Towers of Function Fields over Cubic Finite Fields

Doctoral Thesis by

Jorge Nicolás Caro Montoya

Supervised by

Arnaldo Garcia

IMPA - Instituto Nacional de Matemática Pura e Aplicada
Rio de Janeiro - April 2009

Abstract

In this work we consider two towers of function fields over finite fields with cubic cardinality. For the first of these towers (which was introduced by Bassa, Garcia and Stichtenoth) we explicitly calculate the genus of each one of its steps, using the ramification theory of Artin-Schreier extensions of function fields. For the second tower (which was introduced by Ihara) we prove by structural arguments that its limit is greater or equal than generalized Zink's lower bound, showing in this way its asymptotic goodness; for the proof we use the machinery of completions. We also exhibit the relations between these towers and the tower introduced by Bezerra, Garcia and Stichtenoth.

Keywords: Towers of function fields, cubic finite fields, limits of towers, generalized Zink's bound, completions.

Acknowledgments

Hay muchos a quienes quiero agradecer, pues ciertamente la culminación de este trabajo no fue apenas un esfuerzo académico personal, sino que requirió del apoyo de muchas personas a través de estos largos años.

A Dios, por preservarme (¡por segunda vez!), por darme "salud, dinero y amor" en las justas proporciones, y por haberme agraciado con el gusto por la Matemática.

A mi familia, por haber inculcado en mí tantos valores, incluyendo el amor al estudio, y apoyarme en mi proyecto de vida a pesar de las diversas dificultades.

A mi esposa Milena, por su inagotable amor y paciencia ante la adversidad de la distancia todos estos años, y por el constante soporte anímico y los buenos consejos (los cuales incluían tirones de orejas en los momentos apropiados). No solamente a ella, sino a su familia, por acogerme como un miembro más, y pretendo que estas pocas líneas lo que reflejen en realidad sea la profundidad de mis sentimientos al respecto.

Al IMPA, por concederme esta oportunidad de oro de recibir educación de primera en un ambiente tan favorable, y al CNPq y a CAPES por permitirme llevar a cabo estos estudios sin las odiosas preocupaciones de tipo financiero. Esto no habría sido posible sin el apoyo previo de los profesores (de mi *alma mater* la Universidad Nacional de Colombia, sede Bogotá) Leonardo Rendón, Myriam Campos, Rodrigo De Castro y Stella Huérfano, quienes gentilmente me recomendaron ante el IMPA (recomendaciones, que, felizmente, fueron tenidas en cuenta a mi favor).

A los funcionarios del IMPA, por la constante amabilidad y disposición para ayudarme en los diversos asuntos referentes a mis estudios.

A mi madre en Brasil, la señora Yeda Correia da Costa, *In Memoriam*, por el cariño, las atenciones y su buen humor durante mi estadía en su casa en Rio de Janeiro. Sinceramente espero que ahora esté en un lugar mejor.

A los profesores del IMPA por la excelente formación matemática recibida. Agradezco en particular a los profesores Eduardo Esteves y Arnaldo Garcia por los cursos de álgebra, a la profesora Carolina Araujo por aceptar hacer parte del jurado de mi examen de calificación a última hora, y al profesor Karl-Otto Stöhr por los cursos impartidos y por las discusiones matemáticas fuera de clase, las cuales abarcaban desde aclaraciones en demostraciones técnicas hasta datos históricos, pasando por inquietudes sobre problemas misceláneos del álgebra.

A los miembros del jurado de mi tesis Arnaldo Garcia, Eduardo Esteves, Karl-Otto Stöhr, Amilcar Pacheco y Juscelino Bezerra, particularmente por aceptar juzgar este trabajo a pesar de las imposiciones de tiempo.

A mi orientador, el profesor Arnaldo Garcia, por su disposición hacia mí durante la maestría y principalmente durante el doctorado, pues no solamente recibí de su parte la instrucción adecuada para afrontar un problema de tesis, sino que constante e incondicionalmente me mostró su confianza en mis capacidades (la cual por cierto no tuve durante muchos momentos).

A mis colegas de álgebra Jhon Mira, Saeed Tafazolian, Rodrigo Salomão y André Contiero, por su amistad y camaradería durante nuestra formación en álgebra, principalmente durante la última fase de nuestros respectivos estudios.

A mis compañeros de oficina Francisco Valenzuela y Manuel Canario, por los felices momentos de esparcimiento y compañía durante el doctorado, y por haberme brindado su amistad a pesar de mi carácter: a Francisco por transmitirme una visión más neutral, relajada y optimista acerca de las relaciones humanas, y por intercambiar conmigo sin cuestionamientos todo tipo de modalidades de "perder el tiempo"; a Manuel, por ser un ejemplo de coraje en cuanto a la defensa de las ideas se refiere, y por las clases de Historia Universal recibidas durante nuestras conversaciones informales.

A mis colegas coterráneos Javier Solano, Freddy Hernández, Elio Espejo y Juan Carlos Galvis, quienes me acogieron durante mi llegada al Brasil, pues además de la ayuda con los detalles logísticos referentes a mi instalación en Rio de Janeiro, me ayudaron a habituarme a ser por primera vez extranjero (principalmente en lo emocional).

A mis amigos del IMPA, por brindarme una amistad sincera (después de hacer un lado la primera impresión, claro está). Más que nombrarlos uno a uno (es decir, por "extensión"), los nombraré por "comprensión": la característica que los distingue es que ***ellos saben quiénes son* ;-)** . Sin embargo, hago mención especial de mis más frecuentes compañeros de almuerzo Damián "wikidamian" Fernández, Dalia Bonilla y Juan Gonzalez, por las relajantes (aunque ocasionalmente exaltadas) discusiones sobre los temas más diversos, gracias a las cuales enriquecimos y diversificamos nuestras respectivas nociones de cultura e incultura general.

Un agradecimiento "nerd" a Rodrigo De Castro y a Till Tantau: al primero, por su excelente libro "El universo LaTeX", lleno de guías, trucos y consejos que seguirán sacándome de apuros TeXnicos a pesar de la creciente ayuda brindada por la internet; al segundo, por los paquetes gráficos Ti*k*Z y PGF, los cuales me permitieron realizar los gráficos presentes en este trabajo, y por el paquete BEAMER por las (para mí y mis colegas matemáticos) obvias razones. Gracias a ellos pude ajustar la presentación de este trabajo de acuerdo a mi (a veces meticuloso, intrincado y obsesivo) gusto.

Finalmente, un agradecimiento muy "peculiar" a Ana Tercia Monteiro y a Alien Herrera Torres, pues con su (por muchos conocida) particular forma de ser me mostraron que la mezquindad humana puede alcanzar niveles insospechados, y por esto la mía en particular viene estando, al final de cuentas, dentro de los parámetros normales... bueno, en realidad sería insensato pretender plasmar mi gratitud hacia ellos en tan pocas líneas, así que la siguiente página está enteramente dedicada a ello, y para que sea universalmente comprendida y difundida, excepcionalmente voy a redactarla en inglés:

This page *intentionally* left blank.

Contents

Introduction

Counting solutions of equations defined on finite sets is an interesting and useful subject. Although it is of combinatorial nature, in some cases it can be resorted to more sophisticated machinery in order to solve it; a good example is the study of solutions of algebraic equations over finite fields.

Some history ("The past")

For the historic background of this subject we refer to the surveys [**Ge**],[**To**],[**Ro**]: the latter restricts to the elliptic case of the Riemann hypothesis for function fields over finite fields; the former give a bird's-eye view, but they also include recent developments, which are the concern of this thesis. We also refer to the book [**GaSt**] for the most recent developments in the application of the theory of function fields in various aspects of coding theory and cryptography.

Already in the 19th century, some works of Gauss (no surprisingly!) and Jacobi deal with the number of solutions of certain algebraic equations over prime subfields $\mathbb{Z}/p\mathbb{Z}$; for example, in the "Last Entry" in Gauss' diary, the number of solutions of the congruence $x^2y^2 + x^2 + y^2 \equiv 1 \pmod{p}$ for a prime number $p \equiv 1 \pmod{4}$ is stated explicitly (yet Gauss did not actually give a proof)[†]. Also, in his Disquisitiones of 1801 he counts the number of solutions of the Fermat equation $x^3 + y^3 + z^3 \equiv 0 \pmod{p}$, being p a prime greater than 3. After that the problem was ignored for a long time.

In 1924 Emil Artin introduced the notion of *zeta function* for certain hyperelliptic function fields over finite fields with odd cardinality, inspired by the notion of Dedekind zeta function for number fields. Later Friedrich Karl Schmidt defined the zeta function for a smooth absolutely irreducible projective curve over a finite field. He proved that it is indeed a rational function, whose numerator can be written as a polynomial of degree $2g$, being g the genus of the curve. Around 1932, Helmut Hasse noticed (based

[†]We refer to [**Ro**, Part 1,3], where it is pointed out the connection of this result with the Riemann hypothesis for quadratic function fields

on a conjecture by Artin concerning his respective zeta function) that the following inequality should hold (later known as the *Hasse-Weil* inequality):

$$\left|\#X(\mathbb{F}_q) - (q+1)\right| \leq 2g\sqrt{q}.$$

Here X denotes a (smooth absolutely irreducible projective) curve over the finite field $\mathbb{F}_q$ with genus g, and $\#X(\mathbb{F}_q)$ denotes its number of $\mathbb{F}_q$-rational points. Shortly after he proved Artin conjecture (which is an analog of the analytic Riemann hypothesis) for the case of elliptic curves (i.e., for curves of genus 1), using the so-called theory of correspondences. Max Deuring observed then that the theory of correspondences should be generalized in order to extend the Hasse method of proof to higher genus. This was precisely the achievement made by André Weil, who proved that the numerator in Schmidt's zeta function can be written in the form $L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$, where the α_i are algebraic integers satisfying $|\alpha_i| = \sqrt{q}$ (The "Riemann hypothesis"), which implies the Hasse-Weil inequality.

We remark that an elementary proof of the Riemann hypothesis for function fields over finite fields (i.e., using only the machinery of function fields rather than the theory of correspondences) was given by Enrico Bombieri in [**Bo**] (using ideas of Sergei Stepanov). A self-contained exposition of this proof can be found on [**St**, Chapter V]. About improvements and other proofs of this result, we refer the reader to [**Se83**], [**StVo**] and the commentary following Theorem 0.2. We also point out that the theory of Karl-Otto Stöhr and José Felipe Voloch (see [**StVo**]) has been a fundamental tool for the classification of maximal curves (that is, those algebraic curves attaining Hasse-Weil upper bound).

At this point, the theory of rational points on curves over finite fields took a short hiatus, which ended around 1980, when Valerii Goppa discovered an unexpected connection between linear codes and function fields over finite fields (see [**Go**]; for the basic definitions on linear codes, see section 0.1). In fact, for a long time coding theorists were unable to exhibit codes with relative parameters surpassing the so-called Gilbert-Varshamov bound. Already in 1973 Goppa constructed codes attaining this bound by using values of rational functions over the rational function fields. Later he generalized this construction by taking values of rational functions on algebraic curves, that is, by working on function fields. These are the so-called AG codes (see section 0.2 for the definitions). For this class of codes, the relative parameters are related with the number of rational places and the genus of the underlying function field, and "long and good" AG codes are obtained whenever the genus is large and at the same time the number of rational places is not small compared with the genus.

For this reason, the interest in knowing the relation between the number of rational points of a curve and its genus was renewed. On this direction, Yasutaka Ihara defined in [**Ih82**] the function $A(q)$, which measures how large can be the number of rational

points of curves with large genus (see equation (0.1)). Among other things, he proved that $A(q) \geq \sqrt{q} - 1$ when q is a square, and later Vladimir Drinfeld and Sergei Vladut proved that $A(q) \leq \sqrt{q} - 1$ for *all* q (an outline of the proof of these facts can be found on [**TsVl**]). Using these results, they managed to prove (in joint work with Thomas Zink) the existence of codes of arbitrary length, with parameters above the Gilbert-Varshamov bound for $q \geq 49$ (see Proposition 0.3), which came as a surprising but welcomed novelty for coding theorists.

More generally, *positive* lower bounds for the function A imply the existence of arbitrary long codes with good parameters; unfortunately, for non-square values of q the value of $A(q)$ is unknown. Some isolated lower bounds are the following: $A(2) \geq 2/9$ ([**Sc**]), $A(3) \geq 1/3$ and $A(5) \geq 1/2$ ([**Xi**]), and $A(q^\ell) \geq (\sqrt{\ell(q-\ell)} - 2\ell)/(\ell - 1)$ for ℓ a prime number such that $q > 4\ell + 1$ and $q \equiv 1 \pmod{\ell}$ ([**Pe**]). On the other hand, as examples of general lower bounds we have the Serre bound ($A(q) \geq c \log q$ for a positive constant c and every q; see [**Se83**]) and Zink's bound $A(p^3) \geq 2(p^2 - 1)/(p + 2)$ for all prime p ([**Zi**]). However, the proofs of these results involve deep results from class field theory and modular curves, and in particular they do not provide explicit presentations for the function fields involved, which is necessary for the explicit construction of asymptotic good codes (for a reference describing nonexplicit constructions, using class-field-theoretic techniques, we refer to the book [**NiXi**]).

For this reason it is convenient to consider sequences of explicit function fields with increasing genus, and afterwards to study the number of rational places of such fields. In particular we limit ourselves to the case of *increasing* sequences of function fields: these are known as *towers of function fields* (see Definition 0.7). More specifically, a tower is a strictly increasing sequence $(F_n)_{n\geq 0}$ of function fields over a fixed finite field $\mathbb{F}_q$, such that all the steps F_{n+1}/F_n are separable, and the genera $g(F_n)$ of the fields F_n go to infinity along with n. If $N(F_n)$ denotes the number of $\mathbb{F}_q$-rational places of F_n, it is easily shown that $\lim_{n\to\infty} N(F_n)/g(F_n)$ exists (see Definitions 0.5 and 0.6). This number is called the *limit* of the tower, and it provides lower bounds for the quantity $A(q)$. The "holy grail" of this theory is to determine explicit towers whose limit is the best possible, namely the Ihara quantity $A(q)$. By "explicit" we mean that the equations defining each field are given in explicit form.

The first breakthrough in this setting occurred in 1995, when Arnaldo Garcia and Henning Stichtenoth exhibited in [**GaSt95**] an explicit tower over a square finite field, where each step is an Artin-Schreier extension of function fields, whose limit attains the Drinfeld-Vladut bound. Moreover, the proof of this result is quite elementary, using only basic results on ramification in separable extensions of function fields. Later in 1996 the same authors obtained another example of "optimal" tower over the field $\mathbb{F}_q$, being q a square, but this time all the steps of the tower are simultaneously defined by the same equation (see [**GaSt96-1**]); more precisely, the tower $(F_n)_{n\geq 0}$ is given as

follows: $F_0 = \mathbb{F}_q(X_0)$ is the rational function field over $\mathbb{F}_q$, and for $n \geq 0$ we have $F_{n+1} = F_n(X_{n+1})$, where $f(X_n, X_{n+1}) = 0$ and $f(X, Y)$ is a *fixed* polynomial $f(X, Y) \in \mathbb{F}_q[X, Y]$, which is separable in both variables X and Y. Towers defined in this way (not only when the base field is a finite field) are called *recursive*, and the function field F_1 is called the *basic* function field. A deep understanding of the ramification in the function field F_1 often enables us to estimate the limit of the tower.

Of course, recursive towers form a small subset of the family of towers, but in contrast they have been systematically studied along these years. There are miscellaneous criteria that ensure the asymptotic goodness of a tower, which are based on the notions of "ramification locus" and "total splitting"; ee Propositions 0.30 and 0.31. On the other hand, for "good" recursive towers (i.e., towers with positive limit) the defining polynomial must have equal degree in both variables (see [**GaSt00**]), and not all the extensions can be Galois abelian (in other words, if the tower $\mathcal{F} = (F_n)_{n\geq 0}$ satisfies that all the extensions F_n/F_0 are Galois abelian, then $\mathcal{F}$ is asymptotically bad; see [**FrPeSt**] for a proof). Finally, in [**BeeGaSt**] the authors derive strong conditions on the defining equation of a recursive Artin-Schreier tower of prime degree in order to be asymptotically good.

When all the places in the ramification locus of a tower are tame, and such ramification locus if finite, it is easy to show that the tower is good; see [**GaStTh**, Theorem 2.1]. On the other hand, most interesting towers exhibit the so-called *wild ramification* phenomenon, so the usual approach (via Abhyankar's Lemma) does not work, and it makes necessary to design some different strategies in order to estimate the genus of the function fields involved.

Returning to the history of towers of function fields, it was not until 2002 that an explicit tower attaining Zink's lower bound for cubic finite fields appeared. This recursive tower was constructed by Gerard van der Geer and Marcel van der Vlugt using Artin-Schreier extensions of degree 2 over the finite field with eight elements (see [**GV**]), and they showed (after long calculations) that the limit of this tower is equal to $3/2$, which is the Zink bound for $p = 2$.

This construction was later generalized for any cubic finite field $\mathbb{F}_{q^3}$ by Juscelino Bezerra, Garcia and Stichtenoth in [**BezGaSt**], and they showed (again after long and detailed calculations) that its limit γ satisfies $\gamma \geq 2(q^2 - 1)/(q + 2)$. Therefore Zink's bound can be generalized as follows:

$$A(q^3) \geq \frac{2(q^2 - 1)}{q + 2}, \text{ for all } q \text{ (Bezerra-Garcia-Stichtenoth bound).} \tag{1}$$

Finally, in 2008 Alp Bassa, Garcia and Stichtenoth constructed in [**BaGaSt**] a tower of Galois extensions of function fields which attains the generalized Zink bound. The merit of this construction lies in its simplicity, since it does not resort to complicated

calculations in order to estimate the genera, instead giving a structural argument. Moreover, the limit obtained in the Bezerra-Garcia-Stichtenoth tower is obtained as a corollary: in fact, this tower turns to be a *subtower* of the Bassa-Garcia-Stichtenoth tower (if $\mathcal{F} = (F_n)_{n\geq 0}$ and $\mathcal{G} = (G_n)_{n\geq 0}$ are towers over $\mathbb{F}_q$, we say that $\mathcal{F}$ is a *subtower* of $\mathcal{G}$ if the inclusion $\cup F_n \subseteq \cup G_n$ holds), and it is known that the limit of a subtower is at least as big as the limit of the original tower (see [**GaSt96-1**, Corollary 2.4]). As in the case of the Bezerra-Garcia-Stichtenoth tower, the case $q = 2$ of the Bassa-Garcia-Stichtenoth tower reduces to the tower of van der Geer and van der Vlugt.

As a matter of fact, the towers constructed in [**GaStTh**, Example 2.3] show that $A(q) \geq 2/(q-2)$ for q a nonprime. Of course, this is a far weaker estimate for the function $A(q)$ than that given by Serre, Zink or Ihara (and others...), but at least shows in an elementary fashion that the function A is positive for all nonprime q. Unfortunately, this construction does not work for prime fields, as shown in [**Le**], so the construction of explicit towers over prime finite fields with positive limit remains as a challenge.

We remark that there is indeed a link between the theory of explicit optimal towers over square finite fields and the theory of modular curves. Noam Elkies showed in [**El98**] that some instances of the towers constructed in [**GaSt96-2**] are in fact modular curves. The same author shows in [**El01**] that the tower given in [**GaSt95**] is an example of Drinfeld modular tower. Finally Elkies conjectured in the appendix of the paper [**LiMaSt**] that all optimal recursively constructed towers over square finite fields should be modular.

As a final commentary, it should be pointed up that the range of applications of the theory of function fields over finite fields is not restricted to linear codes. In fact many branches of cryptography and code theory are devoted to function-field-theoretic methods, such as nonlinear codes, hash families, sequences with low discrepancy and bilinear complexity of multiplication in finite fields[¶], among others. For a survey on the state of the art of these topics we recommend the book [**GaSt**].

About this work ("The present")

Now we outline the contents of this thesis. Our results concern two towers over finite cubic fields that are related. The first of these is the Bassa-Garcia-Stichtenoth tower; the second is a subtower of the Bezerra-Garcia-Stichtenoth tower, defined by Ihara.

Chapter 0 is devoted to set all the background and preliminaries required in this

[¶]Roughly speaking, the bilinear complexity of multiplication for a field extension $\mathbb{F}_{q^n}/F_q$ is the minimum number of "nonscalar" multiplications required to perform all the multiplications of elements in $\mathbb{F}_{q^n}$, with the aid of "scalar" multiplication by elements in $\mathbb{F}_q$; see for example [**Ch**] for the rigorous definitions and their relation with the theory of function fields.

work; it is written in crash-course style, and except for the Section 0.4, it can be omitted by the reader acquainted with the basic theory of function fields and linear codes. Section 0.1 contains the basic definitions regarding the theory of linear codes, including the Gilbert-Varshamov bound. In Section 0.2 the rudiments of the theory of algebraic function fields in one variable (more briefly, *function fields*) are presented: places (and rational places), divisors, Riemann-Roch spaces and genus. Afterwards the definition of the so-called *algebraic geometric* codes (which depends on these notions) is given, along with the relation between the parameters of such codes and the number of rational places and the genera of the corresponding function fields. Is at this point where the Hasse-Weil bound (Theorem 0.2) and the Ihara function (see (0.1)), which have to do with the ratio "number of rational places/genus", come into the scene, along with some lower and upper bounds for this function (Ihara, Drinfeld and Vladut, Serre, Zink). Finally, we define the notion of tower of function fields and its asymptotic parameters (genus and splitting rate).

In Section 0.3 we consider ramification in function fields. Basic definitions (ramification and inertial indices, tamely and wild ramification) are given. Moreover, basic results such as the fundamental equality (Lemma 0.8), Kummer's Theorem (Proposition 0.9) and Hurwitz genus formula (Proposition 0.10) are stated, the latter involving the so-called *different exponents*. We do not define rigorously such numbers, but instead we provide with a plethora of results which allow us to calculate them (or at least to estimate them), such that Dedekind's Different Theorem (Proposition 0.11), transitivity of the different (Lemma 0.13), Abhyankar's Lemma (Proposition 0.14), a result concerning constant field extensions of function fields over *perfect* fields (Proposition 0.17), and ramification and different exponents in Kummer and Artin-Schreier extensions (Propositions 0.20 and 0.21). Apart from these, a specific result (Proposition 0.15) about ramification in some special cases is stated and proved. This result proves to be quite useful in the determination of the genus of the new tower (Chapter 2).

All the material of these three sections was borrowed from [**St**], which provides an excellent introduction to the subject. On the other hand, Section 0.4 concerns the problem of estimation of the different exponent for some non-Galois extensions of function fields. In many cases where the extensions involved are Galois, a very nice result that permit us to go through this problem is the so-called "Key Lemma" (see Proposition 0.27). Our interest is to device a technique which allow us to use this result even in non-Galois instances. The theory of completions comes in handy in order to achieve this purpose [‖]. We set the basic definitions and results concerning completions of valued fields and ramification in such fields (completions of valued fields are also valued fields). The main results on this direction are: 1) Determination of the degree of field extensions given by completions of valued fields, as a function of the ramification

[‖] In other words, completions are the "key" for the generalized "Key Lemma".

and inertial indices of the places involved, and 2) The invariance of the different when passing to such field extensions. These results are contained in Propositions 0.22 and 0.23. The reference we used for this theory of valued fields (not just function fields) is the book of Serre [**Se79**]. Finally we "dissect" the proof of the usual Key Lemma, and we determine the condition that can be imposed even for fields not being function fields, in order to the result remains valid. It turns to be that we only require that the residue field of the "lower" place involved must be a perfect field; see Proposition 0.29 for a precise statement of this formulation. In the final part of this section we state two results that provide upper (respectively, lower) bounds for the genus (respectively, splitting rate) of a tower under certain conditions.

Now we discuss Chapter 1, in which we study the Bassa-Garcia-Stichtenoth tower (BaGS for short). In [**BaGaSt**] the authors proved that this tower attains the generalized Zink's bound (1) (see page x), yet they did not determine explicitly the genera of each step.

In Section 1.1 we recall some basic results about the ramification structure in the BaGS tower, and we state two results involving certain basic calculations which will be widely used in the next section. Section 1.2 is the heart of this chapter: since all the steps of the tower are of Artin-Schreier type, we can use Proposition 0.21 in order to determine the ramification behavior of all the places in the tower. For this purpose it becomes necessary to apply the process of "Artin-Schreier reduction". Roughly speaking, if $\wp$ is the additive separable polynomial defining an Artin-Schreier extension, say $L = F(y)$, with $\wp(y) = u \in F$ (in our case we have $\wp(T) = T^q - T$ for the extensions F_{n+1}/F_n, with $n \geq 1$), we are interested in rewrite the element u in the form $u = v + \wp(u')$, in such form that v is either holomorphic at the considered place, or it has pole order relative prime to the characteristic of the field. Lemma 1.4 provides a first result on this direction. A further refinement of this result is given in Lemma 1.7, which is of recursive character. The first application of these results imply total ramification at certain places (see the commentary after equality (1.14), and (1.16),(1.17)). Afterwards a slight but crucial Artin-Schreier reduction is made in Lemma 1.8 in order to determine ramification at the upper levels. For pedagogical purposes the Artin-Schreier reduction process using Lemmas 1.7 and 1.8 is carried out until the fifth iteration (see equations (1.21)-(1.39)), in order to motive the general construction. Already in these steps we observe an alternating ramification behavior, changing from totally ramified to unramified (and vice versa) in each step. Moreover, the elements L_{n+i} defined for $i = 1, 2, 3, 4, 5$ (see (1.16),(1.25),(1.31),(1.37),(1.39)) obey certain common pattern, which we exploit in order to make a general definition, which settle all the remaining cases[§]. This is the content of the main technical result of this chapter, Lemma 1.9. It

[§]In my case, it took me up to the ninth iteration to become convinced about the pattern, due to my diffidence (the autor).

states that alternation of ramification (in the sense described above) occurs up to certain point, followed by total ramification in all the remaining upper steps. This deals with the majority of the cases of interest, and the remaining case (the infinite place at the bottom function field F_0) is handled in Theorem 1.10.

Finally, in Section 1.3 we collect the results of our previous work. We know that the different exponent is equal to $2(q-1)$ for all the ramified places in the extensions F_{n+1}/F_n for $n \geq 1$, so the determination of the genus g_{n+1} of the function field F_{n+1} as function of g_n (the genus of F_n) via Hurwitz genus formula reduces to the counting of ramified places in each step F_{n+1}/F_n for $n \geq 1$, which is a reasonable (but tricky!) task. It involves considerations on the numbers $\lfloor n/4 \rfloor$ (where $\lfloor\ \rfloor$ stands for the integer part), which forces us to work by cases. Finally the genus $g(F_1)$ is obtained using the ramification behavior of the basic function field, which was already determined in [**BaGaSt**], so we are able to give a general formula for the genera of the BaGS tower (we also deduce a one-line expression for this genera, not involving congruences mod 4, just as a curiosity). We remark that the ramification behavior of the BaGS tower is exactly the same as the van der Geer-van der Vlugt tower (introduced in [**GV**]): in fact, all the recursive definitions and results of this chapter are generalizations of the corresponding ones given in such paper. Obviously, further difficulties arise in this more general setting (only to cite a specific example, Lemma 1.8 is unnecessary in the context of the vdG-vdV tower, because of the far simpler form of the defining equation of the tower).

Now we discuss the final chapter of this work. It is related to a new tower over cubic fields introduced by Ihara; see equation (3) in [**Ih07**]. Actually we will work with a modified version of this equation (via a linear fractional change of variables, which is discussed at the end of the chapter). In Section 2.1 we define the equation of our new recursive tower. This equation is not irreducible (that is, its degree is greater than the degree of the corresponding field extension), but this presentation turns to be very convenient for the determination of the splitting rate of the tower. After a change of variables, we obtain a nice, symmetric in two variables, presentation of the basic function field F_1, which enables us to determine the ramification behavior of this basic function field rather easily (see Proposition 2.2; some of its statements are obtained simply by invert the roles of the variables involved).

Section 2.2 concerns the ramification of the tower itself. Using the results of the previous section (actually we only need to do a change of variable) we determine the ramification behavior at all the basic function fields appearing in the tower (that is, the field extensions $k(X_n, X_{n+1})/k(X_n)$ and $k(X_n, X_{n+1})/k(X_{n+1})$ for each $n \geq 0$, where k is the base field, which is assumed to be perfect, and the X_n are the generators of the function fields F_n). This enables us to determine the set known as *ramification locus* of the tower (relative to the field F_0). The study of the ramification behavior of the tower

is reduced, by definition, to the determination of the ramification at the places in this set.

In this context, five possibilities arise (the "Cases"). As a notation we introduce the terminology of "pyramids" and "diamonds", the latter being simply the basic field extensions obtained from composita of fields of the form $k(X_{i-1}, X_i, \ldots, X_j)$ and $k(X_i, X_{i+1}, \ldots X_{j+1})$. Cases 1,3 and 4 are easily solved, because they lie in the situation of tame ramification, and in these cases we know that Abhyankar's Lemma allows to determine both the ramification index and the different exponent. Case 2 is reduced to one of Cases 3,4 and 5. Finally, the more interesting part of the reasoning deals with Case 5: this is the only part where wild ramification occurs at both "bottom edges" of a diamond. It is at this point where the results of Section 0.4 are invoked. Since the field extensions involved are not even Galois, we cannot apply directly the "Key Lemma".

The strategy that we adopt (successfully!) can be briefly described as follows: first, we take the Galois closures of the field extensions involved, and we determine the ramification of the "bottom" place at these new extensions. The construction of these Galois closures involves Kummer extensions, so we use Proposition 0.20. It turns out that the (total) ramification index at both Galois extensions is equal to a power of p =char(k). Taking completions, after which the field extensions become Galois of degree equal to the corresponding ramification indices (by Proposition 0.22, assuming of course that the base field is algebraically closed, which is harmless since the ramification is invariant under constant field extensions), we are in the situation of the General Key Lemma (Proposition 0.29), which enables us to determine the different exponent at the top edges of the completed diamond (as functions of the respective ramification indices). Using again Proposition 0.22 we return to our original diamond, obtaining the desired estimates for the different exponent.

In Section 2.3, using the results of the five Cases considered in the previous section, we are able to estimate the genus of the tower respect to the field F_0, by applying Propositions 0.15,0.16 and 0.30. Finally, in Section 2.4 we obtain a lower bound for the splitting rate of the tower over F_0 for the particular case in that the tower is defined over the field $\mathbb{F}_{q^3}$. As we said before, it is easily done using the nice form of the equation defining the tower, which enables us to conclude that enough places in the field F_0 split totally in all extensions F_n/F_0. Putting together these results we conclude that the limit of the tower is at least as big as the generalized Zink bound, which is the main result of this chapter. At the end of this chapter we show how this new tower is related to the Bezerra-Garcia-Stichtenoth tower: it is in fact a subtower of the BeGS tower. Since the limit of a subtower is greater or equal to that of the original tower, this provides an immediate proof of our main result; however, it is always worthy to prove the asymptotic goodness of a tower more directly, that is, by trying to determine explicitly the genera of the tower and the nature of its rational places.

As a final remark, another generalization of the Key Lemma can be found in the PhD thesis of Bassa (see [**Ba**, Proposition 5.8]). The author also mentions the possibility of using completions in order to use the Key Lemma in a broader setting ([**Ba**, Remark 3.4]), but ultimately he opted by a more elementary (but equally worthy) approach.

Some perspectives ("The future?")

We close this Introduction by listing some future possibilities for further research on the matters treated in this thesis (beginning with the most "reasonable", and ending with the more "platonic").

- Maybe in the future we can add to the data on the Bassa-Garcia-Stichtenoth tower the exact knowledge of the number of rational places at every step F_n (or, even better, the knowledge of the rational places themselves).
- Determine precisely the genera of the fields in the tower of Ihara. The result concerning admissible sequences (see Proposition 2.4) can be useful for this purpose. Afterwards (of course), try to determine the exact number of rational places in the tower (as in the previous item).
- Construct towers over cubic finite fields with limit *greater* than the generalized Zink bound. On this direction, the search for subtowers of good towers can prove to be useful, since limits of subtowers are greater or equal than the limits of the original ones. Of course, it can happen that the Ihara quantity $A(q^3)$ is actually equal to this bound, but the proof of this fact is probably far more difficult♠ .
- Construct asymptotically good *explicit* towers over prime finite fields (we remind the reader that no example of such tower currently exists; the construction of asymptotically good towers for nonprime fields exhibited in [**GaStTh**, Example 2.3] no longer works for prime finite fields, as shown by Lenstra in [**Le**]), and if possible, with limit comparable to, say, the Serre bound. Similarly for finite fields with cardinality other than square and cubic. It might be that the theory of *recursive* towers is not enough to deal with these cases, so perhaps a new approach is necessary.

♠ I personally believe that Zink's bound is not optimal (the autor).

Chapter 0

Preliminaries

In this chapter we define the basic notions involved in our work, namely of function fields, along with basic auxiliary results. Apart from it, we state and prove a result about ramification of places in more general valued fields (that is, not necessarily being function fields), which will be crucial in the proof of the asymptotic goodness of the new tower introduced in Chapter 2.

0.1 Linear codes

For the definitions and results in this section we refer to [**St**, Chapter II and VII]. Let $\mathbb{F}_q$ be the finite field with q elements. A *linear code* over $\mathbb{F}_q$ is just a $\mathbb{F}_q$-subspace C of $\mathbb{F}_q^n$. The elements of C are called *codewords*, the field $\mathbb{F}_q$ is called the *alphabet*, and we call n the *length* of C and $\dim_{\mathbb{F}_q} C$ the *dimension* of C.

Obviously we are interested in non-trivial linear codes, so from now on we assume that $C \neq 0$. Denoting the elements x of $\mathbb{F}_q^n$ by $x = (x_1, \ldots, x_n)$, we define the *Hamming distance* in $\mathbb{F}_q^n$ as the function $d(x, y) := \left|\{k : x_k \neq y_k\}\right|$, which indeed defines a metric on $\mathbb{F}_q^n$. The *minimum distance* of C is defined as $d(C) := \min\{d(a, b) : a, b \in C \text{ and } a \neq b\}$. Finally, we say that C is a $[n, k, d]$-code if it has length n, dimension k and minimum distance d.

For a $[n, k, d]$-code C set $t := \lfloor (d-1)/2 \rfloor$, where $\lfloor\ \rfloor$ stands for the integer part. From the definition of t it follows that for each word $u \in \mathbb{F}_q^n$ there is at most one word $c \in C$ satisfying $d(u, c) \leq t$. For this reason we say that C is *t-error correcting*. We also define the *transmission rate* of C by $R = R(C) := k/n$, and its *relative minimum distance* by $\delta = \delta(C) := d/n$.

Let $V_q := \{(\delta(C), R(C)) : C \text{ is a code over } \mathbb{F}_q\}$. The limit set U_q of V_q is called the *domain of codes* over $\mathbb{F}_q$. By a Theorem of Yuri Manin (see [**Ma**]) the region U_q is bounded by δ and R axis, and by the graph of the *continuous* function $\alpha_q : [0,1] \to [0,1]$ defined by $\alpha_q(\delta) = \sup\{R : (\delta, R) \in U_q\}$. The function α_q is nonincreasing in the interval $[0, 1 - q^{-1}]$, $\alpha_q(0) = 1$ and $\alpha_q(\delta) = 0$ for $1 - q^{-1} \leq \delta \leq 1$.

If $H_q : [0, 1 - q^{-1}] \to \mathbb{R}$ is defined by

$$H_q(\delta) = \begin{cases} 0, & \text{if } \delta = 0; \\ \delta \log_q(q-1) - \delta \log_q(\delta) - (1-\delta)\log_q(1-\delta), & \text{if } 0 < \delta \leq 1 - q^{-1}, \end{cases}$$

then the have the so-called *Gilbert-Varshamov bound*: $\alpha_q(\delta) \geq 1 - H_q(\delta)$ for $0 \leq \delta \leq 1 - q^{-1}$ (see [**St**, Proposition VII.2.3]). Since $H_q(\delta) < 1$ for $0 < \delta \leq 1 - q^{-1}$, this lower bound for α_q guarantees the existence of long codes over $\mathbb{F}_q$ (i.e., with arbitrarily large lengths) with positive transmission rate (the value R), which are capable of correct a positive percentage of errors by word (the value δ).

0.2 Algebraic function fields and AG codes

In this section we introduce the basic notions on function fields. These, along with the definition and basic properties of AG codes can be found on [**St**]. The reader acquainted with the theory of function fields (and with its usual notation) can safely skip this section.

An *algebraic function field on one variable* over a field k is a finitely generated extension F/k with transcendence degree 1. For brevity we refer to this as a *function field* over k. The field k is called the *base field*. In particular, if $\overline{k}_F$ denotes the algebraic closure of k in F, it follows that $F/\overline{k}_F$ is also a function field.

A *place* of a function field F/k is simply the maximal ideal of a discrete valuation ring of F containing k. This ring is denoted by $\mathcal{O}_P$, and the corresponding discrete valuation is denoted by v_P. The set of places of F/k is denoted by $\mathbb{P}(F)$; we can omit the base field k in this notation because it is easily seen that $\mathcal{O}_P \supseteq \overline{k}_F$ for any place P of F/k; actually, for the subsequent development of the theory (divisors, Riemann-Roch theorem, etc.), it is convenient to suppose that the base field is algebraically closed in the function field, so from now on we add this condition to the definition of function field.

