^2 a)x^2$$

are non-singular primes. Two cases are to be considered: $p_2 = 0$ and $p_2 \neq 0$. The first case will correspond to item (ii), while the second case will correspond to item (iii).

Assume first that $p_2 = 0$, so that $p_1 \neq 0$. One can then normalize $p_1 = 1$ and $p_0 = 0$ by replacing x, z, w, y with $p_1^{-4}x + p_1^{-1}p_0$, $p_1^{-2}z$, $p_1^{-1}w$, $p_1^{-2}y$ respectively. Let $\mathfrak{q}$ be the only zero of $\alpha(x) = x^2$, so that the function x is a local parameter at the rational prime $\mathfrak{q}_3$ of $F_3|K = K(x)|K$. We know that the prime $\mathfrak{q}$ must be non-singular, that is, $\delta(\mathfrak{q}) = 0$. Observe that

$$v_{\mathfrak{q}_3}(dy^8) = v_{\mathfrak{q}_3}(x^4 dw^4) = 4,$$

which by [Stö88, Theorem 2.3] implies that $y(\mathfrak{q})$ lies in $K_{\mathfrak{q}_1}$, and that $\mathfrak{q}$ cannot be ramified over F_1 with local parameter y. Note also that $z(\mathfrak{q}) \in K$ necessarily. Indeed, assuming the contrary $z(\mathfrak{q}) \notin K$ we have that $\mathfrak{q}_2$ is inertial over F_3 with residue field $K(z(\mathfrak{q}))$, and since $w(\mathfrak{q}) = z(\mathfrak{q})^{1/2}$ we also have that $\mathfrak{q}_1$ is inertial over F_2 with residue field $K(w(\mathfrak{q}))$; but this contradicts the non-singularity of $\mathfrak{q}$ because $y(\mathfrak{q}) \in K_{\mathfrak{q}_1} = K(w(\mathfrak{q}))$ implies that $f(\mathfrak{q}) = 0$ for some f in $y + K + Kw + Kw^2 + Kw^3$, hence $\mathfrak{q}$ is ramified over F_1 with local parameter f as

$$v_{\mathfrak{q}_3}(df^8) = v_{\mathfrak{q}_3}(dy^8) = 4 < 8,$$

and therefore $\delta(\mathfrak{q}) = \frac{1}{2}v_{\mathfrak{q}_3}(df^8) = 2$, a contradiction.

By substracting from z an element of K we may assume $z(\mathfrak{q}) = 0$, i.e., $c = 0$, and one clearly sees that $\mathfrak{q}_2$ is rational with local parameter z. From the equation

$$z^2 = x + ax^2$$

we get x as a power series in z

$$x = z^2 + az^4 + a^3z^8 + a^7z^{16} + a^{15}z^{32} + \cdots ,$$

and hence w^2 as a power series in z

$$w^2 = a_0 + z + a_1z^2 + (a_2 + a_1a)z^4 + (a_2a^2 + a_1a^3)z^8 + \cdots .$$

By Proposition 2.5, the prime $\mathfrak{q}_1$ is rational if and only if $w(\mathfrak{q}) = a_0^{1/2}$ belongs to K. It follows in particular that $K_{\mathfrak{q}_1} = K(w(\mathfrak{q}))$, whence the condition $y(\mathfrak{q}) \in K_{\mathfrak{q}_1}$ means that by replacing y with an element of $y + K + Kw$ we can normalize $y(\mathfrak{q}) = 0$, i.e., $m_0 = 0$.

Assume first that $\mathfrak{q}_1$ is not rational, i.e., $w(\mathfrak{q}) = a_0^{1/2} \notin K$. Then $n_0 = 0$ necessarily, since we have the relation

$$y^2 = n_0z + m_1x + xw + n_1xz + m_2x^2,$$

and we know that $\mathfrak{q}$ cannot be ramified over F_1 with local parameter y. We claim that the normal form we have obtained guarantees that $\mathfrak{q}$ is non-singular, and hence that $F|K$ has genus $g = 3$. Indeed, dividing y^4 by a power of the local parameter at $\mathfrak{q}_2$ we see that

$$\left(\frac{y}{z}\right)^4 = \frac{m_1^2x^2 + m_2^2x^4 + n_1^2x^2z^2 + x^2w^2}{z^4} = (m_1^2 + a_0) + z + (n_1^2 + a_1)z^2 + \cdots ,$$

and hence $\frac{y}{z}(\mathfrak{q}) \notin K_{\mathfrak{q}_1}$ as $m_1^2 + a_0 \notin K^2$. Therefore $\delta(\mathfrak{q}) = \frac{1}{2}v_{\mathfrak{q}_2}\big(d(\frac{y}{z})^4\big) = 0$ by Theorem 2.3, i.e., $\mathfrak{q}$ is non-singular, thus proving the claim.

Now assume that $\mathfrak{q}_1$ is rational, i.e. $a_0^{1/2} \in K$. We then normalize $a_0 = 0$ by substituting w with $w + a_0^{1/2}$, and so w is a local parameter at $\mathfrak{q}_1$. From the relation

$$w^2 = z + a_1z^2 + (a_2 + a_1a)z^4 + (a_2a^2 + a_1a^3)z^8 + \cdots$$

we obtain z as a power series in w

$$z = w^2 + a_1w^4 + (a_2 + a_1a + a_1^3)w^8 + \cdots ,$$

and hence x and y^2 as power series in w

$$\begin{aligned} x &= w^4 + (a_1^2 + a)w^8 + (a_2^2 + a_1^2a^2 + a_1^6 + aa_1^4 + a^3)w^{16} + \cdots , \\ y^2 &= n_0w^2 + (m_1 + n_0a_1)w^4 + w^5 + n_1w^6 + \cdots . \end{aligned}$$

It then follows from Proposition 2.5 that $\delta(\mathfrak{q}) = 0$ if and only if $n_0 \in K^2$, in which case we may normalize $n_0 = 0$ by replacing y with $y + n_0^{1/2}w$. So this normal form has the properties we want.

To sum up, in the first case $p_2 = 0$ we have obtained the following normal form of $F|K$

$$\begin{aligned} z^2 &= ax^2 + x, \\ w^2 &= a_2x^2 + a_1x + a_0 + z, \\ y^2 &= x(m_2x + m_1 + n_1z + w). \end{aligned}$$

By replacing w with $w + n_1z + m_1 + m_2x$ we can normalize $n_1 = m_1 = m_2 = 0$. And by substituting z with $z + a_1x$ we can normalize as well $a_1 = 0$. This yields the normal form in item (ii).

Now we treat the second case $p_2 \neq 0$, where the polynomial $\alpha(x)$ is separable. Replacing x, z, w, y with $p_2^{-4}x$, $p_2^{-2}z + p_2^{-1}p_0 + p_2^{-5}p_1x$, $p_2^{-1}w$, $p_2^{-1}y$ respectively we may normalize $p_2 = 1$, $p_1 = p_0 = 0$.

Assume initially that the field K is separably closed, so that both the roots of

$$\alpha(x) = ax^2 + x + c$$

lie in K. Let $r \in K$ be one such root and let $\mathfrak{q}$ be the zero of the function $x+r$. Notice that $z(\mathfrak{q}) = 0$ and that $x + r$ is a local parameter of the rational prime $\mathfrak{q}_3$ of $F_3|K = K(x)|K$. We want to see when $\mathfrak{q}$ is non-singular, i.e., when $\delta(\mathfrak{q}) = 0$ occurs. We claim that in fact $\delta(\mathfrak{q}) = 0$ if and only if $w(\mathfrak{q}), y(\mathfrak{q}) \in K$. Since $x(\mathfrak{q}) = r \in K$, to see this one may assume $x(\mathfrak{q}) = 0$, that is, $c = 0$ as $z(\mathfrak{q}) = 0$. This implies that $\mathfrak{q}_2$ is a rational prime with local parameter z. Since

$$v_{\mathfrak{q}_2}(dy^4) = v_{\mathfrak{q}_2}(z^2dw^2) = 2,$$

it follows from Theorem 2.3 that $y(\mathfrak{q}) \in K_{\mathfrak{q}_1}$ whenever $\delta(\mathfrak{q}) = 0$. Assuming that $w(\mathfrak{q}) \notin K$, the prime $\mathfrak{q}_1$ is unramified over F_2 with residue field $K_{\mathfrak{q}_1} = K(w(\mathfrak{q}))$, and if we suppose $\delta(\mathfrak{q}) = 0$ then $y(\mathfrak{q}) \in K_{\mathfrak{q}_1}$ implies that $f(\mathfrak{q}) = 0$ for some f in $K + Kw$, so that $\mathfrak{q}$ is ramified over F_1 with local parameter f as

$$v_{\mathfrak{q}_2}(df^4) = v_{\mathfrak{q}_2}(dy^4) = 2 < 4,$$

and therefore $\delta(\mathfrak{q}) = \frac{1}{2}v_{\mathfrak{q}_2}(df^4) = 1$, a contradiction. Thus the condition $\delta(\mathfrak{q}) = 0$ implies that $w(\mathfrak{q}) \in K$. So in order to prove the claim we may suppose $w(\mathfrak{q}) = 0$, i.e., $a_0 = 0$, in which case $\mathfrak{q}_1$ is ramified (and therefore rational) over F_2 with local parameter w. Since $v_{\mathfrak{q}_1}(dy^2) = v_{\mathfrak{q}_1}(zdw) = 2$ as both differentials dx and dz of $F_1|K$ are zero, one sees from Proposition 2.5 that $\delta(\mathfrak{q}) = 0$ if and only if $y(\mathfrak{q}) \in K$, thus proving the claim. Therefore

$$g = 3 \text{ if and only if } a(r), a(s), m(r), m(s) \in K^2,$$

where $r, s \in K$ are the roots of $\alpha(x)$, $a(x) := a_2x^2+a_1x+a_0$, and $m(x) = m_2x^2+m_1x+m_0$. We conclude that in the general case, i.e., when K is not separably closed, we have

$$g = 3 \text{ if and only if } a(r), a(s), m(r), m(s) \in L^2,$$

where L denotes the separable closure of K and $r, s \in L$ are the roots of $\alpha(x)$.

We must rewrite these conditions on the roots r and s of the polynomial $\alpha(x)$, in such a way that they yield new normalizations. As in the proof of Theorem 3.7, we will achieve this by using symmetric polynomials. Put

$$q := r + s = a^{-1} \in K, \qquad t := rs = ca^{-1} \in K.$$

Notice that the four expressions

$$\begin{aligned} a(r) + a(s) &= a_1q + a_2q^2, \\ r^2a(r) + s^2a(s) &= a_2q^2 + a_1(q^3 + qt) + a_2q^4, \\ m(r) + m(s) &= m_1q + m_2q^2, \\ r^2m(r) + s^2m(s) &= m_0q^2 + m_1(q^3 + qt) + m_2q^4, \end{aligned}$$

lie in $L^2 \cap K = K^2$, say they are equal to σ^2, β^2, θ^2, γ^2 respectively. Since $q \neq 0$ we can perform four normalizations along the following steps: replace w with $w + \frac{\sigma}{q}x$, so that $a(r) + a(s) = 0$; substitute w with $w + \frac{\beta}{q}$, so that $r^2a(r) + s^2a(s) = 0$; replace y with $y + \frac{\theta}{q}x$, so that $m(r) + m(s) = 0$; substitute y with $y + \frac{\gamma}{q}$, so that $r^2m(r) + s^2m(s) = 0$. Thus

$$a(r) + a(s) = r^2a(r) + s^2a(s) = m(r) + m(s) = r^2m(r) + s^2m(s) = 0,$$

i.e., $a(r) = a(s) = m(r) = m(s) = 0$, which means that $ax^2 + x + c$ divides both $a(x)$ and $m(x)$. This implies that by rescaling a_2 and m_2 one gets

$$w^2 = a_2 z^2 + z \quad \text{ and } \quad y^2 = m_2 z^2 + (n_0 + n_1 x)z + zw.$$

We now normalize $m_2 = 0$ by replacing w with $w + m_2 z$.

We remark at this point that what we have hitherto obtained is a normal form as in item (iii) but without the condition $a_2 \notin K^2$. To get the normal form we want we will verify that if this requirement is not met, say $a_2 = r^2$, then our function field can be put into a normal form as in item (i). Indeed, it suffices to observe that by replacing w with $w + rz$ one gets $w^2 = z$ and $y^2 = z(rz + n_0 + n_1 x + w)$, so that $\left(\frac{yw}{z}\right)^2$ lies in $K \oplus Kx \oplus Kz \oplus Kw$.

To complete the proof of the theorem it remains to verify that item (i) occurs if and only if the divisor $\mathfrak{p}^e$ is canonical. We know that this happens if and only if the divisor $\mathfrak{p}^e$ has degree $2g - 2 = 4$ and its space of global sections $H^0(\mathfrak{p}^e)$ is a K-vector space of dimension $g = 3$. Now, if item (i) occurs then $\mathfrak{p}^e$ has degree 4, since $e_1 = 2$ and the divisor $\mathfrak{p}^{e_1 e}$ has degree 8; and the space of global sections of $\mathfrak{p}^e$ is given by

$$H^0(\mathfrak{p}^e) = K \oplus Kw \oplus Ky, \tag{3.14}$$

since both the squares $w^2 = z$, $y^2 = m_1 x + m_0 + n_0 z + w$ of the functions w, y belong to $H^0(\mathfrak{p}_1^{e_1}) = H^0(\mathfrak{p}_1^2)$, and hence to $H^0(\mathfrak{p}^{2e})$, that is, they both lie in $H^0(\mathfrak{p}^e)$.

We prove next that when items (ii) and (iii) occur the divisor $\mathfrak{p}^e$ is not canonical. As is clear from the previous paragraph, we must show that if $e_1 = 2$ then $\dim H^0(\mathfrak{p}^e) < 3$. To achieve this we shall find first the space of global sections of the divisor $\mathfrak{p}^{ee_1}$. Since $H^0(\mathfrak{p}^{ee_1})$ is a 6-dimensional vector space over K, we need to determine a function $u \in F$ such that

$$H^0(\mathfrak{p}^{ee_1}) = K \oplus Kx \oplus Kz \oplus Kw \oplus Ky \oplus Ku. \tag{3.15}$$

We claim that the function

$$u := \begin{cases} \frac{yz}{x}, & \text{if second normal form,} \\ \frac{yw}{z}, & \text{if third normal form,} \end{cases}$$

has the desired properties. Indeed, since its square

$$u^2 = \begin{cases} w(ax+1), & \text{if second normal form,} \\ (a_2 z + 1)(n_0 + n_1 x + w), & \text{if third normal form,} \end{cases}$$

lies in

$$H^0(\mathfrak{p}_1^{2e_1}) = K \oplus Kx \oplus Kx^2 \oplus Kz \oplus Kxz \oplus Kw \oplus Kxw \oplus Kzw,$$

and hence in $H^0(\mathfrak{p}^{2ee_1})$, it is clear that u belongs to $H^0(\mathfrak{p}^{ee_1})$. Now, one can see that 1, x, z, w, y, u are linearly independent over K because their squares 1, x^2, z^2, w^2, y^2, u^2 are linearly independent over K^2.

We finally show that if $e_1 = 2$ then $\dim H^0(\mathfrak{p}^e) < 3$. Note first that the assumption $e_1 = 2$ means that the coefficient of x^2 in the x-expansion of $w^2 + z$ lies in $K^2(a)$, say $a_2 = r_0^2 + r_1^2 a$ if item (ii) occurs or $a_2 = r_0^2 a^{-1} + r_1^2$ if item (iii) occurs. Since $H^0(\mathfrak{p}^e)$ is contained in $H^0(\mathfrak{p}^{ee_1})$, each element h of $H^0(\mathfrak{p}^e)$ may be written as $h = \alpha + \beta x + \theta z + \gamma w + \xi y + \zeta u$, so that h^2 lies in $H^0(\mathfrak{p}^{2e}) \cap F_1 = H^0(\mathfrak{p}_1^2) = K \oplus Kx \oplus Kz \oplus Kw$. If item (ii) occurs, then by looking at the expansion of h^2 we see that $\xi^2 + \zeta^2 a = \beta^2 + \theta^2 a + \gamma^2 a_2 = 0$, and hence that $\xi = \zeta = 0$, $\beta = \gamma r_0$, $\theta = \gamma r_1$ as $a \notin K^2$, so we conclude $h \in K \oplus K(r_0 x + r_1 z + w)$. Similarly, when item (iii) occurs we obtain $\xi^2 + \zeta^2 a_2 = \beta^2 + \theta^2 a + \gamma^2 a_2 a = 0$, and therefore $\zeta r_0 = 0$, $\xi = \zeta r_1$, $\beta = \gamma r_0$, $\theta = \gamma r_1$; since $r_0 \neq 0$ as $a_2 \notin K^2$, we conclude that $h \in K \oplus K(r_0 x + r_1 z + w)$. This completes the proof of the claim. □

As we have done before with the function fields whose normal forms we found, now we find criteria to decide when any two of the function fields in Theorem 3.9 are isomorphic over K.

Theorem 3.10. *The function fields in items* (i), (ii) *and* (iii) *in Theorem 3.9 are pairwise non-isomorphic, i.e., a function field from one item cannot be isomorphic to a function field from another item. Moreover,*

(i) *two function fields $F|K$ and $F'|K$ from item* (i) *with parameters a, c, m_1, m_0, n_0 and a', c', m_1', m_0', n_0' are isomorphic if and only if there exist constants $r_0, t_0, \mu_0, \mu_1, \mu_2$ in K with $\mu_2 \neq 0$ such that*

$$\begin{aligned} \mu_2^8 a' &= a, \\ \mu_2^{-8} c' &= c + r_0^2 a + r_0 + t_0^4, \\ \mu_2^2 n_0' &= n_0 + \mu_1^2, \\ \mu_2^6 m_1' &= m_1, \\ \mu_2^{-2} m_0' &= m_0 + r_0 m_1 + t_0^2 (n_0 + \mu_1^2) + t_0 + \mu_0^2; \end{aligned} \tag{3.16}$$

(ii) *two function fields $F|K$ and $F'|K$ from item* (ii) *with parameters a, a_2, a_0 and a', a_2', a_0' are isomorphic if and only if there exist constants $\mu_1, \mu_2, \mu_4, \mu_5$ in K with $(\mu_4, \mu_5) \neq (0,0)$ such that*

$$\begin{aligned} t_3^6 a_2' &= a_2 + t_1^2, \\ a_0' &= t_3^2 a_0 + t_3 \mu_4 \mu_5 + \mu_2^4 + \mu_5^4 a_2, \\ t_3^4 a' &= a, \end{aligned} \tag{3.17}$$

where $t_3 := \mu_4^2 + \mu_5^2 a \neq 0$ and $t_1 := t_3^{-1}(\mu_1^2 + \mu_2^2 a)$;

(iii) *two function fields $F|K$ and $F'|K$ from item* (iii) *with parameters a, c, a_2, n_0, n_1 and a', c', a_2', n_0', n_1' are isomorphic if and only if there exist constants $r_0, \mu_2, \mu_3, \mu_4, \mu_5$ in K with $(\mu_4, \mu_5) \neq (0,0)$ such that*

$$\begin{aligned} t_3^4 a' &= a, \\ t_3^{-2} c' &= t_3^2 (c + r_0^2 a + r_0) + \mu_5^4, \\ t_3^2 a_2' &= a_2 + t_2^2, \\ t_3^3 n_1' &= n_1, \\ n_0' &= t_3 (n_0 + r_0 n_1) + \mu_3^2 + \mu_4 \mu_5, \end{aligned} \tag{3.18}$$

where $t_3 := \mu_4^2 + \mu_5^2 a_2 \neq 0$ and $t_2 := t_3^{-1}(\mu_2^2 + \mu_3^2 a_2)$.

