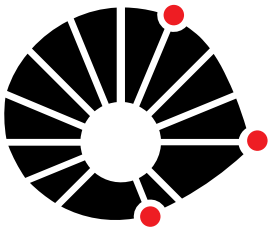


UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

RAFAEL FRONER PRANDO

Lattices from algebraic function fields

Reticulados sobre corpos de funções

Campinas

2024

Rafael Froner Prando

Lattices from algebraic function fields

Reticulados sobre corpos de funções

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática Aplicada.

Dissertation presented to the Institute of Mathematics, Statistics and Scientific Computing of the University of Campinas in partial fulfillment of the requirements for the degree of Master in Applied Mathematics.

Supervisor: Pietro Speziali

Este trabalho corresponde à versão final da Dissertação defendida pelo aluno Rafael Froner Prando e orientada pelo Prof. Dr. Pietro Speziali.

Campinas

2024

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

P885L

Prando, Rafael Froner, 1999-
Lattices from algebraic function fields / Rafael Froner Prando. – Campinas, SP : [s.n.], 2024.

Orientador: Pietro Speziali.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Curvas elípticas. 2. Curva hermitiana. 3. Curva de Fermat. 4. Distância mínima. 5. Número de vizinhos. 6. Reticulados bem arredondados. I. Speziali, Pietro, 1989-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações Complementares

Título em outro idioma: Reticulados sobre corpos de funções
Palavras-chave em inglês:
Elliptic curves
Hermitian curves
Fermat curve
Minimum distance
Kissing number
Well-rounded lattices
Área de concentração: Matemática Aplicada
Titulação: Mestre em Matemática Aplicada
Banca examinadora:
Pietro Speziali [Orientador]
Ethan Guy Cotterill
Nazar Arakelian
Data de defesa: 08-03-2024
Programa de Pós-Graduação: Matemática Aplicada

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0009-0001-5346-0444
- Currículo Lattes do autor: https://lattes.cnpq.br/4957220732488625

Dissertação de Mestrado defendida em 08 de março de 2024 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). PIETRO SPEZIALI

Prof(a). Dr(a). ETHAN GUY COTTERILL

Prof(a). Dr(a). NAZAR ARAKELIAN

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Para Julieta.

Acknowledgements

Agradeço aos meus pais, Geraldo e Mary, pelo incessante apoio e incentivo.

Agradeço ao meu orientador pelas ótimas ideias e pela paciência durante a orientação.

Por fim, agradeço ao Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq (número de processo 135852/2022-6) pelo apoio financeiro que possibilitou a realização desta pesquisa.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Resumo

A presente dissertação explora o tópico de reticulados construídos sobre corpos de funções algébricas de grau de transcendência 1. Primeiramente são estabelecidas as bases da teoria de corpos de funções, da teoria de reticulados e a conexão entre curvas algébricas e corpos de funções. Depois disso, a construção e as propriedades básicas (distância mínima, kissing number, bem arredondado, determinante) dos reticulados sobre corpos de funções são apresentadas e os exemplos conhecidos na literatura são explorados: corpos de funções elípticos e Hermitianos. Por fim, introduzimos uma nova construção: reticulados sobre a curva de Fermat, que apresentam propriedades um tanto distintas dos exemplos até então documentados. Por exemplo, distância mínima maior do que o esperado e kissing number fixo.

Palavras-chave: curvas elípticas. curvas Hermitianas. curvas de Fermat. distância mínima. número de vizinhos. reticulados bem arredondados.

Abstract

This dissertation explores the topic of lattices constructed from algebraic function fields of transcendence degree 1. We start by establishing the basics of function field theory, lattice theory, and the connection between algebraic curves and function fields. After that, the construction and general properties (minimum distance, kissing number, well-roundedness, determinant) of function field lattices are given before the known examples in literature are explored: the elliptic and Hermitian function fields. Finally, we introduce a new construction: lattices over the Fermat curve, which exhibit different properties to all the known examples. For instance, a larger than expected minimum distance and a fixed kissing number.

Keywords: elliptic curves. Hermitian curves. Fermat curves. minimum distance. kissing number. well rounded lattices.

Contents

Introdução

This text explores the topic of lattices constructed from algebraic function fields of one variable. First, the basics of function field theory are established using (STICHTENOTH, 2009) as a foundation. Lattice theory essential definitions and parameters are defined using (COSTA et al., 2017). Also, the connection between algebraic curves and function fields is explored, along with several equivalent formulations of the Riemann-Roch problem as described in (GOPPA, 1988).