For a place $P \in \mathbb{P}(F)$ we define the *residue field at P* as the field $\mathcal{O}_P/P$. Note that the field k is canonically embedded in this field, and in fact we have $[\mathcal{O}_P/P : k] < \infty$ ([**St**, Proposition I.1.14]). This degree is called the *degree* of the place P, and it is denoted by $\deg P$. Places of degree 1 are called *rational places* of $F/\mathbb{F}_q$ or simply $\mathbb{F}_q$-rational

places. Now, the elements of P are precisely those x in F satisfying $v_P(x) > 0$; for such x we say that x has a *zero* at the place P. If $v_P(x) = 1$, then P is equal to the principal ideal $\mathcal{O}_P x$, and we say in this case that x is a *local parameter* at P. Similarly, the complement of $\mathcal{O}_P$ in F is constituted by the elements $y \in F$ such that $v_P(y) < 0$, and for such y we say that y has a *pole* at the place P. For each $x \in \mathcal{O}_P$ we denote by $x(P)$ its equivalence class in $\mathcal{O}_P/P$, and we define $x(P) = \infty$ for any x having a pole at P. For this reason the elements of F are also called *functions* (with values in $\{\infty\} \cup \mathcal{O}_P/P$). Note that in particular we have $x(P) \in k$ and $v_P(x - x(P)) > 0$ whenever P is a rational place and $x \in \mathcal{O}_P$.

For a *divisor* of F/k we meant to be an element, say D, of the free abelian group with basis $\mathbb{P}(F)$, so it is equal to a formal sum $\sum_{P\in\mathbb{P}(F)} n_P P$, with $n_P \in \mathbb{Z}$ and $n_P = 0$ for almost all P. We write $v_P(D)$ for the integer n_P. For a non-zero function x in F we define the *principal divisor of* x as $(x) \coloneqq \sum_{P\in\mathbb{P}(F)} v_P(x)P$. Since x has only a finite number of zeros and poles ([**St**, Corollary I.3.4]), this indeed defines a divisor. If D is any divisor of F/k, we define the *degree* of D as $\deg D \coloneqq \sum_{P\in\mathbb{P}(F)} v_P(D) \deg P$, and we define the *Riemann-Roch space* of the divisor D as the set $L(D) \coloneqq \{x \in F : v_P(x) \geq -v_P(D) \text{ for all } P \in \mathbb{P}(F)\} \cup \{0\}$. It is a finite-dimensional space over k, whose dimension is denoted by $\ell(D)$. Finally, we define the *genus* of the function field F/k as the number $g(F) \coloneqq \max\{\deg D - \ell(D) + 1 : D \text{ is a divisor of } F/k\}$. This number indeed exists, and it is a nonnegative integer ([**St**, Proposition I.4.14]).

Now we can define the so-called *algebraic geometric* codes (briefly, *AG* codes) as follows: for a function field $F/\mathbb{F}_q$ over a finite field and a set $\mathcal{P} = \{P_1, \ldots, P_n\}$ of n distinct places $P_i \in \mathbb{P}(F)$ of degree 1, let L be a linear $\mathbb{F}_q$-subspace of F such that $L \subseteq \mathcal{O}_{P_i}$ for each i. The mapping $\alpha : L \to \mathbb{F}_q^n$ given by $\alpha(x) = (x(P_1), \ldots, x(P_n))$ is well-defined and $\mathbb{F}_q$-linear, so its image is a code over $\mathbb{F}_q$. When L is a Riemann-Roch space of a divisor, say $L = L(D)$, such that $v_{P_i}(D) = 0$ for each i, the corresponding code is called *algebraic geometric code*, and it is denoted by $C_L(\mathcal{P}, D)$ (In [**St**] these are called *geometric Goppa codes*, after V.D. Goppa, who introduced such codes in [**Go**]).

The following result, which is a direct consequence of Riemann-Roch theorem, allow us to estimate the parameters of an AG code:

Proposition 0.1 ([**St**, Corollary II.2.3])**.** *If $n > \deg D$, then $C_L(\mathcal{P}, D)$ is a $[n, k, d]$-code with $k = \ell(D) \geq \deg D + 1 - g(F)$, and equality occurs if $\deg D \geq 2g(F) - 1$; moreover, $d \geq n - \deg D$.*

As a consequence, if we are able to construct function fields with increasing number n of $\mathbb{F}_q$-rational places, and we fix the value $\deg D/n$ (obviously we must modify the divisor D for each function field), then the relative minimum distance of the corresponding AG codes is positive, and their respective transmission rates increase along

with the value $n/g(F)$. For this reason, it is important to estimate the relation between the number of rational points of a function field $F/\mathbb{F}_q$ and its genus $g(F)$. On this direction we have the following celebrated result, which was proved first by Helmut Hasse in the case $g(F) = 1$ ([**Ha**]), and after by André Weil in the general case ([**We**]):

Theorem 0.2 (**Hasse-Weil bound**). *Let $F/\mathbb{F}_q$ be a function field over the finite field $\mathbb{F}_q$. If we denote by $N(F)$ the number of $\mathbb{F}_q$-rational places of F, then we have*

$$N(F) \leq q + 1 + 2g(F)\sqrt{q}\,.$$

Actually this result also provides a *lower bound* for the number of rational places, but for our purposes this additional result is not necessary. We remark that the bound above is sharp: in fact, there are examples of function fields attaining this bound, the so-called *maximal* function fields. Further improvements of this bound were given by J.-P. Serre (the 'Explicit Formulas'; see [**Se83**]) and J. Oesterlé, the latter providing the ultimate strengthening of the Hasse-Weil bound in terms of the genus alone. We also mention that the work of K.-O. Stöhr and J. Voloch provides bounds for the number of rational places, which depend on the geometry of the curve associated to the function field (see [**StVo**]).

When the genus of the function field is large with respect to the cardinality of the base field, the Hasse-Weil bound can be improved substantially. In [**Ih82**], Y. Ihara introduced the following real number:

$$A(q) := \limsup_{g(F)\to\infty} \frac{N(F)}{g(F)}\,, \tag{0.1}$$

where F runs over all the function fields over $\mathbb{F}_q$. He showed that $A(q) \leq \sqrt{2q}$ for any q, thus improving the estimate given by the Hasse-Weil bound $A(q) \leq 2\sqrt{q}$, and he also showed that $A(q) \geq \sqrt{q} - 1$ when q is a square. Later V. G. Drinfeld and S. G. Vladut showed in [**DrVl**] by elementary methods that the reverse inequality $A(q) \leq \sqrt{q} - 1$ holds for *every* q. Thus, the value of $A(q)$ is exactly $\sqrt{q} - 1$ when q is a square. For other cardinalities much less is known. For example, there exists a constant $c > 0$ such that $A(q) \geq c \log q$ for all q (see [**Se83**] for the proof, which uses class field theory). For q a cubic power of a prime number, T. Zink found, by using degeneration of Shimura modular surfaces, the following lower bound (see [**Zi**]):

$$A(p^3) \geq \frac{2(p^2-1)}{p+2}, \text{ for all primes } p\,.$$

The drawback of these proofs lies in the fact that they are too hard to carry out explicitly, that is, they do not provide an explicit description of the function fields in terms of generators and equations. On the other hand, the success of the AG codes method

depends heavily on the knowledge of the function fields involved and of their genera and $\mathbb{F}_q$-rational places, so in particular the defining equations of the function fields involved are highly desirable■ .

In any case, good lower bounds for the function A imply the existence of arbitrarily long codes with good parameters, via the following result (see [**TsVlZi**]; the proof can also be found on [**St**, Proposition VII.2.5]):

Proposition 0.3. *If $A(q) > 1$, then $\alpha_q(\delta) \geq 1 - A(q)^{-1} - \delta$ for all $\delta \in [0, 1 - A(q)^{-1}]$.*

Now we define the concept of tower of function fields, which is the central object of study in this work.

Definition 0.4. A *tower of function fields* over a field k is a sequence $\mathcal{F} = (F_n)_{n\geq 0}$ of function fields over k such that the following conditions hold:

(i) Each field extension F_{n+1}/F_n is finite and separable of degree > 1.

(ii) The field k is algebraically closed in each field F_n (so F_n is indeed a function field over k, according to our definition).

(iii) The genera of the fields F_n satisfy $g(F_n) \to \infty$ when $n \to \infty$.

Definition 0.5 ([**GaStTh**])**.** Given a tower $\mathcal{F} = (F_n)_{n\geq 0}$ over $\mathbb{F}_q$, the following limits do exist, the first as a positive real number; the second, as an extended real number:

$$\nu(\mathcal{F}/F_0) := \lim_{n\to\infty} \frac{N(F_n)}{[F_n : F_0]} \; ; \; \gamma(\mathcal{F}/F_0) := \lim_{n\to\infty} \frac{g(F_n)}{[F_n : F_0]} \, .$$

The (extended) real numbers $\nu(\mathcal{F}/F_0)$ and $\gamma(\mathcal{F}/F_0)$ are called, respectively, the *splitting rate* and the *genus* of the tower $\mathcal{F}$, both relatively to the field F_0.

Sometimes we also refer to the sequence $\big(g(F_n)\big)_{n\geq 0}$ as the *genus* of the tower. Clearly the knowledge of the genus of the tower in this sense allow us to determine the genus of the tower in the sense of the definition above (as a limit).

Definition 0.6. For a tower $\mathcal{F} = (F_n)_{n\geq 0}$ over $\mathbb{F}_q$, the real number

$$\lambda(\mathcal{F}) := \lim_{n\to\infty} \frac{\nu(\mathcal{F}/F_0)}{\gamma(\mathcal{F}/F_0)}$$

is called the *limit* of the tower $\mathcal{F}$ (note that $\lambda(\mathcal{F})$ indeed does not depend on F_0).

From the definition of tower we clearly have $0 \leq \lambda(\mathcal{F}) \leq A(q) \leq \sqrt{q} - 1$.

■ Of course, it remains to tackle the computational implementation issues, but this is another story...

Definition 0.7. A tower $\mathcal{F}$ of function fields over $\mathbb{F}_q$ is said to be:

- *Asymptotically bad*, if $\lambda(\mathcal{F}) = 0$.
- *Asymptotically good*, if $\lambda(\mathcal{F}) > 0$.
- *Asymptotically optimal*, if $\lambda(\mathcal{F}) = A(q)$.

It is clear that a tower $\mathcal{F}$ is asymptotically good if and only if its genus $\gamma(\mathcal{F}/F_0)$ is finite and its splitting rate $\nu(\mathcal{F}/F_0)$ is positive.

0.3 Ramification in function fields

Let F/k be a function field, and let L be an *algebraic* extension of F. From now on we suppose that the extension L/K is *separable*. Then L is a function field over k', where k' is the algebraic closure of k in L. We know that $[k' : k] < \infty$ iff $[L : F] < \infty$ ([**St**, Lemma III.1.2]).

If $P \in \mathbb{P}(F)$ and $Q \in \mathbb{P}(L)$, we say that Q divides P whenever $Q \supseteq P$. This is denoted by $Q|P$. This is equivalent to say that for some integer $e \geq 1$ we have $v_Q(x) = ev_P(x)$ for all $x \in F$, or that $Q \cap F = P$ (see [**St**, Proposition III.1.4]). The integer e is called the *ramification index* of Q over P, and it is denoted by $e(Q|P)$. If $e(Q|P) > 1$, we say that (the extension of places) $Q|P$ is *ramified*; otherwise, we say that $Q|P$ is *unramified*. Finally, we say that a place $P \in \mathbb{P}(F)$ is *ramified* in L/F if $Q|P$ is ramified for some $Q \in \mathbb{P}(L)$ dividing P; otherwise, we say that P is *unramified* in L/F.

On the other hand, if $Q|P$, then there is a canonical embedding $\mathcal{O}_P/P \hookrightarrow \mathcal{O}_Q/Q$. The degree $[\mathcal{O}_Q/Q : \mathcal{O}_P/P]$ is called the *inertial degree* of Q over P, and it is denoted by $f(Q|P)$.

If L/F is a separable algebraic field extension and if $Q \in \mathbb{P}(L)$, then the restriction $Q \cap F$ is a place of F. Finally, if M/L is another separable algebraic extension of fields, and $P \in \mathbb{P}(F), Q \in \mathbb{P}(L), R \in \mathbb{P}(M)$, then we have $e(R|P) = e(R|Q)e(Q|P)$ and $f(R|P) = f(R|Q)f(Q|P)$.

Lemma 0.8 (**Fundamental equality**). *If L/F is a finite extension of function fields, and $P \in \mathbb{P}(F)$, then*

$$\sum_{\substack{Q \in \mathbb{P}(L) \\ Q|P}} e(Q|P)f(Q|P) = [L : F] .$$

For a finite extension L/F of function fields, we say that a place $P \in \mathbb{P}(F)$ is *totally ramified* in L/F if $e(Q|P) = [L : F]$. According to fundamental equality, this implies that there is an unique place $Q \in \mathbb{P}(L)$ dividing P; the converse is true, provided that $f(Q|P) = 1$, which happens if k is algebraically closed, for example. We also say that P is *totally decomposed* in L/F (or that P *splits completely* in L/F) whenever there are $[L : F]$ distinct places in $\mathbb{P}(L)$ dividing P. By fundamental equality, this amounts to say that $e(Q|P) = f(Q|P) = 1$ for each place $Q \in \mathbb{P}(L)$ dividing P.

In determining the ramification behavior of a place in certain field extensions, the following result proves to be useful, but first we need to set some notation. Let $P \in \mathbb{P}(F)$. For any polynomial $f(T) \in \mathcal{O}_P[T]$, say $f(T) = \sum_i a_i T^i$, with $a_i \in \mathcal{O}_P$, we define the *reduction mod P* of f as the polynomial $f_P(T) \coloneqq \sum_i a_i(P)T^i \in (\mathcal{O}_P/P)[T]$. Now we state the result:

Proposition 0.9. *Suppose that the field extension L/F is simple, say $L = F(y)$. Moreover, suppose that y is $\mathcal{O}_P$-integral, so its minimal polynomial over F, say $\varphi(T)$, belongs to $\mathcal{O}_P[T]$. Consider the decomposition of $\varphi_P(T)$ into irreducible factors on $(\mathcal{O}_P/P)[T]$, that is,*

$$\varphi_P(T) = \prod_{i=1}^{r} \gamma_i(T)^{\epsilon_i},$$

where the polynomials $\gamma_i(T)$ are monic, pairwise distinct and irreducible in $(\mathcal{O}_P/P)[T]$. Choose polynomials $\varphi_i(T) \in \mathcal{O}_P[T]$ such that $\deg \gamma_i = \deg \varphi_i$ and $(\varphi_i)_P = \gamma_i$. Then there are places $P_1, \ldots, P_r \in \mathbb{P}(L)$ such that $P_i|P$, $\varphi_i(y) \in P_i$ and $f(P_i|P) \geq \deg \gamma_i$ for each i.

Moreover, if $\epsilon_i = 1$ for each i, then there exists, for each i between 1 and r, exactly one place $P_i \in \mathbb{P}(L)$ such that $P_i|P$ and $\varphi_i(y) \in P_i$. Each extension $P_i|P$ is unramified and satisfies $f(P_i|P) = \deg \gamma_i$ (so by fundamental equality the places $P_1, \ldots, P_r$ are precisely the places in $\mathbb{P}(L)$ dividing P).

This result is commonly known as *Kummer's Theorem*. For a proof see [**St**, Proposition III.3.8].

For finite separable extensions of function fields we have the following classic formula relating the genus of the function fields involved:

Proposition 0.10 (Hurwitz genus formula)**.** *Let F/k be a function field over k, and let L/F be a finite separable field extension, so L is a function field over k', the algebraic closure of k in L. Then we have*

$$(2g(L) - 2) = \frac{[L : F]}{[k' : k]} (2g(F) - 2) + \deg \mathrm{Diff}(L/F),$$

where $\mathrm{Diff}(L/F)$ *denotes the* different *of L/F.*

The *different* of L/F is a divisor of L of the form:

$$\mathrm{Diff}(L/F) = \sum_{P \in \mathbb{P}(F)} \sum_{\substack{Q \in \mathbb{P}(L) \\ Q|P}} d(Q|P)Q\,.$$

The integer $d(Q|P)$, which is nonnegative, is called the *different exponent* of $Q|P$. We refer to [**St**, Section III.4] for the rigorous definition of $d(Q|P)$. We are more interested in the effective determination (or, at least, the estimation) of such numbers. The following results will allow us to do this in our cases of interest.

Proposition 0.11 (Dedekind's Different Theorem)**.** *With notation as before, we have that* $d(Q|P) \geq e(Q|P) - 1$*, and equality holds if and only if* $\mathrm{char}(k)$ *does not divide* $e(Q|P)$*. In particular* $d(Q|P) = 0$ *whenever* $Q|P$ *is unramified.*

Let Q and P be places such that $Q|P$. We say that $Q|P$ is *tamely ramified* if $\mathrm{char}(K)$ does not divide $e(Q|P)$; otherwise we say that $Q|P$ is *wildly ramified*. If $Q|P$ is wildly ramified for some Q dividing P, we say that P is *wildly ramified* in the field extension L/F; otherwise we say that P is *tamely ramified* in L/F.

Proposition 0.12 ([**St**, Proposition III.5.12])**.** *With the notation above, suppose that a extension of places* $Q|P$ *is totally ramified. Let* $t \in L$ *be a local parameter at* Q *(that is,* $v_Q(t) = 1$*). Then we have* $d(Q|P) = v_Q(\varphi'(t))$*, where* $\varphi(T)$ *is the minimal polynomial of* t *over* F*.*

The following result relates the different exponent of a field extension with the different exponents at intermediate fields.

Lemma 0.13 (Transitivity of the different)**.** *Let* M/L *and* L/F *be finite separable extensions, where* F *is a function field, and let* $P \in \mathbb{P}(F), Q \in \mathbb{P}(L), R \in \mathbb{P}(M)$ *be places such that* $R|Q$ *and* $Q|P$*. Then we have*

$$d(R|P) = d(R|Q) + e(R|Q)d(Q|P).$$

For a proof, see [**St**, Corollary III.4.11].

The following fundamental result allow us to determine the ramification index and the different exponent of a compositum of two function fields from the respective data on the subfields, provided that tame ramification occurs in one of them.

Proposition 0.14 (Abhyankar's Lemma)**.** *Let* L/F *be a finite separable extension of function fields, and suppose that* L *is the compositum of two intermediate subfields* $L_1, L_2 \subseteq L$*. Let* $P \in \mathbb{P}(F)$ *and* $Q \in \mathbb{P}(L)$*, and let* $Q_i = Q \cap L_i \in \mathbb{P}(L_i)$ *for* $i = 1, 2$*. If one of the extensions* $Q_i|P$ *is tamely ramified, then*

$$e(Q|P) = \mathrm{LCM}\{e(Q_1|P), e(Q_2|P)\}\,,$$

where LCM *stands for the least common multiple.*

Actually in our work we only need to determine the ramification index and the different exponent in very particular cases. For this reason it will be convenient to state these results explicitly. In the following two results the function fields involved have characteristic $p > 0$, and q is a power of p.

Proposition 0.15. *Let L/F and M/L be finite separable field extensions of function fields, and let $P \in \mathbb{P}(F), Q \in \mathbb{P}(L)$ and $R \in \mathbb{P}(M)$ be places such that $R|Q$ and $Q|P$. Then the following holds:*

(i) If $e(Q|P) = 1$ then $e(R|P) = e(R|Q)$ and $d(R|P) = d(R|Q)$.

(ii) If $e(R|Q) = 1$ then $e(R|P) = e(Q|P)$ and $d(R|P) = d(Q|P)$ (Thus, if one of the intermediate extensions is unramified, the global ramification behavior is the same as in the other intermediate extension).

(iii) If $e(R|Q) = d(R|Q) = q$ then $e(R|P) = qe(Q|P)$ and $d(R|P) = q(d(Q|P) + 1)$.

(iv) If $d(Q|P) = 2(e(Q|P)-1)$ and $d(R|Q) = 2(e(R|Q)-1)$, then $d(R|P) = 2(e(R|P)-1)$.

(v) If $e(Q|P) = q - 1$ and $d(R|Q) = 2(e(R|Q) - 1)$, then $e(R|P) = e(R|Q)(q - 1)$ and $d(R|P) = \left(\frac{q}{q-1}\right)e(R|P) - 2$.

Proof. They are direct consequences of Lemma 0.13 and the multiplicativity of the ramification index. We only prove (v); the proof of the remaining items is even easier. By Proposition 0.11 we have $d(Q|P) = q - 2$, so by Lemma 0.13 we have $d(R|P) = d(R|Q) + e(R|Q)d(Q|P) = 2(e(R|Q) - 1) + e(R|Q)(q - 2) = qe(R|Q) - 2$, the latter being equal to $\left(\frac{q}{q-1}\right)e(R|P) - 2$ because $e(R|P) = (q - 1)e(R|Q)$. □

Proposition 0.16. *Let L/F be a finite separable field extension of function fields, and suppose that $L = L_1 L_2$ for two intermediate subfields L_1, L_2. Let $P \in \mathbb{P}(F)$ and $Q \in \mathbb{P}(L)$ be places such that $Q|P$, and for $i = 1, 2$ let $Q_i = Q \cap L_i$. Then the following holds:*

(i) If $e(Q_1|P) = 1$ then $e(Q|Q_2) = 1, e(Q|Q_1) = e(Q_2|P)$ and $d(Q|Q_1) = d(Q_2|P)$ (Thus, if one of the extensions is unramified, then the liftings of the respective field extensions inherit the ramification behavior).

(ii) If $e(Q_1|P) = q - 1$ and $e(Q_2|P) = d(Q_2|P) = q$, then $e(Q|Q_2) = q - 1$ and $e(Q|Q_1) = q, d(Q|Q_1) = 2(q - 1)$.

Proof. Item (i) is an immediate consequence of items (i) and (ii) of Proposition 0.15, together with Proposition 0.14. As for (ii), note that we have $e(Q|Q_1) = q$ and $e(Q|Q_2) = q - 1$ by Proposition 0.14, so by Lemma 0.13 we have

$$d(Q|P) = d(Q|Q_1) + e(Q|Q_1)d(Q_1|P) = d(Q|Q_1) + q(q - 2) = d(Q|Q_1) + q^2 - 2q$$

and

$$d(Q|P) = d(Q|Q_2) + e(Q|Q_2)d(Q_2|P) = q - 2 + (q-1)q = q^2 - 2\,.$$

Comparing the equalities we get $d(Q|Q_1) = 2q - 2$, as desired. □

Let F be a function field over k. When k is algebraically closed, nice things can happen: for example, "unramified" becomes equivalent to "totally decomposed", and it is possible (in some cases) to conclude directly from Kummer's Theorem (Proposition 0.9) that a given place is totally decomposed. As a consequence the calculation of the genus $g(F)$ becomes easier (at least theoretically). The following result shows that whenever we want to calculate the genus of a function field F, we can replace the base field k by any algebraic extension of it, provided that k is a *perfect* field[♣].

Proposition 0.17. *Let F/k be a function field over a perfect field k, and let k' be an algebraic extension of k (for example $k' = \overline{k}$). Consider the constant field extension $L := Fk'$ of F/k. Then L is a function field over k' (i.e., k' is algebraically closed in L). Moreover, every place $P \in \mathbb{P}(F)$ is unramified in L/F, and we have $g(L) = g(F)$.*

For the proof see [**St**, Theorem III.6.3].

Corollary 0.18. *Let F be a function field over a perfect field k, and let L/F be a finite separable extension. If there exists a place $P \in \mathbb{P}(F)$ that is totally ramified in L/F, then k is algebraically closed in L (so L is also a function field over k).*

Proof. Let k' be the algebraic closure of k in L, and let $L' = Fk'$. Let $Q \in \mathbb{P}(L)$ be a place of L dividing P, and let $Q' = Q \cap L'$. Note that we have $L \supseteq L' \supseteq F$. By Proposition 0.17 we have $e(Q'|P) = 1$; on the other hand, the condition $e(Q|P) = [L : F]$ clearly implies $e(Q|Q') = [L : L']$ and $e(Q'|P) = [L' : F]$ (because the multiplicativity of both the degree of field extensions and the ramification index). Therefore we have $[L' : F] = 1$, so $k' \subseteq L' = F$. Since k is algebraically closed in F by hypothesis, it follows that $k' = k$. This finishes the proof. □

Corollary 0.19. *Let L/F be a finite separable extension of function fields over the same perfect field k (that is, k is algebraically closed in L). Let k' be any algebraic extension of k, and let $L' = Lk', F' = Fk'$. Let $P \in \mathbb{P}(F), Q \in \mathbb{P}(L), P' \in \mathbb{P}(F')$ and $Q' \in \mathbb{P}(L')$ be places such that $Q'|Q|P$ and $Q'|P'|P$. Then we have $e(Q|P) = e(Q'|P')$.*

Proof. Since k is algebraically closed in both F and L, then by Proposition 0.17 we have $e(Q'|Q) = e(P'|P) = 1$. Using that $e(Q'|P) = e(Q'|Q)e(Q|P)$ and $e(Q'|P) = e(Q'|P')e(P'|P)$, the result follows. □

[♣]This assumption is essential: the corresponding result is no longer true if we drop this restriction.

Corollaries 0.18 and 0.19 together are very useful in order to determine the ramification behavior of a separable field extension of function fields: in fact, let L/F be a such extension, where F is a function field over a perfect field k. If we manage to prove (with "bare hands") the existence of a place $P \in \mathbb{P}(F)$ totally ramified in L/F, the first result shows that L is also a function field over k, and the determination of the ramification behavior in the extension L/K becomes more easy if we suppose that k is algebraically closed (especially when we try to apply Kummer's Theorem), and such assumption is possible by the second result.

Now we turn our attention to two special kind of extensions of function fields: the tower studied in Chapter 1 is made of Artin-Schreier extensions, whereas Kummer extensions are considered in a crucial step of the proof of the asymptotic goodness of the new tower (Chapter 2). Now we state just the basic facts about ramification in such extensions that will be needed in the sequel.

Proposition 0.20 (Kummer extensions)**.** *Let F/k be a function field over a perfect field k. Suppose that k contains a primitive n-root of unity, with $n \geq 1$ (so n is relative prime to the characteristic of k). Let $u \in F$ and let $L = F(y)$, where y satisfies $y^n = u$. Then we have:*

(i) The extension L/F is Galois of degree $[L : F] = d$, where d divides n, and the minimal polynomial of y over F is of the form $T^d - w$, with $w \in F$.

(ii) If $P \in \mathbb{P}(F)$ and $Q \in \mathbb{P}(L)$ are places such that $Q|P$, then we have $e(Q|P) = d/r_P$, where $r_P := \mathrm{GCD}(d, v_P(w))$ (so $d(Q|P) = e(Q|P) - 1$ because d/r_P is relative prime to the characteristic of k). Here GCD *denotes the greatest common divisor.*

(iii) With P and Q as in item (ii), if n divides $v_P(u)$, then $Q|P$ is unramified.

Proof. Item (i) is a standard fact from Galois theory. For item (ii) we refer to [**St**, Proposition III.7.3]. Finally, suppose that n divides $v_P(u)$, with P and Q as in item (ii). From equalities $y^n = u$ and $y^d = w$ we get $u = w^{n/d}$ (recall that d divides n), and therefore $v_P(u) = nv_P(w)/d$. Since n divides $v_P(u)$, it follows that d divides $v_P(w)$, hence $r_P = \mathrm{GCD}(d, v_P(w)) = d$, and so $e(Q|P) = d/r_P = 1$ by item (ii). □

Let k be a perfect field of characteristic $p > 0$. A polynomial $\wp(T) \in k[T]$ is said to be *additive* if it has the form $\wp(T) = a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \cdots + a_1 T^p + a_0 T$, with $a_i \in k$. Since $\wp'(T) = a_0$, the necessary and sufficient condition for $\wp(T)$ to be separable is that $a_0 \neq 0$.

Proposition 0.21 (Artin-Schreier extensions)**.** *Let F/k be a function field over a perfect field k of characteristic $p > 0$, and let q be a power of p. Let $\wp(T) \in k[T]$ be an additive*

separable polynomial of degree q which has all its roots in k. Let $u \in F$ and suppose that for any place $P \in \mathbb{P}(F)$ there is an element $z \in F$ (depending on P) such that either

$$v_P(u - \wp(z)) \geq 0$$

or

$$v_P(u - \wp(z)) = -m, \text{ with } m > 0 \text{ and } \mathrm{GCD}\{m, p\} = 1\,.$$

Define $m_P := -1$ in the first case and $m_P := m$ in the second case. Them m_P is a well-defined integer. Suppose that exists a place $Q \in \mathbb{P}(F)$ with $m_Q > 0$, and let $L = F(y)$, where y satisfies $\wp(y) = u$. Then the following holds:

(i) The extension L/F is elementary abelian of exponent p, and $Gal(L/F)$ is isomorphic to the additive group $\{a \in k : \wp(a) = 0\}$.

(ii) Any place $P \in \mathbb{P}(F)$ with $m_P = -1$ is unramified in L/F.

(iii) Any place $P \in \mathbb{P}(F)$ with $m_P > 0$ is totally ramified in L/F, and if Q denotes the unique place in $\mathbb{P}(L)$ dividing P, then the different exponent is given by $d(Q|P) = (q-1)(m_P + 1)$.

(iv) k is algebraically closed in L (by Corollary 0.18 and item (ii), because $m_P > 0$ for some place P).

For the proof, see [**St**, Proposition III.7.10].

0.4 The "Key Lemma" for completions

In this section we state and indicate a proof of a generalization of the result known as "Key Lemma", which gives information about ramification in composita of Galois extensions of function fields of degree a power of p, being $p > 0$ the characteristic of the base field. This result cannot be directly used because the field extensions involved in the new tower (Chapter 2) are not even Galois; however, we resort to the technique of completions in order to solve this problem. Of course, we must assure us that the results about ramification continue to hold in this new setting. The basic reference for this section is [**Se79**, Chapters I-IV].

We remark that ramification theory can be developed in the more general setting of fields of fractions of Dedekind domains. Discrete valuation rings are examples of such rings, and in fact Dedekind domains can be characterized as the noetherian integral domains that are discrete valuation rings *locally*. The unique additional restriction in the case of function fields is that the discrete valuation rings involved must contain the

base field. By dropping this restriction we obtain the definition of discrete valuation ring in more general fields, and if we assume that the field extensions involved are all separable, then all the basic results on ramification remain to be true in this new setting; see [**Se79**, Chapter I].

Now we discuss completions. Since we are more interested in the properties rather than the rigorous definitions, we just set the definitions and state the corresponding properties. Let P be a place of a field F, that is, the maximal ideal of a discrete valuation ring of F, which is denoted (as in the case of function fields) by $\mathcal{O}_P$. Associated to P we have a field $\hat{F}_P$, the *P-adic completion* of the $\mathcal{O}_P$-module F respect to P; moreover we have a canonical embedding $F \hookrightarrow \hat{F}_P$ (though this fact will not be needed). We also consider the P-adic completions of the $\mathcal{O}_P$-modules $\mathcal{O}_P$ and P, which are denoted respectively by $\hat{\mathcal{O}}_P$ and $\hat{P}$. It turns out that $\hat{\mathcal{O}}_P$ is a discrete valuation ring of $\hat{F}_P$, with maximal ideal $\hat{P}$. Moreover, its residue field $\hat{\mathcal{O}}_P/\hat{P}$ is isomorphic to the residue field $\mathcal{O}_P/P$.

Consider now a field extension L/F. Let $P \in \mathbb{P}(F)$ and $Q \in \mathbb{P}(L)$ be places such that $Q|P$. Then we have that $\hat{L}_Q$ is a field extension of $\hat{F}_P$. The following result relates the ramification behavior of $Q|P$ with that of $\hat{Q}|\hat{P}$:

Proposition 0.22 ([**Se79**, II.§3, Theorem 1, Corollary 4])**.** *With the hypotheses above, we have the following:*

(i) The field $\hat{L}_Q$ is an extension of $\hat{F}_P$[♠] of degree $e(Q|P)f(Q|P)$.

(ii) The place $\hat{Q} \in \mathbb{P}(\hat{L}_Q)$ is the unique place dividing $\hat{P}$, and we have $e(Q|P) = e(\hat{Q}\,|\,\hat{P}\,)$ and $f(Q|P) = f(\hat{Q}\,|\,\hat{P}\,)$.

(iii) If L/F is a Galois extension, then $\hat{L}_Q/\hat{F}_P$ is also a Galois extension.

Let L/F be a finite separable extension of fields. The numbers $d(Q|P)$ are also defined in this more general setting (see [**Se79**, II.§3]), and the same results from the theory of function fields continue to hold; moreover, such exponents are preserved after completions. This is the content of the following result:

Proposition 0.23. *Let L/F be a finite separable extension of fields, and let $P \in \mathbb{P}(F)$, $Q \in \mathbb{P}(L)$ be places such that $Q|P$. Then we have the following:*

(i) (Transitivity) If M/L is another finite separable field extension, and $R \in \mathbb{P}(M)$ satisfies $R|Q$, then we have $d(R|P) = d(R|Q) + e(R|Q)d(Q|P)$.

(ii) $d(Q|P) = d(\hat{Q}\,|\,\hat{P})$.

♠ There is a misprint in this result: in page 31 of [**Se79**], line 3 we should read "$\hat{K}$" instead of "K". The original French version of this book is typed correctly at this point.

Proof. For (i), see [**Se79**, II.§4, Proposition 8]. Item (ii) is the content of [**Se79**, II.§4, Proposition 10].

Now we state the required preliminary results used to prove the "Key Lemma" for function fields.

Lemma 0.24 ([**GaSt05**, Lemma 1])**.** *Let F/k be a function field over a perfect field k with* $\mathrm{char}(k) = p > 0$*, and let L_1/F and L_2/F be two distinct Artin-Schreier extensions of degree p. Denote by L the compositum L_1L_2. Let $P \in \mathbb{P}(F)$ and $Q \in \mathbb{P}(L)$ be places such that $Q|P$, and let $Q_i = Q \cap L_i$ for $i = 1, 2$. If $d(Q_i|P) \in \{0, 2p-2\}$ for each i, then we also have $d(Q|Q_i) \in \{0, 2p-2\}$ for $i = 1, 2$.*

In the following two lemmas, we have the following setting: F/k is a function field over a perfect field k of characteristic $p > 0$, L and M are fields such that $M \supseteq L \supseteq F$ and M/F is a finite separable field extension. Finally, $P \in \mathbb{P}(F), Q \in \mathbb{P}(L)$ and $R \in \mathbb{P}(M)$ are places such that $R|Q$ and $Q|P$.

Lemma 0.25 ([**GaSt07**, Proposition 1.2])**.** *If $B > 0$ satisfies $d(R|Q) \leq B(e(R|Q) - 1)$ and $d(Q|P) \leq B(e(Q|P) - 1)$, then we also have $d(R|P) \leq B(e(R|P) - 1)$.*

Lemma 0.26 ([**GaSt07**, Proposition 1.8])**.** *Suppose that M/L is a p-extension, and that both M/L and L/F are Galois extensions. If $d(R|P) \leq 2(e(R|P) - 1)$, then $d(R|Q) \leq 2(e(R|Q) - 1)$ and $d(Q|P) \leq 2(e(Q|P) - 1)$*

Let F, L, P and Q as in the previous lemmas. If L/F is a Galois p-extension and $d(Q|P) \leq 2(e(Q|P) - 1)$, then we actually have $d(Q|P) = 2(e(Q|P) - 1)$. In fact, from the theory of higher ramification groups for Galois extensions of function fields (see [**St**, Section III.8]) we obtain the inequality $d(Q|P) \geq 2(e(Q|P) - 1)$. Now we state the "Key Lemma" for function fields:

Proposition 0.27 ([**GaSt07**, Proposition 1.8])**.** *Let F/k be a function field over a perfect field k of characteristic $p > 0$. Let L_1/F and L_2/F be Galois p-extensions, and let $M = L_1L_2$. Let $P \in \mathbb{P}(F)$ and $Q \in \mathbb{P}(M)$ be places such that $Q|P$, and let $Q_i = Q \cap L_i$ for $i = 1, 2$. Suppose that $d(Q_i|P) = 2(e(Q_i|P) - 1)$ for $i = 1, 2$. Then we also have $d(Q|Q_i) = 2(e(Q|Q_i) - 1)$ for $i = 1, 2$.*

The proof of Lemma 0.24 relies on the following result:

Lemma 0.28 ([**St**, Lemma III.7.7])**.** *Let F be a function field over a perfect field k of characteristic $p > 0$. Given an element $u \in F$ and a place $P \in \mathbb{P}(F)$, the following holds:*

(a) Either there exists an element $z \in F$ such that $v_P(u - (z^p - z)) \geq 0$,

(b) or else, for some $z \in F$ *we have* $v_P(u - (z^p - z)) = -m < 0$*, with* $\mathrm{GCD}(p, m) = 1$.

Actually the proof of this result uses the fact that k is perfect only to conclude that the residue field at P is also perfect. As a consequence, we can replace the perfectness of the base field in the statement of the previous lemma with the perfectness of the residue field at the place considered. The rest of the proof of Lemma 0.24, along with the proofs of Lemmas 0.25 and 0.26 and Proposition 0.27, depend only on the basic results on ramification, which are also true for more general fields (the theory of higher ramification groups in Galois extensions also continues to hold; see [**Se79**, Chapter IV]). In other words, we can apply these proofs in our more general context, *mutatis mutandis*. Therefore we can state the following strengthening of "Key Lemma", which will allow us (with the aid of completions) to estimate completely the ramification behavior of the new tower introduced in Chapter 2:

Proposition 0.29 (General Key Lemma)**.** *Let* F *be a field of characteristic* $p > 0$*, and let* P *be a place of* F *such that the residue field* $\mathcal{O}_P/P$ *is perfect. Let* L_1/F *and* L_2/F *be Galois* p*-extensions, and let* $M = L_1L_2$*. Let* $P \in \mathbb{P}(F)$ *and* $Q \in \mathbb{P}(M)$ *be places such that* $Q|P$*, and let* $Q_i = Q \cap L_i$ *for* $i = 1, 2$*. Suppose that* $d(Q_i|P) = 2\big(e(Q_i|P) - 1\big)$ *for* $i = 1, 2$*. Then we also have* $d(Q|Q_i) = 2\big(e(Q|Q_i) - 1\big)$ *for* $i = 1, 2$.