We remark that since $a \notin K^2$, the non-vanishing of $t_3 = \mu_4^2 + \mu_5^2 a$ in the second item is equivalent to the non-vanishing of the pair (μ_4, μ_5). An analogous remark applies to the third item.

Proof. Because of the condition on the divisor $\mathfrak{p}^e$ at the end of the statement of Theorem 3.9, it is clear that no function field from (i) is isomorphic to a function field from (ii) or (iii). Therefore, to prove the first part of the theorem we must verify that a function field from (ii) cannot be isomorphic to a function field from (iii).

Suppose for contradiction that there is a K-isomorphism $\sigma : F' \xrightarrow{\sim} F$ between a function field $F'|K$ from (iii), with parameters a', c', a'_2, n'_0, n'_1, and a function field $F|K$ from (ii), with parameters a, a_2, a_0. Since σ preserves the only singular primes of $F'|K$ and $F|K$, it induces isomorphisms $H^0(\mathfrak{p}_3^n) \xrightarrow{\sim} H^0(\mathfrak{p}_3'^n)$, $H^0(\mathfrak{p}_2^n) \xrightarrow{\sim} H^0(\mathfrak{p}_2'^n)$, $H^0(n\mathfrak{p}_1) \xrightarrow{\sim} H^0(\mathfrak{p}_1'^n)$, $H^0(\mathfrak{p}^n) \xrightarrow{\sim} H^0(\mathfrak{p}'^n)$. Thus it follows from (3.11), (3.12), (3.13) and (3.15) that there exist constants r_i, s_i, t_i, μ_i with $r_1, s_2, t_3 \neq 0$ and $(\mu_4, \mu_5) \neq (0,0)$ such that

$$\begin{aligned}
\sigma(x') &= r_0 + r_1 x,\\
\sigma(z') &= s_0 + s_1 x + s_2 z,\\
\sigma(w') &= t_0 + t_1 x + t_2 z + t_3 w,\\
\sigma(y') &= \mu_0 + \mu_1 x + \mu_2 z + \mu_3 w + \mu_4 y + \mu_5 u.
\end{aligned}$$

Applying σ to the equation $y'^2 = (n'_0 + n'_1 x' + w')z'$ and using the relations $z^2 = ax^2 + x$, $w^2 = a_2 x^2 + a_0 + z$, $y^2 = xw$, $u^2 = (ax+1)w$ we see that the coefficient of zw on the right must vanish, i.e., $s_2 t_3 = 0$, a contradiction. This proves that no function field from (ii) is isomorphic to a function field from (iii).

(i) We point out that for a given function field $F|K = K(x, z, w, y)|K$ from (i) the following holds

$$H^0(\mathfrak{p}_1) = K \oplus Kw. \tag{3.19}$$

To see this, it suffices to recall from the proof of Theorem 3.9 that $e_1 = 2$, $\dim H^0(\mathfrak{p}_1) = 2$, and that $w^2 = z$ lies in $K \oplus Kx \oplus Kz \oplus Kw = H^0(\mathfrak{p}_1^{e_1}) = H^0(\mathfrak{p}_1^2)$, i.e., $w \in H^0(\mathfrak{p}_1)$.

Suppose now that there is a K-isomorphism $\sigma : F' \xrightarrow{\sim} F$ between two function fields $F'|K$ and $F|K$ from (i), with parameters a', c', m'_1, m'_0, n'_0 and a, c, m_1, m_0, n_0, respectively. Since σ preserves the only singular primes of $F'|K$ and $F|K$, it induces isomorphisms $H^0(\mathfrak{p}_3^n) \xrightarrow{\sim} H^0(\mathfrak{p}_3'^n)$, $H^0(\mathfrak{p}_2^n) \xrightarrow{\sim} H^0(\mathfrak{p}_2'^n)$, $H^0(\mathfrak{p}_1^n) \xrightarrow{\sim} H^0(\mathfrak{p}_1'^n)$, $H^0(\mathfrak{p}^n) \xrightarrow{\sim} H^0(\mathfrak{p}'^n)$. Thus it follows from (3.11), (3.12), (3.14) and (3.19) that there exist constants r_i, s_i, t_i, μ_i with $r_1, s_2, t_1, \mu_2 \neq 0$ such that

$$\begin{aligned}
\sigma(x') &= r_1(r_0 + x),\\
\sigma(z') &= s_2(s_0 + s_1 x + z),\\
\sigma(w') &= t_1(t_0 + w),\\
\sigma(y') &= \mu_2(\mu_0 + \mu_1 w + y).
\end{aligned}$$

Applying σ to the equations $z'^2 = a'x'^2 + x' + c'$, $w'^2 = z'$, $y'^2 = m'_1 x' + m'_0 + n'_0 z' + w'$, and using the relations $z^2 = ax^2 + x + c$, $w^2 = z$, $y^2 = m_1 x + m_0 + n_0 z + w$, we obtain a system of ten equations

$$\begin{aligned}
0 &= r_1^2 a' + s_1^2 s_2^2 + s_2^2 a,\\
0 &= c' + r_0^2 r_1^2 a' + r_0 r_1 + s_0^2 s_2^2 + s_2^2 c,\\
0 &= s_2 n'_0 + \mu_1^2 \mu_2^2 + \mu_2^2 n_0,\\
0 &= r_1 m'_1 + s_1 s_2 n'_0 + \mu_2^2 m_1,\\
0 &= m'_0 + r_0 r_1 m'_1 + s_0 s_2 n'_0 + t_0 t_1 + \mu_0^2 \mu_2^2 + \mu_2^2 m_0,
\end{aligned}$$

$$
\begin{aligned}
0 &= s_1 s_2, \\
0 &= r_1 + s_2^2, \\
0 &= s_2 + t_1^2, \\
0 &= t_1 + \mu_2^2, \\
0 &= s_0 s_2 + t_0^2 t_1^2.
\end{aligned}
$$

We view the first five equations as a system of equations with coefficients in K and indeterminates in F'. We can resolve it, since $r_1, s_2 \neq 0$, and hence we obtain a', c', m_1', m_0', n_0' explicitly in terms of the constants a, c, m_1, m_0, n_0 of the function field $F|K$ and the constants r_i, s_i, t_i, μ_i of the automorphism σ. By eliminating the variables s_1, r_1, s_2, t_1, s_0, we obtain the relations in the statement of the theorem.

Conversely, if the constants $r_0, t_0, \mu_0, \mu_1, \mu_2 \in K$ satisfy these relations and $\mu_2 \neq 0$, then the substitutions

$$
x' \mapsto \mu_2^8(r_0 + x), \quad z' \mapsto \mu_2^4(t_0^2 + z), \quad w' \mapsto \mu_2^2(t_0 + w), \quad y' \mapsto \mu_2(\mu_0 + \mu_1 w + y),
$$

define a K-isomorphism $F' \to F$.

(ii) Suppose there is a K-isomorphism $\sigma : F' \xrightarrow{\sim} F$ between two function fields $F'|K$ and $F|K$ from (ii), with parameters a', a_2', a_0' and a, a_2, a_0, respectively. Since σ preserves the only singular primes of $F'|K$ and $F|K$, it induces isomorphisms $H^0(\mathfrak{p}_3^n) \xrightarrow{\sim} H^0(\mathfrak{p}_3'^n)$, $H^0(\mathfrak{p}_2^n) \xrightarrow{\sim} H^0(\mathfrak{p}_2'^n)$, $H^0(\mathfrak{p}_1^n) \xrightarrow{\sim} H^0(\mathfrak{p}_1'^n)$, $H^0(\mathfrak{p}^n) \xrightarrow{\sim} H^0(\mathfrak{p}'^n)$. Thus we see from (3.11), (3.12), (3.13) and (3.15) that there exist constants r_i, s_i, t_i, μ_i with $r_1, s_2, t_3 \neq 0$ and $(\mu_4, \mu_5) \neq (0, 0)$ such that

$$
\begin{aligned}
\sigma(x') &= r_0 + r_1 x, \\
\sigma(z') &= t_3(s_0 + s_1 x + s_2 z), \\
\sigma(w') &= t_3(t_0 + t_1 x + t_2 z + w), \\
\sigma(y') &= t_3^2(\mu_0 + \mu_1 x + \mu_2 z + \mu_3 w + \mu_4 y + \mu_5 u).
\end{aligned}
$$

Applying σ to the equations $z'^2 = a' x'^2 + x'$, $w'^2 = a_2' x'^2 + a_0' + z'$, $y'^2 = x' w'$, and using the relations $z^2 = a x^2 + x$, $w^2 = a_2 x^2 + a_0 + z$, $y^2 = x w$, $u^2 = (a x + 1) w$ we obtain a system of fourteen equations

$$
\begin{aligned}
0 &= r_1^2 a_2' + t_1^2 t_3^2 + t_2^2 t_3^2 a + t_3^2 a_2, \\
0 &= a_0' + r_0^2 a_2' + s_0 t_3 + t_0^2 t_3^2 + t_3^2 a_0, \\
0 &= r_1^2 a' + s_1^2 t_3^2 + s_2^2 t_3^2 a, \\
0 &= r_1 t_3 t_2, \\
0 &= t_3^4 \mu_3^2 + r_0 t_2 t_3, \\
0 &= t_3 s_1 + t_2^2 t_3^2, \\
0 &= t_3 s_2 + t_3^2, \\
0 &= r_1 + s_2^2 t_3^2, \\
0 &= r_1 t_3 + t_3^4 \mu_4^2 + t_3^4 \mu_5^2 a, \\
0 &= t_3 r_0 + t_3^4 \mu_5^2, \\
0 &= r_1 t_3 t_1 + t_3^4 \mu_1^2 + t_3^4 \mu_2^2 a + t_3^4 \mu_3^2 a_2, \\
0 &= r_1 t_3 t_0 + r_0 t_1 t_3 + t_3^4 \mu_2^2, \\
0 &= t_3^2 s_0^2 + r_0^2 a' + r_0, \\
0 &= t_3^4 \mu_0^2 + r_0 t_0 t_3 + t_3^4 \mu_3^2 a_0.
\end{aligned}
$$

We view the first three equations as a system of equations with coefficients in K and indeterminates in F'. We can resolve it, since $r_1 \neq 0$, and so we get a_2', a_0', a' in terms of the constants a_2, a_0, a of the function field $F|K$ and the constants r_i, s_i, t_i, μ_i of the automorphism σ.

The next five equations tell us that $t_2 = \mu_3 = s_1 = 0$, $s_2 = t_3$, $r_1 = t_3^4$, while the ensuing three equations tell us that t_3, r_0, t_1 and t_0 may be eliminated. Cancelling out the power of $\mu_4^2+\mu_5^2 a \neq 0$ appearing in the next equation we eliminate s_0, and then we can use the last equation to eliminate μ_0. The system we search for consists of the equations that remain.

Conversely, if there are constants $\mu_1, \mu_2, \mu_4, \mu_5 \in K$ with $(\mu_4, \mu_5) \neq (0,0)$ satisfying the three equations of the system, then the substitutions

$$x' \mapsto t_3^3\mu_5^2 + t_3^4 x, \quad z' \mapsto t_3(\mu_4\mu_5 + t_3 z), \quad w' \mapsto t_3(t_0 + t_1 x + w), \quad y' \mapsto t_3^2(\mu_0 + \mu_1 x + \mu_2 z + \mu_4 y + \mu_5 u)$$

where $t_3 := \mu_4^2+\mu_5^2 a \neq 0$, $t_1 := t_3^{-1}(\mu_1^2+\mu_2^2 a)$, $t_0 := t_3^{-1}(t_1\mu_5^2+\mu_2^2)$, $\mu_0 := t_3^{-1}(\mu_1\mu_5^2+\mu_2\mu_4\mu_5)$, define a K-isomorphism $F' \to F$.

(iii) Suppose finally that there is a K-isomorphism $\sigma : F' \xrightarrow{\sim} F$ between two function fields $F'|K$ and $F|K$ from (iii), with parameters a', c', a_2', n_0', n_1' and a, c, a_2, n_0, n_1, respectively. Since σ preserves the only singular primes of $F'|K$ and $F|K$, it induces isomorphisms $H^0(\mathfrak{p}_3^n) \xrightarrow{\sim} H^0(\mathfrak{p}_3'^n)$, $H^0(\mathfrak{p}_2^n) \xrightarrow{\sim} H^0(\mathfrak{p}_2'^n)$, $H^0(\mathfrak{p}_1^n) \xrightarrow{\sim} H^0(\mathfrak{p}_1'^n)$, $H^0(\mathfrak{p}^n) \xrightarrow{\sim} H^0(\mathfrak{p}'^n)$. Thus we see as in the previous case that there exist constants r_i, s_i, t_i, μ_i with $r_1, s_2, t_3 \neq 0$ and $(\mu_4, \mu_5) \neq (0,0)$ such that

$$\begin{aligned}
\sigma(x') &= r_1(r_0 + x),\\
\sigma(z') &= s_0 + s_1 x + s_2 z,\\
\sigma(w') &= t_3(t_0 + t_1 x + t_2 z + w),\\
\sigma(y') &= t_3(\mu_0 + \mu_1 x + \mu_2 z + \mu_3 w + \mu_4 y + \mu_5 u).
\end{aligned}$$

Applying σ to the equations $z'^2 = a'x'^2 + x' + c'$, $w'^2 = a_2' z'^2 + z'$, $y'^2 = (n_0' + n_1' x' + w')z'$, and using the relations $z^2 = ax^2 + x + c$, $w^2 = a_2 z^2 + z$, $y^2 = (n_0 + n_1 x + w)z$, $u^2 = (a_2 z + 1)(n_0 + n_1 x + w)$ we obtain a system of fifteen equations

$$\begin{aligned}
0 &= r_1^2 a' + s_1^2 + s_2^2 a,\\
0 &= c' + r_0^2 r_1^2 a' + r_0 r_1 + s_0^2 + s_2^2 c,\\
0 &= s_2^2 a_2' + s_1 + t_2^2 t_3^2 + t_3^2 a_2,\\
0 &= r_1 s_2 n_1' + s_1 t_2 t_3 + s_2 t_1 t_3 + t_3^2\mu_4^2 n_1 + t_3^2\mu_5^2 a_2 n_1,\\
0 &= s_2 n_0' + r_0 r_1 s_2 n_1' + s_0 t_2 t_3 + s_2 t_0 t_3 + t_3^2\mu_3^2 + t_3^2\mu_4^2 n_0 + t_3^2\mu_5^2 a_2 n_0,\\
0 &= t_3 s_1,\\
0 &= r_1 + s_2^2,\\
0 &= s_2 + t_3^2,\\
0 &= t_3 s_0 + t_3^2\mu_5^2,\\
0 &= t_3^2 t_1^2 + s_1^2 a_2' + s_2^2 a a_2' + t_2^2 t_3^2 a + t_3^2 a a_2,\\
0 &= t_3 s_2 + t_3^2\mu_4^2 + t_3^2\mu_5^2 a_2,\\
0 &= s_2 t_3 t_2 + r_0 r_1 s_1 n_1' + r_1 s_0 n_1' + s_0 t_1 t_3 + s_1 t_0 t_3 + s_1 n_0' + t_3^2\mu_2^2 + t_3^2\mu_3^2 a_2 + t_3^2\mu_5^2 n_1,\\
0 &= t_3^2\mu_1^2 + r_1 s_1 n_1' + s_1 t_1 t_3 + s_2 t_2 t_3 a + t_3^2\mu_2^2 a + t_3^2\mu_3^2 a a_2,\\
0 &= t_3^2 t_0^2 + s_0^2 a_2' + s_0 + s_2^2 c a_2' + t_2^2 t_3^2 c + t_3^2 c a_2,\\
0 &= t_3^2\mu_0^2 + r_0 r_1 s_0 n_1' + s_0 t_0 t_3 + s_0 n_0' + s_2 t_2 t_3 c + t_3^2\mu_2^2 c + t_3^2\mu_3^2 c a_2 + t_3^2\mu_5^2 n_0.
\end{aligned}$$

Viewing the first five equations as a system of equations with coefficients in K and indeterminates in F', we can resolve it, since $r_1, s_2 \neq 0$, and hence we can express a', c', a_2', n_0', n_1' explicitly in terms of the constants a, c, a_2, n_0, n_1 of the function field $K|k$ and the constants r_i, s_i, t_i, μ_i of the automorphism σ.

The next five equations tell us that $s_1 = 0$, $r_1 = t_3^4$, $s_2 = t_3^2$, $s_0 = t_3\mu_5^2$, $t_1 = 0$, while the ensuing two equations tell us that t_3 and t_2 may be eliminated. Cancelling out the powers of $\mu_4^2 + \mu_5^2 a \neq 0$ appearing in the last three equations we eliminate μ_1, t_0 and μ_0. The system we look for consists of the five equations that remain.

Conversely, if there are constants $r_0, \mu_2, \mu_3, \mu_4, \mu_5 \in K$ with $(\mu_4, \mu_5) \neq (0,0)$ satisfying the five equations of the system, then the substitutions

$$x' \mapsto t_3^4(r_0 + x), \quad z' \mapsto t_3\mu_5^2 + t_3^2 z, \quad w' \mapsto t_3(t_0 + t_2 z + w), \quad y' \mapsto t_3(\mu_0 + \mu_2 z + \mu_3 w + \mu_4 y + \mu_5 u),$$

where $t_3 := \mu_4^2 + \mu_5^2 a_2 \neq 0$, $t_2 := t_3^{-1}(\mu_2^2 + \mu_3^2 a_2)$, $t_0 := t_3^{-1}(t_2\mu_5^2 + \mu_4\mu_5)$, $\mu_0 := t_3^{-1}(\mu_2\mu_5^2 + \mu_3\mu_4\mu_5)$, define a k-isomorphism $K' \to K$. $\square$

We mention some consequences of Theorem 3.10.

Suppose first that $F|K$ is a function field as in Theorem 3.9 (i), with parameters a, c, m_1, m_0, n_0. Then the multiplicative classes $a \mod (K^*)^8$ and $m_1 \mod (K^*)^6$ are invariants of $F|K$.

If $m_1 \neq 0$ then we can normalize $m_0 = 0$, and therefore the constant r_0 in (3.16) can be eliminated.