After the basics have been laid out, the construction method and results regarding the minimum distance, kissing number, well-roundedness and determinant of function field lattices, according to (ATEŞ, 2017), are presented. This is followed by an examination of the parameters of all the currently known examples of lattices over function fields in literature: the elliptic and Hermitian function fields, presented in (FUKSHANSKY; MAHARAJ, 2014) and (BÖTTCHER et al., 2016), respectively.

Finally, using (ROHRLICH, 1977) as a base, the construction of the Fermat function field lattice is introduced. This construction proves to be interesting, seeing as it exhibits different properties to the currently known examples of function field lattices: the lower bound $\sqrt{2\gamma}$ for the minimum distance is never attained and the kissing number is fixed for Fermat curves of degree $n \geqslant 5$.

1 Preliminaries

In this first chapter we provide the basic definitions of both lattice theory and algebraic function field theory which will be used for the construction of lattices. The first subsections will discuss topics such places, valuations, divisors, adeles, Weil differentials, as well as the gonality and genus of a function field.

The main reference for this chapter are chapters 1 and 3 of (STICHTENOTH, 2009), which provide all the required basics on algebraic function field theory. For the sake of brevity, some results have their proofs omitted. One can find the detailed arguments for those results in the same reference.

For now, we use K to denote an arbitrary field. At later points we might assume K has different properties, for example, being finite, which will be the most interesting case for lattice construction.

1.1 Places

Definition 1. *An algebraic function field F of one variable over K is an extension field $F \supseteq K$ such that F is a finite algebraic extension of $K(x)$, where $x \in F$ is transcendental over K.*

We shall use the notation $F|K$ to denote a function field F over K. Consider the set $\tilde{K} := \{z \in F : z \text{ is algebraic over } K\}$, which is a subfield of F, since the sums, products and inverses of algebraic elements are also algebraic. $\tilde{K}$ is called the field of constants of $F|K$. We have the following inclusions $K \subseteq \tilde{K} \subseteq F$, and it is evident that we can consider F a function field over $\tilde{K}$. We say K is algebraically closed in F (or K is the full constant field of F) if $K = \tilde{K}$.

Remark 1. *The elements of F that are transcendental over K can be characterized by examining the degree $[F : K(z)]$. If it is finite, then z is transcendental.*

Example 1. *The first and simplest example of an algebraic function field is the rational function field. $F|K$ is called rational if $F = K(x)$ for some $x \in F$ transcendental over K. The name comes from the fact that every element $z \in F^*$ has a unique representation*

$$z = a \cdot \prod_i p_i(x)^{n_i},$$

in which $a \in K^*$, $n_i \in \mathbb{Z}$ and the polynomials $p_i(x) \in K[x]$ are monic, irreducible and pairwise distinct.

Using the previous example, we can represent a function field $F|K$ as a simple algebraic extension of the rational function field $K(x)$, that is, $F = K(x, y)$, where $\varphi(y) = 0$ for some irreducible polynomial $\varphi(T) \in K(x)[T]$. Consider now arbitrary elements $\alpha_1, \ldots, \alpha_n \in K$ and suppose we wish to find all rational functions $f(x) \in K(x)$ with zeroes or poles of prescribed order at $\alpha_1, \ldots, \alpha_n$. In order to formulate this problem for any function field, we introduce the notions of valuation rings and places.

Definition 2. *A valuation ring of the function field $F|K$ is a ring $\mathcal{O} \subseteq F$ such that*

1. *$K \subsetneq \mathcal{O} \subsetneq F$, and*
2. *for all $z \in F$, $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.*

This definition is inspired by an observation in the rational function field: given $p(x) \in K[x]$ a monic irreducible polynomial, consider the set

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x],\ p(x) \nmid g(x) \right\},$$

which is a valuation ring of $K(x)|K$. If $q(x)$ is another irreducible monic polynomial, then $\mathcal{O}_{p(x)} \neq \mathcal{O}_{q(x)}$.

Proposition 1. *Let $\mathcal{O}$ be a valuation ring of $F|K$. The following hold:*

(a) $\mathcal{O}$ has a unique maximal ideal $P = \mathcal{O} \backslash \mathcal{O}^\times$, where $O^\times$ denotes the group of invertible elements of $\mathcal{O}$.

(b) $x \in F^*$. Then $x \in P \iff x^{-1} \notin \mathcal{O}$.

(c) For the field of constants $\tilde{K}$ of $F|K$, we have $\tilde{K} \subseteq \mathcal{O}$ and $\tilde{K} \cap P = \{0\}$.

Proof. (a) We need only prove that $P = \mathcal{O} \backslash \mathcal{O}^\times$ is an ideal of $\mathcal{O}$, since no proper ideal can contain an invertible element and hence, cannot contain P.