Let F be a function field over a perfect field k, and let $B > 0$ be a real constant. A finite separable field extension L/F is said to be *B-bounded* if for all places $P \in \mathbb{P}(F)$ and $Q \in \mathbb{P}(L)$ such that $Q|P$ the inequality $d(Q|P) \leq B(e(Q|P) - 1)$ holds. If $\mathcal{F} = (F_n)_{n\geq 0}$ is a tower of function fields over k, then we say that the tower $\mathcal{F}$ is *B-bounded* whenever each field extension F_n/F_0 is B-bounded. We also define the *ramification locus* of $\mathcal{F}$ over F_0 as the set

$$V(\mathcal{F}/F_0) \coloneqq \{P \in \mathbb{P}(F_0) : P \text{ ramifies in some extension } F_n/F_0\}.$$

We have the following results:

Proposition 0.30 ([**GaSt07**, Proposition 1.5])**.** *Let* $B > 0$ *and suppose that a tower* $\mathcal{F} = (F_n)_{n\geq 0}$ *of function fields is B-bounded and its ramification locus* $V(\mathcal{F}/F_0)$ *over* F_0 *is finite. Then the genus* $\gamma(F/F_0)$ *satisfies the inequality*

$$\gamma(F/F_0) \leq g(F_0) - 1 + \frac{B}{2} \sum_{P \in V(\mathcal{F}/F_0)} \deg P\,.$$

Proposition 0.31. *Let* $\mathcal{F} = (F_n)_{n\geq 0}$ *be a tower of function fields over* $\mathbb{F}_q$*. If* $P_1, \ldots, P_r \in \mathbb{P}(F_0)$ *are distinct* $\mathbb{F}_q$*-rational places such that each* P_i *splits completely in each extension* F_n/F_0*, then the splitting rate of the tower* $\mathcal{F}$ *(relative to* F_0*) satisfies* $\nu(\mathcal{F}/F_0) \geq r$.

Proof. Let i between 1 and r and let $Q \in \mathbb{P}(F_n)$ be a place such that $Q|P_i$. Since P_i is totally decomposed in F_n/F_0, then $f(Q|P) = 1$, and since $\deg P_i = 1$ by hypothesis, it follows that $\deg Q = f(Q|P_i) \deg P_i = 1$, so Q is also a $\mathbb{F}_q$-rational place. Since there are $[F_n : F_0]$ places in $\mathbb{P}(F_n)$ dividing each P_i, it follows that $N(F_n) \geq r[F_n : F_0]$ for each $n \geq 0$. This proves the assertion. □

Chapter 1

The genus of the Bassa-Garcia-Stichtenoth tower

In this chapter we determine explicitly the genera of the fields in the Bassa-Garcia-Stichtenoth (BaGS for short) tower.

1.1 Preliminaries and some calculations

In this section we define and state some properties of the BaGS tower. We refer to [**BaGaSt**] for further details.

Let K be a perfect field of characteristic $p > 0$, let q be a power of p and assume that $\mathbb{F}_q \subseteq K$. The BaGS tower is the sequence $\mathcal{F} = (F_i)_{i\geq 0}$ of function fields over K defined recursively as follows: $F_0 = K(X_0)$ is the rational function field, and for $i \geq 0$ let $F_{i+1} = F_i(X_{i+1})$, where X_{i+1} satisfies the equation

$$\wp(X_{i+1})^{q-1} + 1 = \frac{-X_i^{q(q-1)}}{(X_i^{q-1} - 1)^{q-1}}, \tag{1.1}$$

being $\wp$ is the Artin-Schreier operator defined by $\wp(T) = T^q - T$.

The tower $\mathcal{F}$ has the following properties (see [**BaGaSt**, Thm. 2.2]):

1) The extensions F_{i+1}/F_i are Galois for all $i \geq 0$.

2) K is the full constant field of F_i, for all $i \geq 0$.

3) $[F_1 : F_0] = q(q-1)$ and $[F_{i+1} : F_i] = q$, for all $i \geq 1$.

Regarding property 3), we can say more: in fact, after recursive multiplication of the generators X_i by suitable elements in $\mathbb{F}_q^\times$, they satisfy the relations

$$\wp(X_{i+1}) = z_i \text{ for all } i \geq 1, \text{ where } z_i := \frac{X_{i-1}^q}{(X_{i-1}^{q-1} - 1)(X_i^{q-1} - 1)} \tag{1.2}$$

(see [**BaGaSt**, Lemma 2.7]) ; moreover, the new elements X_i also satisfy relations (1.1). Thus, the extensions F_{i+1}/F_i are of Artin-Schreier type for each $i \geq 1$, so we can try to use Proposition 0.21 in order to find recursive formulas for the genera g_i of the function fields F_i.

As a first step, we can extend the constant field such that $\mathbb{F}_{q^2} \subseteq K$ without changing the genera g_i (see Proposition 0.17). Let $(P_i)_{i\geq 0}$ be a chain of places such that $P_i \in \mathbb{P}(F_i)$ and $P_{i+1}|P_i$ for all $i \geq 0$, and denote by v_i the normalized discrete valuation associated to P_i. We want to determine the ramification behavior of a such chain.

Define $a_i \in \overline{\mathbb{F}_q} \cup \{\infty\}$ as the value of X_i at the place P_i. From now on, let

$$\boldsymbol{\alpha} := \mathbb{F}_q^\times \text{ and } \boldsymbol{\beta} := \mathbb{F}_{q^2} \setminus \mathbb{F}_q \,.$$

Now we state the following preliminary result:

Lemma 1.1.

(i) For each $i \geq 0$ we have the following:

a) $a_i \in \boldsymbol{\alpha} \cup \{\infty\}$ if and only if $a_{i+1} = \infty$; moreover, $a_0 \in \boldsymbol{\alpha} \cup \{\infty\}$ implies $e(P_1|P_0) = q$ and $d(P_1|P_0) = 2(q-1)$.

b) $a_i = 0$ if and only if $a_{i+1} \in \boldsymbol{\beta}$, and $a_0 = 0$ implies $e(P_1|P_0) = 1$.

c) $a_i \in \boldsymbol{\beta}$ if and only if $a_{i+1} \in \boldsymbol{\alpha} \cup \{0\} = \mathbb{F}_q$; moreover, $a_0 \in \boldsymbol{\beta}$ implies $e(P_1|P_0) = q-1$ and $d(P_1|P_0) = q-2$.

(ii) If $i \geq 0$ and $a_i \notin \boldsymbol{\alpha} \cup \boldsymbol{\beta} \cup \{\infty\}$, then the place P_i is unramified in F_{i+1}/F_i.

(iii) If $i \geq 1$ and $a_i \notin \boldsymbol{\alpha} \cup \{\infty\}$, then the place P_i is unramified in F_{i+1}/F_i.

Proof. (i) and (ii) are direct consequences of Lemmas 5.2 and 6.1 of [**BaGaSt**]. As for (iii), note that if $i \geq 1$ satisfies $a_i \in \boldsymbol{\beta}$, then by (i) we have $a_{i-1} = 0$, so we have $v_i(X_{i-1}) > 0$ and $v_i(X_{i-1}^{q-1} - 1) = v_i(X_i^{q-1} - 1) = 0$. Thus, $v_i(z_i) > 0$, so by (ii) of Proposition 0.21 the place P_i is unramified in F_{i+1}/F_i. □

Suppose that the chain (P_i) is ramified in some step F_{n+1}/F_n, for some $n \geq 1$. It follows from (iii) of Lemma 1.1 that $a_n \in \boldsymbol{\alpha} \cup \{\infty\}$. By (i) of the same lemma, either $a_k = \infty$ for $k = 0, \ldots, n$, or for some i between 1 and n we have $a_k = \infty$ for $i \leq k \leq n$ and $a_{i-1} \in \boldsymbol{\alpha}$. Therefore we must determine the ramification behavior of the chain $(P_i)_{i\geq 0}$ in the following cases:

(a) $a_n \in \boldsymbol{\alpha}$ for some $n \geq 1$,

(b) $a_0 \in \boldsymbol{\alpha}$, and

(c) $a_0 = \infty$.

In case (a), by (i) of Lemma 1.1 we have $a_{n-i} \in \boldsymbol{\beta}$ for i odd, $a_{n-i} = 0$ for $i > 0$ even, and $a_j = \infty$ for all $j > n$. In particular, for $0 \leq k \leq n-1$ we have $v_{k+1}(X_{k+1}) \geq 0$, so $v_k(z_k) = v_k(\wp(X_{k+1})) \geq 0$ for $1 \leq k \leq n-1$. As a consequence, each place P_k with $1 \leq k \leq n-1$ is unramified in F_{k+1}/F_k by (ii) of Proposition 0.21, and therefore the place P_1 is unramified in F_n/F_1.

In the general case, if $j \geq 2$ is given, then by (1.2) we have

$$\wp(X_{j+1}) = \frac{X_{j-1}^{q+1} X_j}{\wp(X_{j-1})\wp(X_j)} \quad \text{and} \quad \wp(X_j) = \frac{X_{j-2}^{q+1} X_{j-1}}{\wp(X_{j-2})\wp(X_{j-1})}\,.$$

Replacing the value of $\wp(X_j)$ into the first equality above we obtain

$$\wp(X_{j+1}) = \frac{\wp(X_{j-2}) X_{j-1}^{q}}{X_{j-2}^{q+1}} \cdot X_j = -\wp(X_{j-2}^{-1}) X_{j-1}^{q} X_j\,, \quad \text{for all } j \geq 2. \tag{1.3}$$

The following two results will be frequently used in the next section, the first of these being an elementary result on discrete valuations:

Lemma 1.2. *Let v be a (normalized discrete) valuation and let y, d, y_k, d_k be elements such that $v(y) = v(y_k) = v(d) = v(d_k) = 0$ for $k = 1, \ldots, m$. Then we have:*

(i) $v(y^{-1} - d^{-1}) = v(y - d)$.

(ii) $v(\wp(y) - \wp(d)) = v(y - d)$ *if* $v(y - d) > 0$.

(iii) $v\Big(\prod_{k=1}^{m} y_k - \prod_{k=1}^{m} d_k\Big) \geq \min_{1 \leq k \leq m} v(y_k - d_k)$, *and equality holds if the minimum is attained exactly once.*

(iv) $v(y^{q-1} - d^{q-1}) = v(y - d)$ *if* $v(y - d) > 0$.

Proof.

(i) $v(y^{-1} - d^{-1}) = v\big((y^{-1} - d^{-1})yd\big) = v(y - d)$.

(ii) $v(\wp(y) - \wp(d)) = v((y-d)^q - (y-d))$. Now we apply the strict triangle inequality.

(iii) Immediate from the equality

$$\prod_{k=1}^{m} y_k - \prod_{k=1}^{m} d_k = \sum_{k=1}^{m}\left[\left(\prod_{j<k} y_j\right)(y_k - d_k)\left(\prod_{j>k} d_j\right)\right]$$

(expand the summand to obtain a telescopic sum) and the triangle inequality.

(iv) We have $v(y^q - d^q) = v((y-d)^q) = qv(y-d) > v(y-d)$. Since $v(y-d) = v(y^{-1}-d^{-1})$ by (i), we conclude that $v(y^q - d^q) > v(y^{-1} - d^{-1}) = v(y - d)$. Finally, using (iii) together with the equality $y^{q-1} - d^{q-1} = y^q \cdot y^{-1} - d^q \cdot d^{-1}$ we get the desired result. □

Lemma 1.3. *Let $n \geq 0$, and suppose that $a_n \in \boldsymbol{\alpha}$. Then we have:*

(i) For each $i \geq 0$ even such that $n - i - 2 \geq 0$,

$$v_n(X_{n-i} - a_{n-i}) = q\, v_n(X_{n-i-2} - a_{n-i-2}).$$

(ii) For each $i \geq 0$ even such that $n - i - 1 \geq 0$,

$$(q-1)v_n(X_{n-i} - a_{n-i}) = v_n(X_{n-i-1} - a_{n-i-1}).$$

Proof.

(i) Since $a_{n-i} \in \mathbb{F}_q$ in this case, then $\wp(a_{n-i}) = 0$, so

$$v_n(\wp(X_{n-i})) = v_n(\wp(X_{n-i} - a_{n-i})) = v_n(X_{n-i} - a_{n-i})$$

by (ii) of Lemma 1.2; but $a_{n-i-1} \in \boldsymbol{\beta}$ and $a_{n-i-2} = 0$, and since $c^{q-1} - 1 \neq 0$ for all $c \in \boldsymbol{\beta} \cup \{0\}$, it follows that

$$v_n(z_{n-i-1}) = v_n\left(\frac{X_{n-i-2}^q}{(X_{n-i-2}^{q-1} - 1)(X_{n-i-1}^{q-1} - 1)}\right) = qv_n(X_{n-i-2}) = qv_n(X_{n-i-2} - a_{n-i-2}).$$

Now the equality follows since $\wp(X_{n-i}) = z_{n-i-1}$.

(ii) By (1.1) we have

$$\begin{aligned}\wp(X_{n-i})^{q-1} &= -X_{n-i-1}^{q(q-1)} \cdot \frac{X_{n-i-1}^{q-1} - 1}{(X_{n-i-1}^{q-1} - 1)^q} - 1 \\ &= \frac{-X_{n-i-1}^{q^2-1} + X_{n-i-1}^{q(q-1)} - (X_{n-i-1}^{q(q-1)} - 1)}{(X_{n-i-1}^{q-1} - 1)^q} \\ &= \frac{-X_{n-i-1}^{q^2-1} + 1}{(X_{n-i-1}^{q-1} - 1)^q}\,. \end{aligned} \tag{1.4}$$

Since $X_{n-i-1}^{q^2-1} - 1 = \prod_{\lambda\in\boldsymbol{\alpha}\cup\boldsymbol{\beta}} (X_{n-i-1} - \lambda)$ and $a_{n-i-1} \in \boldsymbol{\beta}$, then $v_n(X_{n-i-1}^{q^2-1} - 1) = v_n(X_{n-i-1} - a_{n-i-1})$. Moreover, since $a_{n-i-1}^{q-1} - 1 \neq 0$, then $v_n(X_{n-i-1}^{q-1} - 1) = 0$. Applying these results to (1.4) we obtain

$$v_n(\wp(X_{n-i})^{q-1}) = v_n(X_{n-i-1} - a_{n-i-1}),$$

which gives the desired result, because $a_{n-i} \in \mathbb{F}_q$, and therefore $v_n(\wp(X_{n-i})^{q-1}) = v_n(\wp(X_{n-i} - a_{n-i})^{q-1}) = (q-1)v_n(X_{n-i} - a_{n-i})$ by (ii) of Lemma 1.2. □

1.2 The ramification behavior

Now we are prepared to carry out the necessary calculations in order to determine the ramification behavior of the tower $\mathcal{F}$. We will deal with a chain $(P_i)_{i\geq 0}$ of places such that $P_i \in \mathbb{P}(F_i)$ and $P_{i+1}|P_i$ for all $i \geq 0$. We must consider two separate cases:

(a) $a_n \in \boldsymbol{\alpha}$ for some $n \geq 0$, and

(b) $a_0 = \infty$.

Case (a) is the most difficult, so we will treat this case first. Some of the calculations involved in this case are also valid for case (b), and they will allow us to handle this case as well.

From now on, we will assume that $a_n \in \boldsymbol{\alpha}$ for some $n \geq 0$ fixed, where $a_i \in \overline{\mathbb{F}_q} \cup \{\infty\}$ is the value of X_i at the place P_i. Recall that this implies $a_{n-i} \in \boldsymbol{\beta}$ for $i \geq 0$ odd, $a_{n-i} = 0$ for $i > 0$ even and $a_j = \infty$ for all $j > n$. Furthermore, $e(P_n|P_1) = 1$ whenever $n \geq 1$. We will introduce the following notation:

- We write $\mathcal{O}_i$ for the valuation ring associated to the place P_i, and v_i for the normalized discrete valuation associated to $\mathcal{O}_i$. We also write $\mathcal{O}_i(1)$ for any element in the valuation ring $\mathcal{O}_i$.
- For any element λ in some ring $\mathcal{O}_i$, we denote its value $\lambda(P)$ at the place P_i by $\overline{\lambda}$. If $P_i \subseteq P_j$, then there is a canonical inclusion $\mathcal{O}_i/P_i \hookrightarrow \mathcal{O}_j/P_j$, so there is no ambiguity in this notation.
- For each integer k we define $m(k) := \lfloor k/2 \rfloor$, where $\lfloor\ \rfloor$ stands for the integer part.

Lemma 1.4. *Let $n \geq 0$ and suppose that $a_n \in \boldsymbol{\alpha}$. For $k = 0, \ldots, m(n)$ we define*

$$\Gamma_k := \frac{\wp(X_{n-2k+1})X_n}{X_{n-2k}}.$$

Then we have

$$\Gamma_j = \wp\left(\frac{-1}{X_{n-2j-1}^{q-1}-1}\,\Gamma_{j+1}\right) + \Gamma_{j+1} + \mathscr{O}_n(1), \;\; \textit{for} \;\; j = 0, \ldots, m(n)-1.$$

Proof. Since $n - 2j \geq 2$ (because $j \leq m(n)-1$, so $2j \leq 2m(n)-2 \leq n-2$), it follows from (1.3) that

$$\wp(X_{n-2j+1}) = \frac{X_{n-2j}X_{n-2j-1}^q}{X_{n-2j-2}^{q+1}}\,(X_{n-2j-2}^q - X_{n-2j-2})\,,$$

hence

$$\Gamma_j = \frac{X_n}{X_{n-2j}}\wp(X_{n-2j+1}) = X_n X_{n-2j-1}^q\left(\frac{1}{X_{n-2j-2}} - \frac{1}{X_{n-2j-2}^q}\right).$$

On the other hand,

$$\frac{-1}{X_{n-2j-1}^{q-1}-1}\,\Gamma_{j+1} = \frac{-\wp(X_{n-2j-1})X_n}{X_{n-2j-2}(X_{n-2j-1}^{q-1}-1)} = -\frac{X_n X_{n-2j-1}}{X_{n-2j-2}}\,,$$

and therefore we have

$$\begin{aligned}
\Gamma_j - \wp\left(\frac{-1}{X_{n-2j-1}^{q-1}-1}\,\Gamma_{j+1}\right) &= \Gamma_j + \wp\left(\frac{X_n X_{n-2j-1}}{X_{n-2j-2}}\right) \\
&= \frac{X_n X_{n-2j-1}^q}{X_{n-2j-2}} - \frac{X_n X_{n-2j-1}^q}{X_{n-2j-2}^q} + \frac{X_n^q X_{n-2j-1}^q}{X_{n-2j-2}^q} - \frac{X_n X_{n-2j-1}}{X_{n-2j-2}} \\
&= \frac{X_n}{X_{n-2j-2}}\wp(X_{n-2j-1}) + \frac{X_{n-2j-1}^q}{X_{n-2j-2}^q}\wp(X_n) \qquad (1.5) \\
&= \Gamma_{j+1} + \frac{X_{n-2j-1}^q}{X_{n-2j-2}^q}\wp(X_n)\,.
\end{aligned}$$

Now $v_n(\wp(X_n)) = v_n(\wp(X_n - a_n)) = v_n(X_n - a_n)$. Iteration of (i) of Lemma 1.3 yields $v_n(X_n - a_n) = q^{j+1}v_n(X_{n-2j-2})$, and since $X_{n-2j-1} \in \boldsymbol{\beta}$ (so $a_{n-2j-1}^q \neq 0$) and $a_{n-2j-2} = 0$, it follows that

$$v_n\left(\frac{X_{n-2j-1}^q}{X_{n-2j-2}^q}\wp(X_n)\right) = v_n(\wp(X_n)) - q\,v_n(X_{n-2j-2}) = (q^{j+1}-q)\,v_n(X_{n-2j-2}) \geq 0\,. \quad \square$$

Remark 1.5. The "tricky" definition of the elements Γ_k in Lemma 1.4 is justified as follows: if $n \geq 2$, then by (1.3) we have

$$\Gamma_0 = \wp(X_{n+1}) = \frac{1}{X_{n-2}^q}\,\theta, \text{ where } \theta = X_n X_{n-1}^q(X_{n-2}^{q-1}-1) \in \mathscr{O}_n^\times\,,$$

so in this particular case we can apply the method of "pole order reduction" (see [**St**, Lemma III.7.7] for the case $q = p$, which always applies). In fact, we are looking for a q-th root of $\overline{\theta}$, and since $a_n = a_n^q$ and $a_{n-2} = 0$, it follows that $\overline{\theta} = a_n^q a_{n-1}^q(-1) = \overline{\delta}^{\,q}$, being $\delta = -X_n X_{n-1}$. Therefore we have

$$z_n = \frac{1}{X_{n-2}^q}\left(\delta^q + \theta - \delta^q\right),$$

so

$$\begin{aligned}
z_n - \wp\left(\frac{\delta}{X_{n-2}}\right) &= \frac{\theta - \delta^q}{X_{n-2}^q} + \frac{\delta}{X_{n-2}} \\
&= \frac{\theta - \delta^q + \delta X_{n-2}^{q-1}}{X_{n-2}^q} \\
&= \frac{X_n X_{n-1}^q (X_{n-2}^{q-1} - 1) + X_n^q X_{n-1}^q - X_n X_{n-1} X_{n-2}^{q-1}}{X_{n-2}^q} \\
&= \frac{X_n X_{n-1}}{X_{n-2}^q}\left[X_{n-1}^{q-1}(X_{n-2}^{q-1} - 1) + X_n^{q-1} X_{n-1}^{q-1} - X_{n-2}^{q-1}\right] \\
&= \frac{X_n X_{n-1}}{X_{n-2}^q}\left[X_{n-2}^{q-1}(X_{n-1}^{q-1} - 1) + X_{n-1}^{q-1}(X_n^{q-1} - 1)\right] \\
&= \frac{\wp(X_{n-1})X_n}{X_{n-2}} + \frac{\wp(X_n)X_{n-1}^q}{X_{n-2}^q},
\end{aligned}$$

which agrees with (1.5) in the case $j = 0$; actually, this process can be repeated, now with Γ_1 instead of Γ_0, after which we obtain formula (1.5) with $j = 1$. As the reader can check, the proof of Lemma 1.4 is just the polished form of this pole order reduction process, applied in all the cases.

For $0 \le j \le m(n)-1$, let $w_{j+1} := -1/(X_{n-2j-1}^{q-1} - 1)$. We would like to change the elements w_{j+1} appearing in the statement of Lemma 1.4 by constants. Since $w_{j+1} \in \mathscr{O}_n^\times$, we can define

$$b_{j+1} := \overline{w_{j+1}} \neq 0, \quad \text{for} \quad j = 0, \ldots, m(n) - 1, \tag{1.6}$$

and these elements are natural candidates for our purpose. By (i) and (iv) of Lemma 1.2 we have $v_n(w_{j+1} - b_{j+1}) = v_n(X_{n-2j-1} - a_{n-2j-1})$. Since $n - 2j - 2 \ge 0$, we can take $i = 2j$ in both parts of Lemma 1.3 to obtain

$$v_n(w_{j+1} - b_{j+1}) = v_n(X_{n-2j-1} - a_{n-2j-1}) = q(q-1)v_n(X_{n-2j-2}). \tag{1.7}$$

On the other hand, since both $\wp(a_{n-2j-1})$ and a_n are not zero, then

$$v_n(\Gamma_{j+1}) = v_n\left(\frac{\wp(X_{n-2j-1})X_n}{X_{n-2j-2}}\right) = -v_n(X_{n-2j-2}). \tag{1.8}$$

Putting together (1.7) and (1.8) we get

$$v_n((w_{j+1} - b_{j+1})\,\Gamma_{j+1}) = (q(q-1)-1)v_n(X_{n-2j-2}) > 0,$$

hence

$$\begin{aligned}\Gamma_j &= \wp(w_{j+1}\,\Gamma_{j+1}) + \Gamma_{j+1} + \mathscr{O}_n(1)\\ &= \wp(b_{j+1}\,\Gamma_{j+1}) + \Gamma_{j+1} + \wp((w_{j+1} - b_{j+1})\,\Gamma_{j+1}) + \mathscr{O}_n(1)\\ &= \wp(b_{j+1}\,\Gamma_{j+1}) + \Gamma_{j+1} + \mathscr{O}_n(1), \quad \text{for } j = 0, \ldots, m(n)-1. \end{aligned} \tag{1.9}$$

Formula (1.9) above represents the expected improvement of Lemma 1.4.

Now let $c \in \mathbb{F}_{q^2}$. Using the identities $\wp(ab) = a^q\,\wp(b) + b\,\wp(a)$ and $\wp(c^q) = -\wp(c)$, which are valid for all a, b in the fields F_i and for all $c \in \mathbb{F}_{q^2}$, we obtain from (1.9), for each k between 0 and $m(n)-1$ and any $c \in \mathbb{F}_{q^2}$:

$$\begin{aligned}c\,\Gamma_k &= c\,\wp(b_{k+1}\,\Gamma_{k+1}) + c\,\Gamma_{k+1} + \mathscr{O}_n(1)\\ &= \wp(c^q\,b_{k+1}\,\Gamma_{k+1}) + (c - b_{k+1}\,\wp(c^q))\,\Gamma_{k+1} + \mathscr{O}_n(1)\\ &= \wp(c^q\,b_{k+1}\,\Gamma_{k+1}) + (c + b_{k+1}\,\wp(c))\,\Gamma_{k+1} + \mathscr{O}_n(1). \end{aligned} \tag{1.10}$$

For any d in $\overline{\mathbb{F}}_q$, let $\mathrm{Tr}\,(d) = d^q + d$. Note that $\mathrm{Tr}\,(d) \in \mathbb{F}_q$ if and only if $d \in \mathbb{F}_{q^2}$. We have $a_{n-2k-1}^{q(q-1)} = a_{n-2k-1}^{q^2-q} = a_{n-2k-1}^{1-q}$, so

$$\begin{aligned}\mathrm{Tr}\,(b_{k+1}) &= \frac{-1}{a_{n-2k-1}^{q(q-1)} - 1} + \frac{-1}{a_{n-2k-1}^{q-1} - 1}\\ &= \frac{-1}{a_{n-2k-1}^{1-q} - 1} + \frac{-1}{a_{n-2k-1}^{q-1} - 1}\\ &= \frac{1 - a_{n-2k-1}^{q-1} + 1 - a_{n-2k-1}^{1-q}}{(a_{n-2k-1}^{q-1} - 1)(a_{n-2k-1}^{1-q} - 1)}\\ &= \quad 1, \quad \text{for } k = 0, \ldots, m(n)-1. \end{aligned} \tag{1.11}$$

In particular, $b_{k+1} \in \mathbb{F}_{q^2}$ and $b_{k+1} = 1 - b_{k+1}^q = (1 - b_{k+1})^q$, and therefore

$$\begin{aligned}c + b_{k+1}\,\wp(c) &= (1 - b_{k+1})c + b_{k+1}\,c^q\\ &= \mathrm{Tr}\,((1 - b_{k+1})c)\\ &= \mathrm{Tr}\,(b_{k+1}^q c), \quad \text{for all } c \in \mathbb{F}_{q^2}. \end{aligned} \tag{1.12}$$

Remark 1.6. Recall that the elements b_k are defined only for $1 \le k \le m(n)$, and they are all not zero; see (1.6).

Lemma 1.7. *Let j, ℓ be such that $0 \le j \le j+\ell \le m(n)$. Then for any elements $C_{j,j}, C_{j,j+1}, \dots, C_{j,j+\ell}$ in $\mathbb{F}_{q^2}$, and for any b_0 in $\mathbb{F}_{q^2}$ whenever $j = 0$ (see Remark 1.6) we have the equality*

$$\sum_{k=j}^{j+\ell} C_{j,k} b_k \Gamma_k = \wp\Big(\sum_{k=j+1}^{j+\ell} C_{j+1,k} b_k \Gamma_k \Big) + C^q_{j+1,j+\ell+1} \Gamma_{j+\ell} + \mathscr{O}_n(1),$$

where $C_{j+1,j}, C_{j+1,j+1}, \dots, C_{j+1,j+\ell+1}$ are defined recursively as follows: $C_{j+1,j} = 0$, and

$$C_{j+1,k} = (C_{j,k-1} b_{k-1})^q + \mathrm{Tr}\,(C_{j+1,k-1} b_{k-1}), \quad \text{for } k = j+1, j+2, \dots, j+\ell+1.$$

In particular we have

$$\wp(C_{j+1,k}) = -\wp(C_{j,k-1} b_{k-1}), \quad \text{for } k = j+1, j+2, \dots, j+\ell+1.$$

Proof. By induction on ℓ. The result holds for $\ell = 0$ because $C_{j+1,j+1} = (C_{j,j} b_j)^q$, so $C^q_{j+1,j+1} = (C_{j,j} b_j)^{q^2} = C_{j,j} b_j$. For the induction step, let ℓ be such that the result holds, with $0 \le j \le j+\ell < m(n)$. If $C_{j,j}, C_{j,j+1}, \dots, C_{j,j+\ell+1}$ are in $\mathbb{F}_{q^2}$, then

$$\begin{aligned}\sum_{k=j}^{j+\ell+1} C_{j,k} b_k \Gamma_k &= C_{j,j+\ell+1} b_{j+\ell+1} \Gamma_{j+\ell+1} + \sum_{k=j}^{j+\ell} C_{j,k} b_k \Gamma_k \\ &= \wp\Big(\sum_{k=j+1}^{j+\ell} C_{j+1,k} b_k \Gamma_k \Big) + C^q_{j+1,j+\ell+1} \Gamma_{j+\ell} + C_{j,j+\ell+1} b_{j+\ell+1} \Gamma_{j+\ell+1} + \mathscr{O}_n(1). \end{aligned} \tag{$*$}$$

Taking $k = j+\ell$ and $c = C^q_{j+1,j+\ell+1}$ in (1.10) and (1.12) we obtain

$$\begin{aligned} C^q_{j+1,j+\ell+1} \Gamma_{j+\ell} &= \wp\Big(C^{q^2}_{j+1,j+\ell+1} b_{j+\ell+1} \Gamma_{j+\ell+1} \Big) + \mathrm{Tr}\,(b^q_{j+\ell+1} C^q_{j+1,j+\ell+1}) \Gamma_{j+\ell+1} + \mathscr{O}_n(1) \\ &= \wp\Big(C_{j+1,j+\ell+1} b_{j+\ell+1} \Gamma_{j+\ell+1} \Big) + \mathrm{Tr}\,(C_{j+1,j+\ell+1} b_{j+\ell+1}) \Gamma_{j+\ell+1} + \mathscr{O}_n(1). \end{aligned} \tag{$**$}$$

Substituting $(**)$ into $(*)$ yields

$$\begin{aligned}\sum_{k=j}^{j+\ell+1} C_{j,k} b_k \Gamma_k &= \wp\Big(\sum_{k=j+1}^{j+\ell} C_{j+1,k} b_k \Gamma_k \Big) + \wp\Big(C_{j+1,j+\ell+1} b_{j+\ell+1} \Gamma_{j+\ell+1} \Big) \\ &\quad + \Big(\mathrm{Tr}\,(C_{j+1,j+\ell+1} b_{j+\ell+1}) + C_{j,j+\ell+1} b_{j+\ell+1} \Big) \Gamma_{j+\ell+1} + \mathscr{O}_n(1) \\ &= \wp\Big(\sum_{k=j+1}^{j+\ell+1} C_{j+1,k} b_k \Gamma_k \Big) + C^q_{j+1,j+\ell+2} \Gamma_{j+\ell+1} + \mathscr{O}_n(1), \end{aligned}$$

by the definition of $C_{j+1,j+\ell+2}$. This finishes the proof. □

Suppose that $a_n \in \boldsymbol{\alpha}$, with $n \geq 0$. Summing up the equalities (1.9) from $j = 0$ to $j = m(n) - 1$ we obtain

$$\Gamma_0 - \Gamma_{m(n)} = \sum_{j=0}^{m(n)-1} \wp(b_{j+1}\,\Gamma_{j+1}) + \mathscr{O}_n(1)\,.$$

Since $\Gamma_0 = \wp(X_{n+1})$, equality above is equivalent to

$$\wp(X_{n+1}) = \wp\left(\sum_{k=1}^{m(n)} b_k\,\Gamma_k\right) + \Gamma_{m(n)} + \mathscr{O}_n(1)\,. \tag{1.13}$$

If $n \geq 2$ then $m(n) \geq 1$, so $0 \leq n - 2m(n) + 1 < n$, which implies $a_{n-2m(n)+1} \in \boldsymbol{\beta}$. In particular we have $\wp(a_{n-2m(n)+1}) \neq 0$. Since we also have $a_n \neq 0$, it follows that

$$v_n(\Gamma_{m(n)}) = v_n\left(\frac{\wp(X_{n-2m(n)+1})X_n}{X_{n-2m(n)}}\right) = -v_n(X_{n-2m(n)}) = -v_n(X_{n-2m(n)} - a_{n-2m(n)}),$$

because $n - 2m(n) < n$, so $a_{n-2m(n)} = 0$ in this case. On the other hand, if $n = 1$ then $a_0 \in \boldsymbol{\beta}$, so $a_0^q, a_0^{q-1} - 1 \neq 0$. Since in this case we have $\Gamma_{m(n)} = \wp(X_2) = z_1$, it follows that

$$\begin{aligned} v_n(\Gamma_{m(n)}) =& v_n\left(\frac{X_0^q}{(X_0^{q-1}-1)(X_1^{q-1}-1)}\right) \\ =& - v_n(X_1^{q-1} - 1) \\ =& - v_n(X_n - a_n) && \text{(by (iv) of Lemma 1.3)} \\ =& - v_n(X_{n-2m(n)} - a_{n-2m(n)}) && \text{(because } m(n) = 0 \text{ in this case).} \end{aligned}$$

This shows that $v_n(\Gamma_{m(n)}) = -v_n(X_{n-2m(n)} - a_{n-2m(n)})$ for all $n \geq 1$, whenever $a_n \in \boldsymbol{\alpha}$, and since the place P_1 is unramified in F_n/F_1 and $n - 2m(n)$ is 0 or 1, it follows that

$$v_n(X_{n-2m(n)} - a_{n-2m(n)}) = v_1(X_{n-2m(n)} - a_{n-2m(n)}).$$

If $n - 2m(n) = 0$, then $e(P_1|P_0) = 1$ by (i),b) of Lemma 1.1, so

$$v_1(X_{n-2m(n)} - a_{n-2m(n)}) = v_1(X_0 - a_0) = v_0(X_0 - a_0) = 1\,;$$

if $n-2m(n) = 1$, taking $i = 2m(n)$ in (ii) of Lemma 1.3 we get the equality $v_1(X_0-a_0) = (q-1)v_1(X_{n-2m(n)} - a_{n-2m(n)})$. Since $e(P_1|P_0) = q - 1$ by (i),c) of Lemma 1.1, then $v_1(X_0 - a_0) = (q-1)v_0(X_0 - a_0)$, so

$$v_1(X_{n-2m(n)} - a_{n-2m(n)}) = v_0(X_0 - a_0) = 1\,.$$

In either case, we conclude that $a_n \in \boldsymbol{\alpha}$ with $n \geq 1$ implies

$$\begin{aligned} v_n(\Gamma_{m(n)}) &= -\, v_n(X_{n-2m(n)} - a_{n-2m(n)}) \\ &= -\, v_1(X_{n-2m(n)} - a_{n-2m(n)}) \\ &= -\, 1. \end{aligned} \tag{1.14}$$

This fact, together with equality (1.13), imply that the place P_n is totally ramified in F_{n+1}/F_n, so $e(P_{n+1}|P_n) = [F_{n+1} : F_n] = q$, and its respective different exponent satisfies $d(P_{n+1}|P_n) = 2(q-1)$, by (iii) of Proposition 0.21. We remark that the same result holds when $n = 0$, that is, if $a_0 \in \boldsymbol{\alpha}$, then $e(P_1|P_0) = q$ and $d(P_1|P_0) = 2(q-1)$; see (i),a) of Lemma 1.1.

On the other hand, the following equality holds for all $n \geq 0$, whenever $a_n \in \boldsymbol{\alpha}$:

$$\begin{aligned} v_n(X_n - a_n) &= q^{m(n)} v_n(X_{n-2m(n)} - a_{n-2m(n)}) \\ &= q^{m(n)}. \end{aligned} \tag{1.15}$$

In fact, the equality is obvious when $n = 0$ (recall the F_0 is the rational function field), whereas for $n \geq 1$ it is obtained applying repeatedly (i) of Lemma 1.3 for $i = 2j$, with $j = 0, 1, \ldots, m(n) - 1$, and using (1.14).

If

$$L_{n+1} = X_{n+1} - \sum_{k=1}^{m(n)} b_k \Gamma_k\,, \tag{1.16}$$

then by (1.13) we have

$$\wp(L_{n+1}) = \Gamma_{m(n)} + \mathscr{O}_n(1)\,, \tag{1.17}$$

and therefore we have $v_{n+1}(L_{n+1}) < 0$ whenever $n \geq 1$ by (1.14), so $v_{n+1}(\wp(L_{n+1})) = q v_{n+1}(L_{n+1})$. Since $v_{n+1}(\Gamma_{m(n)}) = e(P_{n+1}|P_n) v_n(\Gamma_{m(n)}) = -q$, it follows that

$$v_{n+1}(L_{n+1}) = -1, \quad \text{whenever } n \geq 1. \tag{1.18}$$

Now, for every $n \geq 0$ and every $j \geq n+1$ we have (see (1.2))

$$\wp(X_{j+1}) = \lambda_j X_j, \quad \text{being} \quad \lambda_j = \frac{X_{j-1}^q}{(X_{j-1}^{q-1} - 1)\wp(X_j)}\,. \tag{1.19}$$

Suppose that $a_n \in \boldsymbol{\alpha}$. We would like to change the element λ_j by a constant (similarly as in Lemma 1.4; see (1.9)). As before, a natural choice is the value of λ_j at the place P_j, provided that λ_j belongs to the valuation ring $\mathscr{O}_j$. This is indeed the case, as we will see in the following (more general) result.