If $n_0 \in K^2$ then we can normalize $n_0 = 0$, and in this case the constant t_0 in (3.16) can be used to normalize $m_0 = 0$. Thus in this situation the isomorphisms $\sigma : F' \xrightarrow{\sim} F$ between another such function field $F'|K$, with parameters $a', c', m_1', m_0' = 0, n_0' = 0$, are given by the substitutions

$$x' \mapsto \mu_2^8(r_0 + x), \quad z' \mapsto \mu_2^4(t_0^2 + z), \quad w' \mapsto \mu_2^2(t_0 + w), \quad y' \mapsto \mu_2(\mu_0 + y),$$

where the constants $r_0, \mu_0, \mu_2 \in K$ and $t_0 := r_0 m_1 + \mu_0^2$ are such that $\mu_2 \neq 0$ and

$$\begin{aligned} \mu_2^8 a' &= a, \\ \mu_2^{-8} c' &= c + r_0^2 a + r_0 + t_0^4, \\ \mu_2^6 m_1' &= m_1. \end{aligned}$$

If K is separably closed then $c = 0$ may be normalized, and in this case the second equation in (3.16) becomes $r_0^2 a + r_0 + t_0^4 = 0$. Analogously, one may normalize $m_0 = 0$, and then the last equation in (3.16) becomes $r_0 m_1 + t_0^2(n_0 + \mu_1^2) + t_0 + \mu_0^2 = 0$. We cannot guarantee, however, that both of these normalizations can be performed at the same time.

Suppose next that $F|K$ is a function field from Theorem 3.9 (ii), with parameters a, a_2, a_0. Then the multiplicative class $a \mod (K^*)^4$ is an invariant of $F|K$.

Suppose finally that $F|K$ is a function field from Theorem 3.9 (iii), with parameters a, c, a_2, n_0, n_1. Then the multiplicative classes $a \mod (K^*)^4$ and $n_1 \mod (K^*)^3$ are invariants of $F|K$.

If $n_1 \neq 0$ then we can normalize $n_0 = 0$, and therefore the constant r_0 in (3.18) can be eliminated.

If K is separably closed then we may normalize $c = 0$.

We end this section by describing the group $\mathrm{Aut}(F|K)$ of automorphisms of the function fields $F|K$ in Theorem 3.9. Suppose first that $F|K$ is given as in Theorem 3.9 (i), with parameters a, c, m_1, m_0, n_0. By the proof of Theorem 3.10, any automorphism of $F|K$ is defined by a substitution of the form

$$x \mapsto \mu_2^8(r_0 + x), \quad z \mapsto \mu_2^4(t_0^2 + z), \quad w \mapsto \mu_2^2(t_0 + w), \quad y \mapsto \mu_2(\mu_0 + \mu_1 w + y),$$

where the constants $r_0, t_0, \mu_0, \mu_1 \in K$ and $\mu_2 \in K \setminus \{0\}$ satisfy the relations

$$\begin{aligned}
\mu_2^8 a &= a, \\
\mu_2^{-8} c &= c + r_0^2 a + r_0 + t_0^4, \\
\mu_2^2 n_0 &= n_0 + \mu_1^2, \\
\mu_2^6 m_1 &= m_1, \\
\mu_2^{-2} m_0 &= m_0 + r_0 m_1 + t_0^2(n_0 + \mu_1^2) + t_0 + \mu_0^2.
\end{aligned}$$

Note that $\mu_2 = 1$ since $a \neq 0$, and so μ_1, $r_0^2 a + r_0 + t_0^4$ and $r_0 m_1 + t_0^2 n_0 + t_0 + \mu_0^2$ are zero. Therefore, the group $\mathrm{Aut}(F|K)$ of automorphisms of $F|K$ is given by the substitutions

$$x \mapsto r_0 + x, \quad z \mapsto t_0^2 + z, \quad w \mapsto t_0 + w, \quad y \mapsto \mu_0 + y,$$

where the constants $r_0, t_0, \mu_0 \in K$ satisfy the condition $r_0^2 a + r_0 + t_0^4 = r_0 m_1 + t_0^2 n_0 + t_0 + \mu_0^2 = 0$.

Assume next that $F|K$ has a normal form as in Theorem 3.9 (ii), with parameters a, a_2, a_0. An automorphism of $F|K$ is defined by a substitution of the form

$$x \mapsto t_3^3 \mu_5^2 + t_3^4 x, \quad y \mapsto t_3^2(\mu_0 + \mu_1 x + \mu_2 z + \mu_4 y + \mu_5 u).$$

where the constants $\mu_1, \mu_2, \mu_3, \mu_4 \in K$ are such that $(\mu_4, \mu_5) \neq (0, 0)$ and

$$\begin{aligned}
t_3^6 a_2 &= a_2 + t_1^2, \\
a_0 &= t_3^2 a_0 + t_3 \mu_4 \mu_5 + \mu_2^4 + \mu_5^4 a_2, \\
t_3^4 a &= a,
\end{aligned}$$

and where $t_3 := \mu_4^2 + \mu_5^2 a \neq 0$, $t_1 := t_3^{-1}(\mu_1^2 + \mu_2^2 a)$, and $\mu_0 := t_3^{-1}(\mu_1 \mu_5^2 + \mu_2 \mu_4 \mu_5)$. Notice that $t_3 = 1$ because $a \neq 0$, and so $\mu_4 = 1$, $\mu_5 = 0$ as $a \notin K^2$. Thus $t_1 = 0$, which means that $\mu_1 = \mu_2 = 0$ as $a \notin K^2$. This shows that the group $\mathrm{Aut}(F|K)$ is trivial.

Suppose finally that $F|K$ is defined as in Theorem 3.9 (iii), with parameters a, c, a_2, n_0, c_1. An automorphism of $F|K$ is given by a substitution of the form

$$x \mapsto t_3^4(r_0 + x), \quad y \mapsto t_3(\mu_0 + \mu_2 z + \mu_3 w + \mu_4 y + \mu_5 u).,$$

where the constants $\mu_1, \mu_2, \mu_3, \mu_4 \in K$ are such that $(\mu_4, \mu_5) \neq (0, 0)$ and

$$\begin{aligned}
t_3^4 a &= a, \\
t_3^{-2} c &= t_3^2(c + r_0^2 a + r_0) + \mu_5^4, \\
t_3^2 a_2 &= a_2 + t_2^2, \\
t_3^3 n_1 &= n_1, \\
n_0 &= t_3(n_0 + r_0 n_1) + \mu_3^2 + \mu_4 \mu_5,
\end{aligned}$$

and where $t_3 := \mu_4^2 + \mu_5^2 a_2 \neq 0$, $t_2 := t_3^{-1}(\mu_2^2 + \mu_3^2 a_2)$ and $\mu_0 := t_3^{-1}(\mu_2 \mu_5^2 + \mu_3 \mu_4 \mu_5)$. Note that $t_3 = 1$ since $a \neq 0$, and so $\mu_4 = 1$, $\mu_5 = 0$ as $a \notin k^2$. Thus $t_2 = 0$, which means $\mu_2 = \mu_3 = 0$ as $a \notin k^2$, and it follows that $r_0^2 a + r_0 = r_0 n_1 = 0$. Therefore, the group $\mathrm{Aut}(F|K)$ of automorphisms of $F|K$ are given by the substitutions

$$x \mapsto r_0 + x, \quad y \mapsto y,$$

where the constant $r_0 \in K$ satisfies the condition $r_0^2 a + r_0 = r_0 n_1 = 0$. If $n_1 \neq 0$ then $\mathrm{Aut}(F|K)$ is trivial. And if $n_1 = 0$, then $\mathrm{Aut}(F|K)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

3.3 Differentials and regular complete models

In this section we study the space of differentials of the function fields we have examined in the previous sections. We also find their projective models in most of the cases.

Recall that a differential ω of a function field $F|K$ is called *exact* if it can be written as $\omega = df$ for some function $f \in F$.

Proposition 3.11. *Let x be a separating variable of a function field $F|K$ of characteristic two. Then the space of exact differentials of $F|K$ is given by $F_1 dx$.*

Proof. Since x does not belong to F_1 we have $F = F_1 \oplus F_1 x$. The result now follows by observing that $df = 0$ for each function f in $F_1 = KF^2$. □

We denote by C the *canonical field* of $F|K$, i.e., the subfield of $F|K$ generated by the quotients of the non-zero holomorphic differentials. We also consider the subfield E of $C|K$ generated by the quotients of the non-zero exact holomorphic differentials, and call it the *pseudo-canonical field* of $F|K$.

We recall that a function field $F|K$ is hyperelliptic if and only if the canonical field $C|K$ is a quadratic subfield of $F|K$ of genus 0.

Function fields of Theorem 3.4

Let $F|K$ be a function field as in Theorem 3.4 (i) in normal form

$$y^2 = a_0 + x + a_2 x^2 + a_4 x^4 + a_6 x^6 + a_8 x^8,$$

where $a_0, a_2, a_4, a_6 \in K$ and $a_8 \in K \setminus K^2$. Recall that the function x has a pole at the only singular prime $\mathfrak{p}$ of $F|K$, and that the restricted prime $\mathfrak{p}_1$ of $F_1|K$ is rational with local parameter x^{-1}.

By Theorem 2.6, we know that

$$v_{\mathfrak{p}}(dy) = \frac{2\delta(\mathfrak{p}) + v_{\mathfrak{p}_1}(dy^2)}{\deg \mathfrak{p}} = \frac{6-2}{2} = 2,$$

where the equality $v_{\mathfrak{p}_1}(dy^2) = -2$ follows from the fact that the function x^{-1} is a local parameter of the prime $\mathfrak{p}_1$. Furthermore, for any other prime $\mathfrak{q} \neq \mathfrak{p}$ we have $v_{\mathfrak{q}}(y) \geq 0$, which implies that $v_{\mathfrak{q}}(dy) \geq 0$. Therefore, since the divisor $\mathfrak{p}^2$ has degree $4 = 2g - 2$ one has in fact that

$$\operatorname{div}(dy) = \mathfrak{p}^2.$$

Note that $\operatorname{div}_\infty(x) = \mathfrak{p}$. The three differentials

$$dy,\ x\,dy,\ x^2 dy$$

are then holomorphic and linearly independent over K. Since $F|K$ has genus $g = 3$, this shows that they constitute a basis of the space of holomorphic differentials of $F|K$. Moreover, it follows from Proposition 3.11 that every holomorphic differential is exact.

In particular, the canonical and pseudocanonical fields of $F|K$ coincide, and in fact

$$C = E = K(x) = F_1.$$

It follows that $F|K$ is hyperelliptic.

We now find the regular complete model C of $F|K$. Recall from (3.3) that the vector space of global sections of the bi-canonical divisor $\mathfrak{p}^4$, which has degree $8 = 2g + 2$, is given by

$$H^0(\mathfrak{p}^4) = K \oplus Kx \oplus Kx^2 \oplus Kx^3 \oplus Kx^4 \oplus Ky.$$

Since $\overline{C} = C \otimes_K \overline{K}$ is an integral complete hyperelliptic curve of arithmetic genus $g = 3$, it follows from [Stö99, Theorem 2.1] that the global sections of the divisor $\mathfrak{p}^4$ define an embedding

$$(1 : x : x^2 : x^3 : x^4 : y) : \overline{C} \hookrightarrow \mathbb{P}^5(\overline{K}),$$

whose image is contained in the surface

$$S := \left\{ (u_0 : u_1 : u_2 : u_3 : u_4 : v) \;\middle|\; \operatorname{rank} \begin{pmatrix} u_1 & u_2 & u_3 & u_4 \\ u_0 & u_1 & u_2 & u_3 \end{pmatrix} < 2 \right\} \subseteq \mathbb{P}^5(\overline{K}).$$

This means that the extended curve $\overline{C}$ can be realized as a curve on S. Such realization is obtained by intersecting S with the hypersurface in $\mathbb{P}^5(\overline{K})$ cut out by the equation

$$v^2 = a_0u_0^2 + u_0u_1 + a_2u_1^2 + a_4u_2^2 + a_6u_3^2 + a_8u_4^2,$$

so in particular it does not contain the vertex $Q := (0 : 0 : 0 : 0 : 0 : 1)$ of S.

We give a description of $\overline{C}$ in affine charts. The cone S is the union of the projective lines

$$L_u = \left\{ (1 : u : u^2 : u^3 : u^4 : v) \mid (u, v) \in \overline{K}^2 \right\} \cup \{Q\} \qquad (u \in \overline{K})$$

and

$$L_\infty = \left\{ (0 : 0 : 0 : 0 : 1 : v) \mid v \in \overline{K} \right\} \cup \{Q\},$$

where the vertex Q is their only common point. The smooth locus $S\backslash\{Q\}$ of S is described by the atlas consisting of the charts

$$U := S \setminus L_\infty = \left\{ (1 : u : u^2 : u^3 : u^4 : v) \mid (u, v) \in \overline{K}^2 \right\} \xrightarrow{\sim} \overline{K}^2$$

and

$$\breve{U} := S \setminus L_0 = \left\{ (\breve{u}^4 : \breve{u}^3 : \breve{u}^2 : \breve{u} : 1 : \breve{v}) \mid (\breve{u}, \breve{v}) \in \overline{K}^2 \right\} \xrightarrow{\sim} \overline{K}^2.$$

In the first chart U the curve $\overline{C}$ is cut out by the quadratic equation

$$v^2 = a_0 + u + a_2u^2 + a_4u^4 + a_6u^6 + a_8u^8,$$

whereas in the second chart $\breve{U}$ it is defined by the quadratic equation

$$\breve{v}^2 = a_8 + a_6\breve{u}^2 + a_4\breve{u}^4 + a_2\breve{u}^6 + \breve{u}^7 + a_0\breve{u}^8.$$

The point corresponding to the pole $\mathfrak{p}$ of x, namely $(0 : 0 : 0 : 0 : 1 : a_8^{1/2})$, is the only singular point of $\overline{C}$. It has singularity degree 3.

We conclude that the curve C is equal to the intersection of the surface

$$\left\{ (u_0 : u_1 : u_2 : u_3 : u_4 : v) \;\middle|\; \operatorname{rank} \begin{pmatrix} u_1 & u_2 & u_3 & u_4 \\ u_0 & u_1 & u_2 & u_3 \end{pmatrix} < 2 \right\}$$

and the hypersurface cut out by the equation

$$v^2 = a_0u_0^2 + u_0u_1 + a_2u_1^2 + a_4u_2^2 + a_6u_3^2 + a_8u_4^2.$$

Remark 3.12. One can see directly that the embedded curve, i.e., the image of $\overline{C}$ under the embedding $\overline{C} \hookrightarrow S$, is rational and has a unique singular point. One can also verify directly that this point has singularity degree 3 (e.g., by performing blowups), and hence that the curve has arithmetic genus 3.

Now let $F|K$ be a function field as in Theorem 3.4 (ii) in normal form

$$\begin{aligned} z^2 &= a_0 + x + a_2x^2, \\ y^2 &= b_2x^2 + b_3x^3 + b_4x^4 + z, \end{aligned}$$

where $a_0, b_2, b_3, b_4 \in K$ and $a_2 \in K \setminus K^2$. Recall that the function x has a pole at the only singular prime $\mathfrak{p}$ of $F|K$, and that the restricted prime $\mathfrak{p}_2$ of $F_2|K$ is rational.

Applying [BS87, Theorem 2.7] we deduce that

$$v_{\mathfrak{p}}(dy) = \frac{c_{\mathfrak{p}} + v_{\mathfrak{p}_2}(dy^4)}{\deg \mathfrak{p}} = \frac{6-2}{\deg \mathfrak{p}} = e,$$

where e denotes the ramification index of $\mathfrak{p}$ over F_1. Moreover, for any other prime $\mathfrak{q} \neq \mathfrak{p}$ we have $v_{\mathfrak{q}}(y) \geq 0$, and hence $v_{\mathfrak{q}}(dy) \geq 0$. Therefore, since the divisor $\mathfrak{p}^e$ has degree $4 = 2g - 2$ we conclude that

$$\operatorname{div}(dy) = \mathfrak{p}^e.$$

As the pole divisors of both the functions x and z are equal to $\mathfrak{p}^e$, it follows that the three differentials

$$dy,\ x\,dy\ , z\,dy$$

form a basis of the space of holomorphic differentials of $F|K$. In addition, every holomorphic differential is exact by Proposition 3.11. We thus see as in the previous case that the canonical and pseudocanonical fields of $F|K$ coincide with the first Frobenius pullback, that is,

$$C = E = K(x, z) = F_1.$$

In particular, the function field $F|K$ is clearly hyperelliptic.

We now find the regular complete model C of $F|K$. Recall from (3.6) that the vector space of global sections of the bi-canonical divisor $\mathfrak{p}^{2e}$, which has degree $8 = 2g + 2$, is given by

$$H^0(\mathfrak{p}^{2e}) = K \oplus Kx \oplus Kx^2 \oplus Kz \oplus Kxz \oplus Ky,$$

As $\overline{C} = C \otimes_K \overline{K}$ is an integral complete hyperelliptic curve of arithmetic genus $g = 3$, the generators of the ring $H^0(\mathfrak{p}^{2e})$ define an embedding

$$(1 : x : x^2 : z : xz : y) : \overline{C} \longrightarrow \mathbb{P}^5(\overline{K}),$$

and so the extended curve $\overline{C}$ can be realized as a curve on the threefold

$$S' := \left\{ (u_0 : u_1 : u_2 : u_3 : u_4 : v) \;\middle|\; \operatorname{rank} \begin{pmatrix} u_1 & u_2 & u_4 \\ u_0 & u_1 & u_3 \end{pmatrix} < 2 \right\}$$

in the 5-dimensional projective space $\mathbb{P}^5(\overline{K})$. This curve may be obtained by intersecting S' with the hypersurfaces cut out by the equations

$$\begin{aligned} u_0u_3 &= v^2 + b_2u_1^2 + b_3u_1u_2 + b_4u_2^2, \\ u_3^2 &= a_0u_0^2 + u_0u_1 + a_2u_1^2, \\ u_4^2 &= a_0u_1^2 + u_1u_2 + a_2u_2^2, \end{aligned}$$

so in particular it does not contain the vertex $Q' := (0:0:0:0:0:1) \in S$.

We provide a description of $\overline{C}$ in affine charts. The set $S' \setminus \{Q'\}$ can be described by the affine charts

$$\begin{aligned}
U_0 &:= \{\, (1:u:u^2:w:uw:v) \mid u,w,v \in \overline{K} \,\} \xrightarrow{\sim} \mathbb{A}^3, \\
U_2 &:= \{\, (u^2:u:1:uw:w:v) \mid u,w,v \in \overline{K} \,\} \xrightarrow{\sim} \mathbb{A}^3, \\
U_3 &:= \{\, (w:uw:u^2w:1:u:v) \mid w,u,v \in \overline{K} \,\} \xrightarrow{\sim} \mathbb{A}^3, \\
U_4 &:= \{\, (wu^2:wu:w:u:1:v) \mid w,u,v \in \overline{K} \,\} \xrightarrow{\sim} \mathbb{A}^3.
\end{aligned}$$

Note that $\overline{C}$ is contained in the union of the charts U_0 and U_2. In the first chart U_0 the curve $\overline{C}$ is given by the equations

$$w = v^2 + b_2u^2 + b_3u^3 + b_4u^4 \quad \text{and} \quad w^2 = a_0 + u + a_2u^2,$$

so we may view $\overline{C}$ in U_0 as the plane curve in $\mathbb{A}^2$ cut out by the equation

$$v^4 = a_0 + u + a_2u^2 + b_2u^4 + b_3u^6 + b_4u^8,$$

which is clearly smooth. In the second chart U_2 the curve $\overline{C}$ is given by

$$v^2 = u^3w + b_2u^2 + b_3u + b_4 \quad \text{and} \quad w^2 = a_0u^2 + u + a_2;$$

it can be seen that this curve is isomorphic to the plane curve in $\mathbb{A}^2$ defined by the equation

$$v^2 = (w + a_2^{1/2})w^6.$$

The point corresponding to the pole $\mathfrak{p}$ of x, namely $(0:0:1:0:a_2^{1/2}:b_4^{1/2})$, is the only singular point of $\overline{C}$. It has singularity degree 3.

We conclude that the curve C is equal to the intersection of the threefold

$$\left\{ (u_0:u_1:u_2:u_3:u_4:v) \;\middle|\; \operatorname{rank}\begin{pmatrix} u_1 & u_2 & u_4 \\ u_0 & u_1 & u_3 \end{pmatrix} < 2 \right\}$$

and the hypersurfaces cut out by the equations

$$\begin{aligned}
u_0u_3 &= v^2 + b_2u_1^2 + b_3u_1u_2 + b_4u_2^2, \\
u_3^2 &= a_0u_0^2 + u_0u_1 + a_2u_1^2, \\
u_4^2 &= a_0u_1^2 + u_1u_2 + a_2u_2^2.
\end{aligned}$$

An observation similar to Remark 3.12 applies also in this case. In other words, one can deduce the properties of the embedded curve by using extrinsic methods (i.e., the Jacobian criterion, blowups, etc.).

Function fields of Theorem 3.7

Let $F|K$ be a function field from Theorem 3.7 (i) with normal form

$$y^4 = a_0 + x + a_2x^2 + a_4x^4,$$

where $a_0, a_2 \in K$ and $a_4 \in K \setminus K^2$. Recall that the function x has a pole at the only singular prime $\mathfrak{p}$ of $F|K$, and that the restricted prime $\mathfrak{p}_2$ of the second Frobenius pullback $F_2|K$ is rational. Recall also that $\mathfrak{p}$ is unramified over F_2.

By Theorem 2.6, we know that

$$v_{\mathfrak{p}}(dy) = \frac{2\delta(\mathfrak{p}) + v_{\mathfrak{p}_2}(dy^4)}{\deg \mathfrak{p}} = \frac{6-2}{4} = 1.$$

Moreover, for each $\mathfrak{q} \neq \mathfrak{p}$ we have $v_{\mathfrak{q}}(y) \geq 0$, and hence $v_{\mathfrak{q}}(dy) \geq 0$. Because $\mathfrak{p}$ has degree $4 = 2g-2$, this means that $\operatorname{div}(dy) = \mathfrak{p}$, and we see again that the divisor $\mathfrak{p}$ is canonical. Since $H^0(\mathfrak{p}) = K \oplus Kx \oplus Ky$ by (3.9), we conclude that the three differentials

$$dy,\ x\,dy,\ y\,dy$$

form a basis of the space of holomorphic differentials. Clearly, the two differentials

$$dy,\ xdy$$

constitute a basis of the space of exact holomorphic differentials.

The previous considerations let us find the canonical and pseudocanonical fields of $F|K$.

$$\begin{aligned} C &= K(x,y) = F, \\ E &= K(x) = F_2. \end{aligned}$$

In particular, the function field $F|K$ is non-hyperelliptic and the plane projective quartic

$$Y^4 = a_0 Z^4 + XZ^3 + a_2 X^2 Z^2 + a_4 X^4$$

defined over K is its canonical model. [2]

Now we would like to study the holomorphic differentials of a function field $F|K$ from Theorem 3.7 (ii). Recall that $F|K$ is defined by the equations

$$z^2 = c(x)A(x) \quad \text{and} \quad y^2 = c(x)(B(x) + z),$$

where the polynomials $c(x)$, $A(x)$ and $B(x)$ are given by

$$\begin{aligned} c(x) &= c_0 + c_1 x + x^2, \\ A(x) &= (c_0 A_2 + c_1^{-1}) + c_1 A_2 x + A_2 x^2 = A_2 c(x) + c_1^{-1}, \\ B(x) &= B_0 + B_1 x, \end{aligned}$$

and where the constants $c_0, c_1, A_2, B_0, B_1 \in K$ satisfy the conditions $c_1 \neq 0$ and $A_2 \notin K^2$. Recall as well that the only singular prime $\mathfrak{p}$ of $F|K$ is unramified over F_2, and that its restriction $\mathfrak{p}_2$ to F_2 is rational with local parameter x^{-1}.

We find the divisor of dy. In fact, we claim that

$$\operatorname{div}(dy) = \operatorname{div}_0\big(c(x)\big)^{1/2}.$$

Indeed, by making a quadratic separable extension of K if necessary, we may assume that the two roots of the polynomial $c(x)$ lie in K. Then the function $c(x) \in F$ has two zeros, say $\mathfrak{q}'$ and $\mathfrak{q}''$, and

$$\begin{aligned} \operatorname{div}(c(x)) &= (\mathfrak{q}')^{e'e'_1} (\mathfrak{q}'')^{e''e''_1} \mathfrak{p}^{-2} \\ &= (\mathfrak{q}')^{2e'} (\mathfrak{q}'')^{2e''} \mathfrak{p}^{-2}, \end{aligned}$$

[2] Here the term *canonical model* refers to the regular complete model C of the function field $F|K$. The word *canonical* is employed because C is obtained from the vector space of global sections $H^0(\mathfrak{p}) = K \oplus Kx \oplus Ky$ of the *canonical* divisor $\mathfrak{p}$ of $F|K$.

where e', e'' and $e'_1 = e''_1 = 2$ are the ramification indices of $\mathfrak{q}', \mathfrak{q}''$ and $\mathfrak{q}'_1, \mathfrak{q}''_1$ over F_1 and F_2 respectively. By applying Theorem 2.6 we see that

$$\begin{aligned} v_{\mathfrak{p}}(dy) &= \frac{2\delta(\mathfrak{p}) + v_{\mathfrak{p}_2}(dy^4)}{\deg \mathfrak{p}} = \frac{6 + v_{\mathfrak{p}_2}(c(x)^2 dx)}{4} = 0, \\ v_{\mathfrak{q}'}(dy) &= \frac{2\delta(\mathfrak{q}') + v_{\mathfrak{q}'_2}(dy^4)}{\deg \mathfrak{q}'} = \frac{0+2}{\deg \mathfrak{q}'} = e', \end{aligned}$$

and similarly $\mathfrak{q}''(dy) = e''$. Since the divisor $(\mathfrak{q}')^{e'}(\mathfrak{q}'')^{e''}$ has degree $\deg \mathfrak{p} = 4 = 2g-2$ by the product formula for function fields, and since for any prime $\mathfrak{q} \neq \mathfrak{p}$ we have $v_{\mathfrak{q}}(y) \geq 0$, and then $v_{\mathfrak{q}}(dy) \geq 0$, the previous argument shows that

$$\operatorname{div}(dy) = (\mathfrak{q}')^{e'}(\mathfrak{q}'')^{e''}.$$

This proves the claim.

Now we find the space of holomorphic differentials of $F|K$. Since $\big(z/c(x)\big)^2 = A_2 + c_1^{-1}/c(x)$, the pole divisor of $z/c(x)$ is clearly equal to $\frac{1}{2}\operatorname{div}_0(c(x))$. Similarly, since $\big(y/c(x)\big)^4 = A_2 + \big(B(x)^2 + c_1^{-1}c(x)\big)/c(x)^2$, the pole divisor of $y/c(x)$ is smaller than $\frac{1}{2}\operatorname{div}_0(c(x))$. This shows that the three differentials

$$dy,\ \frac{z}{c(x)}dy,\ \frac{y}{c(x)}dy$$

form a basis of the space of holomorphic differentials of $F|K$. In particular, it follows from Proposition 3.11 that the two differentials

$$dy,\ \frac{z}{c(x)}dy$$

form a basis of the space of exact holomorphic differentials of $F|K$.

We now determine the canonical field C and the pseudocanonical field E of $F|K$. By the previous paragraph, these are given by

$$\begin{aligned} C &= K(Z, Y), \\ E &= K(Z), \end{aligned}$$

where the functions $Z := z/c(x)$ and $Y := y/c(x)$ satisfy the relations

$$\begin{aligned} Z^2 &= A_2 + \frac{c_1^{-1}}{c(x)}, \\ Y^2 &= \frac{B_0 + B_1 x}{c(x)} + Z. \end{aligned} \tag{3.20}$$

Since

$$x^2 + c_1 x + c_0 = \frac{c_1^{-1}}{A_2 + Z^2}, \tag{3.21}$$

it is clear that the pseudocanonical field $E = K(Z)$ is a quadratic subfield of $F_1 = K(x, Z)$, and that $F_1|E$ is a separable field extension generated by x. As for the canonical field C, two possibilities may occur.

If $B_1 \neq 0$, then we can normalize $B_0 = 0$ (see Theorem 3.8). Moreover, the function $x = B_1^{-1}c(x)(Y^2 + Z)$ clearly lies in $C = K(Z, Y)$, that is, $C = F$. We conclude that $F = K(Z, Y)$, where the functions Z and Y satisfy the quartic equation

$$c_0(A_2^2 + Z^4) + (B_1^{-1}(Y^2 + Z) + c_1^{-1})(A_2 + Z^2) + B_1^{-2}c_1^{-2}(Y^2 + Z)^2 = 0,$$

which is obtained by replacing $x = B_1^{-1}\frac{c_1^{-1}}{A_2+Z^2}(Y^2 + Z)$ in (3.21). We see in particular that $F|K$ is non-hyperelliptic. The plane projective quartic

$$c_0(A_2^2X^4 + Z^4) + (B_1^{-1}(Y^2 + XZ) + c_1^{-1}X^2)(A_2X^2 + Z^2) + B_1^{-2}c_1^{-2}(Y^4 + X^2Z^2) = 0$$

is its canonical model.

If $B_1 = 0$, then the canonical field $C = K(Z, Y)$ is a quadratic subfield of F as $F = C(x)$ and

$$x^2 + c_1x + c_0 = \frac{c_1^{-1}}{A_2 + Z^2}.$$

Because the functions Z and Y satisfy the quadratic equation

$$Y^2 = Z + c_1B_0(A_2 + Z^2),$$

it is clear that the function field $C|K$ has genus 0, and that $F|K$ is thus hyperelliptic. The hyperelliptic involution is given by the transformation $x \mapsto x + c_1$.

Function fields of Theorem 3.9

Let $F|K$ be a function field as in Theorem 3.9 (i), in normal form

$$\begin{aligned} z^2 &= ax^2 + x + c, && a \notin K^2,\\ w^2 &= z, \\ y^2 &= m_1x + m_0 + n_0z + w. \end{aligned}$$

Recall that there is a unique singular prime $\mathfrak{p}$, whose restriction $\mathfrak{p}_3$ to $F_3 = K(x)$ is rational with local parameter x^{-1}. Recall also that the restricted prime $\mathfrak{p}_1$ of $F_1|K = K(x, z, w)|K$ is ramified over $F_2 = K(x, z)$, and that the prime $\mathfrak{p}_2$ of $F_2|K$ is unramified over F_3.

We find the divisor of dy. Applying Theorem 2.6 we get

$$v_{\mathfrak{p}}(dy) = \frac{2\delta(\mathfrak{p}) + v_{\mathfrak{p}_3}(dy^8)}{\deg \mathfrak{p}} = \frac{6-2}{\deg \mathfrak{p}} = e,$$

where e stands for the ramification index of $\mathfrak{p}$ over F_1. As the divisor $\mathfrak{p}^e$ has degree $4 = 2g-2$, and as $v_{\mathfrak{q}}(y) \geq 0$ for any other prime $\mathfrak{q} \neq \mathfrak{p}$, so that $v_{\mathfrak{q}}(dy) \geq 0$, this shows that $\operatorname{div}(dy) = \mathfrak{p}^e$. So we see again that the divisor $\mathfrak{p}^e$ is canonical. Since $H^0(\mathfrak{p}) = K \oplus Kw \oplus Ky$ by (3.14), the three differentials

$$dy,\ w\,dy,\ y\,dy$$

form a basis of the space of holomorphic differentials. We then see from Proposition 3.11 that the two differentials

$$dy,\ w\,dy$$

form a basis of the space of exact holomorphic differentials.

We deduce from the previous paragraph that the canonical field C and the pseudo-canonical field E of $F|K$ are given by

$$\begin{aligned} C &= K(w, y), \\ E &= K(w). \end{aligned}$$

Since

$$w^4 = ax^2 + x + c,$$

it is clear that E is a quadratic subfield of the Frobenius pullback $F_1 = K(x, z)$, and that $F_1|E$ is a separable field extension generated by x. As for the canonical field C, two possibilities may occur.

If $m_1 \neq 0$, then we can normalize $m_0 = 0$ by replacing x with $x + m_1^{-1} m_0$. Furthermore, the function $x = m_1^{-1}(y^2 + n_0 w^2 + w)$ lies in $C = K(z, w, y)$, that is, $C = F$. Thus $F = K(w, y)$, where the functions w and y satisfy the quartic equation

$$ay^4 + (m_1^2 + an_0^2)w^4 + m_1 y^2 + (a + m_1 n_0)w^2 + m_1 w + m_1^2 c = 0.$$

Note that this equation is obtained by eliminating $x = m_1^{-1}(y^2 + n_0 w^2 + w)$ in $w^4 = ax^2 + x + c$. Therefore, the function field $F|K$ is non-hyperelliptic and the plane projective quartic curve

$$aY^4 + (m_1^2 + an_0^2)Z^4 + m_1 X^2 Y^2 + (a + m_1 n_0)X^2 Z^2 + m_1 X^3 Z + m_1^2 c X^4 = 0$$

is its canonical model.

If $m_1 = 0$, then the canonical field $C = K(z, w, y)$ is a quadratic subfield of F because $F = C(x)$ and

$$ax^2 + x + c + w^4 = 0.$$

Since the functions w and y satisfy the quadratic relation

$$y^2 + n_0 w^2 + w + m_0 = 0,$$

the function field $C|K = K(w, y)|K$ has genus 0, and therefore $F|K$ is hyperelliptic. The hyperelliptic involution is given by the transformation $x \mapsto x + a^{-1}$.

Now let $F|K$ be a function field as in Theorem 3.9 (ii), in normal form

$$\begin{aligned} z^2 &= ax^2 + x, & a \notin K^2, \\ w^2 &= a_2 x^2 + a_0 + z, \\ y^2 &= xw. \end{aligned}$$

Recall that $F|K$ has a unique singular prime $\mathfrak{p}$, whose restriction $\mathfrak{p}_3$ to $F_3 = K(x)$ is rational with local parameter x^{-1}. Recall also that the prime $\mathfrak{p}_2$ of $F_2|K = K(x, z)|K$ is unramified over F_3.

We find the divisor of dy. We claim that

$$\operatorname{div}(dy) = \operatorname{div}_0(x)^{1/2}.$$

Indeed, note first that by applying Theorem 2.6 we get

$$v_{\mathfrak{p}}(dy) = \frac{2\delta(\mathfrak{p}) + v_{\mathfrak{p}_3}(dy^8)}{\deg \mathfrak{p}} = \frac{6 + v_{\mathfrak{p}_3}(x^4 dx)}{\deg \mathfrak{p}} = 0.$$

Now let $\mathfrak{q}'$ denote the only zero of the function x. Observe that the restricted prime $\mathfrak{q}'_3$ of $F_3|K$ is rational, and that the prime $\mathfrak{q}'_2$ is ramified (and therefore rational) over F_3 with local parameter z. Letting e' and e'_1 denote the corresponding ramification indices of $\mathfrak{q}'$ and $\mathfrak{q}'_1$ over F_1 and F_2 respectively we see that

$$v_{\mathfrak{q}'}(dy) = \frac{c_{\mathfrak{q}'} + v_{\mathfrak{q}'_3}(dy^8)}{\deg \mathfrak{q}'} = \frac{0+4}{\deg \mathfrak{q}'} = e'e'_1.$$

As the divisor $(\mathfrak{q}')^{e'e'_1}$ has degree $4 = 2g-2$, and as $v_{\mathfrak{q}}(y) \geq 0$ for any other prime $\mathfrak{q} \neq \mathfrak{p}, \mathfrak{q}'$, so that $v_{\mathfrak{q}}(dy) \geq 0$, this shows that $\operatorname{div}(dy) = (\mathfrak{q}')^{e'e'_1}$. Thus $\operatorname{div}(dy) = \operatorname{div}_0(x)^{1/2}$ and the claim is proved.

We find the space of holomorphic differentials of $F|K$. Since $(z/x)^2 = a + 1/x$, the pole divisor of z/x is equal to $\operatorname{div}_0(x)^{1/2}$. Analogously, since $(y/x)^4 = a_2 + a_0/x^2 + z/x^2$, the pole divisor of y/x is smaller than $\operatorname{div}_0(x)^{1/2}$. Thus the three differentials

$$dy,\ \frac{z}{x}dy,\ \frac{y}{x}dy$$

form a basis of the space of holomorphic differentials. We then see from Proposition 3.11 that the two differentials

$$dy,\ \frac{z}{x}dy$$

form a basis of the space of exact holomorphic differentials.

It follows from the previous paragraph that the canonical field C and the pseudocanonical field E of $F|K$ are given by

$$\begin{aligned} C &= K(Z, Y), \\ E &= K(Z), \end{aligned}$$

where $Z := z/x$ and $Y := y/x$. As the pseudocanonical field E contains the function $x = 1/(a + Z^2)$, it coincides with the second Frobenius pullback $F_2 = K(x, z)$, that is,

$$E = F_2.$$

Because of the equality $w = y^2/x$, the canonical field C is equal to $F = K(x, z, w, y)$, i.e.,

$$C = F.$$

Thus $F = K(Z, Y)$, where the functions Z and Y satisfy the quartic equation

$$Y^4 + a_0 Z^4 + Z^3 + aZ + a_2 + a^2 a_0 = 0,$$

which is obtained by eliminating $x = 1/(a + Z^2)$ in $Y^4 = a_2 + a_0/x^2 + Z/x$. Therefore, the function field $F|K$ is non-hyperelliptic and the plane projective quartic

$$Y^4 + a_0 Z^4 + XZ^3 + aXZ + (a_2 + a^2 a_0)X^4 = 0$$

is its canonical model.

Suppose now that $F|K$ is a function field from Theorem 3.9 (iii) in normal form

$$\begin{aligned} z^2 &= ax^2 + x + c, & a &\notin K^2, \\ w^2 &= a_2 z^2 + z, & a_2 &\notin K^2, \\ y^2 &= (n_0 + n_1 x + w)z. \end{aligned}$$

Recall that $F|K$ has a unique singular prime $\mathfrak{p}$, whose restriction $\mathfrak{p}_3$ to $F_3 = K(x)$ is rational with local parameter x^{-1}. Recall also that the prime $\mathfrak{p}_2$ of $F_2|K = K(x,z)|K$ is unramified over F_3.