Lemma 1.8. *Let $n \geq 0$ and suppose that $a_n \in \boldsymbol{\alpha} \cup \{\infty\}$. Then the following holds:*

(i) $\lambda_j \in \mathscr{O}_j^{\times}$, $\mathrm{Tr}(\overline{\lambda_j}) = 0$ *and* $\overline{\lambda_{j+1}\,\lambda_j} = 1$, *for all* $j \geq n+1$.

(ii) $v_j((\lambda_j - \overline{\lambda_j})X_j) > 0$, *which implies* $\wp(X_{j+1}) = \overline{\lambda_j}\,X_j + \mathscr{O}_j(1)$, *for all* $j \geq n+1$.

(iii) $v_j(z_j) = -q^{m(n)+n-j}\,e(P_j|P_n)$ *for all* $j \geq n+1$, *whenever* $a_n \in \boldsymbol{\alpha}$.

(iv) $v_j(z_j) = -q^{1-j}\,e(P_j|P_1)$ *for all* $j \geq 1$, *whenever* $a_0 = \infty$.

Proof.

(i) We claim that $v_j(\lambda_j^{q-1}+1) > 0$ for all $j \geq n+1$ whenever $a_n \in \boldsymbol{\alpha} \cup \{\infty\}$. In fact,

$$\begin{aligned}
\lambda_j^{q-1} + 1 &= \left(\frac{X_{j-1}^q}{(X_{j-1}^{q-1}-1)\wp(X_j)}\right)^{q-1} + 1 \\
&= \frac{X_{j-1}^{q(q-1)}}{(X_{j-1}^{q-1}-1)^{q-1}} \cdot \frac{1}{\wp(X_j)^{q-1}} + 1 \\
&= -\left(\wp(X_j)^{q-1}+1\right) \cdot \frac{1}{\wp(X_j)^{q-1}} + 1 \quad \text{(by (1.1))} \\
&= \frac{-1}{\wp(X_j)^{q-1}}\,,
\end{aligned}$$

and since $a_n \in \boldsymbol{\alpha} \cup \{\infty\}$ implies $a_j = \infty$ for all $j \geq n+1$ by (i),a) of Lemma 1.1, it follows that $v_j(\wp(X_j)^{q-1}) < 0$ for all $j \geq n+1$, which proves the assertion. In particular we have $\lambda_j \in \mathscr{O}_j^{\times}$ and $\overline{\lambda_j}^{\,q-1} + 1 = 0$, so $\mathrm{Tr}(\overline{\lambda_j}) = 0$ (and $\overline{\lambda_j} \in \mathbb{F}_{q^2}$).

On the other hand, if $j \geq n+1$ then

$$\lambda_{j+1} = \frac{X_j^{q+1}}{\wp(X_j)\wp(X_{j+1})} = \frac{X_j^{q+1}}{\wp(X_j)} \cdot \frac{1}{\lambda_j X_j} = \frac{X_j^q}{\wp(X_j)} \cdot \frac{1}{\lambda_j}\,,$$

so $\overline{\lambda_{j+1}\lambda_j}$ is equal to the value of $X_j^q/\wp(X_j)$ at P_{j+1}; but since $a_j = \infty$, then

$$v_j\left(\frac{X_j^q}{\wp(X_j)} - 1\right) = v_j\left(\frac{X_j}{\wp(X_j)}\right) = (1-q)v_j(X_j) > 0\,,$$

so the value of $X_j^q/\wp(X_j)$ at the place P_{j+1} is equal to 1, and thus $\overline{\lambda_{j+1}\lambda_j} = 1$.

(ii) If $a_n \in \boldsymbol{\alpha} \cup \{\infty\}$, then $\overline{\lambda_j} \in \mathbb{F}_{q^2}$ and $\overline{\lambda_j}^{\,q-1} = -1$ for all $j \geq n+1$ by (i), so $v_j(\lambda_j - \overline{\lambda_j}) = v_j(\lambda_j^{q-1}+1)$ by (iv) of Lemma 1.2; but $v_j(\lambda_j^{q-1}+1) = (1-q)v_j(\wp(X_j)) = (1-q)qv_j(X_j)$ (again by (i)). Therefore $v_j\left((\lambda_j - \overline{\lambda_j})X_j\right) = \big((1-q)q+1\big)v_j(X_j) > 0$ and

$$\begin{aligned}\wp(X_{j+1}) &= \overline{\lambda_j}\, X_j + (\lambda_j - \overline{\lambda_j})X_j \\ &= \overline{\lambda_j}\, X_j + \mathscr{O}_j(1)\,.\end{aligned}$$

(iii),(iv) Let $r \geq 0$ be such that $a_r \in \boldsymbol{\alpha} \cup \{\infty\}$. Then $v_{r+1}(\lambda_{r+1}) = 0$ by (i), and $v_{r+1}\big(\wp(X_{r+1})\big) = qv_{r+1}(X_{r+1})$ (because $a_{r+1} = \infty$ in this case). Using (1.19) we get

$$0 = v_{r+1}(\lambda_{r+1}) = qv_{r+1}(X_r) - v_{r+1}(X_r^{q-1} - 1) - qv_{r+1}(X_{r+1})\,. \tag{$\dagger$}$$

If $a_r = \infty$, then $v_{r+1}(X_r^{q-1} - 1) = (q-1)v_{r+1}(X_r)$. Replacing into (†) we obtain

$$qv_{r+1}(X_{r+1}) = v_{r+1}(X_r) = e(P_{r+1}|P_r)v_r(X_r), \quad \text{whenever } a_r = \infty\,. \tag{$\ddagger$}$$

If $a_r \in \boldsymbol{\alpha}$, then $v_r(X_r^{q-1} - 1) = v_r(X_r - a_r)$ by (iv) of Lemma 1.2, and $v_{r+1}(X_r) = 0$. Moreover, $v_r(X_r - a_r) = q^{m(r)}$ by (1.15). Substituting into (†) we obtain

$$v_{r+1}(X_{r+1}) = -e(P_{r+1}|P_r)q^{m(r)-1}, \quad \text{whenever } a_r \in \boldsymbol{\alpha}\,. \tag{$\ddagger\ddagger$}$$

If $n \geq 0$ satisfies $a_n \in \boldsymbol{\alpha} \cup \{\infty\}$, then $a_r = \infty$ for all $r \geq n+1$, and for each $j \geq n$ we have $v_{j+1}(\lambda_{j+1}) = 0$ and $z_{j+1} = \lambda_{j+1}X_{j+1}$. Therefore

$$\begin{aligned}\frac{v_{j+1}(z_{j+1})}{v_{n+1}(X_{n+1})} &= \prod_{r=n+1}^{j} \frac{v_{r+1}(X_{r+1})}{v_r(X_r)} \\ &= \prod_{r=n+1}^{j} \frac{e(P_{r+1}|P_r)}{q} \quad \text{(by ($\ddagger$))} \\ &= \frac{e(P_{j+1}|P_{n+1})}{q^{j-n}}\,.\end{aligned} \tag{$\maltese$}$$

If $a_n \in \boldsymbol{\alpha}$, then $v_{n+1}(X_{n+1}) = -e(P_{n+1}|P_n)\,q^{m(n)-1}$ by (‡‡), so by (✠) we have $v_{j+1}(z_{j+1}) = q^{n-j}\,e(P_{j+1}|P_{n+1})v_{n+1}(X_{n+1}) = -q^{m(n)+n-j-1}\,e(P_{j+1}|P_n)$, which proves (iii). Finally, if $a_0 = \infty$, then $e(P_1|P_0) = q$ by (i),a) of Lemma 1.1. Taking $r = 0$ in (‡) we obtain $v_1(X_1) = v_0(X_0) = -1$. Taking $n = 0$ in (✠) we get $v_{j+1}(z_{j+1}) = -q^{-j}\,e(P_{j+1}|P_1)$ for all $j \geq 0$, which proves (iv), and the proof is finished. □

From now on, we denote $\overline{\lambda_{n+j}}$ by θ_j, for each $j \geq 1$. Since $\mathrm{Tr}\,(\theta_j) = 0$ for each $j \geq 1$ (by (i) of Lemma 1.8), the following equality holds for any element y in the fields F_i:

$$\wp(\theta_j\, y) = \theta_j^q\, y^q - \theta_j\, y = -\theta_j(y^q + q) = -\theta_j\,\mathrm{Tr}\,(y)\,. \tag{1.20}$$

Now we study the ramification behavior of P_{n+1} in F_{n+2}/F_{n+1}, *assuming that* $m(n) \geq 1$. We have, by (ii) of Lemma 1.8 and (1.16):

$$\begin{aligned}\wp(X_{n+2}) &= \theta_1 X_{n+1} + \mathscr{O}_{n+1}(1) \\ &= \theta_1 L_{n+1} + \sum_{k=1}^{m(n)} \theta_1 b_k \Gamma_k + \mathscr{O}_{n+1}(1)\,. \end{aligned} \tag{1.21}$$

Applying Lemma 1.7 we obtain

$$\sum_{k=1}^{m(n)} \theta_1 b_k \Gamma_k = \wp\left(\sum_{k=2}^{m(n)} A_{2,k} b_k \Gamma_k \right) + A_{2,\,m(n)+1}^{q} \Gamma_{m(n)} + \mathscr{O}_{n+1}(1)\,; \tag{1.22}$$

on the other hand, by (1.17) we have, for any $c \in \mathbb{F}_{q^2}$:

$$\begin{aligned} c^q \Gamma_{m(n)} &= c^q \wp(L_{n+1}) + \mathscr{O}_{n+1}(1) \\ &= \wp(cL_{n+1}) - \wp(c) L_{n+1} + \mathscr{O}_{n+1}(1)\,. \end{aligned} \tag{1.23}$$

Substituting both (1.23) with $c = A_{2,\,m(n)+1}$ and (1.22) into (1.21) we obtain

$$\begin{aligned}\wp(X_{n+2}) &= \wp\left(A_{2,\,m(n)+1} L_{n+1} + \sum_{k=2}^{m(n)} A_{2,k} b_k \Gamma_k \right) + (\theta_1 - \wp(A_{2,\,m(n)+1})) L_{n+1} + \mathscr{O}_{n+1}(1) \\ &= \wp\left(A_{2,\,m(n)+1} L_{n+1} + \sum_{k=2}^{m(n)} A_{2,k} b_k \Gamma_k \right) + \mathscr{O}_{n+1}(1)\,, \end{aligned}$$

because $\wp(A_{2,\,m(n)+1}) = \theta_1$. In fact, $\wp(A_{2,\,m(n)+1}) = -\wp(\theta_1 b_{m(n)})$ by the definition of $A_{2,\,m(n)+1}$ in (1.22) and Lemma 1.7. But $\wp(\theta_1 b_{m(n)}) = -\theta_1 \mathrm{Tr}\,(b_{m(n)})$ by (1.20) and $\mathrm{Tr}\,(b_{m(n)}) = 1$ by (1.11) (recall that we suppose $m(n) \geq 1$; see Remark 1.6). Therefore we have

$$\wp(L_{n+2}) = \mathscr{O}_{n+1}(1)\,, \tag{1.24}$$

where

$$L_{n+2} = X_{n+2} - A_{2,\,m(n)+1} L_{n+1} - \sum_{k=2}^{m(n)} A_{2,k} b_k \Gamma_k\,, \tag{1.25}$$

so the place P_{n+1} is unramified in F_{n+2}/F_{n+1} by (ii) of Proposition 0.21; in particular,

$$v_{n+2}(L_{n+1}) = -1\,. \tag{1.26}$$

Now we arrive at the third stage of our calculation, again assuming that $m(n) \geq 1$. We have

$$\begin{aligned}\wp(X_{n+3}) &= \theta_2 X_{n+2} + \mathscr{O}_{n+2}(1) \\ &= \theta_2 A_{2,\,m(n)+1} L_{n+1} + \theta_2 L_{n+2} + \sum_{k=2}^{m(n)} \theta_2 A_{2,k} b_k \Gamma_k + \mathscr{O}_{n+2}(1) \quad \text{(by (1.25))} \\ &= \theta_2 A_{2,\,m(n)+1} L_{n+1} + \sum_{k=2}^{m(n)} \theta_2 A_{2,k} b_k \Gamma_k + \mathscr{O}_{n+2}(1)\,, \end{aligned} \tag{1.27}$$

because $L_{n+2} = \mathscr{O}_{n+2}(1)$ by (1.24). By Lemma 1.7 and (1.23),

$$\begin{aligned}\sum_{k=2}^{m(n)} \theta_2 A_{2,k} b_k \Gamma_k &= \wp\left(\sum_{k=3}^{m(n)} A_{3,k} b_k \Gamma_k \right) + A^q_{3,\,m(n)+1} \Gamma_{m(n)} + \mathscr{O}_{n+2}(1) \\ &= \wp\left(A_{3,\,m(n)+1} L_{n+1} + \sum_{k=3}^{m(n)} A_{3,k} b_k \Gamma_k \right) - \wp(A_{3,\,m(n)+1}) L_{n+1} + \mathscr{O}_{n+2}(1)\,. \end{aligned} \tag{1.28}$$

Now, $\wp(A_{3,\,m(n)+1}) = -\wp(\theta_2 A_{2,\,m(n)} b_{m(n)}) = \theta_2 \mathrm{Tr}\,(A_{2,\,m(n)} b_{m(n)})$ by Lemma 1.7 and (1.20), so

$$\begin{aligned}\theta_2 A_{2,\,m(n)+1} - \wp(A_{3,\,m(n)+1}) &= \theta_2 (A_{2,\,m(n)+1} - \mathrm{Tr}\,(A_{2,\,m(n)} b_{m(n)})) \\ &= \theta_2 (\theta_1 b_{m(n)})^q \quad \text{(by Lemma 1.7 and (1.22))} \\ &= -\theta_2 \theta_1 b^q_{m(n)} \quad \text{(because } \mathrm{Tr}\,(\theta_1) = 0) \\ &= -b^q_{m(n)} \quad \text{(by (i) of Lemma 1.8)}\,. \end{aligned} \tag{1.29}$$

As a consequence, equality (1.27) takes the form

$$\begin{aligned}\wp(X_{n+3}) &= \wp\left(A_{3,\,m(n)+1} L_{n+1} + \sum_{k=3}^{m(n)} A_{3,k} b_k \Gamma_k \right) + (\theta_2 A_{2,\,m(n)+1} - \wp(A_{3,\,m(n)+1})) L_{n+1} + \mathscr{O}_{n+2}(1) \\ &= \wp\left(A_{3,\,m(n)+1} L_{n+1} + \sum_{k=3}^{m(n)} A_{3,k} b_k \Gamma_k \right) - b^q_{m(n)} L_{n+1} + \mathscr{O}_{n+2}(1). \end{aligned}$$

In other words, we have

$$\wp(L_{n+3}) = -b^q_{m(n)} L_{n+1} + \mathscr{O}_{n+2}(1)\,, \tag{1.30}$$

where

$$L_{n+3} = X_{n+3} - A_{3,\,m(n)+1} L_{n+1} - \sum_{k=3}^{m(n)} A_{3,k} b_k \Gamma_k\,. \tag{1.31}$$

We have $v_{n+2}(-b_{m(n)}^q L_{n+1}) = -1$ by (1.26) and the fact that $b_{m(n)} \neq 0$ (because $m(n) \geq 1$; see remark 1.6). Hence the place P_{n+2} is totally ramified in F_{n+3}/F_{n+2} , and the different exponent satisfies $d(P_{n+3}|P_{n+2}) = 2(q-1)$, by (iii) of Proposition 0.21. Reasoning as in (1.18) we conclude that

$$v_{n+3}(L_{n+3}) = -1\,. \tag{1.32}$$

At this point, we have not yet found a clear pattern that allow us to proceed by induction. Indeed, a such pattern exists, but it is instructive to develop a few more steps in our reasoning in order to make the definitive statement of the result clear. So here we go with the fourth step, but this time *we assume that* $m(n) \geq 2$.

We have, by (1.31),

$$\begin{aligned} \wp(X_{n+4}) &= \theta_3 X_{n+3} + \mathscr{O}_{n+3}(1) \\ &= \theta_3 L_{n+3} + \theta_3 A_{3,\,m(n)+1} L_{n+1} + \sum_{k=3}^{m(n)} \theta_3 A_{3,k} b_k \Gamma_k + \mathscr{O}_{n+3}(1)\,. \end{aligned} \tag{1.33}$$

By Lemma 1.7 and (1.23),

$$\begin{aligned} \sum_{k=3}^{m(n)} \theta_3 A_{3,k} b_k \Gamma_k &= \wp\left(\sum_{k=4}^{m(n)} A_{4,k} b_k \Gamma_k \right) + A_{4,\,m(n)+1}^q \Gamma_{m(n)} + \mathscr{O}_{n+3}(1) \\ &= \wp\left(A_{4,\,m(n)+1} L_{n+1} + \sum_{k=4}^{m(n)} A_{4,k} b_k \Gamma_k \right) - \wp(A_{4,\,m(n)+1}) L_{n+1} + \mathscr{O}_{n+3}(1)\,. \end{aligned} \tag{1.34}$$

Now, $\wp(A_{4,\,m(n)+1}) = -\wp(\theta_3 A_{3,\,m(n)} b_{m(n)}) = \theta_3 \mathrm{Tr}\,(A_{3,\,m(n)} b_{m(n)})$ by Lemma 1.7 and (1.20), so

$$\begin{aligned} \theta_3 A_{3,\,m(n)+1} - \wp(A_{4,\,m(n)+1}) &= \theta_3 (A_{3,\,m(n)+1} - \mathrm{Tr}\,(A_{3,\,m(n)} b_{m(n)})) \\ &= \theta_3 (\theta_2 A_{2,\,m(n)} b_{m(n)})^q \qquad \text{(by Lemma 1.7 and (1.28))} \\ &= -\theta_3 \theta_2 (A_{2,\,m(n)} b_{m(n)})^q \quad \text{(because } \mathrm{Tr}\,(\theta_2) = 0) \\ &= -(A_{2,\,m(n)} b_{m(n)})^q \qquad \text{(by (i) of Lemma 1.8)}\,. \end{aligned} \tag{1.35}$$

On the other hand, by (1.30) we have, for any $c \in \mathbb{F}_{q^2}$:

$$\begin{aligned} -c^q L_{n+1} &= (c b_{m(n)}^{-1})^q \wp(L_{n+3}) + \mathscr{O}_{n+2}(1) \\ &= \wp(c b_{m(n)}^{-1} L_{n+3}) - \wp(c b_{m(n)}^{-1}) L_{n+3} + \mathscr{O}_{n+2}(1)\,. \end{aligned} \tag{1.36}$$

Substituting (1.36) with $c = A_{2,m(n)}b_{m(n)}$, together with (1.35) and (1.34) into (1.33), we get

$$\begin{aligned}\wp(X_{n+4}) &= \wp\left(A_{4,\,m(n)+1}L_{n+1} + \sum_{k=4}^{m(n)} A_{4,k}b_k\Gamma_k\right) - (A_{2,\,m(n)}b_{m(n)})^q L_{n+1} + \theta_3 L_{n+3} + \mathscr{O}_{n+3}(1)\\ &= \wp\left(A_{2,\,m(n)}L_{n+3} + A_{4,\,m(n)+1}L_{n+1} + \sum_{k=4}^{m(n)} A_{4,k}b_k\Gamma_k\right)\\ &\quad + (\theta_3 - \wp(A_{2,\,m(n)}))L_{n+3} + \mathscr{O}_{n+3}(1)\,.\end{aligned}$$

Since $\wp(A_{2,\,m(n)}) = -\wp(\theta_1 b_{m(n)-1}) = \theta_1 \mathrm{Tr}\,(b_{m(n)-1})$ by Lemma 1.7 and (1.20), $\mathrm{Tr}\,(b_{m(n)-1}) = 1$ by (1.11) (we are assuming that $m(n) \geq 2$) and $\theta_3 = \theta_1$ by (i) of lemma 1.8, it follows that

$$\wp(L_{n+4}) = \mathscr{O}_{n+3}(1)\,,$$

where

$$L_{n+4} = X_{n+4} - A_{2,\,m(n)}L_{n+3} - A_{4,\,m(n)+1}L_{n+1} - \sum_{k=4}^{m(n)} A_{4,k}b_k\Gamma_k\,. \tag{1.37}$$

so the place P_{n+3} is unramified in F_{n+4}/F_{n+3} by (ii) of Proposition 0.21, and we have $L_{n+4} = \mathscr{O}_{n+4}(1)$.

Now a last step before the general case: we assume again that $m(n) \geq 2$. By (1.37) and the fact that $L_{n+4} = \mathscr{O}_{n+4}(1)$:

$$\begin{aligned}\wp(X_{n+5}) &= \theta_4\, X_{n+4} + \mathscr{O}_{n+4}(1)\\ &= \theta_4\, A_{2,m(n)}L_{n+3} + \theta_4\, A_{4,\,m(n)+1}L_{n+1} + \sum_{k=4}^{m(n)} \theta_4\, A_{4,k}b_k\Gamma_k + \mathscr{O}_{n+4}(1)\,.\end{aligned}$$

Using Lemma 1.7 and (1.23), and proceeding as in (1.35) we obtain

$$\wp(X_{n+5}) = \wp\left(A_{5,\,m(n)+1}L_{n+1} + \sum_{k=5}^{m(n)} A_{5,k}b_k\Gamma_k\right) - (A_{3,\,m(n)}b_{m(n)})^q L_{n+1} + \theta_4 A_{2,\,m(n)}L_{n+3} + \mathscr{O}_{n+3}(1)\,. \tag{1.38}$$

Taking $c = A_{3,\,m(n)}b_{m(n)}$ in (1.36) we obtain

$$\begin{aligned}-(A_{3,\,m(n)}b_{m(n)})^q L_{n+1} &= \wp(A_{3,\,m(n)}L_{n+3}) - \wp(A_{3,\,m(n)})L_{n+3} + \mathscr{O}_{n+4}(1)\\ &= \wp(A_{3,\,m(n)}L_{n+3}) - \theta_2 \mathrm{Tr}\,(A_{2,\,m(n)-1}b_{m(n)-1})L_{n+3} + \mathscr{O}_{n+4}(1)\,,\end{aligned}$$

by Lemma 1.7 and (1.20). Finally, $\theta_4 A_{2,\,m(n)} - \theta_2 \mathrm{Tr}\,(A_{2,\,m(n)-1}b_{m(n)-1}) = -b^q_{m(n)-1}$ by Lemma 1.7 and the fact that $\theta_4 = \theta_2$ (by (i) of Lemma 1.8); the proof is similar to that in (1.29). Replacing these equalities into (1.38) we conclude that

$$\wp(L_{n+5}) = -b^q_{m(n)-1}L_{n+3} + \mathscr{O}_{n+4}(1)\,,$$

where

$$L_{n+5} = X_{n+5} - A_{3,\,m(n)}L_{n+3} - A_{5,\,m(n)+1}L_{n+1} - \sum_{k=5}^{m(n)} A_{5,k}b_k\,\Gamma_k\,, \tag{1.39}$$

and since $v_{n+4}(-b^q_{m(n)-1}L_{n+3}) = v_{n+3}(L_{n+3}) = -1$ by (1.32) and the fact that $b_{m(n)-1} \neq 0$ (because $m(n) \geq 2$; see Remark 1.6), it follows from (iii) of Proposition 0.21 that the place P_{n+4} is totally ramified in F_{n+5}/F_{n+4} and the different exponent satisfies $d(P_{n+5}|P_{n+4}) = 2(q-1)$. Moreover $v_{n+5}(L_{n+5}) = -1$.

Before we state the main result of this chapter in full generality, we recall some facts and fix some notation. Recall that for all $j \geq 1$ we defined θ_j as $\overline{\lambda_{n+j}}$, where λ_{n+j} is given by (1.19). If we define $\theta_0 := \theta_1^{-1}$, then $\mathrm{Tr}\,(\theta_0) = \mathrm{Tr}\,(\theta_1)/\theta_1^{q+1}$, so we have $\mathrm{Tr}\,(\theta_j) = 0$ for all $j \geq 0$ by (i) of Lemma 1.8. The same result, together with the definition of θ_0, imply that

$$\theta_s = \theta_t \ \text{ whenever } \ s \equiv t \,(\mathrm{mod}\, 2) \ \text{ and } \ \theta_s\theta_t = 1 \ \text{ otherwise.} \tag{1.40}$$

Let $b_0 = 1$ and $A_{0,0} = \theta_1$ (see remark 1.6), and let $A_{0,k} = 0$ for $k = 1, 2, \ldots, m(n)$. For $0 \leq j \leq m(n)$, let

$$\sum_{k=j}^{m(n)} \theta_j A_{j,k}b_k\,\Gamma_k = \wp\Bigg(\sum_{k=j+1}^{m(n)} A_{j+1,k}b_k\,\Gamma_k\Bigg) + A^{\,q}_{j+1,\,m(n)+1}\,\Gamma_{m(n)} + \mathscr{O}_n(1)\,, \tag{1.41}$$

where the coefficients b_k are defined as in (1.6) (see Remark 1.6), and the coefficients $A_{j+1,k}$ are given by Lemma 1.7, that is, $A_{j+1,\,j} = 0$ and

$$\begin{aligned} A_{j+1,k} &= (\theta_j A_{j,k-1}b_{k-1})^q + \mathrm{Tr}\,(A_{j+1,k-1}b_{k-1}) \\ &= -\,\theta_j(A_{j,k-1}b_{k-1})^q + \mathrm{Tr}\,(A_{j+1,k-1}b_{k-1}), \quad \text{for } \ j+1 \leq k \leq m(n)+1 \end{aligned} \tag{1.42}$$

(recall that $\theta_j^q = -\theta_j$ for all $j \geq 0$). In particular we have

$$\begin{aligned} \wp(A_{j+1,k}) &= \wp\big(-\theta_j(A_{j,k-1}b_{k-1})^q\big) \\ &= \theta_j\,\mathrm{Tr}\,(A_{j,k-1}b_{k-1}), \quad \text{for } \ j+1 \leq k \leq m(n)+1\,, \end{aligned} \tag{1.43}$$

where the latter equality is consequence of (1.20) (note that (1.20) also holds for $j = 0$ because $\mathrm{Tr}\,(\theta_0) = 0$).

Finally, if we define

$$B_j = \begin{cases} \displaystyle\sum_{k=j}^{m(n)} A_{j,k}b_k\,\Gamma_k, & \text{for } \ j = 0, 1, \ldots, m(n), \\ \qquad 0, & \text{for } \ j = m(n)+1, m(n)+2, \ldots, 2m(n)\,, \end{cases} \tag{1.44}$$

and we define $A_{j+1,\,m(n)+1} = 0$ for $m(n)+1 \le j \le 2m(n)$, then by (1.41) we have

$$\theta_j B_j = \wp(B_{j+1}) + A^q_{j+1,\,m(n)+1}\,\Gamma_{m(n)} + \mathscr{O}_n(1), \quad \text{for } j = 0, 1, \ldots, 2m(n)\,. \tag{1.45}$$

Note that $\theta_0 B_0 = \Gamma_0$ because $A_{0,0} = \theta_1 b_0^{-1}$ and $A_{0,k} = 0$ for $1 \le k \le m(n)$; on the other hand, by (1.42) we have $A_{1,1} = (\theta_0 A_{0,0} b_0)^q + \mathrm{Tr}\,(A_{1,0} b_0) = (\theta_0\theta_1)^q = 1$, and if k between 2 and $m(n)+1$ satisfies $A_{1,k-1} = 1$, then using (1.42) again we obtain $A_{1,k} = (\theta_0 A_{0,k-1} b_{k-1})^q + \mathrm{Tr}\,(A_{1,k-1} b_{k-1}) = \mathrm{Tr}\,(b_{k-1})$, the latter being equal to 1 by (1.11) since $k - 1 \ge 1$. Thus,

$$A_{1,k} = 1 \text{ for } 1 \le k \le m(n)+1, \tag{1.46}$$

which shows that equation (1.45) in the case $j = 0$ reduces to equality (1.13), as expected.

Looking at the elements L_{n+r} already defined (that is, for $1 \le r \le 5$; see (1.16), (1.25), (1.31), (1.37) and (1.39)) we are motivated to define the elements L_{n+r}, for $r \ge 2$, in the following manner:

$$L_{n+r} = X_{n+r} - B_r - \sum_i A_{r-2i,\,m(n)+1-i} L_{n+2i+1}\,, \tag{1.47}$$

where i varies over a certain interval. Now we try to determine this interval in the most natural way. First, clearly we must have $i \ge 0$ and $2i + 1 < r$ (this is a recursive definition after all), that is, $r - 2i \ge 2$. Now, for any $j \ge 0$, the elements $A_{j+1,k}$ are defined only if $j \le k \le m(n)+1$; but $A_{j+1,j} = 0$ by definition, so we may ignore this term, and therefore we can impose the conditions $1 \le j+1 \le k \le m(n)+1$. In our case $j + 1 = r - 2i$ and $k = m(n) + 1 - i$ (because we are dealing with the elements $A_{r-2i,\,m(n)+1-i}$). Thus, we are led to impose the conditions

$$1 \le r - 2i \le m(n) + 1 - i \le m(n) + 1, \;\; r - 2i \ge 2 \quad \text{and} \quad i \ge 0,$$

which are clearly equivalent to

$$2i \le r - 2, \;\; i \ge r - m(n) - 1 \;\; \text{and} \;\; i \ge 0.$$

The first inequality is equivalent to $i \le \lfloor r/2 \rfloor - 1 = m(r) - 1$, whereas the second and third inequalities together are equivalent to $i \ge \gamma(r)$, being $\gamma(r) := \max\{0, r - m(n) - 1\}$. Finally, we impose the condition that the summation interval be nonempty, that is, $\gamma(r) \le m(r) - 1$. Since $\gamma(r)$ is an integer, this is equivalent to $\gamma(r) \le (r/2) - 1$, that is, $2\gamma(r) = \max\{0, 2r - 2m(n) - 2\} \le r - 2$. This happens if and only if $r - 2 \ge 0$ and $r - 2 \ge 2r - 2m(n) - 2$, which can be expressed as $2 \le r \le 2m(n)$. As we will see in the following theorem, which is the heart of this chapter, this choice of the summation interval for the parameter i indeed works.

Theorem 1.9. *Let $n \geq 0$ and suppose that $a_n \in \boldsymbol{\alpha}$. With the previous notation, let*

$$L_{n+1} = X_{n+1} - B_1 \,,$$

and for $2 \leq r \leq 2m(n)$ define $\gamma(r) := \max\{0, r - m(n) - 1\}$, and let

$$L_{n+r} = X_{n+r} - B_r - \sum_{i=\gamma(r)}^{m(r)-1} A_{r-2i,\, m(n)+1-i} L_{n+2i+1} \,. \tag{1.48}$$

Then the elements L_{n+r} satisfy the following properties:

(i) $\wp(L_{n+1}) = \Gamma_{m(n)} + \mathscr{O}_n(1)$, and $v_n(\Gamma_{m(n)}) = -1$ whenever $n \geq 1$[♠]; moreover, we have $e(P_{n+1}|P_n) = q, d(P_{n+1}|P_n) = 2(q-1)$, and $v_{n+1}(L_{n+1}) = -1$ whenever $n \geq 1$.

(ii) For $3 \leq r \leq 2m(n)$ and r odd we have $\wp(L_{n+r}) = -b^q_{m(n)-m(r)+1} L_{n+r-2} + \mathscr{O}_{n+r-1}(1)$ and $v_{n+r-1}(L_{n+r-2}) = -1$; in particular, the place P_{n+r-1} is totally ramified in F_{n+r}/F_{n+r-1} (i.e., $e(P_{n+r}|P_{n+r-1}) = [F_{n+r} : F_{n+r-1}] = q$), $v_{n+r}(L_{n+r}) = -1$ and the different exponent satisfies $d(P_{n+r}|P_{n+r-1}) = 2(q-1)$[■].

(iii) For $2 \leq r \leq 2m(n)$ and r even we have $\wp(L_{n+r}) = \mathscr{O}_{n+r-1}(1)$; in particular, the place P_{n+r-1} is unramified in F_{n+r}/F_{n+r-1}, and $L_{n+r} = \mathscr{O}_{n+r}(1)$.

(iv) For every $i \geq n + 2m(n)$ we have $e(P_{i+1}|P_i) = q$ and $d(P_{i+1}|P_i) = 2(q-1)$.

Proof. Property (i) was already proved; see (1.14),(1.17) and (1.18), and the commentary after equation (1.46). In order to prove properties (ii) and (iii) we proceed by induction on r. By (1.24) and (1.25) we know that the result holds in the case $r = 2$ (note that (1.22) is the equality (1.45) for $j = 1$). Now let s be such that $2 \leq s < 2m(n)$ and suppose that both (ii) and (iii) hold for every r such that $2 \leq r \leq s$. Then by (ii) of Lemma 1.8, (1.48) and (1.45) we have

$$\begin{aligned}
\wp(X_{n+s+1}) &= \theta_s X_{n+s} + \mathscr{O}_{n+s}(1) \\
&= \theta_s L_{n+s} + \theta_s B_s + \sum_{i=\gamma(s)}^{m(s)-1} \theta_s A_{s-2i,\, m(n)+1-i} L_{n+2i+1} + \mathscr{O}_{n+s}(1) \\
&= \theta_s L_{n+s} + \wp(B_{s+1}) + A^q_{s+1,\, m(n)+1}\, \Gamma_{m(n)} + \sum_{i=\gamma(s)}^{m(s)-1} \theta_s A_{s-2i,\, m(n)+1-i} L_{n+2i+1} + \mathscr{O}_{n+s}(1) \,.
\end{aligned} \tag{1.49}$$

[♠] For $n = 0$ the expression $v_n(\Gamma_{m(n)})$ makes no sense because in this case $\Gamma_{m(n)} = \wp(X_1)$ does not belong to F_0 for $q > 2$; see (1.1) with $i = 0$.

[■] Because $m(n) - m(r) + 1 \geq 1$, so $b_{m(n)-m(r)+1} \neq 0$ (see Remark 1.6), which implies $v_{n+r-1}(-b^q_{m(n)-m(r)+1} L_{n+r-2}) = v_{n+r-1}(L_{n+r-2}) = -1$. Now we apply (iii) of Proposition 0.21.

Claim. The following equality (1.50) holds for each t such that $\gamma(s) \le t \le m(s) - 1$, no matter if s is even or odd. The equality also holds for $t = m(s)$, whenever s is odd:

$$\begin{aligned} &A^q_{s+1,\,m(n)+1}\,\Gamma_{m(n)} + \sum_{i=\gamma(s)}^{t} \theta_s A_{s-2i,\,m(n)+1-i} L_{n+2i+1} \\ &= \wp\Bigg(\sum_{i=\gamma(s+1)}^{t} A_{s+1-2i,\,m(n)+1-i} L_{n+2i+1} \Bigg) - (A_{s-1-2t,\,m(n)-t}\, b_{m(n)-t})^q L_{n+2t+1} + \mathscr{O}_{n+s}(1)\,. \end{aligned} \tag{1.50}$$

The proof of this claim is by induction on t. For $t = \gamma(s)$ we must treat separately the cases $s \le m(n)$ and $s \ge m(n) + 1$. Suppose at first that $s \le m(n)$. Then $\gamma(s) = \gamma(s+1) = 0$. Taking $c = A_{s+1,\,m(n)+1}$ in (1.23) we get

$$A^q_{s+1,\,m(n)+1}\,\Gamma_{m(n)} = \wp(A_{s+1,\,m(n)+1} L_{n+1}) - \wp(A_{s+1,\,m(n)+1}) L_{n+1} + \mathscr{O}_{n+s}(1),$$

and since $0 \le s \le m(n)$, we can take $j = s$ and $k = m(n) + 1$ in (1.43), obtaining

$$\wp(A_{s+1,\,m(n)+1}) = \theta_s \mathrm{Tr}\,(A_{s,\,m(n)} b_{m(n)})\,.$$

Therefore we have

$$\begin{aligned} \theta_s A_{s,\,m(n)+1} - \wp(A_{s+1,\,m(n)+1}) &= \theta_s (A_{s,\,m(n)+1} - \mathrm{Tr}\,(A_{s,\,m(n)} b_{m(n)})) \\ &= \theta_s (-\theta_{s-1} (A_{s-1,\,m(n)} b_{m(n)})^q) \text{ (by (1.42))} \\ &= -(A_{s-1,\,m(n)} b_{m(n)})^q \text{ (by (1.40))}\,. \end{aligned}$$

Putting together these equalities we conclude that

$$A^q_{s+1,\,m(n)+1}\,\Gamma_{m(n)} + \theta_s A_{s,\,m(n)+1} L_{n+1} = \wp(A_{s+1,\,m(n)+1} L_{n+1}) - (A_{s-1,\,m(n)} b_{m(n)})^q L_{n+1} + \mathscr{O}_{n+s}(1)\,,$$

which proves (1.50) in the case $t = \gamma(s)(= 0)$ when $s \le m(n)$. On the other hand, if $s \ge m(n) + 1$, then $A_{s+1,\,m(n)+1} = 0$ by definition. Moreover, $\gamma(s) = s - m(n) - 1$ and $\gamma(s+1) = s - m(n)$. Therefore we have $s - 2\gamma(s) = m(n) + 1 - \gamma(s)$, so

$$\begin{aligned} A^q_{s+1,\,m(n)+1}\,\Gamma_{m(n)} + \sum_{i=\gamma(s)}^{\gamma(s)} \theta_s A_{s-2i,\,m(n)+1-i} L_{n+2i+1} &= \theta_s A_{s-2\gamma(s),\,m(n)+1-\gamma(s)} L_{n+2\gamma(s)+1} \\ &= \theta_s A_{s-2\gamma(s),\,s-2\gamma(s)} L_{n+2\gamma(s)+1}\,, \end{aligned}$$

whereas

$$\begin{aligned} &\wp\Bigg(\sum_{i=\gamma(s+1)}^{\gamma(s)} A_{s+1-2i,\,m(n)+1-i} L_{n+2i+1} \Bigg) - (A_{s-1-2\gamma(s),\,m(n)-\gamma(s)}\, b_{m(n)-\gamma(s)})^q L_{n+2\gamma(s)+1} \\ &\qquad = -(A_{s-1-2\gamma(s),\,s-1-2\gamma(s)}\, b_{s-1-2\gamma(s)})^q L_{n+2\gamma(s)+1} \end{aligned}$$

(because $\gamma(s+1) > \gamma(s)$, so the sum above is equal to 0). Now, $s-2\gamma(s) = 2m(n)+2-s \geq 1$ because $s-1 \leq 2m(n)$, and $s-2\gamma(s) = m(n)+1-\gamma(s) \leq m(n)+1$, so we can take $j+1 = k = s-2\gamma(s)$ in (1.42) and use the fact that $A_{j+1,j} = 0$ to obtain

$$\begin{aligned}\theta_s A_{s-2\gamma(s),\,s-2\gamma(s)} L_{n+2\gamma(s)+1} &= \theta_s(-\theta_{s-1-2\gamma(s)}(A_{s-1-2\gamma(s),\,s-1-2\gamma(s)} b_{s-1-2\gamma(s)})^q) L_{n+2\gamma(s)+1} \\ &= -(A_{s-1-2\gamma(s),\,s-1-2\gamma(s)} b_{s-1-2\gamma(s)})^q L_{n+2\gamma(s)+1} \quad \text{(by (1.40))}\,.\end{aligned}$$

This proves equality (1.50) for $t = \gamma(s)$ when $s \geq m(n)+1$.