We find the divisor of dy. We claim that

$$\operatorname{div}(dy) = \operatorname{div}_0(z)^{1/2} = \operatorname{div}_0(ax^2 + x + c)^{1/4}.$$

Indeed, by making a quadratic separable extension of K if necessary, we may assume that the two roots of the polynomial ax^2+x+c belong to K. Then the function $ax^2+x+c \in F$ has two zeros, say $\mathfrak{q}'$ and $\mathfrak{q}''$, and

$$\begin{aligned}\operatorname{div}(ax^2 + x + c) &= (\mathfrak{q}')^{e'e_1'e_2'}(\mathfrak{q}'')^{e''e_1''e_2''}\mathfrak{p}^{-2ee_1}\\ &= (\mathfrak{q}')^{4e'}(\mathfrak{q}'')^{4e''}\mathfrak{p}^{-2ee_1},\end{aligned}$$

where $e', e_1' = e_2' = 2$ and $e'', e_1'' = e_2'' = 2$ are the ramification indices of $\mathfrak{q}', \mathfrak{q}_1', \mathfrak{q}_2''$ and $\mathfrak{q}'', \mathfrak{q}_1'', \mathfrak{q}_2''$ over F_1, F_2, F_3 respectively. Applying Theorem 2.6 gives

$$\begin{aligned} v_{\mathfrak{p}}(dy) &= \frac{2\delta(\mathfrak{p}) + v_{\mathfrak{p}_3}(dy^8)}{\deg \mathfrak{p}} = \frac{6 + v_{\mathfrak{p}_3}(z^4 dx)}{\deg \mathfrak{p}} = 0,\\ v_{\mathfrak{q}'}(dy) &= \frac{2\delta(\mathfrak{q}') + v_{\mathfrak{q}_3'}(dy^8)}{\deg \mathfrak{q}'} = \frac{0+2}{\deg \mathfrak{q}'} = e',\end{aligned}$$

and similarly $\mathfrak{q}''(dy) = e''$. As the divisor $(\mathfrak{q}')^{e'}(\mathfrak{q}'')^{e''}$ has degree $\frac{1}{2}\deg \mathfrak{p}^{ee_1} = 4$ by the product formula, and as $v_{\mathfrak{q}}(y) \geq 0$ for any other prime $\mathfrak{q} \neq \mathfrak{p}$, so that $v_{\mathfrak{q}}(dy) \geq 0$, the previous argument shows that $\operatorname{div}(dy) = (\mathfrak{q}')^{e'}(\mathfrak{q}'')^{e''}$. Thus $\operatorname{div}(dy) = \operatorname{div}_0(ax^2+x+c)^{1/4}$ and the claim is proved.

Now we find the space of holomorphic differentials of $F|K$. Since $(w/z)^2 = a_2 + 1/z$, the pole divisor of w/z is equal to $\operatorname{div}_0(z)^{1/2}$. Analogously, since $(y/z)^4 = n_0^2/z^2 + n_1^2x^2/z^2 + (w/z)^2$, the pole divisor of y/x is smaller than $\operatorname{div}_0(z)^{1/2}$. Thus the three differentials

$$dy,\ \frac{w}{z}dy,\ \frac{y}{z}dy$$

form a basis of the space of holomorphic differentials. And it follows from Proposition 3.11 that the two differentials

$$dy,\ \frac{w}{z}dy$$

form a basis of the space of exact holomorphic differentials.

We deduce from the previous paragraph that the canonical field C and the pseudo-canonical field E of $F|K$ are given by

$$\begin{aligned} C &= K(W,Y),\\ E &= K(W),\end{aligned}$$

where $W := w/z$ and $Y := y/z$. Since the pseudocanonical field E contains the function $z = 1/(a_2 + W^2)$, it is generated over K by the functions z and w, i.e., $E = K(z,w)$. Because of the polynomial relation

$$ax^2 + x + c = z^2, \tag{3.22}$$

the pseudocanonical field E is clearly a quadratic subfield of the Frobenius pullback $F_1 = K(z,w,x)$, and $F_1|E$ is separably generated by x. As to the canonical field $C = K(z,w,y)$, there are two possibilities that can happen.

If $n_1 \neq 0$, then we can normalize $n_0 = 0$ by replacing x with $x + n_1^{-1}n_0$. Moreover, the function $x = n_1^{-1}z(Y^2 + W)$ clearly belongs to $C = K(W, Y)$, that is, $C = F$. We conclude that $F = K(W, Y)$, where the functions W and Y satisfy the quartic equation

$$aY^4 + n_1Y^2W^2 + n_1^2cW^4 + n_1W^3 + aW^2 + n_1a_2Y^2 + n_1a_2W + (ca_2^2 + 1)n_1^2 = 0.$$

Note that this relation is obtained by eliminating $z = 1/(a_2+W^2)$ and $x = n_1^{-1}z(Y^2+W)$ in (3.22). Thus the function field $F|K$ is non-hyperelliptic and the plane projective quartic

$$aY^4 + n_1Y^2Z^2 + n_1^2cZ^4 + n_1XZ^3 + aX^2Z^2 + n_1a_2X^2Y^2 + n_1a_2X^3Z + (ca_2^2 + 1)n_1^2X^4 = 0$$

is its canonical model.

If $n_1 = 0$, then the canonical field $C = K(z, w, y)$ is a quadratic subfield of F because $F = C(x)$ and

$$ax^2 + x + c + z^2 = 0.$$

As the functions Y and W satisfy the quadratic relation

$$Y^2 + W + n_0 = 0,$$

the function field $C|K = K(W, Y)|K$ has genus 0, and so $F|K$ is hyperelliptic. The hyperelliptic involution is given by the transformation $x \mapsto x + a^{-1}$.

Chapter 4

Fibrations by singular curves of arithmetic genus 3

In this chapter we bring the results of Chapter 3 from the language of function fields to the setting of curves and fibrations by curves, as discussed in Section 2.1. To accomplish this task, we shall take advantage of the projective models found in Section 3.3.

In the first section we study two families of regular but non-smooth curves of arithmetic genus 3 and geometric genus 0. Whereas the first one comprises hyperelliptic curves with a unique singular point that is non-decomposed, the second one consists of non-hyperelliptic curves. We determine all such curves in a explicit manner (Theorems 4.1 and 4.2), and then give criteria to determine when any two of them are isomorphic.

The curves in the first section are used in the second one to construct fibrations by rational singular curves of arithmetic genus 3. Interestingly (or fortunately), the total spaces of these fibrations are smooth, which is a pleasant feature that does not always occur. Indeed, the total space of a fibration that has been constructed from a curve usually has singularities, which in some cases may cause difficulties. When the total space is a surface it may be possible to get rid of them by performing blowups (see the last section).

In the last section we build two one-dimensional fibrations by rational singular curves of arithmetic genus 3, which, unlike the fibrations in Section 4.2, have total spaces with singularities. To be more precise, these are singular surfaces that are fibered over the projective line. Hence the theory of (relatively) minimal fibrations comes into place. Motivated by the work of Kodaira and Néron on the classification of special fibres of minimal fibrations by elliptic curves, we then construct the minimal proper regular models of our fibrations, determine the structure of the bad fibres and study the geometry of the total spaces.

Before getting started, we recall a notion that will appear in many instances in this chapter. The *singularity degree* (also known as *δ-invariant*) of a point P on a curve X over an algebraically closed field k is defined as $\delta_P = \dim_k(\widetilde{\mathcal{O}_{X,P}}/\mathcal{O}_{X,P})$.

Throughout this chapter, we shall use the notation and terminology introduced in Sections 2.1 and 2.2.

4.1 Geometrically rational curves of genus 3

To avoid unnecessary repetition, in this section the symbol C will always denote a *geometrically integral regular complete curve* defined over (the spectrum of) a field K of characteristic p.[1]

Recall that there is a deep connection between the curves C satisfying these properties and the class of separable one-dimensional function fields $F|K$ (see Section 2.1). Essentially, the curve C associated to a function field $F|K$ is the regular complete model of $F|K$, that is, the one-dimensional scheme with function field $F|K$, whose non-generic points consist of the primes $\mathfrak{p}$ of $F|K$ and whose local rings are the corresponding valuation rings $\mathcal{O}_{\mathfrak{p}}$. Therefore, the curves C satisfying the above properties and the class of function fields are equivalent objects, and so we can study these curves from the point of view of function field theory.

We introduce some notation. Let g denote the arithmetic genus of C, which coincides with the genus of its function field $F|K = K(C)|K$ because C is regular. Let g_n denote the arithmetic genus of the normalization of the extended curve over K^{1/p^n}

$$C \otimes_K K^{1/p^n},$$

i.e., the genus of the extended function field $K^{1/p^n} \cdot F|K^{1/p^n}$. We also let $\overline{g}$ denote the geometric genus of the extended integral curve defined over $\overline{K}$

$$\overline{C} = C \otimes_K \overline{K},$$

i.e., the arithmetic genus of the normalization of $\overline{C}$, or equivalently, the genus of the extended function field $\overline{K}F|\overline{K}$. Note that the curves $C \otimes_K K^{1/p^n}$ and $\overline{C}$ have arithmetic genus g, for the arithmetic genus of a curve is invariant under base field extensions.

Even though the curve C is regular, it may have non-smooth points. A point of C is non-smooth if it lies below a singular point of the extended integral curve $\overline{C} = C \otimes_K \overline{K}$. Since the non-smooth points of C correspond to the singular primes of its function field $F|K = K(C)|K$, it follows that C is non-smooth if and only if $F|K$ is non-conservative, that is, if $g > \overline{g}$. Equivalently, C is non-smooth if and only if $\overline{C}$ is singular.

We focus our attention on the class of curves C that are directly related to the function fields in Chapter 3. So we assume that our curve C is defined over a field K of characteristic $p = 2$ and that it has arithmetic genus $g = 3$. By the genus drop formula (2.4), the geometric genus $\overline{g}$ of $\overline{C}$ can take three values, namely 0, 1 and 2, and cases $\overline{g} = 0$ and $\overline{g} = 1$ can be divided into subcases depending on the number of non-smooth points that appear. Table 4.1 exhibits the ensuing division.[2] In contrast to the situation in characteristics 3, 5 and 7, in characteristic $p = 2$ *all* of these possibilities can occur (see Chapter 5 and Examples 3.1, 3.2 and 3.3).

We now assume that the curve C is geometrically rational, i.e., $\overline{g} = 0$, and that it has a unique non-smooth point that is possibly non-decomposed. (As in Section 2.3, a point of C is non-decomposed if there is a unique point of $\overline{C}$ lying over it.) As is clear from Corollary 2.13, in this case the arithmetic genus g_1 of the normalization of $C \otimes_K K^{1/2}$ can take two values, namely 0 and 1. Note that $g_2 = 0$.

The following result is a consequence of Theorem 3.4 and Section 3.3 (see pages 54 and 56).

[1]More precisely, C is a geometrically integral one-dimensional complete regular scheme of finite type over K.

[2]The singularity degree of a closed point $c \in C$ is its singularity degree as a prime of the function field $F|K = K(C)|K$ (see Section 2.2). The singularity degree of $c \in C$ is equal to the sum of the singularity degrees of the points of $\overline{C}$ lying over c.

$\overline{g}$	Number of non-smooth points	Singularity degrees
0	1	3
	2	1 and 2
	3	1
1	1	2
	2	1
2	1	1

Table 4.1: Possibilities for non-smooth points and their singularity degrees

Theorem 4.1. *A geometrically integral regular complete curve C over a field K of characteristic $p = 2$ has genera $g = 3$, $g_1 = 0$ and admits a unique non-smooth non-decomposed point, if and only if, it is isomorphic to one of the following projective curves defined over K.*

(i) *The intersection of the surface*

$$\left\{(u_0 : u_1 : u_2 : u_3 : u_4 : v) \,\middle|\, \operatorname{rank}\begin{pmatrix} u_1 & u_2 & u_3 & u_4 \\ u_0 & u_1 & u_2 & u_3 \end{pmatrix} < 2\right\} \subseteq \mathbb{P}^5$$

and the hypersurface cut out by the equation

$$v^2 = a_0u_0^2 + u_0u_1 + a_2u_1^2 + a_4u_2^2 + a_6u_3^2 + a_8u_4^2,$$

where $a_0, a_2, a_4, a_6 \in K$ and $a_8 \in K \setminus K^2$.

(ii) *The intersection of the threefold*

$$\left\{(u_0 : u_1 : u_2 : u_3 : u_4 : v) \,\middle|\, \operatorname{rank}\begin{pmatrix} u_1 & u_2 & u_4 \\ u_0 & u_1 & u_3 \end{pmatrix} < 2\right\} \subseteq \mathbb{P}^5$$

and the three hypersurfaces cut out by the equations

$$\begin{aligned} u_0u_3 &= v^2 + b_2u_1^2 + b_3u_1u_2 + b_4u_2^2, \\ u_3^2 &= a_0u_0^2 + u_0u_1 + a_2u_1^2, \\ u_4^2 &= a_0u_1^2 + u_1u_2 + a_2u_2^2, \end{aligned}$$

where $b_i \in K$, $a_2 \in K \setminus K^2$ and $a_0 \in K$ are constants satisfying one of the following relations

- $b_4^{1/2} \notin K(a_2^{1/2})$;
- $b_2 = b_4 = 0$ *and* $b_3 \neq 0$.

Note that due to the condition $g_1 = 0$, the curves in the theorem are necessarily hyperelliptic. To get examples of non-hyperelliptic curves, we must look at the function fields in Theorems 3.7 and 3.9, whose first Frobenius pullbacks have genus $g_1 = 1$. These theorems together with Section 3.3 (see pages 57, 59, 60, 61 and 63) yield the following characterization of non-hyperelliptic curves of genera $g = 3$ and $\overline{g} = 0$.

Theorem 4.2. *A geometrically integral regular complete curve C over a field K of characteristic $p = 2$ is non-hyperelliptic and has genera $g = 3$ and $\overline{g} = 0$, if and only if, it is isomorphic to one of the following plane projective quartics.*

(i) $Y^4 + a_0Z^4 + XZ^3 + a_2X^2Z^2 + a_4X^4 = 0$, *where* $a_0, a_2 \in K$ *and* $a_4 \in K \setminus K^2$.

(ii) $c_0(A_2^2X^4+Z^4)+(B_1(Y^2+XZ)+c_1X^2)(A_2X^2+Z^2)+B_1^2c_1^2(Y^4+X^2Z^2) = 0$, *where* $c_0, c_1, A_2, B_1 \in K$ *are constants satisfying the conditions* $B_1, c_1 \neq 0$ *and* $A_2 \notin K^2$.

(iii) $aY^4 + (m_1^2 + an_0^2)Z^4 + m_1X^2Y^2 + (a + m_1n_0)X^2Z^2 + m_1X^3Z + m_1^2cX^4 = 0$, *where* $a, c, m_1, n_0 \in K$ *are constants satisfying the conditions* $m_1 \neq 0$ *and* $a \notin K^2$.

(iv) $Y^4 + a_0Z^4 + XZ^3 + aXZ + (a_2 + a^2a_0)X^4 = 0$, *where* $a_0, a_2 \in K$ *and* $a \in K \setminus K^2$.

(v) $aY^4+n_1Y^2Z^2+n_1^2cZ^4+n_1XZ^3+aX^2Z^2+n_1a_2X^2Y^2+n_1a_2X^3Z+(ca_2^2+1)n_1^2X^4 = 0$, *where* $a, c, a_2, n_1 \in K$ *are constants satisfying the conditions* $a, a_2 \notin K^2$ *and* $n_1 \neq 0$.

Each of these curves has a unique non-smooth point, which is non-decomposed.

We remark that the uniqueness and non-decomposedness of the non-smooth point of a non-hyperelliptic curve C with genera $g = 3$, $\overline{g} = 0$ come from the fact that the normalization of the extended curve $C \otimes_K K^{1/2}$ has genus $g_1 = 1$ (see Corollaries 2.13 and 2.9).

Theorems 4.1 and 4.2 give us seven classes of curves of genera $g = 3$ and $\overline{g} = 0$, two of them hyperelliptic and the remaining five non-hyperelliptic. These classes are pairwise disjoint, or more precisely, no curve from one class is isomorphic to a curve from another class. This follows from Theorems 3.5, 3.8 and 3.10, from which we can also obtain very precise criteria to decide when any two curves in a given class are isomorphic.

Theorem 4.3. *No curve from item* (i) *in Theorem 4.1 is isomorphic to a curve from item* (ii)*. Moreover,*

(i) *two curves* C *and* C' *from item* (i) *with constants* a_0, a_2, a_4, a_6, a_8 *and* $a_0', a_2', a_4', a_6', a_8'$ *are isomorphic if and only if there exist constants* $c_0, c_1, c_2, c_3, c_4, t, b \in K$ *with* $t \neq 0$ *such that*

$$\begin{aligned}
t^{-2}a_0' &= a_0 + c_0^2 + c_1^2b^2 + c_2^2b^4 + c_3^2b^6 + c_4^2b^8 + b^8a_8 + b^6a_6 + b^4a_4 + b^2a_2 + b,\\
t^2a_2' &= a_2 + c_1^2 + c_3^2b^4 + b^4a_6,\\
t^6a_4' &= a_4 + c_2^2 + c_3^2b^2 + b^2a_6,\\
t^{10}a_6' &= a_6 + c_3^2,\\
t^{14}a_8' &= a_8 + c_4^2.
\end{aligned}$$

(ii) *two curves* C *and* C' *from item* (ii) *with constants* a_0, a_2, b_2, b_3, b_4 *and* $a_0', a_2', b_2', b_3', b_4'$ *are isomorphic if and only if there exist constants* $r_0, t, t_0, t_1, t_2, t_3, t_4 \in K$ *with* $t \neq 0$ *such that*

$$\begin{aligned}
t^{14}b_4' &= b_4 + t_2^2 + t_4^2a_2,\\
t^{10}b_3' &= b_3 + t_4^2,\\
t^6b_2' &= b_2 + r_0t_4^2 + r_0b_3 + t_1^2 + t_3^2a_2 + t_4^2a_0,\\
t^4a_2' &= a_2 + r_0^4t_4^4 + r_0^4b_3^2 + t_3^4,\\
t^{-4}a_0' &= a_0 + r_0^8t_2^4 + r_0^8t_4^4a_2^2 + r_0^8b_4^2 + r_0^6t_4^4 + r_0^6b_3^2 + r_0^4t_1^4 + r_0^4t_3^4a_2^2\\
&\quad + r_0^4t_4^4a_0^2 + r_0^4b_2^2 + r_0^2t_3^4 + r_0^2a_2 + r_0 + t_0^4 + t_3^4a_0^2.
\end{aligned}$$

Theorem 4.4. *The curves in items* (i), (ii), (iii), (iv) *and* (v) *in Theorem 4.2 are pairwise non-isomorphic, that is, a curve from one item cannot be isomorphic to a curve from another item. Moreover,*

(i) *two curves C and C' from item* (i) *with constants a_0, a_2, a_4 and a'_0, a'_2, a'_4 are isomorphic if and only if there exist constants $b, c_0, c_1, t \in K$ with $t \neq 0$ such that*

$$\begin{aligned} t^4 a'_2 &= a_2, \\ t^{12} a'_4 &= a_4 + c_1^4, \\ t^{-4} a'_0 &= a_0 + b^2 a_2 + b^4 a_4 + c_0^4 + c_1^4 b^4 + b; \end{aligned}$$

(ii) *two curves C and C' from item* (ii) *with constants c_0, c_1, A_2, B_0, B_1 and $c'_0, c'_1, A'_2, B'_0, B'_1$ are isomorphic if and only if there exist constants $r_0, t_2, t_3, t_4, t_5 \in K$ with $(t_4, t_5) \neq (0, 0)$ such that*

$$\begin{aligned} t^6 A'_2 &= A_2 + s_2^2, \\ t^2 c'_1 &= c_1, \\ t^{-3} c'_0 &= r_0^2 t + r_0 t c_1^{-1} + t_5^2 c_1 + t c_0, \\ B'_1 &= t B_1, \\ B'_0 &= (r_0 B_1^{-1} + B_0) t + c_1^{-1}(t_4 t_5 + t_3^2), \end{aligned}$$

where $t := t_4^2 + t_5^2 A_2 \neq 0$ and $s_2 := t^{-1}(t_2^2 + t_3^2 A_2)$.

(iii) *two curves C and C' from item* (iii) *with constants a, c, m_1, m_0, n_0 and a', c', m'_1, m'_0, n'_0 are isomorphic if and only if there exist constants $r_0, t_0, \mu_0, \mu_1, \mu_2$ in K with $\mu_2 \neq 0$ such that*

$$\begin{aligned} \mu_2^8 a' &= a, \\ \mu_2^{-8} c' &= c + r_0^2 a + r_0 + t_0^4, \\ \mu_2^2 n'_0 &= n_0 + \mu_1^2, \\ \mu_2^6 m'_1 &= m_1, \\ \mu_2^{-2} m'_0 &= m_0 + r_0 m_1 + t_0^2(n_0 + \mu_1^2) + t_0 + \mu_0^2; \end{aligned}$$

(iv) *two curves C and C' from item* (iv) *with constants a, a_2, a_0 and a', a'_2, a'_0 are isomorphic if and only if there exist constants $\mu_1, \mu_2, \mu_4, \mu_5$ in K with $(\mu_4, \mu_5) \neq (0, 0)$ such that*

$$\begin{aligned} t_3^6 a'_2 &= a_2 + t_1^2, \\ a'_0 &= t_3^2 a_0 + t_3 \mu_4 \mu_5 + \mu_2^4 + \mu_5^4 a_2, \\ t_3^4 a' &= a, \end{aligned}$$

where $t_3 := \mu_4^2 + \mu_5^2 a \neq 0$ and $t_1 := t_3^{-1}(\mu_1^2 + \mu_2^2 a)$;

(v) *two curves C and C' from item* (v) *with constants a, c, a_2, n_0, n_1 and a', c', a'_2, n'_0, n'_1 are isomorphic if and only if there exist constants $r_0, \mu_2, \mu_3, \mu_4, \mu_5$ in K with $(\mu_4, \mu_5) \neq$*

(0, 0) *such that*

$$\begin{aligned} t_3^4 a' &= a, \\ t_3^{-2} c' &= t_3^2(c + r_0^2 a + r_0) + \mu_5^4, \\ t_3^2 a_2' &= a_2 + t_2^2, \\ t_3^3 n_1' &= n_1, \\ n_0' &= t_3(n_0 + r_0 n_1) + \mu_3^2 + \mu_4\mu_5, \end{aligned}$$

where $t_3 := \mu_4^2 + \mu_5^2 a_2 \neq 0$ *and* $t_2 := t_3^{-1}(\mu_2^2 + \mu_3^2 a_2)$.

We note that the groups of automorphisms of the curves in items (ii), (iv) and (v) of Theorem 4.2 are trivial (see the discussions following the proofs of Theorems 3.8 and 3.10).

Finally, to complete the picture we remark that even though in this section we studied geometrically rational curves of arithmetic genus 3 with only *one* non-smooth point, there are examples of curves with several non-smooth points (see Section 5.3). Of course, these curves will be hyperelliptic by Corollary 2.13.

4.2 Fibrations by singular curves

In this section we construct fibrations by singular curves by using the regular but non-smooth curves in Theorems 4.1 and 4.2. As follows from Section 2.1, the curves C will become the generic fibres of our fibrations, and the extended curves $\overline{C}$ will become their general fibres, that is, most of the fibres will inherit their properties from $\overline{C}$.

The idea here is to construct the base of the fibration by using the constants of the curve C, i.e., the constants appearing in its equations. In this way, the parameters of C will become the *parameters* of the fibration; in other words, we will obtain families of curves parameterized by them.

Let k be an algebraically closed field of characteristic 2. We start with the curves in Theorem 4.1 (i). Define the cone

$$S := \left\{ (u_0 : u_1 : u_2 : u_3 : u_4 : v) \in \mathbb{P}^5(k) \;\middle|\; \operatorname{rank} \begin{pmatrix} u_1 & u_2 & u_3 & u_4 \\ u_0 & u_1 & u_2 & u_3 \end{pmatrix} < 2 \right\}$$

and let $Q = (0 : 0 : 0 : 0 : 0 : 1)$ be its vertex. The smooth locus $S \setminus \{Q\}$ of S can be described by the affine charts

$$\begin{aligned} U &= \left\{ (1 : u : u^2 : u^3 : u^4 : v) \mid (u, v) \in k^2 \right\} \xrightarrow{\sim} k^2, \\ \breve{U} &= \left\{ (\breve{u}^4 : \breve{u}^3 : \breve{u}^2 : \breve{u} : 1 : \breve{v}) \mid (\breve{u}, \breve{v}) \in k^2 \right\} \xrightarrow{\sim} k^2. \end{aligned}$$

Theorem 4.5. *The algebraic variety*

$$\begin{aligned} Z := \{ &((u_0 : u_1 : u_2 : u_3 : u_4 : v), (a_0, a_2, a_4, a_6, a_8)) \in S \times \mathbb{A}^5 \mid \\ &v^2 + a_0 u_0^2 + u_0 u_1 + a_2 u_1^2 + a_4 u_2^2 + a_6 u_3^2 + a_8 u_4^2 = 0 \} \end{aligned}$$

is an irreducible smooth sixfold. The projection

$$\pi : Z \longrightarrow \mathbb{A}^5$$

is proper and flat, and its fibres are rational projective curves of arithmetic genus 3*, which do not pass through the vertex* Q *of* S*. Each fibre has exactly one singular point.*

Before proving the theorem we remark that the projection $\pi : Z \to \mathbb{A}^5$ provides a 5-dimensional family of algebraic varieties (in fact curves, as follows from the theorem) on the punctured cone $S \setminus \{Q\}$.

Proof. The closed subvariety Z of $S \times \mathbb{A}^5$ is clearly contained in the smooth open subvariety $S \setminus \{Q\} \times \mathbb{A}^5$, and it is described in the charts $U \times \mathbb{A}^5 \cong \mathbb{A}^7$ and $\breve{U} \times \mathbb{A}^5 \cong \mathbb{A}^7$ by the following equations

$$v^2 + a_0 + u + a_2u^2 + a_4u^4 + a_6u^6 + a_8u^8 = 0$$

and

$$\breve{v}^2 + a_0\breve{u}^8 + \breve{u}^7 + a_2\breve{u}^6 + a_4\breve{u}^4 + a_6\breve{u}^2 + a_8 = 0$$

respectively. Hence Z is irreducible, smooth and of dimension 6.

As S is projective, the projection π is proper. The fibre over each point $(a_0, a_2, a_4, a_6, a_8)$ in the base $\mathbb{A}^5$ is the algebraic curve given in the charts U and $\breve{U}$ by the above equations. Observe that the total space Z is Cohen-Macaulay because it is smooth. Since the base $\mathbb{A}^5$ is smooth and the dimension of each fibre is equal to $\dim(Z) - \dim(\mathbb{A}^5) = 1$, it follows from [Eis91, Theorem 18.16] that the morphism π is flat.

By applying the Jacobian criterion to the charts of $S \setminus \{Q\}$, we deduce that each curve of the family has a unique singular point, namely

$$(0 : 0 : 0 : 0 : 1 : a_8^{1/2}),$$

which is unibranch of multiplicity 2 and singularity degree 3, as follows from the blowup sequences. In particular, each curve of the family is rational and has arithmetic genus 3. $\square$

Remark. The dimension of the base $\mathbb{A}^5$ can be reduced by setting some of the constants a_0, a_2, a_6, a_8 to be zero. That is, if we start with an equation of C where some of these constants are zero then the number of parameters will decrease, and so will the dimension of the base in the corresponding fibration. Note, however, that we cannot set $a_8 = 0$, since a_8 is required to lie outside K^2 in the equation of C.

Now we get to the curves in Theorem 4.1 (ii). Define the three-dimensional cone

$$S' := \left\{ (u_0 : u_1 : u_2 : u_3 : u_4 : v) \in \mathbb{P}^5(k) \;\middle|\; \operatorname{rank} \begin{pmatrix} u_1 & u_2 & u_4 \\ u_0 & u_1 & u_3 \end{pmatrix} < 2 \right\}$$

and let $Q' = (0 : 0 : 0 : 0 : 0 : 1)$ be its vertex. The punctured cone $S' \setminus \{Q'\}$ can be described by the affine charts

$$\begin{aligned}
U_0 &:= \{ (1 : u : u^2 : w : uw : v) \mid u, w, v \in k \} \xrightarrow{\sim} \mathbb{A}^3, \\
U_2 &:= \{ (u^2 : u : 1 : uw : w : v) \mid u, w, v \in k \} \xrightarrow{\sim} \mathbb{A}^3, \\
U_3 &:= \{ (w : uw : u^2w : 1 : u : v) \mid w, u, v \in k \} \xrightarrow{\sim} \mathbb{A}^3, \\
U_4 &:= \{ (wu^2 : wu : w : u : 1 : v) \mid w, u, v \in k \} \xrightarrow{\sim} \mathbb{A}^3.
\end{aligned}$$

Theorem 4.6. *The algebraic variety*

$$\begin{aligned}
Z' :=\{ \, & ((u_0 : u_1 : u_2 : u_3 : u_4 : v), (a_0, a_2, b_2, b_3, b_4)) \in S' \times \mathbb{A}^5 \mid \\
& v^2 + u_0u_3 + b_2u_1^2 + b_3u_1u_2 + b_4u_2^2 = 0, \\
& u_3^2 + a_0u_0^2 + u_0u_1 + a_2u_1^2 = 0, \\
& u_4^2 + a_0u_1^2 + u_1u_2 + a_2u_2^2 = 0 \, \}
\end{aligned}$$

is an irreducible smooth sixfold. The projection

$$\pi' : Z' \longrightarrow \mathbb{A}^5$$

is proper and flat, and its fibres are rational projective curves of arithmetic genus 3*, which do not pass through the vertex* Q' *of* S'*. Each fibre has exactly one singular point.*

As in Theorem 4.5, we note that the projection $\pi' : Z' \to \mathbb{A}^5$ provides a 5-dimensional family of curves on the punctured cone $S' \setminus \{Q'\}$.

Proof. The closed subvariety Z' of $S' \times \mathbb{A}^5$ is clearly contained in the smooth open subvariety $(U_0 \cup U_2) \times \mathbb{A}^5$. In the first chart $U_0 \times \mathbb{A}^5 \cong \mathbb{A}^8$, the set Z' is described by the equations

$$v^2 + w + b_2u^2 + b_3u^3 + b_4u^4 = 0 \quad \text{and} \quad w^2 + a_0 + u + a_2u^2 = 0,$$

and so in this chart Z' is isomorphic to $\mathbb{A}^6$. In the second chart $U_2 \times \mathbb{A}^5 \cong \mathbb{A}^8$ the set Z' is given by the equations

$$v^2 + u^3w + b_2u^2 + b_3u + b_4 = 0 \quad \text{and} \quad w^2 + a_0u^2 + u + a_2 = 0,$$

whence also in this chart Z' is isomorphic to $\mathbb{A}^6$. Hence Z is irreducible, smooth and of dimension 6.

As S' is projective, the projection π' is proper. The fibre over the point $(a_0, a_2, a_4, a_6, a_8)$ in the base $\mathbb{A}^5$ is the algebraic curve given in the charts U_0 and U_2 by the above equations. In the first chart it is isomorphic to the smooth plane algebraic curve

$$v^4 + a_0 + u + a_2u^2 + b_2u^4 + b_3u^6 + b_4u^8 = 0,$$

while in the second chart it is isomorphic to the plane algebraic curve

$$v^2 + (w + a_2^{1/2})w^6 = 0,$$

whose only singular point $(0, 0)$ is unibranch of multiplicity 2 and singularity degree 3. Thus the fibres of $\pi' : Z' \to \mathbb{A}^5$ are rational curves of arithmetic genus 3, each with a unique singular point at

$$(0 : 0 : 1 : 0 : a_2^{1/2} : b_4^{1/2}).$$

Observe that the total space Z' is Cohen-Macaulay because it is smooth. Since the base $\mathbb{A}^5$ is smooth and the dimension of each fibre is equal to $\dim(Z) - \dim(\mathbb{A}^5) = 1$, it follows from [Eis91, Theorem 18.16] that the morphism π' is flat. □

4.3 Pencils of singular plane quartic curves in characteristic 2

In this section we investigate the geometry of two non-birationally equivalent fibrations by quartics over the projective line. Here the total spaces are surfaces which, unlike the total spaces in the previous section, have singularities, hence making it possible to apply the theory of (relatively) minimal surfaces. Accordingly, we will construct the minimal proper regular model of each fibration, and then we will study the structure of the new total spaces.

Throughout this section, k will denote a fixed algebraically closed field of characteristic 2.

First fibration

We build our first fibration out of the regular but non-smooth curves in Theorem 4.2 (iii), by setting $c = n_0 = 0$ and $m_1 = 1$.

Consider the projective algebraic surface over k

$$S \subseteq \mathbb{P}^2 \times \mathbb{P}^1$$

cut out by the bihomogeneous polynomial equation

$$T_0(Z^4 + X^2Y^2 + X^3Z) + T_1(Y^4 + X^2Z^2) = 0,$$

where X, Y, Z and T_0, T_1 represent the homogenous coordinates of $\mathbb{P}^2$ and $\mathbb{P}^1$ respectively. By the Jacobian criterion, the surface S has just one singular point, namely $P = ((1:0:0),(0:1))$. The second projection

$$\phi : S \longrightarrow \mathbb{P}^1$$

is clearly a proper map, and it yields a fibration by plane projective curves over $\mathbb{P}^1$. The fibre over each "finite" point $(1:t)$ of the base can be identified with the plane projective quartic

$$C_t : Z^4 + X^2Y^2 + X^3Z + t(Y^4 + X^2Z^2) = 0,$$

which has a unique singular point at

$$P_t := (0:1:t^{1/4})$$

of singularity degree 3. The only tangent line at the singular point P_t of C_t has multiplicity 2 (if $t^3 \neq 1$) or 3 (if $t^3 = 1$), while the tangent lines at the non-singular points of C_t are all bitangents (if $t \neq 0$) or lines meeting the curve at just one point (if $t = 0$). The fibre C_t is thus a rational plane projective quartic of arithmetic genus 3 with no inflection points.

Over the "infinite" point $(0:1)$ the fibre degenerates to the non-reduced curve

$$(Y^2 + XZ)^2 = 0.$$

Since its behaviour clearly differs from that of the other fibres, one might call it the *bad fibre* of the fibration.

The first projection $S \to \mathbb{P}^2$ is a birational map whose inverse is given by the assignment

$$(x:y:z) \longmapsto \big((x:y:z),(y^4 + x^2z^2 : z^4 + x^2y^2 + x^3z)\big).$$

By composing this inverse with ϕ we obtain a rational map

$$\tau : \mathbb{P}^2 \dashrightarrow \mathbb{P}^1, \quad (x:y:z) \longmapsto (y^4 + x^2z^2 : z^4 + x^2y^2 + x^3z),$$

which is not defined at $(1:0:0)$. This means that our fibration is a pencil of quartics, as the fibres of ϕ are precisely the elements of the linear system associated to τ (see the commutative diagram below).

$$\begin{tikzcd} \mathbb{P}^2 \times \mathbb{P}^1 & \supseteq & S \arrow[r] \arrow[d, "\phi"'] & \mathbb{P}^2 \arrow[dl, dashed, bend left, "\tau"] \\ & & \mathbb{P}^1 & \end{tikzcd}$$

Since our fibration $\phi : S \to \mathbb{P}^1$ is basically a singular surface fibered over the projective line, the theory of (relatively) minimal fibrations comes into place. So we can ask for a minimal proper regular model of $\phi : S \to \mathbb{P}^1$. And we can also ask for a minimal non-singular projective model of S, i.e., a minimal model of a desingularization of S.

There are two natural procedures we can follow to answer these questions. Firstly, we may resolve the indeterminacy locus of τ, i.e., blow up $\mathbb{P}^2$ at the point $(1:0:0)$. And secondly, we may resolve the singularity of S, i.e., blow up S at $P = ((1:0:0),(0:1))$.

Blowing up the surface S over its singular point P eight times we get a new fibration $f : \widetilde{S} \to S \xrightarrow{\phi} \mathbb{P}^1$. Its exceptional fibre is equal to a linear combination of smooth rational curves

$$\begin{aligned} f^*(0:1) = 2Z + E_1^{(1)} + E_2^{(1)} + 2E_1^{(2)} + 2E_2^{(2)} + 3E_1^{(3)} + 3E_2^{(3)} + 4E_1^{(4)} + 4E_2^{(4)} \\ + 5E_1^{(5)} + 5E_2^{(5)} + 6E_1^{(6)} + 6E_2^{(6)} + 7E_1^{(7)} + 7E_2^{(7)} + 8E_8^{(8)}, \end{aligned} \tag{4.1}$$

whose components intersect transversely according to the Coxeter-Dynkin diagram of Figure 4.1, where the dashed line means that the strict transform H of the curve $(1:0:0) \times \mathbb{P}^1$ in S does not actually belong to $f^*(0:1)$. We remark that the vertex Z represents the strict transform of the bad fibre.

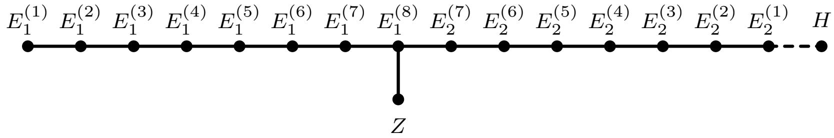

Figure 4.1: Dual diagram of the exceptional fibre $f^*(0:1)$

Since a fibre meets its components with intersection number zero, we can compute the self-intersection numbers of each component of $f^*(0:1)$. Thus

$$Z \cdot Z = -4, \qquad E_j^{(i)} \cdot E_j^{(i)} = -2 \text{ for each } i, j.$$

We see in particular that the non-singular surface $\widetilde{S}$ is relatively minimal over $\mathbb{P}^1$, that is, the fibre $f^*(0:1)$ contains no curves of self-intersection -1. We have thus proved the following result.