Now let t be such that either

(a) $\gamma(s) \leq t < m(s)-1$, or

(b) $t = m(s)-1$ and s is odd,

and suppose that equality (1.50) holds. Then

$$\begin{aligned}&A^q_{s+1,\,m(n)+1}\,\Gamma_{m(n)} + \sum_{i=\gamma(s)}^{t+1} \theta_s A_{s-2i,\,m(n)+1-i} L_{n+2i+1} \\ &= \left(A^q_{s+1,\,m(n)+1}\,\Gamma_{m(n)} + \sum_{i=\gamma(s)}^{t} \theta_s A_{s-2i,\,m(n)+1-i} L_{n+2i+1}\right) + \theta_s A_{s-2t-2,\,m(n)-t} L_{n+2t+3} \\ &= \wp\left(\sum_{i=\gamma(s+1)}^{t} A_{s+1-2i,\,m(n)+1-i} L_{n+2i+1}\right) - (A_{s-1-2t,\,m(n)-t}\, b_{m(n)-t})^q L_{n+2t+1} \\ &\quad + \theta_s A_{s-2t-2,\,m(n)-t} L_{n+2t+3} + \mathscr{O}_{n+s}(1) \quad \text{(by induction hypothesis)}\,. \qquad (1.51)\end{aligned}$$

In case (a) we have $0 \leq t \leq m(s)-2$, so $3 \leq 2t+3 \leq 2m(s)-1 \leq s-1$, whereas in case (b) we have $3 \leq 2t+3 = 2m(s)+1 \leq s+1$ and s is odd, so necessarily $2t+3 \leq s$. In either case we see that $3 \leq 2t+3 \leq s$, so property (ii) holds for $r = 2t+3$ by the induction hypothesis. Since $m(2t+3) = t+1$, this means that $\wp(L_{n+2t+3}) = -b^q_{m(n)-t} L_{n+2t+1} + \mathscr{O}_{n+2t+2}(1)$, and so for any $c \in \mathbb{F}_{q^2}$ we have

$$\begin{aligned}-c^q L_{n+2t+1} &= (c b^{-1}_{m(n)-t})^q \wp(L_{n+2t+3}) + \mathscr{O}_{n+2t+2}(1) \\ &= \wp(c b^{-1}_{m(n)-t} L_{n+2t+3}) - \wp(c b^{-1}_{m(n)-t}) L_{n+2t+3} + \mathscr{O}_{n+2t+2}(1)\,.\end{aligned}$$

Taking $c = A_{s-1-2t,\,m(n)-t} b_{m(n)-t}$ we obtain

$$\begin{aligned}-(A_{s-1-2t,\,m(n)-t}\, b_{m(n)-t})^q L_{n+2t+1} &= \wp(A_{s-1-2t,\,m(n)-t} L_{n+2t+3}) \\ &\quad - \wp(A_{s-1-2t,\,m(n)-t}) L_{n+2t+3} + \mathscr{O}_{n+2t+2}(1)\,. \qquad (1.52)\end{aligned}$$

On the other hand, if $t \leq m(s)-2$ then $1 \leq s-2-2t$, and if $t = m(s)-1$, then s is odd, so $s = 2m(s)+1$, hence $s-2-2t = s-2-2m(s)+2 = 1$. Now, since

$s - m(n) - 1 \le \gamma(s) \le t$, it follows that $s - 1 - 2t \le m(n) - t$. Finally, we have trivially $m(n) - t \le m(n) + 1$. As a consequence, we have the following inequalities:

$$1 \le s - 2 - 2t < s - 1 - 2t \le m(n) - t \le m(n) + 1\,. \tag{1.53}$$

In particular, we can take $j + 1 = s - 1 - 2t$ and $k = m(n) - t$ in (1.43) to obtain $\wp(A_{s-1-2t,\,m(n)-t}) = \theta_{s-2-2t}\mathrm{Tr}\,(A_{s-2-2t,\,m(n)-t-1}b_{m(n)-t-1})$. Since $\theta_{s-2-2t} = \theta_s$ by (1.40), it follows that

$$\theta_s A_{s-2t-2,\,m(n)-t} - \wp(A_{s-1-2t,\,m(n)-t}) = \theta_s(A_{s-2-2t,\,m(n)-t} - \mathrm{Tr}\,(A_{s-2-2t,\,m(n)-t-1}b_{m(n)-t-1}))\,.$$

Again by (1.53) we can take $j + 1 = s - 2 - 2t$ and $k = m(n) - t$ in (1.42), obtaining $A_{s-2-2t,\,m(n)-t} - \mathrm{Tr}\,(A_{s-2-2t,\,m(n)-t-1}b_{m(n)-t-1}) = -\theta_{s-3-2t}(A_{s-2t-3,\,m(n)-t-1}b_{m(n)-t-1})^q$, so the previous equality becomes

$$\begin{aligned}\theta_s A_{s-2t-2,\,m(n)-t} - \wp(A_{s-1-2t,\,m(n)-t}) &= \theta_s(-\theta_{s-3-2t}(A_{s-2t-3,\,m(n)-t-1}b_{m(n)-t-1})^q)\\ &= -(A_{s-2t-3,\,m(n)-t-1}b_{m(n)-t-1})^q \quad \text{(by (1.40))}\,.\end{aligned} \tag{1.54}$$

Replacing (1.52) and (1.54) into (1.51) yields

$$\begin{aligned}&A^q_{s+1,\,m(n)+1}\,\Gamma_{m(n)} + \sum_{i=\gamma(s)}^{t+1}\theta_s A_{s-2i,\,m(n)+1-i}L_{n+2i+1}\\ &= \wp\Bigg(\sum_{i=\gamma(s+1)}^{t} A_{s+1-2i,\,m(n)+1-i}L_{n+2i+1}\Bigg) + \wp(A_{s-1-2t,\,m(n)-t}L_{n+2t+3})\\ &\quad + (\theta_s A_{s-2t-2,\,m(n)-t} - \wp(A_{s-1-2t,\,m(n)-t}))L_{n+2t+3} + \mathscr{O}_{n+s}(1)\\ &= \wp\Bigg(\sum_{i=\gamma(s+1)}^{t+1} A_{s+1-2i,\,m(n)+1-i}L_{n+2i+1}\Bigg) - (A_{s-2t-3,\,m(n)-t-1}b_{m(n)-t-1})^q L_{n+2t+3} + \mathscr{O}_{n+s}(1)\,,\end{aligned}$$

which proves equality (1.50) for $t + 1$. This finishes the proof of our claim.

If s is even, taking $t = m(s) - 1$ in (1.50) and substituting into (1.49) yields

$$\begin{aligned}\wp(X_{n+s+1}) = \theta_s L_{n+s} + \wp(B_{s+1}) + \wp\Bigg(\sum_{i=\gamma(s+1)}^{m(s)-1} A_{s+1-2i,\,m(n)+1-i}L_{n+2i+1}\Bigg)\\ - (A_{s-1-2(m(s)-1),\,m(n)-(m(s)-1)}\,b_{m(n)-(m(s)-1)})^q L_{n+2(m(s)-1)+1} + \mathscr{O}_{n+s}(1)\,.\end{aligned}$$

We have $L_{n+s} = \mathscr{O}_{n+s}(1)$ by the induction hypothesis (property (iii)). Now $s = 2m(s)$, so $s - 1 - 2(m(s) - 1) = 1$, and since $m(n) - (m(s) - 1) \ge 1$ (because $2m(s) = s \le 2m(n)$, so

$m(s) \le m(n)$), then $A_{s-1-2(m(s)-1),\,m(n)-(m(s)-1)} = 1$ by (1.46). Moreover, $m(s) = m(s+1)$. Using these facts we can rewrite the equality above as

$$\wp(X_{n+s+1}) = \wp(B_{s+1}) + \wp\left(\sum_{i=\gamma(s+1)}^{m(s+1)-1} A_{s+1-2i,\,m(n)+1-i} L_{n+2i+1}\right) - b^q_{m(n)-m(s+1)+1} L_{n+(s+1)-2} + \mathscr{O}_{n+s}(1)\,,$$

which implies

$$\begin{aligned}\wp(L_{n+s+1}) &= \wp\left(X_{n+s+1} - B_{s+1} - \sum_{i=\gamma(s+1)}^{m(s+1)-1} A_{s+1-2i,\,m(n)+1-i} L_{n+2i+1}\right) \quad \text{(by (1.48))}\\ &= -\, b^q_{m(n)-m(s+1)+1} L_{n+(s+1)-2} + \mathscr{O}_{n+(s+1)-1}(1).\end{aligned}$$

Since P_{n+s-1} is unramified in F_{n+s}/F_{n+s-1} by property (iii), it follows that

$$v_{n+(s+1)-1}(L_{n+(s+1)-2}) = v_{n+s-1}(L_{n+s-1}),$$

the latter being equal to -1 by property (i) (whenever $s-1=1$) or (ii) (whenever $s-1 \ge 3$). This proves that property (ii) holds for $r = s+1$.

Now, if s is odd, then $s - 2m(s) = 1$ and $m(s+1) = m(s)+1$. Moreover we have $m(n) - m(s) \ge 1$ (because $2m(s+1) = s+1 \le 2m(n)$, so $m(s+1) = m(s)+1 \le m(n)$), and thus $A_{s-2m(s),\,m(n)+1-m(s)} = 1$ by (1.46). Therefore

$$\theta_s L_{n+s} + \sum_{i=\gamma(s)}^{m(s)-1} \theta_s A_{s-2i,\,m(n)+1-i} L_{n+2i+1} = \sum_{i=\gamma(s)}^{m(s)} \theta_s A_{s-2i,\,m(n)+1-i} L_{n+2i+1}\,.$$

Replacing into (1.49) yields

$$\wp(X_{n+s+1}) = \wp(B_{s+1}) + A^q_{s+1,\,m(n)+1}\,\Gamma_{m(n)} + \sum_{i=\gamma(s)}^{m(s)} \theta_s A_{s-2i,\,m(n)+1-i} L_{n+2i+1} + \mathscr{O}_{n+s}(1)\,. \quad (1.55)$$

Taking $t = m(s)$ in (1.50) (which is permissible because s is odd) and replacing into (1.55) we obtain

$$\wp(X_{n+s+1}) = \wp(B_{s+1}) + \wp\left(\sum_{i=\gamma(s+1)}^{m(s)} A_{s+1-2i,\,m(n)+1-i} L_{n+2i+1}\right) - (A_{s-1-2m(s),\,m(n)-m(s)} b_{m(n)-m(s)})^q L_{n+2m(s)+1} + \mathscr{O}_{n+s}(1)$$

Since $s-1-2m(s)=0$ and $m(n)-m(s)\geq 1$, then $A_{s-1-2m(s),\,m(n)-m(s)}=A_{0,\,m(n)-m(s)}=0$ by definition. Using this and the fact that $m(s)=m(s+1)-1$ we can rewrite the equation above as

$$\wp(X_{n+s+1})=\wp(B_{s+1})+\wp\Bigg(\sum_{i=\gamma(s+1)}^{m(s+1)-1}A_{s+1-2i,\,m(n)+1-i}L_{n+2i+1}\Bigg)+\mathscr{O}_{n+s}(1)\,,$$

or, equivalently,

$$\wp(L_{n+s+1})=\mathscr{O}_{n+s}(1)\,,$$

according with the definition of L_{n+s+1} (see (1.48)). This proves that property (iii) holds for $r=s+1$ in this case, and this finishes the proof by induction of the properties (i)-(iii) stated in the theorem.

Finally, we want to show property (iv), i.e., that $e(P_{i+1}|P_i)=q$ and $d(P_{i+1}|P_i)=2(q-1)$ for all $i\geq n+2m(n)$. We proceed by induction on i. First of all, for all r such that $0\leq r\leq 2m(n)$ we have

$$\begin{aligned}e(P_{n+r}|P_n)&=e(P_{n+r}|P_{n+2m(r)})\prod_{t=0}^{m(r)-1}e(P_{n+2t+2}|P_{n+2t+1})\,e(P_{n+2t+1}|P_{n+2t})\\&=e(P_{n+r}|P_{n+2m(r)})\prod_{t=0}^{m(r)-1}1\cdot q\quad\text{(by properties (i)-(iii))}\\&=e(P_{n+r}|P_{n+2m(r)})\,q^{m(r)}\,.\end{aligned}$$

If r is even then $r=2m(r)$, so $e(P_{n+r}|P_{n+2m(r)})=1$; otherwise (i.e., if $r=2m(r)+1$) we have $e(P_{n+r}|P_{n+2m(r)})=q$ by (i) and (ii) of Theorem 1.9. In either case we conclude that $e(P_{n+r}|P_{n+2m(r)})=q^{r-2m(r)}$, so

$$e(P_{n+r}|P_n)=\ q^{r-m(r)}\ \text{ for }\ 0\leq r\leq 2m(n),\ \text{ whenever }\ a_n\in\boldsymbol{\alpha}.\tag{1.56}$$

In particular, taking $r=2m(n)$ and using that $m(2m(n))=m(n)$ we get $e(P_{n+2m(n)}|P_n)=q^{m(n)}$. Since $e(P_{n+1}|P_n)=q$ and $d(P_{n+1}|P_n)=2(q-1)$ by (i), the case $i=n+2m(n)$ is solved whenever $m(n)=0$. Otherwise (i.e., if $m(n)\geq 1$), taking $j=n+2m(n)$ in (iii) of Lemma 1.8 we obtain

$$v_{n+2m(n)}(z_{n+2m(n)})=-q^{m(n)+n-n-2m(n)}e(P_{n+2m(n)}|P_n)=-1.$$

This implies that $e(P_{n+2m(n)+1}|P_{n+2m(n)})=[F_{n+2m(n)+1}:F_{n+2m(n)}]=q$ and the different exponent satisfies $d(P_{n+2m(n)+1}|P_{n+2m(n)})=2(q-1)$, by (iii) of Proposition 0.21.

For the induction step, let $i\geq n+2m(n)$ be such that $e(P_{k+1}|P_k)=q$ and $d(P_{k+1}|P_k)=2(q-1)$ for $k=n+2m(n),n+2m(n)+1,\ldots,i$. Then $e(P_{i+1}|P_{n+2m(n)})=q^{i+1-n-2m(n)}$.

Taking $j = i + 1$ in (iii) of Lemma 1.8 we obtain

$$\begin{aligned} v_{i+1}(z_{i+1}) &= -\, q^{m(n)+n-i-1}\, e(P_{i+1}|P_{n+2m(n)})\, e(P_{n+2m(n)}|P_n) \\ &= -\, q^{m(n)+n-i-1}\, q^{i+1-n-2m(n)}\, q^{m(n)} \\ &= -\, 1, \end{aligned}$$

so from (iii) of Proposition 0.21 we conclude that $e(P_{i+2}|P_{i+1}) = q$ and $d(P_{i+2}|P_{i+1}) = 2(q-1)$. The proof by induction is done. □

Theorem 1.10. *If $a_0 = \infty$, then $e(P_{i+1}|P_i) = q$ and $d(P_{i+1}|P_i) = 2(q-1)$ for all $i \geq 0$.*

Proof. By induction on i. The case $i = 0$ is consequence of (i),a) of Lemma 1.1, and if $i \geq 0$ satisfies $e(P_{k+1}|P_k) = q$ and $d(P_{k+1}|P_k) = 2(q-1)$ for $k = 0, 1, \ldots, i$, then $e(P_{i+1}|P_1) = q^i$. Taking $j = i + 1$ in (iv) of Lemma 1.8 we obtain $v_{i+1}(z_{i+1}) = -q^{1-i-1}\, e(P_{i+1}|P_1) = -1$. Therefore the place P_{i+1} is totally ramified in F_{i+2}/F_{i+1} (i.e., $e(P_{i+2}|P_{i+1}) = [F_{i+2} : F_{i+1}] = q$) and the different exponent satisfies $d(P_{i+2}|P_{i+1}) = 2(q-1)$ by (iii) of Proposition 0.21. This finishes the proof. □

1.3 The genus of the tower

In this section we will determine the genus of the tower $\mathcal{F}$ in the case $K = \mathbb{F}_{q^3}$. Now that the ramification behavior of the tower is completely determined (that is, we know in what cases ramification occurs in some step of the tower, along with the respective ramification index and different exponent), we can calculate explicitly its genus.

We already proved (see Theorems 1.9, 1.10 and Lemma 1.1) that for all $n \geq 1$ the places $P \in \mathbb{P}(F_n)$ that are ramified in F_{n+1}/F_n satisfy $e(Q|P) = q$ and $d(Q|P) = 2(q-1)$, where Q denotes the unique place in $\mathbb{P}(F_{n+1})$ above the place P. Thus, it remains to determine the number of ramified places in each step F_{n+1}/F_n for all $n \geq 1$, which, together with Hurwitz genus formula (Proposition 0.10), will provide recursive formulas for the genus g_n of the field F_n/K, for $n > 1$. On the other hand, the genus g_1 of the field F_1/K will be explicitly calculated using (i) and (ii) of Lemma 1.1.

Since the genus is invariant under constant field extensions (see Proposition 0.17), we extend our field K of constants to all $\overline{\mathbb{F}}_q$ [♣]. In this case all the inertial degrees are

[♣] so we indeed will calculate the genus of the tower whenever the base field K is a finite field containing $\mathbb{F}_{q^2}$.

equal to 1, so the places satisfy the duality "ramified/totally decomposed", which will make easier our counting task. For each $n \geq 0$ let

$$\Lambda_n^{(r)} := \{P \in \mathbb{P}(F_n) : \ P \text{ is ramified in } F_{n+1}/F_n\}. \tag{1.57}$$

If $n \geq 1$ and $P \in \Lambda_n^{(r)}$, then by Lemma 1.1 we have two options: either $X_0(P) = \infty$, or $X_i(P) \in \boldsymbol{\alpha}$ for some i such that $0 \leq i \leq n$. In the second case, by Theorem 1.9 we have $n \in D_i$, where

$$D_i := \{i + 2k : 0 \leq k \leq m(i)\} \cup \{k : k > i + 2m(i)\}. \tag{1.58}$$

For each $i, r \geq 0$ and each place $P \in \mathbb{P}(F_i)$, let

$$C_{i,r}(P) := \{Q \in \mathbb{P}(F_{i+r}) : Q \supseteq P\}. \tag{1.59}$$

We have the following preliminary result.

Lemma 1.11. *Let $i \geq 0$ and $P \in \mathbb{P}(F_i)$ with $X_i(P) \in \boldsymbol{\alpha}$. Then the sets $C_{i,r}(P)$ satisfy*

$$|C_{i,r}(P)| = \begin{cases} \delta_i q^{m(r)}, & \text{for } r = 0, 1, \ldots, 2m(i); \\ \delta_i q^{m(i)}, & \text{for } r > 2m(i), \end{cases}$$

where $\delta_i = q - 1$ if $i = 0$ and $\delta_i = 1$ otherwise.

Proof. Let $(P_k)_{k \geq i}$ be any chain of places such that $P_i = P$, $P_k \in \mathbb{P}(F_k)$ and $P_{k+1} \supseteq P_k$ for all $k \geq i$. For any $s \geq 0$, the extension F_{i+s+1}/F_{i+s} is Galois, so the formula $[F_{i+s+1} : F_{i+s}] = e(P_{i+s+1}|P_{i+s}) f(P_{i+s+1}|P_{i+s}) \, |C_{i+s,1}(P_{i+s})|$ holds ([**St**, Corollary III.7.2]). Since $f(P_{i+s+1}|P_{i+s}) = 1$, then we have $[F_{i+s+1} : F_{i+s}] = e(P_{i+s+1}|P_{i+s}) \, |C_{i+s,1}(P_{i+s})|$.

On the other hand, the number $e(P_{i+s+1}|P_{i+s})$ depends only on $i + s$ by Theorem 1.9 (recall that we are assuming $X_i(P_i) \in \boldsymbol{\alpha}$), and therefore $|C_{i+s,1}(P_{i+s})|$ depends only on $i + s$, provided that $X_i(P_{i+s}) \in \boldsymbol{\alpha}$. In particular, if $Q \in C_{i,s}(P)$, then $|C_{i+s,1}(Q)| = |C_{i+s,1}(P_{i+s})|$. Consequently we have $|C_{i,s+1}(P)| = \sum_{Q \in C_{i,s}(P)} |C_{i+s,1}(Q)|$, this sum being equal to $|C_{i,s}(P)| \, |C_{i+s,1}(P_{i+s})|$, so we can write, for any $r \geq 0$:

$$\begin{aligned} |C_{i,r}(P)| &= \frac{|C_{i,r}(P)|}{|C_{i,0}(P)|} \\ &= \prod_{s=0}^{r-1} \frac{|C_{i,s+1}(P)|}{|C_{i,s}(P)|} \\ &= \prod_{s=0}^{r-1} \frac{[F_{i+s+1} : F_{i+s}]}{e(P_{i+s+1}|P_{i+s})} \\ &= \frac{[F_{i+r} : F_i]}{e(P_{i+r}|P_i)}. \end{aligned}$$

According to the definition of δ_i we have $[F_{i+r} : F_i] = \delta_i q^r$ (because $[F_1 : F_0] = q(q-1)$ and $[F_{k+1} : F_k] = q$ for all $k \geq 1$). On the other hand, if $0 \leq r \leq 2m(i)$, then by (1.56) we have $e(P_{i+r}|P_i) = q^{r-m(r)}$, and in particular $e(P_{i+2m(i)}|P_i) = q^{m(i)}$; if $r > 2m(i)$, then we know that $e(P_{i+r}|P_{i+2m(i)}) = q^{r-2m(i)}$ by Theorem 1.9, and so $e(P_{i+r}|P_i) = e(P_{i+r}|P_{i+2m(i)})e(P_{i+2m(i)}|P_i) = q^{r-2m(i)}q^{m(i)} = q^{r-m(i)}$. Putting these results together we conclude that

$$\frac{[F_{i+r} : F_i]}{e(P_{i+r}|P_i)} = \begin{cases} \dfrac{\delta_i q^r}{q^{r-m(r)}}, & \text{for } 0 \leq r \leq 2m(i); \\ \dfrac{\delta_i q^r}{q^{r-m(i)}}, & \text{for } r > 2m(i), \end{cases}$$

which gives the desired result. □

Thus, the number $|C_{i,r}(P)|$ does not depend on the place P, as long as $X_i(P) \in \boldsymbol{\alpha}$. From now on, we will denote this cardinality simply by $C_{i,r}$ in this case.

If $n \geq 1$ and $i \geq 0$ satisfy $n \in D_i$ (see (1.58)), then each place $P \in \mathbb{P}(F_i)$ such that $X_i(P) \in \boldsymbol{\alpha}$ has exactly $C_{i,n-i}$ places above in $\mathbb{P}(F_n)$, all of which belong to $\Lambda_n^{(r)}$, by Theorem 1.9 and the definition of the set D_i. On the other hand, for every $k \geq 0$ and every place $P \in \mathbb{P}(F_k)$ above the infinite place in F_0, the ramification index of P in the extension F_{k+1}/F_k is equal to q by Theorem 1.10, and therefore the number of places in $\mathbb{P}(F_{k+1})$ above P is equal to $[F_{k+1} : F_k]/q$ by fundamental equality (Lemma 0.8). In particular, the infinite place in F_0 has exactly $q-1$ places above in F_1, all of which are totally ramified in F_k/F_1 for all $k \geq 1$, and so for every $n \geq 1$ there are exactly $q-1$ places above the infinite place in F_0, which belong to $\Lambda_n^{(r)}$.

The discussion preceding definition (1.58) shows that, conversely, all the places in $\Lambda_n^{(r)}$ with $n \geq 1$ are necessarily of the form described above. Consequently, if we define

$$\Lambda_k^{(\alpha)} := \{P \in \mathbb{P}(F_k) : X_k(P) \in \boldsymbol{\alpha}\}, \text{ for all } k \geq 0, \tag{1.60}$$

then we conclude for all $n \geq 1$ that the cardinality of the set $\Lambda_n^{(r)}$ is given by

$$\left|\Lambda_n^{(r)}\right| = q - 1 + \sum_{\substack{i \geq 0 \\ n \in D_i}} C_{i,n-i} \left|\Lambda_i^{(\alpha)}\right|. \tag{1.61}$$

Thus, we are led to calculate $\left|\Lambda_k^{(\alpha)}\right|$ for all $k \geq 0$. But if $Q \in \Lambda_k^{(\alpha)}$ and $k \geq 1$, then $P = Q \cap F_{k-1}$ satisfies $X_{k-1}(P) \in \boldsymbol{\beta}$ by (i),c) of Lemma 1.1, so we are forced to consider, for all $k \geq 0$, the sets

$$\Lambda_k^{(\beta)} := \{P \in \mathbb{P}(F_k) : X_k(P) \in \boldsymbol{\beta}\}; \tag{1.62}$$

$$\Lambda_k^{(0)} := \{P \in \mathbb{P}(F_k) : X_k(P) = 0\}. \tag{1.63}$$

Lemma 1.12. *For each $k \geq 0$ we have the following:*

(i) $\left|\Lambda_{k+1}^{(\alpha)}\right| = (q-1)\left|\Lambda_k^{(\beta)}\right|$.

(ii) $\left|\Lambda_{k+1}^{(0)}\right| = \left|\Lambda_k^{(\beta)}\right|$.

(iii) $\left|\Lambda_{k+1}^{(\beta)}\right| = [F_{k+1} : F_k]\left|\Lambda_k^{(0)}\right|$.

Proof. Let $w = X_0^{q(q-1)}/(X_0^{q-1}-1)^{q-1}$ and define

$$g(T) = \begin{cases} \wp(T) - z_k, & \text{if } k \geq 1; \\ \wp(T)^{q-1} + 1 + w, & \text{if } k = 0. \end{cases}$$

Then by (1.1) and (1.2) we have $F_{k+1} = F_k(X_{k+1})$, where X_{k+1} satisfies $g(X_{k+1}) = 0$; moreover, $g(T)$ is the minimal polynomial of X_{k+1} over F_k. Let $P \in \mathbb{P}(F_k)$ and $Q \in \mathbb{P}(F_{k+1})$ be such that $Q \supseteq P$.

If $X_k(P) \in \boldsymbol{\beta}$, then by (i),c) of Lemma 1.1 we have $X_{k+1}(Q) \in \boldsymbol{\alpha} \cup \{0\}$, so $\wp(X_{k+1}(Q)) = 0$. This implies $z_k = \wp(X_{k+1}) \in Q \cap F_k = P$ whenever $k \geq 1$, and $1 + w = -\wp(X_1)^{q-1} \in Q \cap F_0 = P$ whenever $k = 0$. In either case we have $g(T) \in \mathscr{O}_P[T]$, and the reduction mod P of g is given by

$$g_P(T) = \begin{cases} \wp(T), & \text{if } k \geq 1; \\ \wp(T)^{q-1}, & \text{if } k = 0. \end{cases}$$

As a consequence, each polynomial of the form $T - \lambda$, with $\lambda \in \boldsymbol{\alpha} \cup \{0\}$, is an irreducible factor of g_P (recall that by assumption the residue field at P is equal to $\overline{\mathbb{F}}_q$). By Kummer's Theorem (Proposition 0.9), for each $\lambda \in \boldsymbol{\alpha} \cup \{0\}$ there exists a place $Q_\lambda \in \mathbb{P}(F_{k+1})$ above P such that $X_{k+1}(Q_\lambda) = \lambda$. On the other hand, for every place $Q \in \mathbb{P}(F_{k+1})$ above P we have $e(Q|P) = [F_{k+1} : F_k]/q$ by (i),c) and (iii) of Lemma 1.1, so it follows from fundamental equality (Lemma 0.8) that the Q_λ are all the places in $\mathbb{P}(F_{k+1})$ above P (because $\sum_{\lambda \in \boldsymbol{\alpha} \cup \{0\}} e(Q_\lambda|P) = \left|\alpha \cup \{0\}\right|[F_{k+1} : F_k]/q = [F_{k+1} : F_k]$). Thus, there are exactly $q-1$ places in $\Lambda_{k+1}^{(\alpha)}$ above P and exactly one place in $\Lambda_{k+1}^{(0)}$ above P, which proves both (i) and (ii).

Finally, if $P \in \mathbb{P}(F_k)$ satisfies $X_k(P) = 0$, then for all place $Q \in \mathbb{P}(F_{k+1})$ above P we have $e(Q|P) = 1$ and $X_{k+1}(Q) \in \boldsymbol{\beta}$ by (i),b) and (ii) of Lemma 1.1, so by fundamental equality (Lemma 0.8) there are exactly $[F_{k+1} : F_k]$ places in $\Lambda_{k+1}^{(\beta)}$ above P, which proves (iii). □

Since F_0 is the rational function field, then we have $\left|\Lambda_0^{(\alpha)}\right| = |\boldsymbol{\alpha}| = q-1$, $\left|\Lambda_0^{(\beta)}\right| = |\boldsymbol{\beta}| = q(q-1)$ and $\left|\Lambda_0^{(0)}\right| = 1$. From this, together with the previous lemma, we conclude that $\left|\Lambda_k^{(\alpha)}\right|$, $\left|\Lambda_k^{(\beta)}\right|$ and $\left|\Lambda_k^{(0)}\right|$ are not zero for all $k \geq 0$. Now, if $k \geq 1$ and $0 \leq j < m(k)$,

then $k-2j \geq 2$, so $[F_{k-2j} : F_{k-2j-1}] = q$; moreover, by (ii) and (iii) of the previous lemma we have

$$\begin{aligned}\left|\Lambda_{k-2j}^{(\beta)}\right| &= [F_{k-2j} : F_{k-2j-1}]\left|\Lambda_{k-2j-1}^{(0)}\right| \\ &= [F_{k-2j} : F_{k-2j-1}]\left|\Lambda_{k-2j-2}^{(\beta)}\right| \\ &= q\left|\Lambda_{k-2j-2}^{(\beta)}\right|,\end{aligned}$$

hence

$$\begin{aligned}\frac{\left|\Lambda_{k}^{(\beta)}\right|}{\left|\Lambda_{k-2m(k)}^{(\beta)}\right|} &= \prod_{j=0}^{m(k)-1}\frac{\left|\Lambda_{k-2j}^{(\beta)}\right|}{\left|\Lambda_{k-2j-2}^{(\beta)}\right|} \\ &= \prod_{j=0}^{m(k)-1} q \\ &= q^{m(k)}.\end{aligned}$$

If k is even, then $k-2m(k) = 0$, so $\left|\Lambda_{k-2m(k)}^{(\beta)}\right| = \left|\Lambda_{0}^{(\beta)}\right| = q(q-1)$; if k is odd, then $k-2m(k) = 1$, so by (iii) of the previous lemma we have $\left|\Lambda_{k-2m(k)}^{(\beta)}\right| = [F_1 : F_0]\left|\Lambda_{0}^{(0)}\right| = q(q-1)$. In either case we conclude that $\left|\Lambda_{k}^{(\beta)}\right| = q^{m(k)+1}(q-1)$ for all $k \geq 1$. Since this equality also holds when $k = 0$, it follows from (i) of the previous lemma that

$$\left|\Lambda_{k}^{(\alpha)}\right| = (q-1)\left|\Lambda_{k-1}^{(\beta)}\right| = q^{m(k-1)+1}(q-1)^2 = q^{m(k+1)}(q-1)^2, \quad \text{for all } \ k \geq 1,$$

and since $\left|\Lambda_{0}^{(\alpha)}\right| = q-1$, then we can write

$$\left|\Lambda_{k}^{(\alpha)}\right| = q^{m(k+1)}(q-1)^2/\delta_k, \quad \text{for all } \ k \geq 0,$$

where δ_k is as in Lemma 1.11. Thus, equality (1.61) can be rewritten as

$$\left|\Lambda_{n}^{(r)}\right| = q - 1 + (q-1)^2 \sum_{\substack{i\geq 0 \\ n\in D_i}} C_{i,n-i}\,\frac{q^{m(i+1)}}{\delta_i}, \quad \text{for all } n \geq 1. \tag{1.64}$$

Now, D_i is the disjoint union of the sets H_i and E_i, where $H_i = \{i+2k : 0 \leq k \leq m(i)\}$ and $E_i = \{k : k > i + 2m(i)\}$. If $n \in H_i$, then $n = i+2k$, with $0 \leq k \leq m(i)$, and so $0 \leq 2k = n-i \leq 2m(i)$. Therefore $C_{i,n-i} = \delta_i q^{m(n-i)}$ by Lemma 1.11. On the other hand, if $n \in E_i$, then $n-i > 2m(i)$, so $C_{i,n-i} = \delta_i q^{m(i)}$ by the same lemma. Since $\{i \geq 0 : n \in D_i\}$ is the disjoint union of the sets $\{i \geq 0 : n \in H_i\}$ and $\{i \geq 0 : n \in E_i\}$, equality (1.64) becomes

$$\left|\Lambda_{n}^{(r)}\right| = q-1+(q-1)^2\left(\sum_{\substack{i\geq 0 \\ n\in H_i}} \delta_i q^{m(n-i)}\,\frac{q^{m(i+1)}}{\delta_i} + \sum_{\substack{i\geq 0 \\ n\in E_i}} \delta_i q^{m(i)}\,\frac{q^{m(i+1)}}{\delta_i}\right), \quad \text{for all } n \geq 1. \tag{1.65}$$

If $n \in H_i$, then $n = i + 2k$, with $0 \le k \le m(i)$. Therefore we have $0 \le 2k \le 2m(i) = 2m(n-2k) \le n-2k$ and so $0 \le k \le \lfloor n/4 \rfloor$. Conversely, if $i = n-2k$, with $0 \le k \le \lfloor n/4 \rfloor$, then $n \in H_i$, $m(n-i) = k$ and $m(i+1) = m(n+1) - k$. Consequently,

$$\sum_{\substack{i\ge 0\\ n\in i}} \delta_i q^{m(n-i)} \frac{q^{m(i+1)}}{\delta_i} = \sum_{k=0}^{\lfloor n/4\rfloor} q^k q^{m(n+1)-k} = (\lfloor n/4\rfloor + 1)\, q^{m(n+1)}. \tag{1.66}$$

Now, if $n \in E_i$, then $n > i + 2m(i)$. If $i = 2k + \ell$, with $k \ge 0$ and $\ell = 0$ or 1, then $i + 2m(i) = 4k + \ell$, so we have $4k + \ell \le n - 1$, and thus $2i = 4k + 2\ell \le n - 1 + \ell$. Therefore $i \le m(n - 1 + \ell)$; conversely, if $i \ge 0$ satisfies $i \le m(n - 1 + \ell)$, where ℓ is the residue of i modulo 2, then $n \in E_i$. In particular, $\{i \ge 0 : n \in E_i\} \subseteq \{0, 1, \dots, m(n)\}$, and since $m(n) - 1 = m(n-2) \le m(n - 1 + \ell)$ for $\ell = 0, 1$, it follows that $\{i \ge 0 : n \in E_i\}$ contains the set $\{i \in \mathbb{N} : 0 \le i \le m(n) - 1\}$. Thus, in order to determine precisely the set $\{i \ge 0 : n \in E_i\}$, it is suffices to determine when n belongs to $E_{m(n)}$.

We claim that $n \notin E_{m(n)}$ if and only if $n \equiv 0 \pmod 4$. In fact, if $m(n)$ is odd, then $\ell = 1$, so certainly $m(n) \le m(n - 1 + \ell)$; this is the case when $n \equiv 2$ or 3 (mod 4). If $n \equiv 1 (\text{mod } 4)$, say $n = 4k + 1$, then $m(n) = 2k$ is even, so $\ell = 0$, and $m(n - 1 + \ell) = m(4k) = 2k = m(n)$. Finally, if $n = 4k$, then $m(n) = 2k$, so $\ell = 0$ and $m(n - 1 + \ell) = m(n - 1) = 2k - 1 < m(n)$. This proves that

$$\{i \ge 0 : n \in E_i\} = \begin{cases} \{0, 1, \dots, m(n)\}, & \text{if } n \not\equiv 0 \pmod 4; \\ \{0, 1, \dots, m(n)\} \setminus \{m(n)\} & \text{otherwise.} \end{cases}$$

On the other hand, for all integer i we have $m(i) + m(i + 1) = i$. Putting together these facts we obtain

$$\sum_{\substack{i\ge 0\\ n\in E_i}} \delta_i q^{m(i)} \frac{q^{m(i+1)}}{\delta_i} = \sum_{\substack{i\ge 0\\ n\in E_i}} q^i = \frac{q^{m(n)+b(n)} - 1}{q - 1}, \text{ where } b(n) = \begin{cases} 1, & \text{if } n \not\equiv 0 \pmod 4; \\ 0 & \text{otherwise.} \end{cases} \tag{1.67}$$

Replacing (1.66) and (1.67) into (1.65) we obtain, for all $n \ge 1$:

$$\begin{aligned} \left|\Lambda_n^{(r)}\right| &= q - 1 + (q-1)^2 \left((\lfloor n/4\rfloor + 1)\, q^{m(n+1)} + \frac{q^{m(n)+b(n)} - 1}{q-1} \right) \\ &= q - 1 + (q-1)^2 (\lfloor n/4\rfloor + 1)\, q^{m(n+1)} + (q-1)(q^{m(n)+b(n)} - 1) \\ &= q - 1 + (q-1)^2 (\lfloor n/4\rfloor + 1)\, q^{m(n+1)} + (q-1) q^{m(n)+b(n)} - (q-1) \\ &= (q-1)^2 (\lfloor n/4\rfloor + 1)\, q^{m(n+1)} + (q-1) q^{m(n)+b(n)}. \end{aligned} \tag{1.68}$$

For $n \ge 0$, let g_n be the genus of the function field F_n/K. If $n \ge 1$, then $[F_{n+1} : F_n] = q$, so by Riemann-Hurwitz formula we have

$$2g_{n+1} - 2 = (2g_n - 2)q + \sum_{P\in\Lambda_n^{(r)}} \sum_{\substack{Q\in\mathbb{P}(F_{n+1})\\ Q\supseteq P}} d(Q|P).$$

By Theorems 1.9 and 1.10, each place $P \in \Lambda_n^{(r)}$ has an unique place $Q \in \mathbb{P}(F_{n+1})$ (because P is totally ramified in F_{n+1}/F_n), and $d(Q|P) = 2(q-1)$. Therefore

$$2g_{n+1} - 2 = (2g_n - 2)q + 2(q-1)\left|\Lambda_n^{(r)}\right|,$$

so

$$\begin{aligned} g_{n+1} &= qg_n + (q-1)\left|\Lambda_n^{(r)}\right| - q + 1 \\ &= qg_n + (q-1)(\left|\Lambda_n^{(r)}\right| - 1). \end{aligned}$$

Dividing both sides of the equality above by q^{n+1} we get

$$\frac{g_{n+1}}{q^{n+1}} = \frac{g_n}{q^n} + \frac{(q-1)(\left|\Lambda_n^{(r)}\right| - 1)}{q^{n+1}}.$$

Consequently, for each $n \geq 0$ we have

$$\begin{aligned} \frac{g_{n+1}}{q^{n+1}} - \frac{g_1}{q} &= \sum_{k=1}^{n} \left(\frac{g_{k+1}}{q^{k+1}} - \frac{g_k}{q^k} \right) \\ &= \sum_{k=1}^{n} \frac{(q-1)(\left|\Lambda_k^{(r)}\right| - 1)}{q^{k+1}}. \end{aligned}$$

From this we obtain the following formula for the genus g_n, for all $n \geq 1$:

$$\begin{aligned} g_n &= q^{n-1}g_1 + (q-1)\sum_{k=1}^{n-1} q^{n-k-1}(\left|\Lambda_k^{(r)}\right| - 1) \\ &= q^{n-1}g_1 + (q-1)\sum_{k=1}^{n-1} q^{n-k-1}\left|\Lambda_k^{(r)}\right| - (q-1)\sum_{k=1}^{n-1} q^{n-k-1} \\ &= q^{n-1}g_1 + 1 - q^{n-1} + (q-1)\sum_{k=1}^{n-1} q^{n-k-1}\left|\Lambda_k^{(r)}\right|. \end{aligned} \tag{1.69}$$

For $\ell = 1, 2, 3, 4$, let

$$S_\ell = \sum_{k \in A_\ell} q^{n-k-1}\left|\Lambda_k^{(r)}\right|, \quad \text{where} \quad A_\ell = \{k \in \mathbb{N} : 1 \leq k \leq n-1 \text{ and } k \equiv \ell \pmod 4\}.$$

We have $A_\ell = \{4s + \ell : 0 \leq s \leq d(\ell)\}$, where $d(\ell) = \left\lfloor \frac{n-1-\ell}{4} \right\rfloor$. Note that $d(\ell) \geq -1$ (because $n \geq 1$) and

$$\sum_{k=1}^{n-1} q^{n-k-1}\left|\Lambda_k^{(r)}\right| = \sum_{\ell=1}^{4} S_\ell. \tag{1.70}$$

Using (1.68) we get

$$S_\ell = \sum_{s=0}^{d(\ell)} q^{n-(4s+\ell)-1}\Big((q-1)^2\Big(\Big\lfloor\frac{4s+\ell}{4}\Big\rfloor+1\Big)q^{m(4s+\ell+1)}+(q-1)q^{m(4s+\ell)+b(4s+\ell)}\Big).$$

Now $\Big\lfloor\dfrac{4s+\ell}{4}\Big\rfloor = s+\Big\lfloor\dfrac{\ell}{4}\Big\rfloor$, $b(4s+\ell)=b(\ell)$ and $m(4s+t)=2s+m(t)$ for any t, so equality above becomes

$$\begin{aligned}
S_\ell &= (q-1)^2\sum_{s=0}^{d(\ell)}\Big(s+1+\Big\lfloor\frac{\ell}{4}\Big\rfloor\Big)q^{n-4s-\ell-1+2s+m(\ell+1)}+(q-1)\sum_{s=0}^{d(\ell)}q^{n-4s-\ell-1+2s+m(\ell)+b(\ell)}\\
&= (q-1)^2\sum_{s=0}^{d(\ell)}\Big(s+1+\Big\lfloor\frac{\ell}{4}\Big\rfloor\Big)q^{n-\ell-1+m(\ell+1)-2s}+(q-1)\sum_{s=0}^{d(\ell)}q^{n-\ell-1+m(\ell)+b(\ell)-2s}\\
&= (q-1)^2q^{n-\ell-1+m(\ell+1)}\sum_{s=0}^{d(\ell)}(s+1)\,q^{-2s}+(q-1)q^{n-\ell-1}G(\ell)\sum_{s=0}^{d(\ell)}q^{-2s},
\end{aligned}$$

where $G(\ell)=(q-1)\lfloor\ell/4\rfloor\,q^{m(\ell+1)}+q^{m(\ell)+b(\ell)}$. If $\ell=1,2,3$, then $b(\ell)=1$ and $\lfloor\ell/4\rfloor=0$, so $G(\ell)=q^{m(\ell)+1}$; if $\ell=4$, then $b(\ell)=0$ and $\lfloor\ell/4\rfloor=1$, so in this case we have $G(\ell)=(q-1)q^{m(4+1)}+q^{m(4)}=(q-1)q^2+q^2=q^3=q^{m(\ell)+1}$. This proves that $G(\ell)=q^{m(\ell)+1}$, and therefore we have

$$\begin{aligned}
S_\ell &= (q-1)^2q^{n-\ell-1+m(\ell+1)}\sum_{s=0}^{d(\ell)}(s+1)\,q^{-2s}+(q-1)q^{n-\ell+m(\ell)}\sum_{s=0}^{d(\ell)}q^{-2s}\\
&= (q-1)^2q^{n-m(\ell)-1}\sum_{s=0}^{d(\ell)}(s+1)\,q^{-2s}+(q-1)q^{n-m(\ell+1)}\sum_{s=0}^{d(\ell)}q^{-2s}
\end{aligned}\tag{1.71}$$

(because $m(\ell)+m(\ell+1)=\ell$ for all ℓ). On the other hand, for any integer k with $k\geq -1$ and all $x>0$ with $x\neq 1$ we have

$$\sum_{s=0}^{k}x^{s+1}=\frac{x^{k+2}-x}{x-1}$$

(the sum with $k=-1$ is meant to be 0). Differentiating with respect to x gives

$$\begin{aligned}
\sum_{s=0}^{k}(s+1)x^s &= \frac{(x-1)((k+2)x^{k+1}-1)-(x^{k+2}-x)}{(x-1)^2}\\
&= \frac{(k+1)x^{k+2}-(k+2)x^{k+1}+1}{(x-1)^2}\,.
\end{aligned}\tag{1.72}$$

Suppose at first that $n \equiv 1 \pmod 4$. Then for $\ell = 1, 2, 3, 4$ we have

$$d(\ell) = \frac{n-1}{4} + \left\lfloor \frac{-\ell}{4} \right\rfloor = \frac{n-1}{4} - 1\,,$$

so in this case $d(\ell)$ is independent of ℓ, say c. Using (1.71) we get

$$\sum_{\ell=1}^{4} S_\ell = (q-1)^2 q^{n-1} \left(\sum_{s=0}^{c} (s+1)\, q^{-2s} \right) \left(\sum_{\ell=1}^{4} q^{-m(\ell)} \right) + (q-1) q^n \left(\sum_{s=0}^{c} q^{-2s} \right) \left(\sum_{\ell=1}^{4} q^{-m(\ell+1)} \right).$$

Now $\sum_{\ell=1}^{4} q^{-m(\ell)} = q^{-0} + q^{-1} + q^{-1} + q^{-2} = (q^2 + 2q + 1)/q^2 = (q+1)^2/q^2$, whereas $\sum_{\ell=1}^{4} q^{-m(\ell+1)} = q^{-1} + q^{-1} + q^{-2} + q^{-2} = 2(q+1)/q^2$. Using these values and the value of (1.72) with $k = c$ the previous sum becomes

$$\begin{aligned}
\sum_{\ell=1}^{4} S_\ell &= (q-1)^2 q^{n-1} \, \frac{(q+1)^2}{q^2} \, \frac{\left[(c+1)q^{-2c-4} - (c+2)q^{-2c-2} + 1\right]}{(q^{-2}-1)^2} \\
&\quad + (q-1) q^n \, \frac{2(q+1)}{q^2} \, \frac{1 - q^{-2c-2}}{1 - q^{-2}} \\
&= (q^2-1)^2 q^{n-1} \, \frac{q^2}{q^4} \, \frac{\left[cq^{-2c-4}(1-q^2) + q^{-2c-4}(1-2q^2) + 1\right]}{(q^{-2}-1)^2} \\
&\quad + \frac{2(q^2-1) q^n (1 - q^{-2c-2})}{q^2 - 1} \\
&= \frac{(q^2-1)^2 q^{n+1} \left[cq^{-2c-4}(1-q^2) + q^{-2c-4}(1-2q^2) + 1\right]}{(q^2-1)^2} + 2q^n(1 - q^{-2c-2}) \\
&= q^{n+1}\left[cq^{-2c-4}(1-q^2) + q^{-2c-4}(1-2q^2) + 1\right] + 2q^n(1 - q^{-2c-2}) \\
&= c(1-q^2) q^{n-2c-3} + (1-2q^2) q^{n-2c-3} + q^{n+1} + 2q^n - 2q^{n-2c-2} \\
&= q^{n+1} + 2q^n + q^{n-2c-3}(c(1-q^2) + 1 - 2q^2 - 2q)\,.
\end{aligned}$$

Now $2c + 3 = 3 + 2(n-5)/4 = 3 + (n-5)/2 = (n+1)/2$, so $n - 2c - 3 = (n-1)/2$. Moreover we have $\lfloor n/4 \rfloor = (n-1)/4$ (because $n \equiv 1 \pmod 4$) $= c + 1$. Using these facts together with the equality above and replacing into (1.70) we get the following equality, which is valid whenever $n \geq 1$ and $n \equiv 1 \pmod 4$:

$$\begin{aligned}
\sum_{k=1}^{n-1} q^{n-k-1} \left| \Lambda_k^{(r)} \right| &= q^{n+1} + 2q^n + q^{(n-1)/2}(\lfloor n/4 \rfloor (1-q^2) - 1 + q^2 + 1 - 2q^2 - 2q) \\
&= q^{n+1} + 2q^n + q^{(n-1)/2}(\lfloor n/4 \rfloor (1-q^2) - q^2 - 2q). \qquad (1.73)
\end{aligned}$$

Now suppose $n \geq 1$ and $n \equiv 2 \pmod 4$. Then necessarily $n-1 \geq 1$ and $n-1 \equiv 1 \pmod 4$. On the other hand, we have

$$\begin{aligned}\sum_{k=1}^{n-1} q^{n-k-1} \left|\Lambda_k^{(r)}\right| &= q^{n-(n-1)-1} \left|\Lambda_{n-1}^{(r)}\right| + \sum_{k=1}^{n-2} q^{n-k-1} \left|\Lambda_k^{(r)}\right| \\ &= \left|\Lambda_{n-1}^{(r)}\right| + q \sum_{k=1}^{(n-1)-1} q^{(n-1)-k-1} \left|\Lambda_k^{(r)}\right|. \end{aligned} \tag{1.74}$$

The first summand can be calculated using (1.68), whereas the second can be calculated using (1.73). We also have $\lfloor (n-1)/4 \rfloor = \lfloor n/4 \rfloor$. Thus, we have

$$\begin{aligned}\left|\Lambda_{n-1}^{(r)}\right| &= (q-1)^2(\lfloor (n-1)/4 \rfloor + 1)\, q^{m(n)} + (q-1) q^{m(n-1)} q^{b(n-1)} \\ &= (q-1)^2(\lfloor n/4 \rfloor + 1)\, q^{n/2} + (q-1) q^{(n-2)/2}\, q \\ &= (q-1)^2(\lfloor n/4 \rfloor + 1)\, q^{n/2} + (q-1) q^{n/2}, \end{aligned}$$

whereas

$$\begin{aligned} q \sum_{k=1}^{(n-1)-1} q^{(n-1)-k-1} \left|\Lambda_k^{(r)}\right| &= q\Big(q^n + 2q^{n-1} + q^{(n-2)/2}(\lfloor (n-1)/4 \rfloor (1-q^2) - q^2 - 2q)\Big) \\ &= q^{n+1} + 2q^n + q^{n/2}(\lfloor n/4 \rfloor (1-q^2) - q^2 - 2q). \end{aligned}$$

Replacing these equalities into (1.74) we obtain the following equality, which is valid for $n \geq 1$ and $n \equiv 2 \pmod 4$:

$$\begin{aligned}\sum_{k=1}^{n-1} q^{n-k-1} \left|\Lambda_k^{(r)}\right| &= q^{n/2}\Big((q-1)^2(\lfloor n/4 \rfloor + 1) + q - 1\Big) \\ &\quad + q^{n/2}\Big(\lfloor n/4 \rfloor (1-q^2) - q^2 - 2q\Big) + q^{n+1} + 2q^n \\ &= q^{n+1} + 2q^n + q^{n/2}(\lfloor n/4 \rfloor (2-2q) - 3q). \end{aligned} \tag{1.75}$$

Now suppose $n \geq 1$ and $n \equiv 3 \pmod 4$. Then $n-1 \geq 1$ and $n-1 \equiv 2 \pmod 4$. We have again $\lfloor (n-1)/4 \rfloor = \lfloor n/4 \rfloor$. By (1.68) we have

$$\begin{aligned}\left|\Lambda_{n-1}^{(r)}\right| &= (q-1)^2(\lfloor (n-1)/4 \rfloor + 1)\, q^{m(n)} + (q-1) q^{m(n-1)} q^{b(n-1)} \\ &= (q-1)^2(\lfloor n/4 \rfloor + 1)\, q^{(n-1)/2} + (q-1) q^{(n-1)/2}\, q \\ &= (q-1)^2(\lfloor n/4 \rfloor + 1)\, q^{(n-1)/2} + (q^2-q) q^{(n-1)/2}, \end{aligned}$$

and from (1.75) we get

$$\begin{aligned} q \sum_{k=1}^{(n-1)-1} q^{(n-1)-k-1} \left|\Lambda_k^{(r)}\right| &= q\Big(q^n + 2q^{n-1} + q^{(n-1)/2}(\lfloor (n-1)/4 \rfloor (2-2q) - 3q)\Big) \\ &= q^{n+1} + 2q^n + q^{(n-1)/2}(\lfloor n/4 \rfloor (2q-2q^2) - 3q^2). \end{aligned}$$

Replacing these values into (1.74) we obtain the following equality for $n \geq 1$ and $n \equiv 3 \pmod 4$:

$$\begin{aligned}\sum_{k=1}^{n-1} q^{n-k-1}\left|\Lambda_k^{(r)}\right| &= q^{(n-1)/2}\Big((q-1)^2(\lfloor n/4\rfloor+1)+q^2-q\Big)\\ &\quad + q^{(n-1)/2}\Big(\lfloor n/4\rfloor(2q-2q^2)-3q^2\Big)+q^{n+1}+2q^n\\ &= q^{n+1}+2q^n+q^{(n-1)/2}(\lfloor n/4\rfloor(1-q^2)-q^2-3q+1)\,. \end{aligned} \tag{1.76}$$

Finally, suppose $n \geq 1$ and $n \equiv 4 \pmod 4$. Then $n-1 \geq 1$ and $n-1 \equiv 3 \pmod 4$. Unlike the previous cases, in this case we have $\lfloor (n-1)/4\rfloor = \lfloor n/4\rfloor - 1$. By (1.68) we have

$$\begin{aligned}\left|\Lambda_{n-1}^{(r)}\right| &= (q-1)^2(\lfloor (n-1)/4\rfloor+1)\,q^{m(n)}+(q-1)q^{m(n-1)}q^{b(n-1)}\\ &= (q-1)^2\lfloor n/4\rfloor\,q^{n/2}+(q-1)q^{(n-2)/2}\,q\\ &= (q-1)^2\lfloor n/4\rfloor\,q^{n/2}+(q-1)q^{n/2}\,,\end{aligned}$$

and from (1.76) we get

$$\begin{aligned}q\sum_{k=1}^{(n-1)-1} q^{(n-1)-k-1}\left|\Lambda_k^{(r)}\right| &= q\Big(q^n+2q^{n-1}+q^{(n-2)/2}(\lfloor (n-1)/4\rfloor(1-q^2)-q^2-3q+1)\Big)\\ &= q^{n+1}+2q^n+q^{n/2}((\lfloor n/4\rfloor-1)(1-q^2)-q^2-3q+1)\,.\end{aligned}$$

Replacing these values into (1.74) we obtain the following equality for $n \geq 1$ and $n \equiv 4 \pmod 4$:

$$\begin{aligned}\sum_{k=1}^{n-1} q^{n-k-1}\left|\Lambda_k^{(r)}\right| &= q^{n/2}\Big((q-1)^2\lfloor n/4\rfloor+q-1\Big)\\ &\quad + q^{n/2}\Big((\lfloor n/4\rfloor-1)(1-q^2)-q^2-3q+1\Big)+q^{n+1}+2q^n\\ &= q^{n+1}+2q^n+q^{n/2}(\lfloor n/4\rfloor(2-2q)-2q-1)\,.\end{aligned} \tag{1.77}$$

Now we will calculate g_1. This can be done using Hurwitz genus formula (Proposition 0.10) and Lemma 1.1. The only ramified places in F_1/F_0 are of the form $(X_0 = a)$, with $a \in \boldsymbol{\alpha} \cup \boldsymbol{\beta} \cup \{\infty\}$. Therefore we have

$$\begin{aligned}2g_1-2 &= (2g_0-2)[F_1:F_0]+\sum_{a\in\boldsymbol{\alpha}\cup\{\infty\}}\sum_{\substack{P\in\mathbb{P}(F_1)\\ X_0(P)=a}} d(P\,|(X_0=a))+\sum_{a\in\boldsymbol{\beta}}\sum_{\substack{P\in\mathbb{P}(F_1)\\ X_0(P)=a}} d(P\,|(X_0=a))\\ &= -2q(q-1)+\sum_{a\in\boldsymbol{\alpha}\cup\{\infty\}}\sum_{\substack{P\in\mathbb{P}(F_1)\\ X_0(P)=a}} 2(q-1)+\sum_{a\in\boldsymbol{\beta}}\sum_{\substack{P\in\mathbb{P}(F_1)\\ X_0(P)=a}}(q-2)\,.\end{aligned}$$

Now if $a \in \boldsymbol{\alpha} \cup \{\infty\}$, then $e(P|(X_0 = a)) = q$ for any place $P \in \mathbb{P}(F_1)$ such that $P|(X_0 = a)$ by (i),a) of Lemma 1.1. Since we are assuming that the base field is algebraically closed, all the inertial indices are equal to 1. Therefore the number of places $P \in \mathbb{P}(F_1)$ such that $P|(X_0 = a)$ is equal to $[F_1 : F_0]/q = q - 1$, by fundamental equality (Lemma 0.8). Similarly, for each $a \in \boldsymbol{\beta}$ the number of places $P \in \mathbb{P}(F_1)$ such that $P|(X_0 = a)$ is equal to $[F_1 : F_0]/(q-1) = q$ (by (i),c) of Lemma 1.1), so the equality above becomes

$$\begin{aligned} 2g_1 - 2 = & -2q(q-1) + 2(q-1)\big|\boldsymbol{\alpha} \cup \{\infty\}\big|\big|\{P \in \mathbb{P}(F_1) : X_0(P) = a\}\big| \\ & + (q-2)\,|\boldsymbol{\beta}|\,\big|\{P \in \mathbb{P}(F_1) : X_0(P) = a\}\big| \\ = & -2q(q-1) + 2(q-1)q(q-1) + (q-2)(q^2-q)q \\ = & \, q(q-1)(-2 + 2(q-1) + (q-2)q) \\ = & \, q(q-1)(q^2-4) \\ = & \, q^4 - q^3 - 4q^2 + 4q\,. \end{aligned}$$

Thus, the genus g_1 is given by

$$g_1 = \frac{q^3(q-1)}{2} - 2q^2 + 2q + 1\,. \tag{1.78}$$

Using (1.69),(1.73),(1.75),(1.76),(1.77) and (1.78) we obtain our main result:

Theorem 1.13. *The genera g_n of the tower of function fields given by* (1.1) *is given by*

$$g_n = q^{n-1}(g_1 - 1) + 1 + (q-1)T_n\,,$$

where g_1 is given by (1.78) *and*

$$T_n = q^{n+1} + 2q^n + \begin{cases} q^{(n-1)/2}(\lfloor n/4 \rfloor(1-q^2) - q^2 - 2q), & \text{if} \quad n \equiv 1 \pmod 4, \\ q^{n/2}(\lfloor n/4 \rfloor(2-2q) - 3q), & \text{if} \quad n \equiv 2 \pmod 4, \\ q^{(n-1)/2}(\lfloor n/4 \rfloor(1-q^2) - q^2 - 3q + 1), & \text{if} \quad n \equiv 3 \pmod 4, \\ q^{n/2}(\lfloor n/4 \rfloor(2-2q) - 2q - 1), & \text{if} \quad n \equiv 4 \pmod 4. \end{cases}$$

For those who dislike formulas given by cases.

Let $n \geq 1$. We have $\lfloor n/4 \rfloor(1-q^2) - q^2 - 2q = (\lfloor n/4 \rfloor + 1)(1-q^2) - 2q - 1$, whereas $\lfloor n/4 \rfloor(1-q^2) - q^2 - 3q + 1 = (\lfloor n/4 \rfloor + 1)(1-q^2) - 3q$. Therefore we can write

$$T_n - q^{n+1} - 2q^n = \begin{cases} q^{(n-1)/2}((\lfloor n/4 \rfloor + 1)(1-q^2) - 2q - 1), & \text{if} \quad n \equiv 1 \pmod 4, \\ q^{n/2}(\lfloor n/4 \rfloor(2-2q) - 3q), & \text{if} \quad n \equiv 2 \pmod 4, \\ q^{(n-1)/2}((\lfloor n/4 \rfloor + 1)(1-q^2) - 3q), & \text{if} \quad n \equiv 3 \pmod 4, \\ q^{n/2}(\lfloor n/4 \rfloor(2-2q) - 2q - 1), & \text{if} \quad n \equiv 4 \pmod 4. \end{cases}$$

Now if $n \equiv 1$ or $4 \pmod 4$ then $m(n)$ is even, that is, $m(n) = 2m(m(n)) = 2\lfloor n/4 \rfloor$, so we have $-2q - 1 = -2q - q^0 = -2q - q^{m(n)-2\lfloor n/4 \rfloor}$; similarly, if $n \equiv 2$ or $3 \pmod 4$ then $m(n)$ is odd, so $m(n) = 2\lfloor n/4 \rfloor + 1$, and therefore $-3q = -2q - q^1 = -2q - q^{m(n)-2\lfloor n/4 \rfloor}$. Thus, we can "simplify" the expression above, obtaining

$$T_n - q^{n+1} - 2q^n = \begin{cases} q^{(n-1)/2}((\lfloor n/4 \rfloor + 1)(1-q^2) - 2q - q^{m(n)-2\lfloor n/4 \rfloor}), & \text{if} \quad n \equiv 1 \pmod 4, \\ q^{n/2}(\lfloor n/4 \rfloor (2-2q) - 2q - q^{m(n)-2\lfloor n/4 \rfloor}), & \text{if} \quad n \equiv 2 \pmod 4, \\ q^{(n-1)/2}((\lfloor n/4 \rfloor + 1)(1-q^2) - 2q - q^{m(n)-2\lfloor n/4 \rfloor}), & \text{if} \quad n \equiv 3 \pmod 4, \\ q^{n/2}(\lfloor n/4 \rfloor (2-2q) - 2q - q^{m(n)-2\lfloor n/4 \rfloor}), & \text{if} \quad n \equiv 4 \pmod 4. \end{cases}$$

Finally, if $n \equiv 2$ or $4 \pmod 4$ then n is even, so we have $m(n) = n/2$ and $0 = n - 2m(n)$, which implies $2 - 2q = 2(1-q) = (1+1)(1-q) = (1+q^0)(1-q) = (1+q^{n-2m(n)})(1-q)$; on the other hand, if $n \equiv 1$ or $3 \pmod 4$ then n is odd, so we have $m(n) = (n-1)/2$ and $1 = n - 2m(n)$, and therefore $1 - q^2 = (1+q)(1-q) = (1+q^1)(1-q) = (1+q^{n-2m(n)})(1-q)$. Putting together these facts we can write the formula above as the following single expression[■] :

$$T_n = q^{n+1} + 2q^n + q^{m(n)}\Big((\lfloor n/4 \rfloor + n - 2m(n))(1 + q^{n-2m(n)})(1-q) - 2q - q^{m(n)-2\lfloor n/4 \rfloor}\Big).$$

■ Which is, admittedly, rather unnatural...

Chapter 2

A new tower over cubic finite fields

In this chapter we introduce a new tower over cubic finite fields attaining the generalized Zink bound. This tower was considered by Ihara (see equation (3) in [**Ih07**]) as a subtower of the Bezerra-Garcia-Stichtenoth tower (introduced in [**BezGaSt**]), in order to point out some interesting features of the BeGS tower. Ihara's presentation of the tower is slightly different from ours; in Section 2.4 we prove that this tower is indeed a subtower of the BeGS tower, and that the tower constructed by Ihara and the tower described in this work are the same.

2.1 The basic (and the auxiliary) equation

Let k be a *perfect* field of characteristic $p > 0$, and let q be a power of p. Let $\mathcal{F} = (F_n)_{n\geq 0}$ be the sequence of function fields over k defined recursively as follows: $F_0 = k(X_0)$, the rational function field over k, and for $n \geq 0$ let $F_{n+1} = F_n(X_{n+1})$, where X_{n+1} satisfies the following:

$$f(X_n, X_{n+1}) = 0, \quad \text{where} \quad f(X,Y) = Y^{q+1} + Y - \left(\frac{X+1}{X^{q+1}}\right) \text{ and } X_{n+1} \notin k(X_n)\,. \tag{2.1}$$

Remark 2.1. Regarding equation (2.1) above, we claim that equation $f(X,Y) = 0$ has an unique root Y in $k(X)$, namely, $Y = -(X+1)/X$. In fact, let $z := -1/X$. If $Y \in k(X) = k(z)$ satisfies $f(X,Y) = 0$, then $Y^{q+1} + Y = Y(Y+1)^q = (-z)^q + (-z)^{q+1} = (z-1)z^q$. Thus, Y is $k[z]$-integral, so Y belongs to $k[z]$ (because $k[z]$ is an UFD, hence integrally closed). Comparing degrees we get $\deg_z Y = 1$, so $Y + 1 = cz$, with $c \in k^\times$. Replacing we obtain $(cz-1)c^q z^q = (z-1)z^q$, so $c^{q+1} = 1$ and $c^q = 1$. Consequently we have $c = 1$ and $Y = z - 1$, and since the polynomial $f(X,Y)$ is separable respect to the variable

Y (because $\partial_Y f(X,Y) = (q+1)Y^q + 1 = (Y+1)^q$, so f and $\partial_Y f$ are relative prime in $k(X)[Y]$), our claim is proved.

Now let $x = -1/X_n$ and $y = X_{n+1} + 1$. Imitating the calculations made in the remark above we get $X_{n+1}^{q+1} + X_{n+1} = (y-1)y^q$ and $(X_n+1)/X_n^{q+1} = (x-1)x^q$. Since $X_{n+1} \notin k(X_n)$, this means that

$$(y-1)y^q = (x-1)x^q \text{ and } x \neq y\,. \tag{2.2}$$

Note the symmetry on this equation. For this reason, we will first study the ramification behavior in this more abstract setting. Let k be a *perfect* field of characteristic $p > 0$, and let x, y be such that (2.2) holds. Clearly x is transcendent over k iff y is too, so we assume that x is transcendent over k. If $Q \in \mathbb{P}(k(x,y))$, then by (2.2) we have

$$x(Q) = \infty \text{ iff } y(Q) = \infty, \text{ and } x(Q) \in \{0,1\} \text{ iff } y(Q) \in \{0,1\}. \tag{2.3}$$

On the other hand, by (2.2) we have $y^{q+1} - x^{q+1} = y^q - x^q = (y-x)^q$. Since $y^{q+1} - x^{q+1} = y^{q+1} - yx^q + yx^q - x^{q+1} = y(y-x)^q + x^q(y-x)$, it follows that $x^q(y-x) + y(y-x)^q = (y-x)^q$, and since $y \neq x$, we conclude that

$$x^q + (y-1)(y-x)^{q-1} = 0. \tag{2.4}$$

This polynomial is symmetric in x and y (being the quotient of two symmetric polynomials), so we also have

$$y^q + (x-1)(x-y)^{q-1} = 0. \tag{2.5}$$

Now, dividing (2.4) by $(y-x)^q$ we obtain $\left(\dfrac{x}{y-x}\right)^q + \dfrac{y-1}{y-x} = 0$. Since $\dfrac{y-1}{y-x} = \dfrac{x-1+y-x}{y-x} = 1 + \dfrac{x-1}{x}\,\dfrac{x}{y-x}$, then we can write

$$Z^q + (1-x^{-1})Z + 1 = 0, \text{ with } Z = \frac{x}{y-x}\,. \tag{2.6}$$

Similarly, dividing (2.5) by $(x-y)^q$ we obtain

$$W^q + (1-y^{-1})W + 1 = 0, \text{ with } W = \frac{y}{x-y}\,. \tag{2.7}$$

Now we will determine the ramification in the extensions $k(x,y)/k(x)$ and $k(x,y)/k(y)$ of function fields over k. Let $P \in \mathbb{P}(k(x))$ and $Q \in \mathbb{P}(k(x,y))$ be such that $Q|P$.

Suppose at first that $x(P) = 1$. Then by (2.3) we have $y \in \mathcal{O}_Q$. Using (2.5) we get $y(Q)^q + (x(P)-1)(y(Q)-x(P))^{q-1} = 0$, so $y(Q) = 0$. Thus, $(y-x)(Q) = -1$, so

$y - x \in \mathscr{O}_Q^\times$, and therefore $Z \in \mathscr{O}_Q$ and $Z(Q) = x(Q)/(y-x)(Q) = -1$. We can rewrite (2.6) as

$$\begin{aligned} Z^q + (1-x^{-1})Z + 1 &= (Z+1)^q + (1-x^{-1})(Z+1-1) \\ &= (Z+1)^q + (1-x^{-1})(Z+1) + x^{-1} - 1 \\ &= 0\,. \end{aligned} \tag{2.8}$$

Since $v_Q(Z+1) > 0$, then $v_Q((1-x^{-1})(Z+1)) > v_Q(x^{-1}-1)$, so by triangle inequality we necessarily have $v_Q((Z+1)^q) = v_Q(x^{-1}-1)$, that is, $qv_Q(Z+1) = v_Q(x^{-1}-1)$; but $v_Q(x) = 0$ (because $x(Q) = 1$), which implies $v_Q(x^{-1}-1) = v_Q(x(x^{-1}-1)) = v_Q(x-1) = e(Q|P)v_P(x-1) = e(Q|P)$. Consequently we have $qv_Q(Z+1) = e(Q|P)$.

On the other hand, by (2.5) we have $[k(x,y) : k(x)] \leq q$, so in particular we have $e(Q|P) \leq q$. Putting these facts together we conclude that $e(Q|P) = q = [k(x,y) : k(x)]$ and $v_Q(Z+1) = 1$. In particular, the element $Z+1$ is a local parameter at the place Q, with minimal polynomial over $k(x)$ equal to $\varphi(T) = T^q + (1-x^{-1})T + x^{-1} - 1$ by (2.8), so by Proposition 0.12 we have $d(Q|P) = v_Q(\varphi'(Z+1)) = v_Q(1-x^{-1}) = e(Q|P) = q$. Note that since the place P is totally ramified in $k(x,y)/k(x)$, it follows that k is algebraically closed in $k(x,y)$ by Corollary 0.18. Using this fact together with Corollary 0.19, we can suppose in the sequel that the field k is *algebraically closed* in order to determine the ramification behavior.

Now suppose $x(P) = 0$. Again by (2.3) we have $y \in \mathscr{O}_Q$. Since $[k(x,y) : k(x)] = q$ by the previous case, it follows from (2.5) that the minimal polynomial of y over $k(x)$ is given by $\theta(T) = T^q + (x-1)(T-x)^{q-1}$. Its reduction mod P is given by $\theta_P(T) = T^q - T^{q-1} = T^{q-1}(T-1)$, hence by Kummer's Theorem (Proposition 0.9) there exist $Q_i \in \mathbb{P}(k(x,y))$ with $i = 0, 1$ such that $Q_i|P$ and $y(Q_i) = i$. Using (2.4) we get the equality $v_{Q_0}(x^q) = v_{Q_0}((y-1)(y-x)^{q-1})$, that is, $qv_{Q_0}(x) = (q-1)v_{Q_0}(y-x)$ (because $v_{Q_0}(y-1) = 0$). As a consequence, $q-1$ divides $v_{Q_0}(x) = e(Q_0|P)v_P(x) = e(Q_0|P)$.

Now by fundamental equality we have $q = [k(x,y) : k(x)] = \sum_Q e(Q|P)f(Q|P)$, where Q ranges over the places in $\mathbb{P}(k(x,y))$ dividing P. Since $e(Q_0|P) \geq q-1$ and $e(Q_1|P) \geq 1$, then necessarily Q_0 and Q_1 are the unique places in $\mathbb{P}(k(x,y))$ above the place P, and we have $e(Q_0|P) = q-1$ and $e(Q_1|P) = f(Q_0|P) = f(Q_1|P) = 1$.

Finally, it remains to consider the case $v_P(x) \leq 0$ and $x(P) \neq 1$. By (2.6) we have $k(x,y) = k(x)(Z)$, and if $\psi(T)$ denotes the minimal polynomial of Z over $k(x)$, then $\psi(T) = T^q + (1-x^{-1})T + 1$. Since $x(P) \neq 1$, it follows that $x^{-1} \in \mathscr{O}_P$, and $x^{-1}(P) = x(P)^{-1}$. The reduction mod P of this polynomial is given by $\psi_P(T) = T^q + (1-x(P)^{-1})T + 1$, which is separable because $\psi_P'(T) = 1 - x(P)^{-1} \neq 0$. In particular, since we are assuming that k is algebraically closed, then $\psi_P(T)$ decomposes completely into distinct linear factors in $(\mathscr{O}_P/P)[T] = k[T]$, so by Kummer's Theorem (Proposition 0.9) the place P is totally decomposed in $k(x,y)/k(x)$.

We recall that similar results hold for the field extension $k(x,y)/k(y)$, by the symmetry of equation (2.2). Now we summarize all these results.

Proposition 2.2. *Let k be a perfect field of characteristic $p > 0$, and let q be a power of p. Let x, y be transcendent elements over k satisfying relation* (2.2)*. For the function fields $k(x), k(y)$ and $k(x,y)$ over k the following holds:*

(i) The field extensions $k(x,y)/k(x)$ and $k(x,y)/k(y)$ are both separable of degree q, and k is algebraically closed in $k(x,y)$.

(ii) For a place $Q \in \mathbb{P}(k(x,y))$, let $P_x = Q \cap k(x)$ and $P_y = Q \cap k(y)$. Then $x(Q) = \infty$ iff $y(Q) = \infty$, and $x(Q) \in \{0,1\}$ iff $y(Q) \in \{0,1\}$. More specifically, the following relations hold:

a) $x(Q) = 1$ implies $y(Q) = 0$. In that case we have $e(Q|P_x) = d(Q|P_x) = q$ and $e(Q|P_y) = 1$.

b) $y(Q) = 1$ implies $x(Q) = 0$. In that case we have $e(Q|P_y) = d(Q|P_y) = q$ and $e(Q|P_x) = 1$.

c) $x(Q) = 0$ implies $y(Q) = 0$ or 1. If $y(Q) = 0$, then $e(Q|P_x) = e(Q|P_y) = q - 1$. Moreover, exactly two places Q in $\mathbb{P}(k(x,y))$ satisfy $x(Q) = 0$, say Q_0 and Q_1, and $\{y(Q_0), y(Q_1)\} = \{0,1\}$ (so both possibilities on $y(Q)$ indeed occur).

d) $y(Q) = 0$ implies $x(Q) = 0$ or 1. If $x(Q) = 0$, then $e(Q|P_x) = e(Q|P_y) = q - 1$. Moreover, exactly two places Q in $\mathbb{P}(k(x,y))$ satisfy $y(Q) = 0$, say Q_0 and Q_1, and $\{x(Q_0), x(Q_1)\} = \{0,1\}$.

e) The places $(x = 0)$ and $(x = 1)$ are the unique ramified places in $k(x,y)/k(x)$, and similarly $(y = 0)$ and $(y = 1)$ are the unique ramified places in $k(x,y)/k(y)$. In particular $e(Q|P_x) = e(Q|P_y) = 1$ whenever $x(Q) = \infty$ (which is equivalent to $y(Q) = \infty$).