Theorem 4.7. *The fibration $f : \widetilde{S} \to \mathbb{P}^1$ is the minimal proper regular model of the fibration $\phi : S \to \mathbb{P}^1$. Its fibres over the points $(1:t)$ coincide with the corresponding fibres of ϕ, while its fibre over the infinite point $(0:1)$ is a linear combination of smooth rational curves as in (4.1), which intersect transversely according to the diagram in Figure 4.1.*

Even though $\widetilde{S}$ is relatively minimal over $\mathbb{P}^1$, it is not relatively minimal over the spectrum of k, that is, it is not a *relatively minimal model* according to the terminology of [Sha13, p. 121]. Indeed, there is a horizontal contractible curve on $\widetilde{S}$.

Theorem 4.8. *The strict transform $H \subseteq \widetilde{S}$ of the curve $(1:0:0) \times \mathbb{P}^1$ is a horizontal smooth rational curve of self-intersection -1. If we blow down succesively the curves H, $E_2^{(1)}$, $E_2^{(2)}$, …, $E_1^{(2)}$ and $E_1^{(1)}$, then we obtain a minimal surface isomorphic to the projective plane.*

Proof. In order to prove the theorem, we shall give an alternative construction of the non-singular model $\widetilde{S}$ and the fibres of f. This can be done by resolving the indeterminacy locus of the rational map $\tau : \mathbb{P}^2 \dashrightarrow \mathbb{P}^1$, which is birationally equivalent to our original fibration $\phi : S \to \mathbb{P}^1$, i.e., by blowing up $\mathbb{P}^2$ sixteen times over $(1:0:0)$. Hence we get a smooth surface $\overline{S}$, a birational morphism $\overline{S} \to \mathbb{P}^2$ and sixteen smooth rational curves $E_1, E_2, \ldots, E_{16}$ of self-intersection $-2, -2, \ldots, -1$ respectively, that are contracted to $(1:0:0)$ and whose configuration is given by the Dynkin diagram in Figure 4.2. Note that as in Figure 4.1, here the dashed line means that the strict transform E of the bad fibre $V(Y^2 + XZ)$ does not lie in the exceptional fibre of $\overline{S}$. As both dual diagrams suggest, we will show that there exists an isomorphism $\widetilde{S} \xrightarrow{\sim} \overline{S}$ under which the two diagrams correspond.

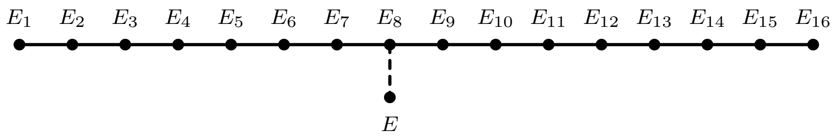

Figure 4.2: Dual diagram of the exceptional fibre of $\overline{S}$

The morphism $\overline{S} \to \mathbb{P}^1$ obtained in the first paragraph together with the map $\overline{S} \to \mathbb{P}^2$ induces a birational morphism $\overline{S} \to S$ such that the diagram

$$\begin{tikzcd}
\widetilde{S} \arrow[d] & \overline{S} \arrow[dl] \arrow[d] \\
S \arrow[r] \arrow[d, "\phi"'] & \mathbb{P}^2 \arrow[dl, dashed, bend left, "\tau"] \\
\mathbb{P}^1 &
\end{tikzcd}$$

is commutative. Since the morphism $\overline{S} \to \mathbb{P}^1$ contracts the bunch of curves $\{E_1, \ldots, E_{15}\}$ to $(0:1)$ and maps the curve E_{16} onto $\mathbb{P}^1$ (this follows from the blowup computations), the morphism $\overline{S} \to S$ contracts the bunch $\{E_1, \ldots, E_{15}\}$ to the singularity P of S and maps E_{16} onto the curve $(1:0:0) \times \mathbb{P}^1$.

Because the map $\widetilde{S} \to S \to \mathbb{P}^2$ contracts the sixteen curves $E_1^{(1)}, E_1^{(2)}, \ldots, E_2^{(1)}, H$ to the point $(1:0:0)$ and induces an isomorphism

$$\widetilde{S} \setminus (E_1^{(1)} \cup E_1^{(2)} \cup \cdots \cup E_2^{(1)} \cup H) \xrightarrow{\sim} \mathbb{P}^2 \setminus \{(1:0:0)\},$$

it can be written as a composition of sixteen blowups (see [Sha13, Theorem 4.10]), that is, there is a unique isomorphism $\widetilde{S} \xrightarrow{\sim} \overline{S}$ making the above diagram commute. By the previous paragraph, the isomorphism identifies $H = E_{16}$, $E_2^{(1)} = E_{15}$, $E_2^{(2)} = E_{14}$, and so on. This completes the proof of the theorem. $\square$

We highlight the fact that a non-singular projective model $\overline{S}$ of S was constructed by blowing up surfaces at *non-singular* points.

Second fibration

Now we get to our second fibration, which will be obtained from Theorem 4.2 (i) by setting $a_0 = a_2$. The analysis will be quite similar to that of the first one, and so some details will be omitted.

Consider the projective algebraic surface over k

$$S \subseteq \mathbb{P}^2 \times \mathbb{P}^1$$

defined by the bihomogeneous polynomial

$$T_0(Y^3Z + X^4) + T_1Z^4,$$

which by the Jacobian criterion has a unique singular point, namely $P = ((0:1:0),(0:1))$. The second projection

$$\phi : S \longrightarrow \mathbb{P}^1$$

is a proper map, and it yields a fibration by plane projective curves over $\mathbb{P}^1$. The fibre over each "finite" point $(1:t)$ of the base can be identified with the plane curve

$$C_t : Y^3Z + X^4 + tZ^4 = 0.$$

The only singular point $P_t = (t^{1/4} : 0 : 1)$ of C_t is unibranch of multiplicity 3 and singularity degree 3, and its tangent line meets the curve only at P_t. The fibre C_t is thus a rational plane projective quartic of arithmetic genus 3, with no inflection points.

The fibre over the "infinite" point $(0:1)$ can be identified with the degenerated curve

$$Z^4 = 0,$$

and since its properties differ from those of the other fibres, we say it is the *bad fibre* of the fibration.

The first projection $S \to \mathbb{P}^2$ is a birational map whose inverse is given by the assignment

$$(x:y:z) \longmapsto \big((x:y:z),(z^4 : x^4 + y^3z)\big).$$

By composing this inverse with ϕ we obtain a rational map

$$\tau : \mathbb{P}^2 \dashrightarrow \mathbb{P}^1, \quad (x:y:z) \longmapsto (z^4 : x^4 + y^3z),$$

which is not defined at $(0:1:0)$. This means that our fibration is a pencil of quartics, as the fibres of ϕ are precisely the elements of the linear system associated to τ.

Since there is one bad fibre and the total space is a surface, as in the previous example we may ask for the minimal models associated to ϕ. As before, we will obtain them by resolving the singularity of $\widetilde{S}$ and by resolving the indeterminacy locus of τ.

Blowing up the singularity P of S eight times we get a new fibration $f : \tilde{S} \to S \xrightarrow{\phi} \mathbb{P}^1$. Its exceptional fibre is equal to a linear combination of smooth rational curves

$$\begin{aligned} f^*(0:1) = 4Z &+ 3E_1^{(1)} + E_2^{(1)} + 6E_1^{(2)} + 2E_2^{(2)} + 9E_1^{(3)} + 3E_2^{(3)} + 12E_1^{(4)} + 4E_2^{(4)} \\ &+ 11E_1^{(5)} + 5E_2^{(5)} + 10E_1^{(6)} + 6E_2^{(6)} + 9E_1^{(7)} + 7E_2^{(7)} + 8E_8^{(8)}, \end{aligned} \tag{4.2}$$

whose configuration is given by the Coxeter-Dynkin diagram in Figure 4.3, where the dashed line means that the birational transform H of the curve $(1:0:0) \times \mathbb{P}^1$ does not lie in $f^*(0:1)$. Observe that the point Z represents the strict transform of the bad fibre.

Since a fibre meets its components with intersection number zero, we can compute the self-intersection numbers of each component of $f^*(0:1)$. Therefore,

$$Z \cdot Z = -3, \qquad E_j^{(i)} \cdot E_j^{(i)} = -2 \text{ for each } i, j.$$

We see in particular that $f^*(0:1)$ contains no curves of self-intersection -1. We have thus proved the following result.

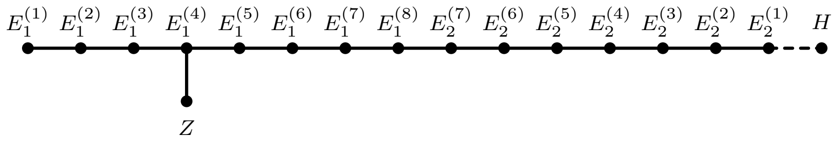

Figure 4.3: Dual diagram of the exceptional fibre $f^*(0:1)$

Theorem 4.9. *The fibration* $f : \widetilde{S} \to \mathbb{P}^1$ *is the minimal proper regular model of the fibration* $\phi : S \to \mathbb{P}^1$. *Its fibres over the points* $(1:t)$ *coincide with the corresponding fibres of* ϕ*, while its fibre over the infinite point* $(0:1)$ *is a linear combination of smooth rational curves as in* (4.2)*, which intersect transversely according to the diagram in Figure 4.3.*

Even though $f : \widetilde{S} \to \mathbb{P}^1$ is the minimal model of the fibration $\phi : S \to \mathbb{P}^1$, the surface $\widetilde{S}$ is not relatively minimal over $\operatorname{Spec} k$. In fact, it contains a horizontal contractible curve.

Theorem 4.10. *The strict transform* $H \subseteq \widetilde{S}$ *of the curve* $(0:1:0) \times \mathbb{P}^1$ *is a horizontal smooth rational curve of self-intersection* -1. *If we blow down succesively the curves* H, $E_2^{(1)}$, $E_2^{(2)}$, $\dots$, $E_1^{(2)}$ *and* $E_1^{(1)}$*, then we obtain a minimal surface isomorphic to the projective plane.*

The proof is entirely similar to that of Theorem 4.8. Here we will outline only the most important ideas.

Proof. In order to obtain an alternative realization of the minimal model of the fibration $\phi : S \to \mathbb{P}^1$ we resolve the indeterminacy locus of the rational map $\tau : \mathbb{P}^2 \dashrightarrow \mathbb{P}^1$. We can achieve this by blowing up $\mathbb{P}^2$ sixteen times over $(0:1:0)$. We thus get a smooth surface $\overline{S}$, a birational map $\overline{S} \to \mathbb{P}^2$ and sixteen rational curves E_1, E_2, $\dots$, E_{16} of self-intersection -2, -2, $\dots$, -1 respectively, that are contracted to $(0:1:0)$ by $\overline{S} \to \mathbb{P}^2$. The morphism $\widetilde{S} \to S \to \mathbb{P}^2$ will in turn induce an isomorphism $\widetilde{S} \to \overline{S}$, under which Diagrams 4.3 and 4.4 will correspond. $\square$

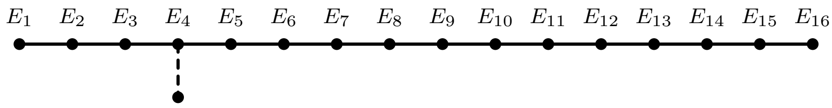

Figure 4.4: Dual diagram of the exceptional fibre of $\overline{S}$

Chapter 5

More examples

In this chapter we collect some examples of function fields, curves and fibrations by curves that did not fit well into the previous chapters. To this end, we shall employ the notation and terminology introduced in Sections 2.1 and 2.2.

In the previous chapters the emphasis was placed on non-conservative function fields of genera $g = 3$, $\overline{g} = 0$; equivalently, we focussed mainly on fibrations by rational curves of arithmetic genus 3. Now we complete the picture by exhibiting fibrations and function fields such that $g = 3$ and such that the value of $\overline{g}$ is positive.

In the first section we construct a fibration by geometrically elliptic curves of arithmetic genus 3 out of a function field of genera $g = 3$, $\overline{g} = 1$ with a unique singular (non-decomposed) prime of singularity degree 2. This fibration gives rise to an interesting phenomenon: the j-invariant associated to the normalization of each fibre varies in accordance with the value of the point on the base.

In the second section we present a one-dimensional fibration by curves of arithmetic genus 3 and geometric genus 2, while in the last section we present examples of function fields of genera $g = 3$, $\overline{g} = 0$ with several singular primes. By the genus drop formula (2.4), a function field with $g = 3$, $\overline{g} = 0$ can have two or three singular primes, and we verify that the two cases can occur. More than that, when the function field has two singular primes, one of singularity degree 1 and the other of singularity degree 2, we show that the singular prime of singularity degree 2 can be decomposed for one family of examples, and non-decomposed for another.

5.1 A fibration by singular curves of arithmetic genus 3 and geometric genus 1

We present in this section a fibration by geometrically elliptic curves of arithmetic genus 3.

The function field

Consider the function field $F|K = K(x, y)|K$ in characteristic 2 defined by the equation

$$y^4 + xy^2 = x^3 + ax, \quad a \in K \setminus K^2.$$

We claim that $F|K$ is has genera

$$g = 3, \qquad \overline{g} = 1,$$

and furthermore, that it has a unique singular prime of singularity degree 2.

Since the Frobenius pullback $F_1|K = K(x, y^2)|K$ is defined by the polynomial equation in y^2 and x

$$(y^2)^2 + xy^2 = x^3 + ax,$$

it is an elliptic function field with discriminant $\Delta = a^2 \neq 0$. Thus the function field $F_1|K$ has genus 1, and so does the extended function field $\overline{K}F_1|\overline{K}$. Equivalently, $g_1 = g_2 = \cdots = 1$, whence $\overline{g} = 1$. The j-invariant of $F|K$, as introduced by Tate [Tat74] in characteristic 2, is equal to $j = a^{-2}$.

Since the center $(x(\mathfrak{p}), y(\mathfrak{p}))$ of every singular prime $\mathfrak{p}$ is necessarily a singular point of the plane curve (see [Sal11, Corollary 4.5]), it follows from the Jacobian criterion that $x(\mathfrak{p}) = a^{1/2}$ and $y(\mathfrak{p}) = 0$, that is, $v_\mathfrak{p}(x^2 + a) > 0$ and $v_\mathfrak{p}(y) > 0$. We shall see that there is only one prime satisfying these conditions, and that it has singularity degree 2. This will then imply by the genus drop formula (2.4) that $F|K$ has genus $g = 3$.

Set the function $t := x^2 + a \in F$ and note that the second Frobenius pullback $F_2|K = K(t, y^4)|K$ is defined by the cubic polynomial equation in t and y^4

$$(y^4)^2 + (t + a)y^4 = (t + a)t^2.$$

Let $\mathfrak{p}$ be a prime of $F|K$ satisfying the condition $x(\mathfrak{p}) = a^{1/2}$, i.e, such that $t(\mathfrak{p}) = 0$, or equivalently $v_\mathfrak{p}(t) > 0$. From the above equation, it follows that the value $y^4(\mathfrak{p})$ of $y^4 \in F_2$ at $\mathfrak{p}$ belongs to $\{0, a\}$. Without loss of generality we may assume that $y^4(\mathfrak{p}) = 0$. Indeed, since the function y^4 is a root of the separable irreducible polynomial $T^2 + (t + a)T + t^2(t + a) \in K(t)[T]$ there is a $K(t)$-automorphism σ of $F_2 = K(t, y^4)$ mapping y^4 to $y^4 + t + a$, and therefore if $y^4(\mathfrak{p}) = a$ occurs then there will be another prime $\mathfrak{p}'$ with the property that $v_{\mathfrak{p}'_2} := v_{\mathfrak{p}_2} \circ \sigma$, i.e., such that $t(\mathfrak{p}') = 0$ and $y^4(\mathfrak{p}') = 0$.

The previous argument together with the fundamental inequality shows that there are exactly two primes of $F_2|K = K(t, y^4)|K$ (the restricted prime $\mathfrak{p}_2$ being one of them) lying over the rational prime of $K(t)|K$ whose local parameter is the function t. Since the argument shows as well that both primes are rational, we conclude that $\mathfrak{p}_2$ is a rational prime with local parameter t, and hence that we can compute the singularity degree $\delta(\mathfrak{p})$ of $\mathfrak{p}$ by using the algorithm developed in [BS87] (see Theorem 2.3 and the discussion that follows). We conclude in addition that the prime $\mathfrak{p}$ is uniquely determined by the conditions $x(\mathfrak{p}) = a^{1/2}$ and $y(\mathfrak{p}) = 0$.

It remains to show that $\mathfrak{p}$ has singularity degree 2. Indeed, because $x(\mathfrak{p}) = a^{1/2}$ does not belong to K the prime $\mathfrak{p}_1$ is unramified over F_2 with residue field $K_{\mathfrak{p}_1} = K(x(\mathfrak{p}))$, and so the equality $x^2 = a + t$ implies that $\delta(\mathfrak{p}_1) = \frac{1}{2}v_{\mathfrak{p}_2}(dx^2) = \frac{1}{2}v_{\mathfrak{p}_2}(dt) = 0$ by Theorem 2.3. From the relation

$$(y^4)^2 + (t + a)y^4 = t^2(t + a)$$

we obtain y^4 as a power series in t

$$y^4 = t^2 + a^{-1}t^4 + a^{-2}t^5 + \cdots .$$

Since $v_{\mathfrak{p}_2}(y^4) = 2$, which means that $\mathfrak{p}$ is ramified over F_1 with local parameter y, we conclude from Theorem 2.3 that $\mathfrak{p}$ has singularity degree $\delta(\mathfrak{p}) = \frac{1}{2}v_{\mathfrak{p}_2}(dy^4) = 2$, as desired.

The curve

The geometrically integral regular complete curve C over K that is associated to $F|K$ is defined by the quartic polynomial equation

$$Y^4 + XY^2Z + X^3Z + aXZ^3 = 0,$$

where we recall that $a \in K \setminus K^2$. This curve has arithmetic genus $g = 3$, it is non-smooth and it has a unique non-smooth point of singularity degree 2, which is non-decomposed.