Figure 2.1 (page 60) describes succinctly the ramification behavior in the field extensions $k(x,y)/k(x)$ and $k(x,y)/k(y)$. From now on, whenever no confusion arises, we will denote by e the ramification index, and we denote by d the respective different exponent. Moreover, we will omit the value of d in the figures whenever tame ramification occurs, because in that case we know that $d = e - 1$.

2.2 The ramification behavior of the tower

Now we return to our original sequence of function fields over k, which is defined recursively by equation (2.1). Recall that equation (2.2) was obtained after the change

of variables $x = -1/X_n$ and $y = X_{n+1} + 1$. By reversing this substitution we translate the contents of Proposition 2.2 to our original context, obtaining the following result:

Proposition 2.3. *Let k be a perfect field of characteristic $p > 0$, and let q be a power of p. Let $\mathcal{F} = (F_n)_{n\geq 0}$ be the sequence of function fields over k defined recursively by equation* (2.1)*. Then we have the following:*

(i) For each $n \geq 0$, the field extensions $k(X_n, X_{n+1})/k(X_n)$ and $k(X_n, X_{n+1})/k(X_{n+1})$ are both separable of degree q, and k is algebraically closed in $k(X_n, X_{n+1})$.

(ii) For a place $Q \in \mathbb{P}(F_{n+1})$, let $P_n = Q \cap k(X_n)$, $P_{n+1} = Q \cap k(X_{n+1})$ and $P = Q \cap k(X_n, X_{n+1})$. Then the following relations hold:

a) $P_n = (X_n = -1)$ implies $P_{n+1} = (X_{n+1} = -1)$. In that case, $e(P|P_n) = d(P|P_n) = q$ and $e(P|P_{n+1}) = 1$.

b) $P_{n+1} = (X_{n+1} = 0)$ implies $P_n = (X_n = \infty)$. In that case, $e(P|P_{n+1}) = d(P|P_{n+1}) = q$ and $e(P|P_n) = 1$.

c) $P_n = (X_n = \infty)$ implies $P_{n+1} = (X_{n+1} = \alpha)$, with $\alpha \in \{-1, 0\}$. If $\alpha = -1$, then $e(P|P_n) = e(P|P_{n+1}) = q - 1$.

d) $P_{n+1} = (X_{n+1} = -1)$ implies $P_n = (X_n = \alpha)$, with $\alpha \in \{-1, \infty\}$.

e) The places $(X_n = \infty)$ and $(X_n = -1)$ are the unique ramified places in the extension $k(X_n, X_{n+1})/k(X_n)$, and $(X_{n+1} = -1)$ and $(X_{n+1} = 0)$ are the unique ramified places in $k(X_n, X_{n+1})/k(X_{n+1})$.

f) $P_n = (X_n = 0)$ iff $P_{n+1} = (X_{n+1} = \infty)$. In that case $e(P|P_n) = e(P|P_{n+1}) = 1$.

Proof. As we said before, we take $x = -1/X_n$ and $y = X_{n+1} + 1$, so we are in the situation of Proposition 2.2. Moreover, for a place $Q \in \mathbb{P}(F_{n+1})$ we have the following relations between the values of x, y, X_n and X_{n+1} at the place Q:

$x(Q)$	$X_n(Q)$
1	-1
0	∞
∞	0

$y(Q)$	$X_{n+1}(Q)$
0	-1
1	0
∞	∞

Now we simply rewrite the statements of Proposition 2.2 using the table above, obtaining items i) and ii). This finishes the proof. □

We remark that, for each $n \geq 0$, all the possibilities stated in item (ii) of the previous result can be realized. More precisely, we call a sequence $(\alpha_n)_{n\geq 0}$ of elements in $\{-1, 0, \infty\}$ *admissible* if the following holds for each $n \geq 0$:

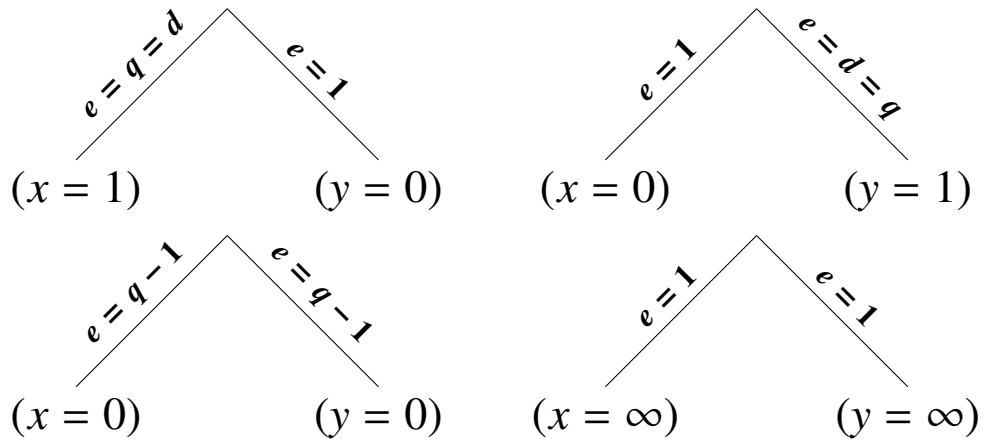


FIGURE 2.1: RAMIFICATION IN $k(x, y)/k(x)$ AND $k(x, y)/k(y)$.

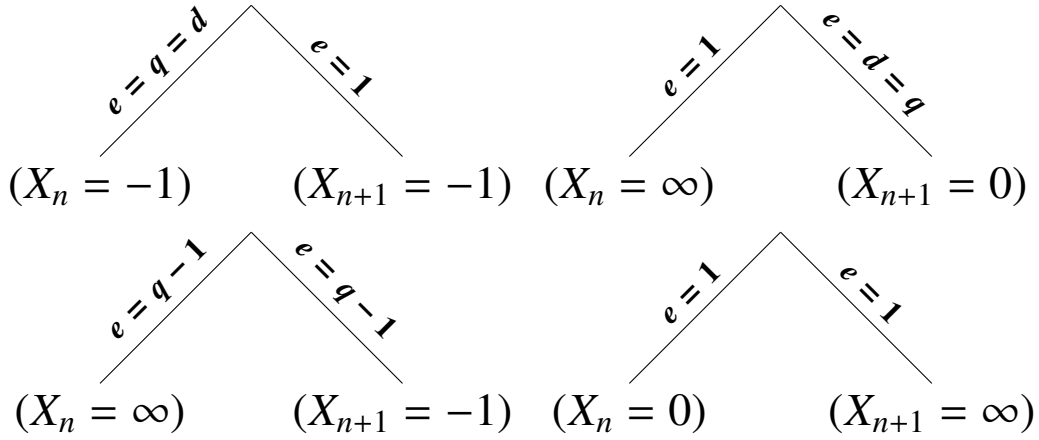


FIGURE 2.2: RAMIFICATION IN $k(X_n, X_{n+1})/k(X_n)$ AND $k(X_n, X_{n+1})/k(X_{n+1})$.

- $\alpha_n = -1$ implies $\alpha_{n+1} = -1$.
- $\alpha_{n+1} = 0$ implies $\alpha_n = \infty$.
- $\alpha_n = \infty$ implies $\alpha_{n+1} = -1$ or 0.
- $\alpha_{n+1} = -1$ implies $\alpha_n = -1$ or ∞.
- $\alpha_n = 0$ iff $\alpha_{n+1} = \infty$.

Proposition 2.4. *For any admissible sequence $(\alpha_n)_{n\geq 0}$, there exists a sequence $(Q_n)_{n\geq 0}$ of places $Q_n \in \mathbb{P}(F_n)$ such that $X_n(Q_n) = \alpha_n$ and $Q_{n+1}|Q_n$ for all $n \geq 0$.*

The proof of this result will be given after Corollary 2.6.

Recall that the ramification locus of the tower $\mathcal{F}$ is defined as the set

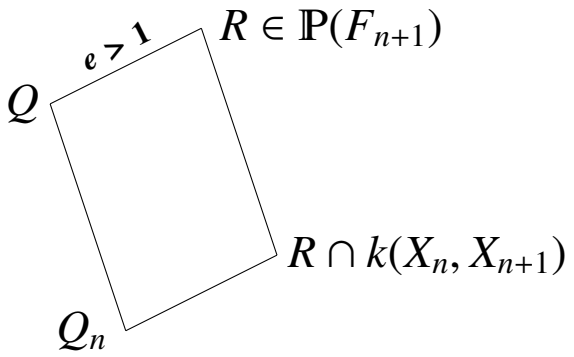
$$V(\mathcal{F}/F_0) = \{P \in \mathbb{P}(F_0) : P \text{ is ramified in } F_m/F_0 \text{ for some } m = m(P) \geq 1\}.$$

In order to estimate the genus of the tower, we first need to know which are the places in $\mathbb{P}(F_0)$ belonging to $V(\mathcal{F}/F_0)$, and afterwards to estimate the ramification behavior (i.e., the ramification index and the different exponent) of such places. Since the genus is invariant under constant field extensions (Proposition 0.17), we can assume that the base field k is algebraically closed. A straight application of Proposition 2.3 in this case solves the first problem.

Lemma 2.5. *Suppose that k is algebraically closed. Then the ramification locus of $\mathcal{F}$ over F_0 satisfies*

$$V(\mathcal{F}/F_0) \subseteq \{(X_0 = \alpha) : \alpha = -1, 0 \text{ or } \infty\}.$$

Proof. Let $n \geq 0$ and suppose that a place $Q \in \mathbb{P}(F_n)$ is ramified in F_{n+1}/F_n. For $i = 0, \ldots, n$, let $Q_i = Q \cap k(X_i)$. Then we have the following situation



so by Abhyankar's Lemma (Proposition 0.14) we have that Q_n ramifies in the extension $k(X_n, X_{n+1})/k(X_n)$. Therefore we have $Q_n = (X_n = \alpha)$, with $\alpha \in \{-1, \infty\}$, by (ii) of Proposition 2.3. The same result, together with (descending) induction, allow us to conclude that $Q_i = (X_i = \alpha)$, with $\alpha \in \{-1, 0, \infty\}$, for $i = n, n-1, \ldots, 1, 0$. This proves the lemma. □

Our next step is to estimate (or, if possible, to determine) the ramification behavior of the places $(X_0 = \alpha)$, with $\alpha \in \{-1, 0, \infty\}$. On the other hand, two conditions remain to be verified in order to conclude that the sequence $\mathcal{F} = (F_n)$ indeed defines a *tower* of function fields over *any* perfect field k, namely, that the base field k is algebraically closed in each field F_n, and that the genera of the fields F_n satisfy $g(F_n) \to \infty$ when

$n \to \infty$ (see Definition 0.4). Later we will prove these assertions using the ramification behavior at the places $(X_0 = -1)$ and $X_0 = \infty$, together with Proposition 2.4.

From now on, let

$$F^{i,j} = k(X_i, X_{i+1}, \ldots, X_j), \text{ for each } i, j \text{ in } \mathbb{N} \text{ with } i \leq j\,. \tag{2.9}$$

In particular we have $F_n = F^{0,n}$ and $k(X_n) = F^{n,n}$ for all $n \geq 0$. The *pyramid* associated to the sequence $\mathcal{F}$ of function fields is just the lattice of fields $(F^{i,j})_{0\leq i\leq j}$ ordered by inclusion. In particular, the sequence $\mathcal{F}$ corresponds to the left edge of the pyramid, and the basic fields $k(X_i)$ correspond to its basement. Note that the pyramid is composed of "diamonds", which correspond to field extensions of the form $F^{i-1,j+1}/F^{i,j}$, with $1 \leq i \leq j$, together with the two intermediate fields $F^{i-1,j}$ and $F^{i,j+1}$; see Figure 2.3 below.

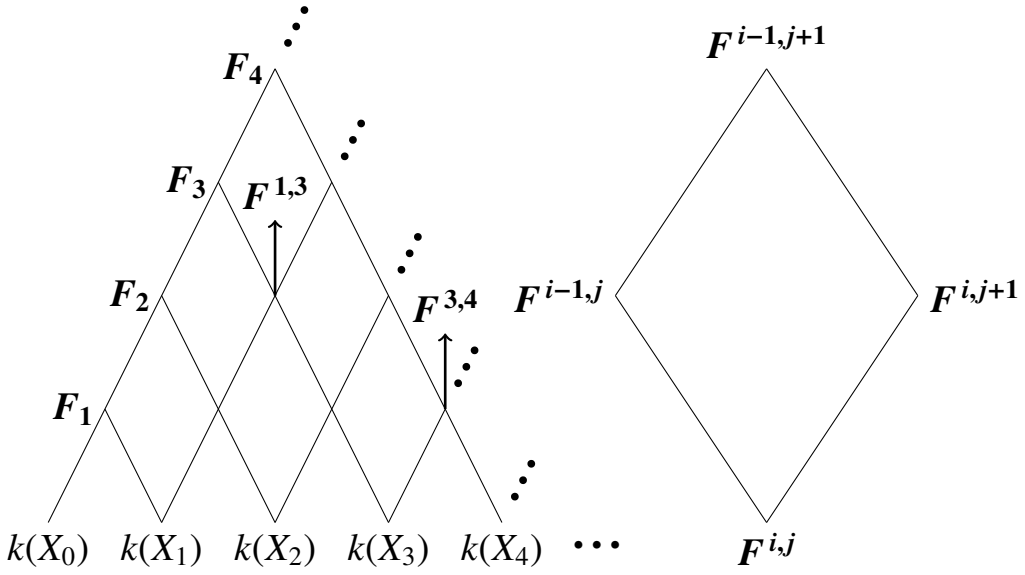


FIGURE 2.3: THE PYRAMID AND A DIAMOND.

Consider a family $(P_{i,j})_{0\leq i\leq j}$ of places $P_{i,j} \in \mathbb{P}(F^{i,j})$, such that $P_{k,\ell}$ contains $P_{i,j}$ whenever $F^{k,\ell} \supseteq F^{i,j}$ (i.e., whenever $k \leq i \leq j \leq \ell$). Moreover, suppose that we have $P_{0,0} = (X_0 = \alpha)$, with $\alpha \in \{-1, 0, \infty\}$. We want to estimate the values $e(P_{0,n}|P_{0,0})$ and $d(P_{0,n}|P_{0,0})$ for each $n \geq 0$, in order to estimate the genus of the tower $\mathcal{F}$.

Suppose that, for every diamond, we can determine the ramification behavior at the top edges from the ramification behavior at the bottom ones (we call it "solving" the diamond). By Proposition 2.2, we know the ramification behavior at the basement of the pyramid, so by the hypothesis we can solve all the diamonds at the bottom of

the pyramid. In particular, we know the ramification behavior at the bottom edges of the diamonds at the second level of the pyramid. Repeating this argument, (that is, "climbing up" the pyramid), we manage to solve all the diamonds, and in particular we are able to determine the values $e(P_{0,n+1}|P_{0,n})$ and $d(P_{0,n+1}|P_{0,n})$ for each $n \geq 0$. Using the multiplicativity of the ramification index and the transitivity of the different exponent (Lemma 0.13) we attain our objective.

If tame ramification occurs at some bottom edge of a given diamond, then by Proposition 0.14 and Lemma 0.13 we can determine the ramification behavior at the top edges of the diamond; this will be indeed the situation of the majority of the diamonds involved in our reasoning, so in that cases we will be able to "solve" explicitly those diamonds. But what happens if we have wild ramification at both bottom edges?. This is, of course, the interesting (and hard) case to deal with, which requires a more sophisticated approach (the use of completions, as it was said in the Introduction). We will treat this case at the end of the section.

Finally, we note that in some cases we do not need to restrict ourselves to the "basic diamonds" discussed above, but instead we can work directly with larger field extensions (in the presence of unramified extensions, for instance). With all these remarks in mind, we can start our reasoning. According to (ii) of Proposition 2.2, we can distinguish the following cases:

Case 1: $X_0(P_{0,0}) = -1$. Then $X_n(P_{n,n}) = -1$ for all $n \geq 0$.

Case 2: $X_0(P_{0,0}) = 0$. Then $X_1(P_{1,1}) = \infty$.

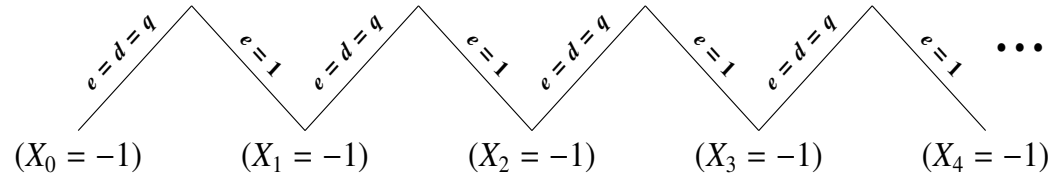
Case 3: $X_0(P_{0,0}) = \infty$ and $X_1(P_{1,1}) = -1$. Then $X_n(P_{n,n}) = -1$ for all $n \geq 1$.

Case 4: $X_0(P_{0,0}) = \infty, X_1(P_{1,1}) = 0$ and $X_n(P_{n,n}) \neq -1$ for all $n \geq 3$. In this case $X_n(P_{n,n}) = \infty$ for all n even and $X_n(P_{n,n}) = 0$ for all n odd.

Case 5: $X_0(P_{0,0}) = \infty, X_1(P_{1,1}) = 0$ and $X_n(P_{n,n}) = -1$ for some $n \geq 3$. Supposing that n is minimal, then since we started with $X_0(P_{0,0}) = \infty$, plus the fact that the values ∞ and 0 alternate at the bottom for $k < n$, we conclude that n is odd, $X_k(P_{k,k}) = \infty$ for $k = 2, 4, \ldots, n-1$ and $X_k(P_{k,k}) = 0$ for $k = 1, 3, \ldots, n-2$. Of course, we also have $X_k(P_{k,k}) = -1$ for all $k \geq n$.

Case 1 ($X_n(P_{n,n}) = -1$ for all $n \geq 0$)

In this case we conclude from Proposition 2.3 that the basement of the pyramid has the following form:



Using (i) of Proposition 0.16, we see that both the bottom left and top right edges of all the diamonds are unramified. The same result implies that for the bottom right and top left edges of all the diamonds we have $e = d = q$. Thus, the tower is explicitly solved in this case as depicted in Figure 2.4 below:

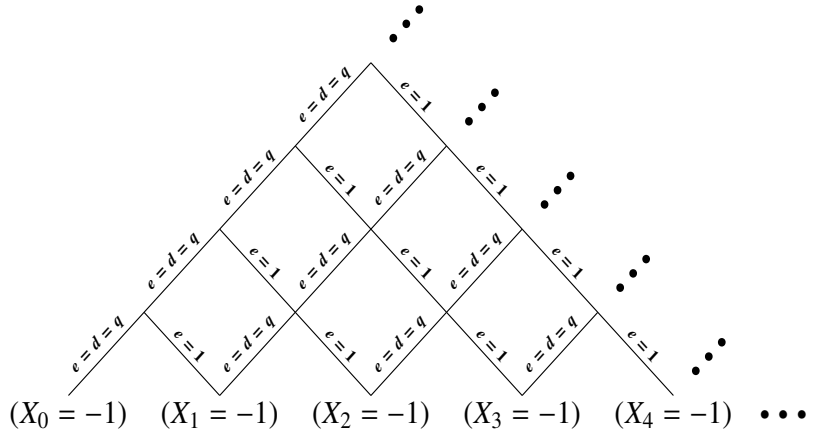


FIGURE 2.4: CASE 1.

On the other hand, for any diamond in the tower, each one of its edges is a lifting of an edge on the basement of the pyramid, which is a separable field extension of degree q. Therefore all the edges are separable extensions of degree less or equal than q. Since $e = q$ for all the bottom right and top left edges, it follows that such edges have degree equal to q. In particular, all the diamonds at the basement of the pyramid satisfy that three of its edges have degree q. By multiplicativity of the degree of field extensions, we conclude that the remaining edge (of the diamond) also has degree q. This in turn implies that all the diamonds appearing at the second level of the tower satisfy that three of its edges have degree q. Repeating this argument we conclude that all the "basic" edges are separable field extensions of degree q.

Corollary 2.6. *The field k is algebraically closed in F_n for each $n \geq 0$. Moreover, for each $i, j \geq 0$ with $i \leq j$, the field extensions $F^{i,j+1}/F^{i,j}$ and $F^{i-1,j}/F^{i,j}$ (whenever $i \geq 1$) are separable of degree q.*

Proof of Proposition 2.4 (page 60). We construct recursively the places Q_n: first we take $Q_0 = (X_0 = \alpha_0)$, and assuming that $Q_0, \ldots, Q_n$ are constructed satisfying the

desired conditions, let $P_n = Q_n \cap k(X_n)$. If $\alpha_n = -1$ or 0, any place $Q_{n+1} \in \mathbb{P}(F_{n+1})$ dividing Q_n will work. On the other hand, if $\alpha_n = \infty$, then $\alpha_{n+1} = -1$ or 0. Taking $x = -1/X_n$ and $y = X_{n+1} + 1$, and using (ii),c) of Proposition 2.2, we obtain a place $Q' \in \mathbb{P}(k(X_n, X_{n+1}))$ such that $Q'|P_n$ and $X_{n+1}(Q') = \alpha_{n+1}$. In order to finish the proof, it is suffices to find a place $Q_{n+1} \in \mathbb{P}(F_{n+1})$ lying above both Q' and Q_n simultaneously. It is easy to see from Corollary 2.6 (by comparing degrees) that the fields F_n and $F^{n,n+1} = k(X_n, X_{n+1})$ satisfy $F_n \cap F^{n,n+1} = F^{n,n} = k(X_n)$, and they are linearly disjoint over $k(X_n)$. The existence of the place Q_{n+1} follows from the following result:

Lemma 2.7 ([**Wu**, Lemma 2.1.3])**.** *Let F_1, F_2 be function fields over a perfect field k. Suppose that F_1 and F_2 are linearly disjoint over $F = F_1 \cap F_2$, and let $P \in \mathbb{P}(F)$ and $P_i \in \mathbb{P}(F_i)$ for $i = 1, 2$ be places such that $P_1|P$ and $P_2|P$. If the compositum F_1F_2 is defined, then exists a place $Q \in \mathbb{P}(F_1F_2)$ such that $Q|P_1$ and $Q|P_2$.*

Case 2 ($X_0(P_{0,0}) = 0$ and $X_1(P_{1,1}) = \infty$)

Consider the "truncated" pyramid $(F^{i,j})_{1 \le i \le j}$, that is, that obtained from the original by suppressing the variable X_0, and denote by $\mathcal{F}'$ the sequence of function fields corresponding to the left edge of this truncated pyramid. Since we are dealing with a recursive tower, then in particular the tower $\mathcal{F}'$ has the same ramification behavior as the original tower, and since $X_1(P_{1,1}) = \infty$, we conclude that $\mathcal{F}'$ lies in some of the Cases 3-5. Moreover, since $e(P_{0,1}|P_{0,0}) = e(P_{0,1}|P_{1,1}) = 1$ by ii),f) of Proposition 2.3, it follows from (i) of Proposition 0.16 that the tower $\mathcal{F}'' = (F_n)_{n \ge 1}$ inherits the ramification behavior of $\mathcal{F}'$; see Figure 2.5 below. In other words, we see that this case can be reduced to the remaining Cases 3,4 and 5.

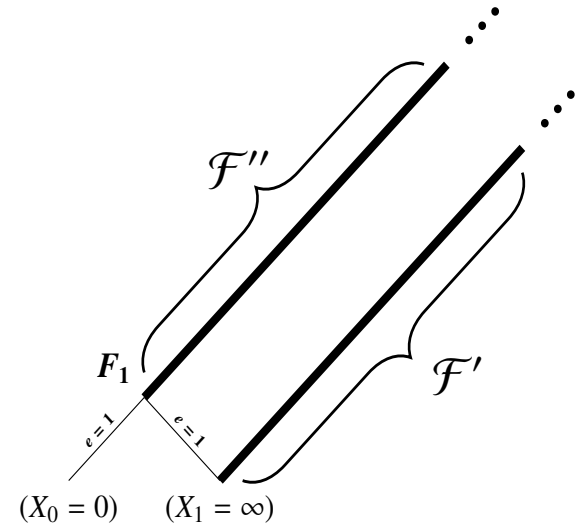
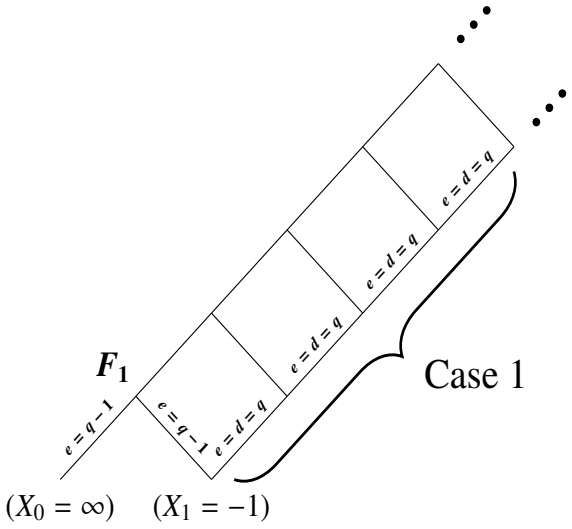


Figure 2.5: Case 2. Bold-faced edges have the same ramification behavior.

Case 3 ($X_0(P_{0,0}) = \infty$ and $X_n(P_{n,n}) = -1$ for all $n \geq 1$)

As in Case 2, we consider the truncated pyramid $(F^{i,j})_{1 \leq i \leq j}$. Since $X_1(P_{1,1}) = -1$, we are in the situation of Case 1, which was already solved. Moreover, by ii),c) of Proposition 2.3 we have $e(P_{0,1}|P_{0,0}) = e(P_{0,1}|P_{1,1}) = q - 1$. Thus, we have the following:



Repeated applications of (ii) of Proposition 0.16 yield $e(P_{0,n}|P_{1,n}) = q - 1$ for all $n \geq 1$. The same result allows to solve all the diamonds at the left side of the *original* pyramid, and we obtain $e(P_{0,n+1}|P_{0,n}) = q$ and $d(P_{0,n+1}|P_{0,n}) = 2(q-1)$ for all $n \geq 1$. This solves the tower in this case, as depicted in Figure 2.6 below:

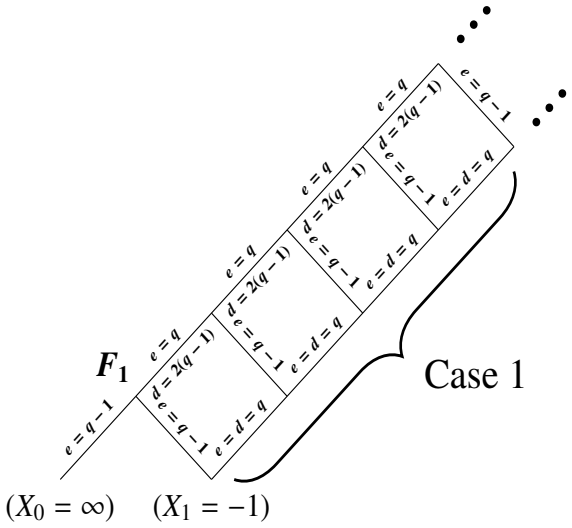


Figure 2.6: Case 3.

Corollary 2.8. *The genera $g(F_n)$ of the function fields F_n satisfy $g(F_n) \to \infty$ when $n \to \infty$.*

Proof. By Riemann-Hurwitz formula and Corollary 2.6 we have, for all $n \geq 0$:

$$\begin{aligned} 2g(F_{n+1}) - 2 =& [F_{n+1} : F_n](2g(F_n) - 2) + \deg \operatorname{Diff}(F_{n+1}/F_n) \\ =& q(2g(F_n) - 2) + \deg \operatorname{Diff}(F_{n+1}/F_n)\,. \end{aligned}$$

Now if $\alpha_0 = -1, \beta_0 = \infty$ and $\alpha_n = \beta_n = -1$ for all $n \geq 1$, then the sequences (α_n) and (β_n) are admissible, so by Proposition 2.4 there exist sequences $(Q_n), (Q'_n)$ of places $Q_n, Q'_n \in \mathbb{P}(F_n)$ such that for each $n \geq 0$ we have $Q_{n+1}|Q_n\,, Q'_{n+1}|Q'_n\,, X_n(Q_n) = \alpha_n$ and $X_n(Q'_n) = \beta_n$. From Case 1 we conclude that $d(Q_{n+1}|Q_n) = q$ for each $n \geq 0$, and similarly from Case 3 we get that $d(Q'_{n+1}|Q'_n) \geq q - 1$ for each $n \geq 0$. As a consequence we have $\deg \operatorname{Diff}(F_{n+1}/F_n) \geq d(Q_{n+1}|Q_n) + d(Q'_{n+1}|Q'_n) \geq 2q - 1$, hence

$$2g(F_{n+1}) - 2 \geq q(2g(F_n) - 2) + 2q - 1\,,$$

which implies $2g(F_{n+1}) > 2g(F_n)q$. From this our assertion easily follows. □

Note that Cases 1 and 3 were solved without assuming that the base field k is algebraically closed, so from Corollaries 2.6 and 2.8, together with i) of Proposition 2.3 we conclude the following:

Corollary 2.9. *For any perfect field k of characteristic $p > 0$ and for every power q of p, the sequence $\mathcal{F} = (F_n)_{n\geq 0}$ of function fields defined recursively by equation* (2.1) *is indeed a tower of function fields over k.*

In that follows, we will assume that the base field k is *algebraically closed*. In particular we have $\mathbb{F}_q \subseteq k$, which will be needed specifically in Case 5.

Case 4 ($X_n(P_{n,n}) = \infty$ for all n even and $X_n(P_{n,n}) = 0$ for all n odd)

This is the most trivial case: in fact, by ii), b) and f) of Proposition 2.3 we have that the bottom right edges of the diamonds in the basement of the pyramid are all unramified. Since each field extension F_{n+1}/F_n is a lifting from a such edge, it follows from (i) of Proposition 0.16 that $e(P_{0,n+1}|P_{0,n}) = 1$ for all $n \geq 0$, so in this case the place $(X_0 = \infty)$ is unramified in F_n/F_0 for all $n \geq 0$.

Now we draw some additional results about this case, which will be useful in the study of the remaining case. Let $m \geq 0$ even, and suppose that $X_i(P_{i,i}) = \infty$ for $i = 0, 2, 4, \ldots, m$ and $X_i(P_{i,i}) = 0$ for $i = 1, 3, 5, \ldots, m - 1$. In other words, we restrict our attention to the finite subpyramid $(F^{i,j})_{0\leq i\leq j\leq m}$. The same reasoning used above

shows that the bottom right and the top left edges of all the diamonds appearing in this subpyramid are unramified. As a consequence, we have the situation depicted in Figure 2.7 below:

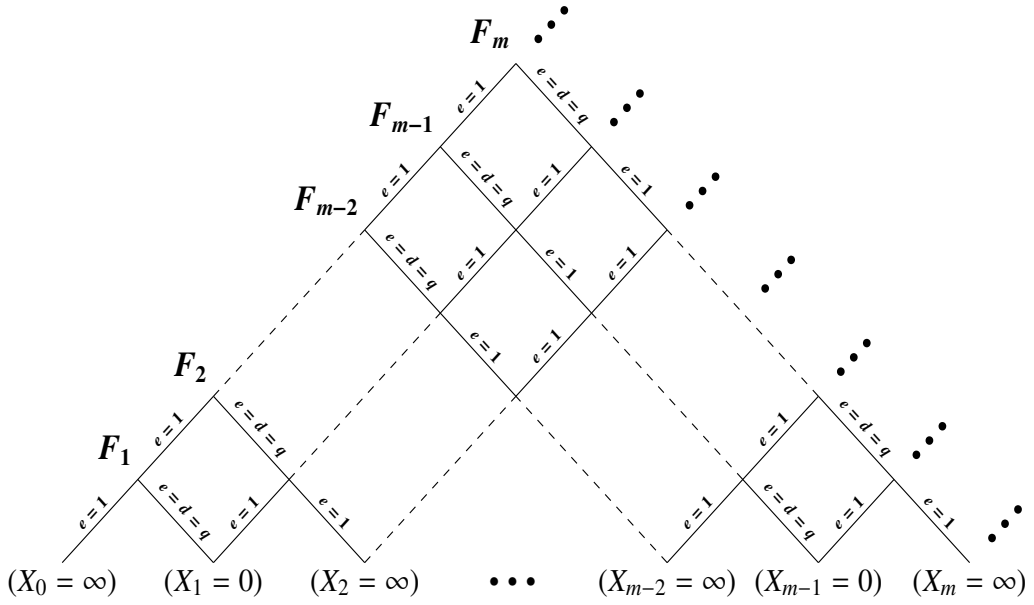


FIGURE 2.7

Note that in particular the place $(X_0 = \infty)$ is unramified in F_m/F_0.

Case 5 ($X_k(P_{k,k}) = -1$ for all $k \geq n$, $X_k(P_{k,k}) = \infty$ for $k = 0, 2, 4, \ldots, n-1$, and $X_k(P_{k,k}) = 0$ for $k = 1, 3, 5, \ldots, n-2$, for some $n \geq 3$ odd)

As we said earlier, this is the only case when wild ramification occurs at both bottom edges of some diamonds.

Consider the subpyramids $\mathcal{G} = (F^{i,j})_{0 \leq i \leq j \leq n-1}$ and $\mathcal{H} = (F^{i,j})_{n-1 \leq i \leq j}$. Note that $\mathcal{G}$ corresponds to the finite subpyramid studied in Case 4 (taking $m = n - 1$; see Figure 2.7), so we can solve it. Similarly, subpyramid $\mathcal{H}$ corresponds to Case 3, hence $\mathcal{H}$ can be also solved. Figure 2.8 (page 69) illustrates the solutions of both pyramids, which together constitute a partial solution to our original pyramid[¶].

[¶]Since notation becomes cumbersome at this point, we strongly encourage the reader to follow the reasoning through the figures.

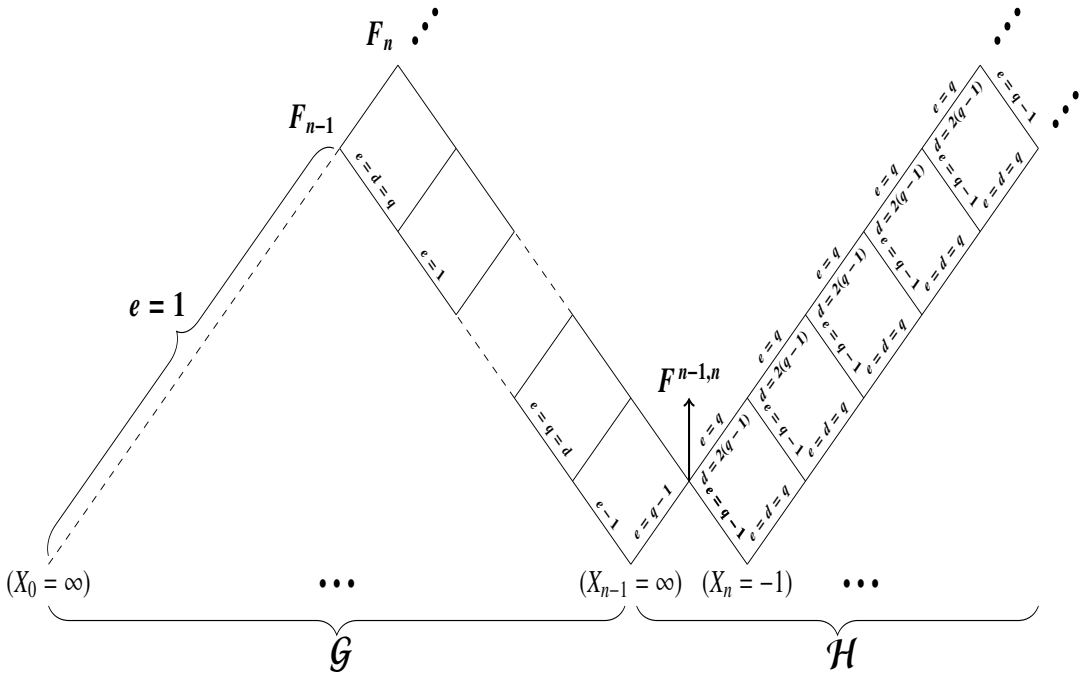


FIGURE 2.8

Note that the steps of the right edge of pyramid $\mathcal{G}$ (that is, the extensions $F^{k-1,n-1}/F^{k,n-1}$, with $1 \leq k \leq n-1$) alternate non-ramification and total ramification, in the latter case the different exponent d being equal to q. Since $e(P_{n-1,n}|P_{n-1,n-1}) = q-1$, it follows that $e(P_{k,n}|P_{k,n-1}) = q-1$ for $k = 0, 1, \ldots, n-1$, by (i) and (ii) of Proposition 0.16. If k between 1 and $n-1$ satisfies $e(P_{k-1,n-1}|P_{k,n-1}) = 1$, then obviously $e(P_{k-1,n}|P_{k,n}) = 1$; otherwise, we must have $e(P_{k-1,n-1}|P_{k,n-1}) = d(P_{k-1,n-1}|P_{k,n-1}) = q$, and in this case from (ii) of Proposition 0.16 we get $e(P_{k-1,n}|P_{k,n}) = q$ and $d(P_{k-1,n}|P_{k,n}) = 2(q-1)$.

Thus, if $\mathcal{R}$ denotes the lattice bounded below by the edges $F^{0,n}/F^{n-1,n}$ (the left-side finite edge) and $(F^{n-1,k})_{k\geq n}$ (the right-side infinite edge), then it remains to solve all the diamonds contained in $\mathcal{R}$. Now, for each k between 1 and $n-1$ we have that $e(P_{k-1,n}|P_{k,n})$ divides q and $d(P_{k-1,n}|P_{k,n}) = 2(e(P_{k-1,n}|P_{k,n}) - 1)$. The same situation holds in the extensions $F^{n-1,k+1}/F^{n-1,k}$ for $k \geq n$, that is, $e(P_{n-1,k+1}|P_{n-1,k})$ divides q and $d(P_{n-1,k+1}|P_{n-1,k}) = 2(e(P_{n-1,k+1}|P_{n-1,k}) - 1)$. In other words, at each step of the edges $F^{0,n}/F^{n-1,n}$ and $(F^{n-1,k})_{k\geq n}$ we have e divides q and $d = 2(e-1)$. Moreover, both edges are "surrounded" below by extensions with ramification index $e = q-1$. We describe pictorially this situation in Figure 2.9 below:

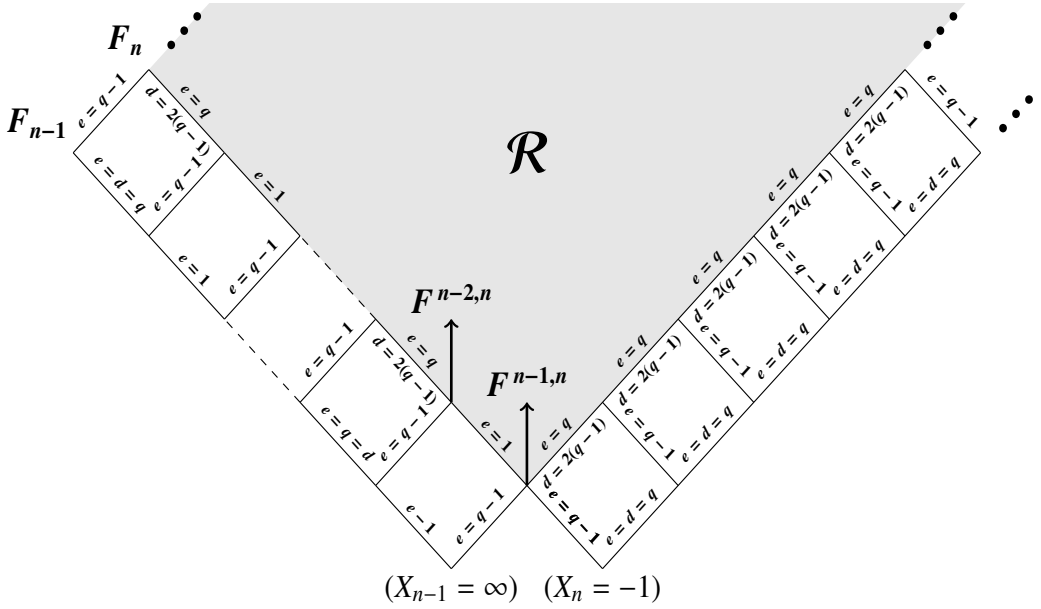


FIGURE 2.9: SHADOWED REGION CORRESPONDS TO LATTICE $\mathcal{R}$.

Finally, since $e(P_{n-2,n}|P_{n-1,n}) = 1$, then applying (i) of Proposition 0.16 we get the equalities $e(P_{n-2,n+1}|P_{n-2,n}) = q$ and $d(P_{n-2,n+1}|P_{n-2,n}) = 2(q-1)$; see Figure 2.10 below:

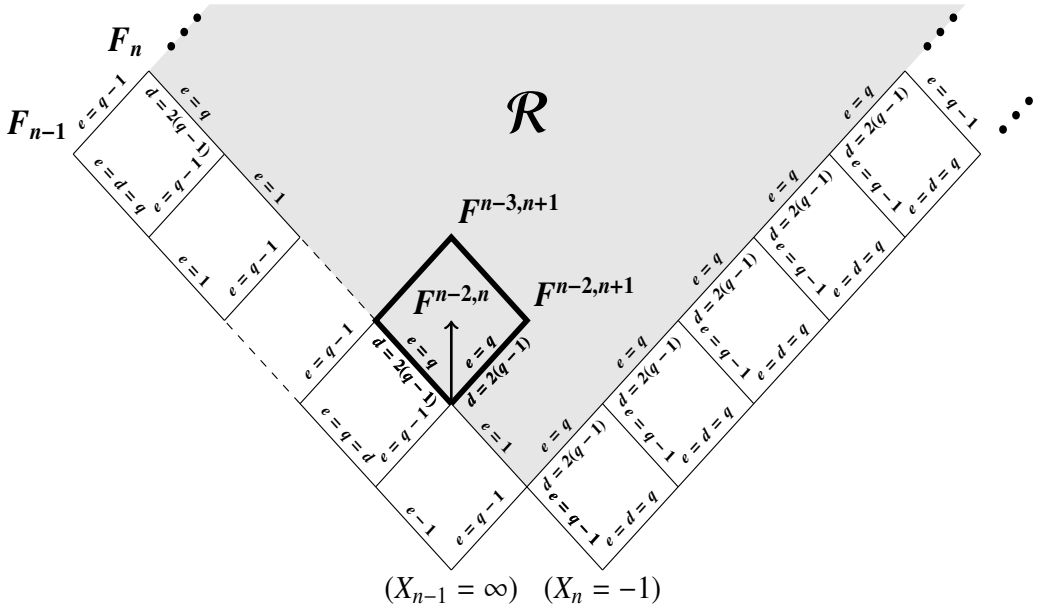


FIGURE 2.10: BOLDFACED DIAMOND CANNOT BE SOLVED DIRECTLY BECAUSE IT HAS WILD RAMIFICATION AT BOTH BOTTOM EDGES.

Let L/K be a field extension, and let $P \in \mathbb{P}(K), Q \in \mathbb{P}(L)$ be places such that $Q|P$. We say that L/K has *property* ★ *at places* P *and* Q if $e(Q|P)$ divides q and $d(Q|P) = 2(e(Q|P) - 1)$. When no confusion arises about Q and P, we simply say that L/K has property ★. In our situation, all the steps in the lower edges of the lattice $\mathcal{R}$ have property ★, as depicted in Figure 2.11 below:

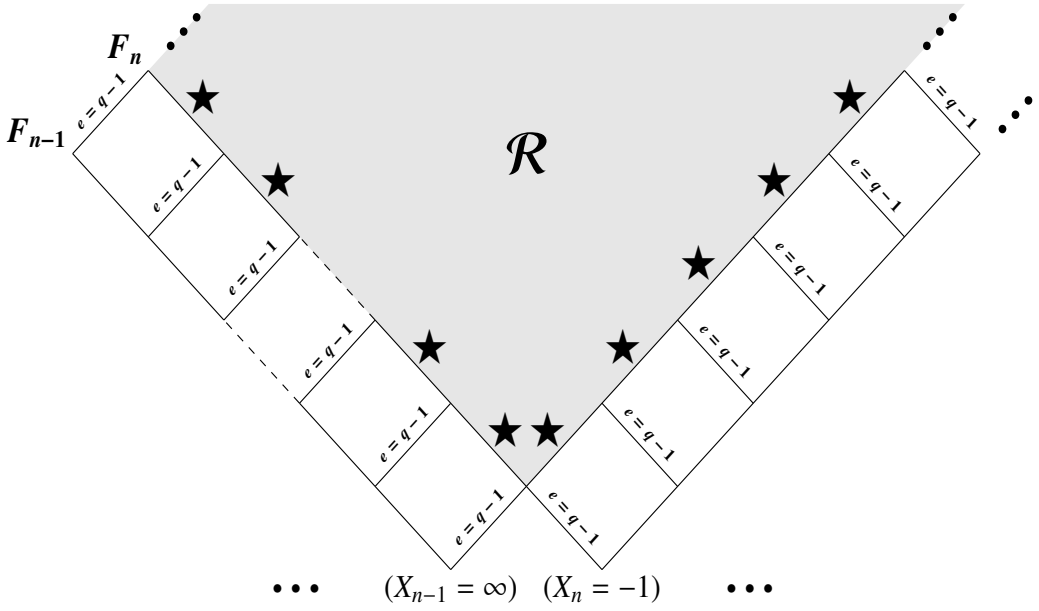


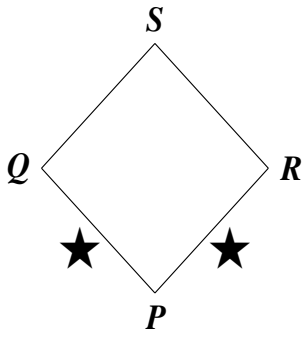
Figure 2.11

Now we state the main technical result of this chapter: it will permit us to solve the lattice $\mathcal{R}$.

Proposition 2.10. *For any given diamond in* $\mathcal{R}$*, if both bottom edges have property* ★*, then the top edges also have property* ★*.*

It follows from repeated applications of Proposition 2.10 that, for each diamond in $\mathcal{R}$, all of its edges have property ★, and in particular for all $k \geq n$ we have that $e(P_{0,n+1}|P_{0,n})$ divides q and $d(P_{0,n+1}|P_{0,n}) = 2(e(P_{0,n+1}|P_{0,n}) - 1)$.

Proof of the Proposition. The bottom vertex of any diamond in $\mathcal{R}$ is a field of the form $K = F^{i,j}$, with $1 \leq i \leq n-1$ and $j \geq n$ (see Figure 2.11 above). The other vertices of such diamond are the fields $L = F^{i-1,j}$, $M = F^{i,j+1}$ and $E = LM = F^{i-1,j+1}$, and the corresponding places are $P = P_{i,j}$, $Q = P_{i-1,j}$, $R = P_{i,j+1}$ and $S = P_{i-1,j+1}$. Suppose that the following holds:



Let $\mathbb{L}/K$ be the Galois closure of L/K. If $x = -1/X_{i-1}, y = X_i + 1$ and $W = y/(x - y)$, then we have $L = K(W)$ and $h(W) = 0$, where $h(T) = T^q + (1 - y^{-1})T + 1$: this follows directly from the equation (2.7). Since $[L : K] = q$ by Corollary 2.6, it turns out that $h(T)$ is indeed the minimal polynomial of W over K. If $W + a$ is a root of $h(T)$, then we have $(W + a)^q + (1 - y^{-1})(W + a) + 1 = 0 = h(W) + a^q + (1 - y^{-1})a$, hence $a^q = (y^{-1} - 1)a$. Consequently, if ω satisfies $\omega^{q-1} = y^{-1} - 1$, then the roots of $h(T)$ are of the form $W + t\omega$, with $t \in \mathbb{F}_q \subseteq k$. This proves that $\mathbb{L} = L(\omega)$, so $\mathbb{L}/L$ is a Kummer extension with degree dividing $q - 1$.

Similarly, let $\mathbb{M}/K$ be the Galois closure of M/K. If $x_0 = -1/X_j, y_0 = X_{j+1} + 1$ and $Z = x_0/(y_0 - x_0)$, then we have $M = K(Z)$ and $g(Z) = 0$, where $g(T) = T^q + (1 - x_0^{-1})T + 1$ (by (2.6)), and $g(T)$ is the minimal polynomial of Z over K by Corollary 2.6. If σ satisfies $\sigma^{q-1} = x_0^{-1} - 1$, then we conclude that $\mathbb{M} = M(\sigma)$, so $\mathbb{M}/M$ is a Kummer extension whose degree divides $q - 1$.

Let v, w be, respectively, the discrete valuations associated to the places Q and R. Let $Q' \in \mathbb{P}(\mathbb{L})$ and $R' \in \mathbb{P}(\mathbb{M})$ be places such that $Q'|Q$ and $R'|R$. Now $y^{-1} - 1 \in k(X_i)$, so $v(y^{-1} - 1)$ is an integer multiple of $e(P_{i-1,j}|P_{i,i})$, which is in turn a multiple of $e(P_{i,n}|P_{i,n-1}) = q - 1$, and similarly, $x_0^{-1} - 1$ belongs to $k(X_j)$, so $w(x_0^{-1} - 1)$ is multiple of $e(P_{i,j+1}|P_{j,j})$, which is multiple of $e(P_{n-1,j}|P_{n,j}) = q - 1$ (see Figure 2.11). Therefore, by (iii) of Proposition 0.20 we obtain $e(Q|P_{i-1,j}) = e(R|P_{i,j+1}) = 1$. Consequently, we are in the situation depicted below:

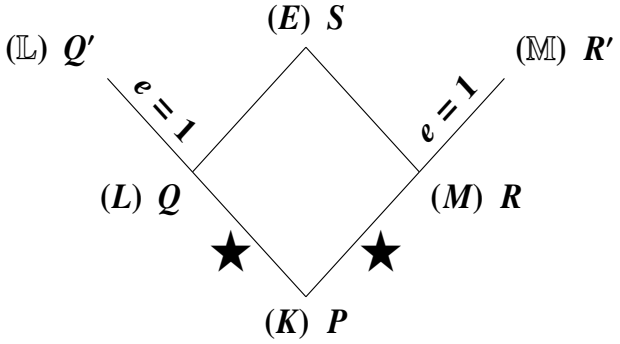


Figure 2.12: Auxiliary Kummer extensions; the respective fields are indicated in parentheses.

We have $e(Q'|P) = e(Q|P)$ (which divides q) and $d(Q'|P) = d(Q|P)$, by (ii) of Proposition 0.15, so $d(Q'|P) = 2(e(Q'|P) - 1)$. Similarly, $e(R'|P) = e(R|P)$ divides q and $d(R'|P) = 2(e(R'|P) - 1)$. Passing to completions (see Section 0.4) we have the following picture:

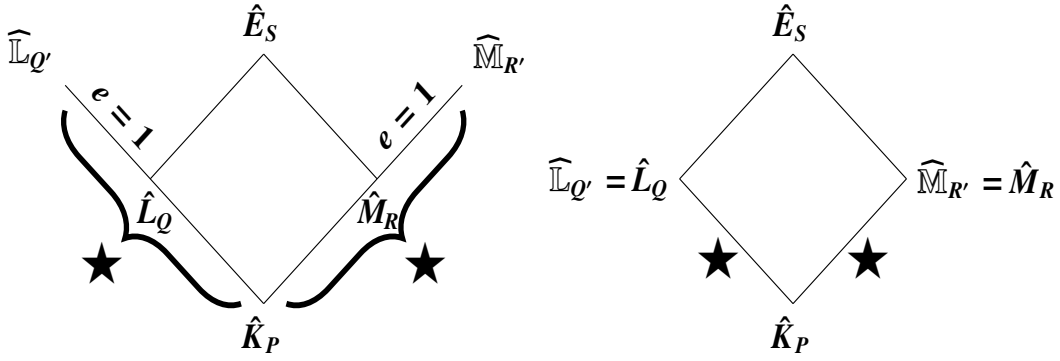


Figure 2.13: Edges in braces are Galois p-extensions with property ★ (left), and unramification collapse field extensions (right).

In fact, by (i) and (iii) of Proposition 0.22 we have that $\widehat{\mathbb{L}}_{Q'}/\hat{K}_P$ is a Galois extension of degree equal to $e(Q'|P)f(Q'|P) = e(Q'|P)$ (because we are assuming that the base field k is algebraically closed, so all the inertial indices are equal to 1), and the same result shows that $[\widehat{\mathbb{L}}_{Q'} : \hat{L}_Q] = e(Q'|Q)f(Q'|Q) = 1$, that is, $\widehat{\mathbb{L}}_{Q'} = \hat{L}_Q$. Therefore $\hat{L}_Q/\hat{K}_P$ is a Galois extension of degree $e(Q|P)$; similarly we have $\widehat{\mathbb{M}}_{R'} = \hat{M}_R$ and $\hat{M}_R/\hat{K}_P$ is a Galois extension of degree $e(R|P)$. On the other hand, we know by (ii) of Proposition 0.22 that the places $\hat{P} \in \mathbb{P}(\hat{K}_P), \hat{Q} \in \mathbb{P}(\hat{L}_Q), \hat{R} \in \mathbb{P}(\hat{M}_R)$ and $\hat{S} \in \mathbb{P}(\hat{E}_S)$ satisfy $e(\hat{Q}\,|\,\hat{P}) = e(Q|P), e(\hat{R}\,|\,\hat{P}) = e(R|P), e(\hat{S}\,|\hat{Q}) = e(S\,|Q)$ and $e(\hat{S}\,|\hat{R}) = e(S\,|R)$, and similar equalities hold for the different exponent (by (ii) of Proposition 0.23). Finally, the residue fields at P and $\hat{P}$ are isomorphic, and since we are assuming that the base field k is algebraically closed, it follows that $k = \mathscr{O}_P/P = \hat{\mathscr{O}}_P/\hat{P}$.

As a consequence, we are in the situation of Proposition 0.29 (the "General Key Lemma"), so we conclude that both $e(\hat{S}\,|\hat{Q})$ and $e(\hat{S}\,|\hat{R})$ divide q, and moreover $d(\hat{S}\,|\hat{Q}) = 2(e(\hat{S}\,|\hat{Q}) - 1), d(\hat{S}\,|\hat{R}) = 2(e(\hat{S}\,|\hat{R}) - 1)$. Turning back to our original field extensions via Propositions 0.22 and 0.23, we conclude that both E/L and E/M have property ★, which finishes the proof. □

2.3 The genus of the tower

Now we are able to estimate the genus of the tower $\mathcal{F}$, using the results from the previous section. As before, we suppose that the field k is algebraically closed. Let

$(P_n)_{n\geq 0}$ be a chain of places $P_n \in \mathbb{P}(F_n)$ such that $P_{n+1}|P_n$ for all $n \geq 0$. If some place P_k is ramified in F_{k+1}/F_k, then we know from Lemma 2.5 that $X_0(P_0) \in \{-1, 0, \infty\}$, and therefore we are in some of the Cases 1,2,3 of 5 of the previous section (recall that in Case 4 we get that the corresponding place is unramified in all the extensions). Now we will write the different exponent $d(P_n|P_0)$ in terms of $e(P_n|P_0)$ in all these cases. For brevity we denote $e(P_n|P_0)$ by E_n and $d(P_n|P_0)$ by D_n.

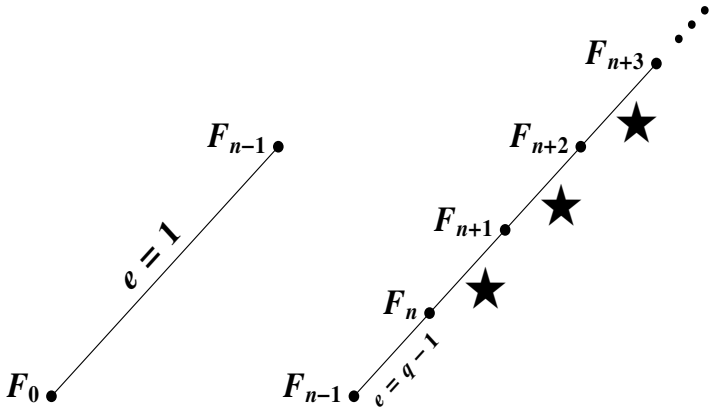


FIGURE 2.14: CASE 5.

Case 1: In this case we have $e(P_{n+1}|P_n) = d(P_{n+1}|P_n) = q$ for all $n \geq 0$, so clearly we have $E_n = q^n$. If $m \geq 0$ satisfies $D_m = q(q^m - 1)/(q - 1)$, then by (iii) of Proposition 0.15 we have $D_{m+1} = q(D_m + 1)$, and so $D_{m+1} = q(q^{m+1} - 1)/(q - 1)$. As a consequence, $D_n = q(E_n - 1)/(q - 1)$ for all $n \geq 0$.

Case 3: We have $E_1 = q - 1, D_1 = q - 2$ and $e(P_{n+1}|P_n) = q, d(P_{n+1}|P_n) = 2(q - 1)$ for all $n \geq 1$. Therefore for each $n \geq 1$ we have $E_n = q^{n-1}(q - 1)$. Repeated applications of (iv) of Proposition 0.15 yields $d(P_n|P_1) = 2(e(P_n|P_1) - 1)$ for all $n \geq 1$, so from (v) of Proposition 0.15 we obtain $D_n = \left(\frac{q}{q-1}\right)E_n - 2$ for all $n \geq 1$.

Case 5: Let k be such that $X_j(P_j) = \infty$ for $j = 0, 2, 4, \ldots, k - 1, X_j(P_j) = 0$ for $j = 1, 3, \ldots, k - 2$ and $X_j(P_j) = -1$ for all $j \geq k$. We know that $E_j = 1$ for $j = 0, 1, \ldots, k-1$ and $e(P_k|P_{k-1}) = q-1$, so $E_k = q-1$ and $D_k = q-2$. Moreover, for all $j \geq k$ the extensions F_{k+1}/F_k have property ★, that is, $e(P_{k+1}|P_k)$ divides q and $d(P_{k+1}|P_k) = 2(e(P_{k+1}|P_k) - 1)$; see Figure 2.14. In particular, for all $j \geq k$ we have $d(P_j|P_k) = 2(e(P_j|P_k) - 1)$, by (iv) of Proposition 0.15, and therefore $D_j = \left(\frac{q}{q-1}\right)E_j - 2$ for all $j \geq k$ by (v) of the same Proposition.

As a consequence, in all these cases we have $D_n \leq q(E_n - 1)/(q - 1)$ for all $n \geq 0$ (because $\frac{q}{q-1} \leq 2$). It remains to consider Case 2; but as we already saw, for this case

we have $E_1 = 1$, and the ramification behavior of the remaining places is exactly as in one of the Cases 3,4 or 5. In other words, for all $n \geq 1$ we have $e(P_n|P_1) = E'_{n-1}$ and $d(P_n|P_1) = D'_{n-1}$, where $(E'_m)_{m\geq 0}$ and $(D'_m)_{m\geq 0}$ are sequences as in Cases 1,3 or 5 above, so they satisfy $D'_m \leq q(E'_m - 1)/(q-1)$ for all $m \geq 0$. Since $e(P_1|P_0) = 1$, it follows from (i) of Proposition 0.15 that $E_n = e(P_n|P_1)$ and $D_n = d(P_n|P_1)$ for all $n \geq 1$, and therefore we again obtain $D_n \leq q(E_n - 1)/(q-1)$ for all $n \geq 0$.

We remark that the inclusion in Lemma 2.5 is actually an equality. In fact, by Proposition 2.4 each one of Cases 1,2,3 and 5 indeed occurs, and we saw that in all these cases we have ramification at some step of the tower. If $B = q/(q-1)$, then for all place Q of the tower (i.e., of some function field F_n) lying above P we have $d(Q|P) \leq B(e(Q|P) - 1)$. Applying Proposition 0.30 we obtain that the genus of the tower $\mathcal{F}$ relative to F_0 satisfies

$$\begin{aligned}\gamma(\mathcal{F}/F_0) &\leq g(F_0) - 1 + \frac{1}{2}\sum_{P\in V(\mathcal{F}/F_0)} B \cdot \deg P \\ &= -1 + \frac{3}{2}B \\ &= \frac{q+2}{2(q-1)}\,. \end{aligned} \tag{2.10}$$

2.4 The splitting rate and the limit of the tower

In this section we restrict our attention to the case $k = \mathbb{F}_{q^3}$ of the tower $\mathcal{F}$. We will show that at least $q+1$ places in F_0 are totally splitting over $\mathbb{F}_{q^3}$ in all the extensions F_n/F_0, so the splitting rate of the tower relative to F_0 satisfies $\nu(\mathcal{F}/F_0) \geq q+1$ by Proposition 0.31.

We claim that the equation $T^{q+1} + T = -1$ in $\overline{\mathbb{F}}_q$ has $q+1$ distinct solutions, all of them belonging to $\mathbb{F}_{q^3}$. In fact, since the polynomial $\phi(T) = T^{q+1} + T + 1 \in \mathbb{F}_q[T]$ satisfies $\phi'(T) = (q+1)T^q + 1 = T^q + 1 = (T+1)^q$ and $\phi(-1) \neq 0$, it follows that ϕ and ϕ' have no common roots in $\overline{\mathbb{F}}_q$, so ϕ is separable. Moreover, if $a \in \overline{\mathbb{F}}_q$ satisfies $a^{q+1} + a + 1 = 0$, then

$$\begin{aligned} a^{q^2+q+1} &= a(a^{q+1})^q \\ &= a(-(a+1))^q \\ &= -a(a+1)^q \\ &= -a(a^q+1) \\ &= -a^{q+1} - a = 1\,, \end{aligned}$$

so $a^{q^3-1} = (a^{q^2+q+1})^{q-1} = 1$, so $a \in \mathbb{F}_{q^3}$. This proves our claim.

Recall that the tower is given recursively by $Y^{q+1} + Y = (X+1)/X^{q+1}$ (see (2.1)), hence $X^{q+1} + X + 1 = 0$ implies that $Y^{q+1} + Y + 1 = 0$. From this it follows that the places $(X_0 = a) \in \mathbb{P}(F_0)$, with $a \in \mathbb{F}_{q^3}$ satisfying $\phi(a) = 0$ split completely in all the steps F_n/F_0 of the tower, as we want to show.

Now we can state the main result of this chapter:

Theorem 2.11. *The tower $\mathcal{F}$ over $k = \mathbb{F}_{q^3}$ defined recursively by equation* (2.1) *is asymptotically good, with limit $\lambda(\mathcal{F}) \geq \dfrac{2(q^2-1)}{q+2}$.*

Proof. We already saw that $\nu(\mathcal{F}/F_0) \geq q+1$, and $\gamma(\mathcal{F}/F_0) \leq \dfrac{q+2}{2(q-1)}$ by (2.10)). Since $\lambda(\mathcal{F}) = \nu(\mathcal{F}/F_0)/\gamma(\mathcal{F}/F_0)$, the result follows. □

Remark 2.12. In this note we show the relationship between the tower given by (2.1) and the tower given by Ihara in [**Ih07**].

Let p be a prime number, q a power of p, and let k be a perfect field with $\mathrm{char}(k) = p$. The Bezerra-Garcia-Stichtenoth tower over k is the sequence $\mathcal{E} = (E_n)_{n\geq 0}$ of function fields defined as follows: $E_0 = k(v_0)$ is the rational function field over k, and for $n \geq 0$, let $E_{n+1} = E_n(v_{n+1})$, where v_{n+1} satisfies the following equation:

$$\frac{1 - v_{n+1}}{v_{n+1}^q} = \frac{v_n^q + v_n - 1}{v_n}. \tag{2.11}$$

For each $n \geq 0$, let $y_n = (v_n^q + v_n - 1)/v_n$. Then we have the following recursive relation (equation (3) in [**Ih07**]), which is used to define the Ihara tower:

$$\frac{-y_n^q}{(1-y_n)^{q+1}} = \frac{y_{n+1} - 1}{y_{n+1}^{q+1}}, \text{ for all } n \geq 0. \tag{2.12}$$

The proof of this equality is as follows: for simplicity write $V = v_n, W = v_{n+1}$. Let

$$Y := \frac{V^q + V - 1}{V} = \frac{1 - W}{W^q} \quad \text{(by (2.11))}$$

and

$$Z := \frac{W^q + W - 1}{W} = \frac{(W-1)^q}{W} + 1.$$

Then we have

$$YW^q = 1 - W \text{ and } ZW = (W-1)^q + W. \tag{2.13}$$

We want to show that

$$\frac{-Y^q}{(1-Y)^{q+1}} = \frac{Z-1}{Z^{q+1}},$$

which is equivalent to

$$\frac{-Y^q W^{q^2}}{(1-Y)^{q+1} W^{q(q+1)}} \cdot \frac{W^{q(q+1)}}{W^{q^2}} = \frac{(Z-1)W}{Z^{q+1} W^{q+1}} \cdot \frac{W^{q+1}}{W},$$

that is,

$$\frac{-(YW^q)^q}{(W^q - YW^q)^{q+1}} \cdot W^q = \frac{ZW - W}{(ZW)^{q+1}} \cdot W^q.$$

Thus, we are reduced to prove the following equality:

$$-(YW^q)^q (ZW)^{q+1} = (ZW - W)(W^q - YW^q)^{q+1}.$$

Replacing the values given by (2.13) in the equality above, we are led to prove that

$$-(1-W)^q [(W-1)^q + W]^{q+1} = (W-1)^q (W^q - 1 + W)^{q+1},$$

which is trivially true (recall that $(-1)^q = -1$). This proves our claim.

If $Y_n := (1/y_n) - 1$, then $k(Y_n) = k(y_n)$, so the tower of Ihara coincides with the tower $\mathcal{F} = (F_n)_{n \geq 0}$, where $F_n = k(Y_0, Y_1, \ldots, Y_n)$. Now we prove that $\mathcal{F}$ is precisely the tower considered in this chapter. In fact, we can write equality (2.12) as

$$\frac{-y_n^q (Y_n + 1)^q}{(1-y_n)^{q+1} (Y_n + 1)^{q+1}} \cdot (Y_n + 1) = \frac{(y_{n+1} - 1)(Y_{n+1} + 1)}{y_{n+1}^{q+1} (Y_{n+1} + 1)^{q+1}} \cdot (Y_{n+1} + 1)^q,$$

and so

$$\frac{-[y_n (Y_n + 1)]^q (Y_n + 1)}{[Y_n + 1 - y_n (Y_n + 1)]^{q+1}} = \frac{[y_{n+1}(Y_{n+1} + 1) - Y_{n+1} - 1](Y_{n+1} + 1)^q}{[y_{n+1}(Y_{n+1} + 1)]^{q+1}}.$$

Since $y_n (Y_n + 1) = 1$, it follows that

$$\frac{-(Y_n + 1)}{Y_n^{q+1}} = -Y_{n+1} (Y_{n+1} + 1)^q,$$

which is precisely our basic equation (2.1). Thus, we conclude that our tower is the same as the tower of Ihara, which is a subtower of the Bezerra-Garcia-Stichtenoth tower $\mathcal{E}$ given by (2.11).

Bibliography

[**Ba**] Alp Bassa, *Towers of function fields over cubic fields*, PhD Thesis, University of Duisburg-Essen, 2007. Available at `http://duepublico.uni-duisburg-essen.de/servlets/DerivateServlet/Derivate-16184/bassathesis.pdf`

[**BaGaSt**] Alp Bassa, Arnaldo Garcia and Henning Stichtenoth, *A new tower over cubic finite fields*, Moscow Mathematical Journal **8** (2008), no. 3, 401-418.

[**BeeGaSt**] Peter Beelen, Arnaldo Garcia and Henning Stichtenoth, *On towers of function fields of Artin-Schreier type*, Bull. Braz. Math. Soc. (N.S.) **35** (2004), no. 2, 151-164.

[**BezGaSt**] Juscelino Bezerra, Arnaldo Garcia and Henning Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, J. Reine Angew. Math. **589** (2005), 159-199.

[**Bo**] Enrico Bombieri, *Counting points on curves over finite fields (d'après S. A. Stepanov)*, Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 430, pp. 234-241.

[**Ch**] Jean Chaumine, *Corps de fonctions algébriques et algorithme de D.V. Chudnovsky and G.V. Chudnovsky pour la multiplication dans les corps finis)*, Thèse de doctorat, Université de la Polynésie Française, 2005.

[**DrVl**] Vladimir Gershnovich Drinfeld and Sergei G. Vladut, *The number of points of an algebraic curve*, Functional Anal. Appl. **17** (1983), no. 1, 53-54.

[**El98**] Noam Elkies, *Explicit modular towers*, Proceedings of the Thirty-fifth Annual Allerton Conference on Communication, Control and Computing

(Urbana, IL, 1997), 23-32, Univ. Illinois, Urbana, IL, 1998. Also available at http://arxiv.org/abs/math/0103107

[**El01**] Noam Elkies, *Explicit towers of Drinfeld modular curves*, European Congress of Mathematics, Vol. II (Barcelona, 2000), 189-198, Progr. Math., 202, Birkhäuser, Basel, 2001.

[**FrPeSt**] Gerhard Frey, Marc Perret and Henning Stichtenoth, *On the different of abelian extensions of global fields*, Coding theory and algebraic geometry (Luminy, 1991), 26-32, Lecture Notes in Math., 1518, Springer, Berlin, 1992.

[**GaSt95**] Arnaldo Garcia and Henning Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. Math. **121** (1995), no. 1, 211-222.

[**GaSt96-1**] Arnaldo Garcia and Henning Stichtenoth, *On the asymptotic behaviour of some towers of function fields over finite fields*, J. Number Theory **61** (1996), no. 2, 248-273.

[**GaSt96-2**] Arnaldo Garcia and Henning Stichtenoth, *Asymptotically good towers of function fields over finite fields*, C. R. Acad. Sci. Paris Sér. I Math. **322** (1996), no. 11, 1067-1070.

[**GaSt00**] Arnaldo Garcia and Henning Stichtenoth, *Skew pyramids of function fields are asymptotically bad*, Coding theory, cryptography and related areas (Guanajuato, 1998), 111-113, Springer, Berlin, 2000.

[**GaSt05**] Arnaldo Garcia and Henning Stichtenoth, *Some Artin-Schreier Towers Are Easy*, Moscow Mathematical Journal **5** (2005), no. 4, 767-774.

[**GaSt07**] Arnaldo Garcia and Henning Stichtenoth, *On the Galois Closure of Towers*, Recent trends in coding theory and its applications, 83-92, AMS/IP Stud. Adv. Math., 41, Amer. Math. Soc., Providence, RI, 2007.

[**GaSt**] Arnaldo Garcia and Henning Stichtenoth (Editors), *Topics in geometry, coding theory and cryptography.*, Algebra and Applications, 6. Springer, Dordrecht, 2007.

[**GaStTh**] Arnaldo Garcia, Henning Stichtenoth and Michael Thomas, *On Towers and Composita of Towers of Function Fields over Finite Fields*, Finite Fields Appl. **3** (1997), no. 3, 257–274.

[**Ge**] Gerard van der Geer, *Curves over Finite Fields and Codes*, European Congress of Mathematics, Vol. II (Barcelona, 2000), 225-238, Progr. Math., 202, Birkhäuser, Basel, 2001. Also available at
`http://www.science.uva.nl/~geer/barcelona1.ps`

[**GV**] Gerard van der Geer and Marcel van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, Bull. London Math. Soc. **34** (2002), no. 3, 291-300.

[**Go**] Valerii Denisovich Goppa, *Codes on algebraic curves*, Soviet Math. Dokl. **24** (1981), no. 1, 170-172.

[**Ha**] Helmut Hasse, *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper*, J. Reine Angew. Math. **172** (1934), 37-54.

[**Ih82**] Yasutaka Ihara, *Some remarks on the number of points of algebraic curves over Finite Fields*, J. Fac. Sci. Tokyo **28** (1982), 721-724.

[**Ih07**] Yasutaka Ihara, *Some remarks on the BGS tower over finite cubic fields*, Proceedings of the conference "Arithmetic Geometry, Related Area and Applications" (Chuo University, April 2006), 2007, pp. 127-131.

[**Le**] Hendrik Lenstra, *On a problem of Garcia, Stichtenoth, and Thomas*, Finite Fields Appl. 8 (2002), no. 2, 166-170.

[**LiMaSt**] Wen-Ching Li, Hiren Maharaj and Henning Stichtenoth, *New optimal tame towers of function fields over small finite fields (with an appendix by Noam Elkies)*, Algorithmic number theory (Sydney, 2002), 372-389, Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002.

[**Ma**] Yuri Ivanovitch Manin, *What is the maximum number of points on a curve over $\mathbb{F}_2$?*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, 715-720.

[**NiXi**] Harald Niederreiter and Chao Ping Xing, 'Rational points on curves over finite fields: theory and applications'. London Mathematical Society Lecture Note Series, 285. Cambridge University Press, Cambridge, 2001.

[**Pe**] Marc Perret, *Tours ramifiées infinies de corps de classes.*, J. Number Theory **38** (1991), no. 3, 300-322.

[**Ro**] Peter Roquette, *The Riemann hypothesis in characteristic p, its origin and development, parts 1-3*. Available at
`http://www.rzuser.uni-heidelberg.de/~ci3/manu.html`

[**Sc**] René Schoof, *Algebraic Curves over $\mathbb{F}_2$ with Many Rational Points*, J. Number Theory **41** (1992), no. 1, 6-14.

[**Se79**] Jean-Pierre Serre, 'Local Fields', Translated from the French by Marvin Jay Greenberg. GTM 67, Springer-Verlag, 1979.

[**Se83**] Jean-Pierre Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris Sér. I Math. **296** (1983), no. 9, 397-402.

[**St**] Henning Stichtenoth, 'Algebraic Function Fields and Codes'. Universitext, Springer-Verlag, Berlin, 1993.

[**StVo**] Karl-Otto Stöhr and José Felipe Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) **52** (1986), no. 1, 1-19.

[**To**] Fernando Torres, *Algebraic Curves with Many Points over Finite Fields*, available at
`www.ime.unicamp.br/~ftorres/RESEARCH/ARTS_PDF/survey_curves.pdf`

[**TsVl**] Michael A. Tsfasman and Sergei G. Vladut, 'Algebraic-geometric Codes'. Kluwer Academic Publishers Group, Dordrecht, 1991.

[**TsVlZi**] Michael A. Tsfasman, Sergei G. Vladut and Thomas Zink, *Modular curves, Shimura curves, and Goppa codes, better than the Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21-28.

[**We**] André Weil, 'Courbes algébriques et Variétés abéliennes'. Hermann, Paris, 1971.

[**Wu**] Jörg Wulftange, *Zahme Türme algebraischer Funktionenkörper*, PhD Thesis, University of Essen, 2002. Available at
`http://deposit.ddb.de/cgi-bin/dokserv?idn=968562639`

[**Xi**] Chao Ping Xing, *Multiple Kummer extension and the number of prime divisors of degree one in function fields*, J. Pure Appl. Algebra **84** (1993), no. 1, 85-93.

[**Zi**] Thomas Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, Fundamentals of computation theory (Cottbus, 1985), 503-511, Lecture Notes in Comput. Sci., 199, Springer, Berlin, 1985.