The base extension $\overline{C} = C \otimes_K \overline{K}$ is an integral complete algebraic curve over $\overline{K}$ of arithmetic genus $g = 3$ and geometric genus $\overline{g} = 1$, with a unique singular point at

$$(a^{1/2} : 0 : 1)$$

of multiplicity 2 and singularity degree 2. The normalization of $\overline{C}$ is an elliptic curve over $\overline{K}$ with cubic model

$$y^2 + xy = x^3 + a^{-1/2}x,$$

and with discriminant and j-invariant equal to

$$\Delta = a \neq 0 \quad \text{and} \quad j = a^{-1}.$$

The fibration

We now construct a fibration out of the above curve C. Let k be an algebraically closed field of characteristic 2. Consider the surface

$$S \subseteq \mathbb{P}^2 \times \mathbb{A}^1$$

cut out by the equation

$$Y^4 + XY^2Z + X^3Z + TXZ^3 = 0,$$

where X, Y, Z represent the homogeneous coordinates of $\mathbb{P}^2$, and where T represents the only affine coordinate of $\mathbb{A}^1$. It has a unique singular point at $P := ((0 : 0 : 1), 0)$. The projection

$$\phi : S \longrightarrow \mathbb{A}^1$$

is a proper map ($\mathbb{P}^2$ is projective) and yields a fibration by plane projective curves. The fibre over the point t of the base $\mathbb{A}^1$ can be identified with the plane projective quartic

$$C_t : Y^4 + XY^2Z + X^3Z + tXZ^3 = 0,$$

which by the Jacobian criterion has a unique singular point, namely

$$P_t = (t^{1/2} : 0 : 1).$$

If $t \neq 0$ then P_t is a unibranch point of multiplicity 2 and singularity degree 2, and C_t is an irreducible curve of arithmetic genus 3, whose normalization is an elliptic curve of discriminant t and j-invariant t^{-1}.

If $t = 0$ then P_t is a two-branched point of multiplicity 3 and singularity degree 3, and C_t is a rational irreducible curve of arithmetic genus 3. Thus the behaviour of the fibre C_0 differs from that of the other fibres, and hence one might call it the *bad fibre* of the fibration.

We note that the only singular point P of the surface S is contained in the bad fibre. Thus it seems possible to find the minimal model of the fibration $\phi : S \to \mathbb{A}^1$ by proceeding as in Section 4.3 . The strategy would consist in blowing up S at P in an attempt to get rid of the bad fibre, so that after finitely many blowups it hopefully becomes a union of rational curves.

5.2 A fibration by singular curves of arithmetic genus 3 and geometric genus 2

In this section we construct a fibration by projective curves of arithmetic genus 3 and geometric genus 2. Since computing the genus of the function field is difficult in this case, we present the fibration directly, before the curve and the function field. In this way, the genera g and $\overline{g}$ can be computed by looking at the fibres, by means of extrinsic methods (blowups).

The fibration

Let k be an algebraically closed field of characteristic 2. Consider the surface

$$S \subseteq \mathbb{P}^2 \times \mathbb{A}^1$$

cut out by the equation

$$Y^3Z + X^4 + X^3Z + T(X^2Z^2 + XZ^3) = 0,$$

where X, Y, Z stand for the homogeneous coordinates of $\mathbb{P}^2$, and where T stands for the only affine coordinate of $\mathbb{A}^1$. It has three singular points, namely $P = ((1 : 0 : 0), 0)$, $Q = ((0 : 0 : 1), 0)$ and $R = ((1 : 0 : 1), 1)$. The projection

$$\phi : S \longrightarrow \mathbb{A}^1$$

is proper ($\mathbb{P}^2$ is projective) and yields a fibration by plane projective curves. The fibre over the point t of the base $\mathbb{A}^1$ can be identified with the plane projective quartic

$$C_t : Y^3Z + X^4 + X^3Z + t(X^2Z^2 + XZ^3) = 0,$$

which by the Jacobian criterion has a unique singular point, namely

$$P_t = (t^{1/2} : 0 : 1).$$

If $t \neq 0, 1$ then P_t is a unibranch point of multiplicity 2 and singularity degree 1, and C_t is an irreducible curve of arithmetic genus 3, whose normalization is a curve of arithmetic genus 2.

If $t = 0$ or $t = 1$ then P_t is a three-branched point of multiplicity 3 and singularity degree 3, and C_t is a rational irreducible curve of arithmetic genus 3. Thus the behaviour of the fibres C_0 and C_1 differ from that of the other fibres, and hence one might call them the *bad fibres* of the fibration.

A similar remark as in the end of Section 5.1 applies here. Since the three singular points P, Q and R of the surface S are contained in the bad fibres C_0 and C_1, that is, $P, Q \in C_0$ and $R \in C_1$, it seems possible to find the minimal model of the fibration $\phi : S \to \mathbb{A}^1$ by proceeding as in Section 4.3 . The strategy would consist in blowing up S at the three points P, Q, R in an attempt to get rid of the bad fibres, so that after finitely many blowups they hopefully become unions of rational curves.

The curve

The geometrically integral regular complete curve C over K that is associated to the fibration $\phi : T \to B$ is the plane projective curve defined by the quartic polynomial equation

$$Y^3Z + X^4 + X^3Z + a(X^2Z^2 + XZ^3) = 0,$$

where $a \in K \setminus K^2$. This curve has arithmetic genus $g = 3$, it is non-smooth and it has a unique non-smooth point of singularity degree 1, which is non-decomposed by Proposition 2.8.

The base extension $\overline{C} = C \otimes_K \overline{K}$ is an integral complete algebraic curve over $\overline{K}$ of arithmetic genus 3 and geometric genus $\overline{g} = 2$, with a unique singular point at

$$(a^{1/2} : 0 : 1)$$

of multiplicity 2 and singularity degree 1. The normalization of $\overline{C}$ is a smooth curve of arithmetic genus 2.

The function field

The function field $F|K$ of the curve C is given by $F|K = K(x, y)|K$, where the functions x and y satisfy the following relation

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

and where we recall that $a \in K \setminus K^2$. This function field has genera $g = 3$, $\overline{g} = 2$ and a unique singular prime $\mathfrak{p}$ of singularity degree 1. The prime $\mathfrak{p}$ is centered at $(x(\mathfrak{p}), y(\mathfrak{p})) = (a^{1/2}, 0)$, that is, it satisfies the conditions $v_{\mathfrak{p}}(x^2 + a) > 0$ and $v_{\mathfrak{p}}(y) > 0$.

5.3 Geometrically rational function fields with several singular primes

The following proposition provides examples of function fields of genera $g = 3$ and $\overline{g} = 0$ with two and three singular primes.

Proposition 5.1. *Consider the function field $F|K = K(x, z, y)|K$ in characteristic $p = 2$ defined by the following normal form*

$$z^2 = ax^2 + x + c,$$
$$y^2 = z(x^2 + c_1x + c_0) + a_4,$$

where $c, a, c_0, c_1, a_4 \in K$ are constants satisfying the conditions $a, a_4 \notin K^2$ and $c_1 \neq 0$. Then $F|K$ has genera $g = 3$, $\overline{g} = 0$ and the following assertions hold.

(i) *If the roots of the polynomial $x^2 + c_1x + c_0$ lie in K, then $F|K$ has three singular primes, each of singularity degree* 1.

(ii) *If the roots of the polynomial $x^2+c_1x+c_0$ do not lie in K, then $F|K$ has two singular primes of singularity degrees* 1 *and* 2. *In this case the singular prime of singularity degree* 2 *is decomposed.*

Proof. We start by noting that the Frobenius pullbacks of $F|K$ are equal to

$$F_1|K = K(x,z)|K,$$
$$F_2|K = K(x)|K,$$

so in particular $g_2 = \overline{g} = 0$. Let $\mathfrak{p}$ be the pole of x, i.e., the only prime $\mathfrak{p}$ of $F|K$ such that $v_{\mathfrak{p}}(x) < 0$. Since $F|K$ is the function field of the affine plane curve over K

$$y^4 = (ax^2 + x + c)(x^4 + c_1^2 x^2 + c_0^2) + a_4^2,$$

it follows from the Jacobian criterion that every prime $\mathfrak{q} \neq \mathfrak{p}$ that is not a zero of the function

$$\frac{dy^4}{dx} = x^4 + c_1^2 x^2 + c_0^2 \in F$$

is non-singular. We shall see that the prime $\mathfrak{p}$ and the zeros of the function $x^2 + c_1 x + c_0 \in F$ are the only singular primes of $F|K$, and that the sum of their singularity degrees is equal to 3. This will then imply by the genus drop formula (2.4) that $F|K$ has genus $g = 3$.

We prove that the prime $\mathfrak{p}$ has singularity degree $\delta(\mathfrak{p}) = 1$. To this end, we introduce the functions $\breve{x} := x^{-1}$, $\breve{z} := zx^{-1}$ and $\breve{y} := yx^{-2}$, which satisfy the relations

$$\breve{z}^2 = a + \breve{x} + c\breve{x}^2,$$
$$\breve{y}^2 = \breve{z}(\breve{x} + c_1\breve{x}^2 + c_0\breve{x}^3) + a_4\breve{x}^4.$$

Note that $\breve{x}$ is a local parameter at the rational prime $\mathfrak{p}_2$ of $F_2|K$. Since $\breve{z}(\mathfrak{p}) = a^{1/2} \notin K$, the prime $\mathfrak{p}_1$ is unramified over F_2 with residue field $K_{\mathfrak{p}_1} = K(\breve{z}(\mathfrak{p}))$, and so $\delta(\mathfrak{p}_1) = \frac{1}{2}v_{\mathfrak{p}_2}(d\breve{z}^2) = 0$ by Theorem 2.3. As $v_{\mathfrak{p}_1}(\breve{y}^2) = 1$, it follows that $\mathfrak{p}$ is ramified over F_1 with local parameter $\breve{y}$, so we conclude $\delta(\mathfrak{p}) = \frac{1}{2}v_{\mathfrak{p}_2}(d\breve{y}^4) = 1$, again by Theorem 2.3.

Now we prove items (i) and (ii).

(i) We must show that the two zeros of the function $x^2 + c_1 x + c_0 \in F$, which correspond to the two roots of the polynomial $x^2 + c_1 x + c_0 \in K[x]$, have singularity degree 1. Let $r \in K$ be one such root and let $\mathfrak{q}$ be the zero of the function $x + r$. Replacing x with $x + r$ we may assume that $c_0 = 0$ and that x is a local parameter at the rational prime $\mathfrak{q}_2$ of $F_2|K = K(x)|K$.

Assume that $z(\mathfrak{q}) = c^{1/2} \notin K$. Then $\mathfrak{q}_1$ is unramified over F_2 with residue field $K_{\mathfrak{q}_1} = K(z(\mathfrak{q}))$ and $\delta(\mathfrak{q}_1) = \frac{1}{2}v_{\mathfrak{q}_2}(dz^2) = 0$ by Theorem 2.3. If $y(\mathfrak{q}) \notin K_{\mathfrak{q}_1}$, then $\mathfrak{q}$ is inertial over F_1 with residue field $K_{\mathfrak{q}} = K(z(\mathfrak{q}), y(\mathfrak{q}))$ and so $\delta(\mathfrak{q}) = \frac{1}{2}v_{\mathfrak{q}_2}(dy^4) = 1$ by Theorem 2.3. In the opposite case $y(\mathfrak{q}) \in K(z(\mathfrak{q}))$ we have $f(\mathfrak{q}) = 0$ for some function f in $y + K + Kz$, so that $\mathfrak{q}$ is ramified over F_1 with local parameter f as

$$v_{\mathfrak{q}_2}(df^4) = v_{\mathfrak{q}_2}(dy^4) = 2 < 4,$$

and therefore $\delta(\mathfrak{q}) = \frac{1}{2}v_{\mathfrak{q}_2}(dy^4) = 1$ by Theorem 2.3.

Suppose next that $z(\mathfrak{q}) = c^{1/2} \in K$. Then $\mathfrak{q}_1$ is ramified (and therefore rational) over F_2 with local parameter $w := z + c^{1/2} \in F_1$. From the relation $x + ax^2 = w$ we obtain x as a power series in w

$$x = w^2 + aw^4 + a^3w^8 + a^7w^{16} + \cdots,$$

and hence y^2 as a power series in w

$$y^2 = a_4 + c_1w^3 + (c^{1/2}c_1a + a^{1/2})w^4 + \cdots.$$

Since $a_4 \notin K^2$, we thus see from Proposition 2.5 that $\delta(\mathfrak{q}) = \frac{1}{2}(3 - 0 - 1) = 1$.

(ii) Item (ii) follows from item (i). Indeed, in this case there is only one prime $\mathfrak{q}$ of $F|K$ such that $v_{\mathfrak{q}}(x^2+c_1x+c_0) > 0$, which decomposes on extending the base field of $F|K$ from K to the splitting field L of the quadratic polynomial $x^2 + c_1x + c_0 \in K[x]$. Thus there are exactly two primes $\mathfrak{q}', \mathfrak{q}''$ of $LF|L$ lying over $\mathfrak{q}$, one for each root of $x^2+c_1x+c_0$, and the two of them have singularity degree 1 by the proof of item (i). Since separable base field extensions preserve singularity degrees (see page 14), this implies that $\mathfrak{q}$ has singularity degree 2. $\square$

Remark. By following the same ideas in the proof one can show that if in the normal form the constants c, c_1 and c_0 are set to be zero, that is,

$$\begin{aligned} z^2 &= ax^2 + x, && a \notin K^2, \\ y^2 &= zx^2 + a_4, && a_4 \notin K^2, \end{aligned}$$

then the resulting function field has genera $g = 3$, $\overline{g} = 0$, with two singular primes of singularity degrees 1 and 2. In this case the singular prime of singularity degree 2 *is non-decomposed.*

Bibliography

[Art67] E. Artin. *Algebraic Numbers and Algebraic Functions.* Gordon and Breach, New York, 1967.

[Ber82] E. Bertini. Sui sistemi lineari. *Instit. Lombardo Accad. Sci. Lett. Rend. A Istituto(II)*, 15:24–28, 1882.

[BM76] E. Bombieri and D. Mumford. Enriques' classification of surfaces in char. p. III. *Invent. Math.*, 35:197–232, 1976.

[BN79] H. Borges Neto. *Mudança de gênero e classificação de corpos de gênero 2.* PhD thesis, Instituto de Matemática Pura e Aplicada, 1979.

[BS87] H. Bedoya and K.-O. Stöhr. An algorithm to compute discrete invariants of singular primes in function fields. *J. of Number Theory*, 27(3):310–323, 1987.

[Che51] C. Chevalley. *Introduction to the Theory of Algebraic Functions of One Variable.* Number VI in Mathematical Surveys. American Mathematical Society, New York, 1951.

[DW82] R. Dedekind and H. Weber. Theorie der algebraischen Functionen einer Veränderlichen. *J. Reine Angew. Math.*, 92:181–290, 1882.

[Eis91] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1991.

[GD67] A. Grothendieck and J. Dieudonné. Éléments de géométrie algébrique. *Inst. Hautes Études Sci. Publ. Math.*, (4, 8, 11, 17, 20, 24, 28, 32), 1961–1967.

[Hir57] H. Hironaka. On the arithmetic genera and the effective genera of algebraic curves. *Mem. Coll. Sci. Univ. Kyoto Ser. A. Math.*, 30:177–195, 1957.

[HL02] K. Hensel and G. Landsberg. *Theorie der algebraischen Funktionen einer Variabeln und ihre Anwendung auf algebraische Kurven und Abelsche Integrale.* B. G. Teubner, Leipzig, 1902.

[Kim69] J. Kimura. On nonconservativity of algebraic function fields. *Proc. Japan Acad.*, 45:595–597, 1969.

[Kod63] K. Kodaira. On compact analytic surfaces. II, III. *Ann. of Math. (2)*, 78:1–40, 1963.

[Lan79] W. Lang. Quasi-elliptic surfaces in characteristic three. *Ann. Sci. École Norm. Sup. (4)*, 12(4):473–500, 1979.

[Liu02] Q. Liu. *Algebraic Geometry and Arithmetic Curves.* Oxford University Press, New York, 2002.

[Mat50] T. Matsusaka. The theorem of Bertini on linear systems in modular fields. *Mem. Coll. Sci. Univ. Kyoto Ser. A. Math.*, 26:51–62, 1950.

[Nér64] A. Néron. Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. *Inst. Hautes Études Sci. Publ. Math.*, (21), 1964.

[Que71] C. Queen. Non-conconservative function fields of genus 1. I. *Arch. Math. (Basel)*, 22:712–623, 1971.

[Ray78] M. Raynaud. Contre-exemple au "vanishing theorem" en caractéristique $p > 0$. In *C. P. Ramanujam—a tribute*, number 8, pages 271–278, Berlin-New York, 1978. Tata Inst. Fund. Res. Studies in Math., Springer-Verlag.

[Ros52] M. Rosenlicht. Equivalence relations on algebraic curves. *Ann of Math. (2)*, 56:169–191, 1952.

[Sal11] R. Salomão. Fibrations by nonsmooth genus three curves in characteristic three. *Journal of Pure and Applied Algebra*, 215(8):1967–1979, 2011.

[Sal14] R. Salomão. Fibrations by curves with more than one nonsmooth point. *Bull. Braz. Math. Soc. (N.S.)*, 45(2):267–292, 2014.

[Sch09] S. Schröer. On genus change in algebraic curves over imperfect fields. *Proc. Amer. Math. Soc.*, 137(4):1239–1243, 2009.

[SCS16] A. Simarra Cañate and K-O. Stöhr. Fibrations by non-smooth projective curves of arithmetic genus two in characteristic two. *J. Pure Appl. Algebra*, 220(9):3282–3299, 2016.

[Ser58] J.-P. Serre. Sur la topologie des variétés algébriques en caractéristique p. In *Symposium internacional de topología algebraica International symposium on algebraic topology*, pages 24–53, Mexico City, 1958. Universidad Nacional Autónoma de México and UNESCO.

[Ser00] J.-P. Serre. *Local Algebra.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.

[Sev08] F. Severi. *Lezioni di geometria algebrica: geometria sopra una curva: superficie di Riemann; integrali abeliani.* Number VI. Draghi, Padova, 1908.

[Sha13] I. R. Shafarevich. *Basic Algebraic Geometry 1.* Springer-Verlag, Berlin Heidelberg, third edition, 2013.

[Sti78] H. Stichtenoth. Zur Konservativität algebraischer Funktionenkörper. *J. Reine Angew. Math.*, 301:30–45, 1978.

[Stö88] K.-O. Stöhr. On singular primes in function fields. *Arch. Math.*, 50(2):156–163, 1988.

[Stö99] K.-O. Stöhr. Hyperelliptic Gorenstein curves. *J. Pure Appl. Algebra*, 135(1):93–105, 1999.

[Stö04] K.-O. Stöhr. On Bertini's theorem in characteristic p for families of canonical curves in $\mathbb{P}^{(p-3)/2}$. *Proc. Lond. Math. Soc.*, 189(3):291–316, 2004.

[Stö07] K.-O. Stöhr. On Bertini's theorem for fibrations by plane projective quartic curves in characteristic five. *J. Algebra*, 315(2):502–526, 2007.

[Tat52] J. Tate. Genus change in inseparable extensions of function fields. *Proc. Amer. Math. Soc.*, 3:400–406, 1952.

[Tat74] J. Tate. The arithmetic of elliptic curves. *Invent. Math.*, 23:179–206, 1974.

[Zar44] O. Zariski. The theorem of Bertini on the variable singular points of a linear system of varieties. *Trans. Am. Math. Soc.*, 56:130–140, 1944.