First, let $x \in P,\ z \in \mathcal{O}$. Then $xz \notin \mathcal{O}$, since otherwise, there would exist $v \in \mathcal{O}$ such that $xzv = 1$, which would imply $x^{-1} = zv \in \mathcal{O}$, contradicting the fact that $x \in P$.

Now, let $x, y \in P$. Since $\frac{x}{y} \in F$, we can assume, without loss of generality that $\frac{x}{y} \in \mathcal{O}$. Then, $1 + \frac{x}{y} \in \mathcal{O}$ and $x + y = y\left(1 + \frac{x}{y}\right) \in P$ by the previous observation. This proves P is an ideal of $\mathcal{O}$.

(b) $x \in P \implies x \notin \mathcal{O}^\times \implies x^{-1} \notin \mathcal{O}$. Conversely, $x^{-1} \notin \mathcal{O} \implies x \in \mathcal{O} \implies x \in P$.

(c) Let $z \in \tilde{K}$. Assume $z \notin \mathcal{O}$. Then, $z^{-1} \in \mathcal{O}$. Since z^{-1} is algebraic over K, there are elements $a_1, \ldots, a_r \in K$ with $a_r(z^{-1})^r + \cdots + a_1 z^{-1} + 1 = 0$, implying $z^{-1}(a_r(z^{-1})^{r-1} +$

$\cdots + a_1) = -1$ and therefore $z = -(a_r(z^{-1})^{r-1} + \cdots + a_1) \in K[z^{-1}] \subseteq \mathcal{O}$, so $z \in \mathcal{O}$, contradicting the assumption that $z \notin \mathcal{O}$. Hence, $\tilde{K} \subseteq \mathcal{O}$.

Now, let $z \in \tilde{K}^*$. Since $\tilde{K}$ is a field, $z^{-1} \in \tilde{K} \subseteq \mathcal{O}$, which implies $z \in \mathcal{O}^\times$. Therefore $\tilde{K} \cap P = \{0\}$.

□

Theorem 1. *Let $\mathcal{O}$ be a valuation ring of $F|K$ and let P be its maximal ideal. The following hold:*

(a) P is a principal ideal.

(b) If $P = t\mathcal{O}$, then each $z \in F^*$ has a unique representation of the form $z = t^n u$ for some $n \in \mathbb{Z}$ and $u \in \mathcal{O}^\times$.

(c) $\mathcal{O}$ is a principal ideal domain. More precisely, if $P = t\mathcal{O}$ and $\{0\} \neq I \subseteq \mathcal{O}$ is an ideal, then $I = t^n\mathcal{O}$ for some $n \in \mathbb{N}$.

A ring that has the above properties is called a discrete valuation ring. In order to prove the preceding theorem, we will need the following lemma:

Lemma 1. *Let $\mathcal{O}$ be a valuation ring of $F|K$, let P be its maximal ideal and $x \in P^*$. Let $x_1, \ldots x_n \in P$ such that $x_1 = x$ and $x_i \in x_{i+1}P$ for $i = 1, \ldots, n-1$. Then we have $n \leqslant [F : K(x)] < \infty$.*

Proof. It follows from Remark 1 and Proposition 1(c) that $F|K(x)$ is a finite extension, so we only need to show that $x_1, \ldots, x_n$ are linearly independent over $K(x)$. Assume there is a non-trivial linear combination $\sum_{i=1}^{n} \varphi_i(x)x_i = 0$ with $\varphi_i(x) \in K(x)$. By considering the least common multiple of all the polynomials, we may suppose all $\varphi_i(x)$ are polynomials in x and x does not divide any of them. Set $a_i := \varphi_i(0)$ and define $j \in \{1, \ldots, n\}$ by the condition $a_j \neq 0$, but $a_i = 0$ for all $i > j$. We have

$$-\varphi_j(x)x_j = \sum_{i \neq j} \varphi_i(x)x_i \tag{1.1}$$

with $\varphi_i(x) \in \mathcal{O}$ for $i = 1, \ldots, n$, since $x = x_1 \in P$, $x_i \in x_jP$ for $i < j$ and $\varphi_i(x) = xg_i(x)$ for $i > j$ with $g(x) \in K[x]$. Dividing (1.1) by x_j yields

$$-\varphi_j(x) = \sum_{i<j} \varphi_i(x)\frac{x_i}{x_j} + \sum_{i>j} \frac{x}{x_j} g_i(x)x_i.$$

All the elements on the right side belong to P, therefore $\varphi(x) \in P$. On the other hand, $\varphi_j(x) = a_j + xg_j(x)$ with $g_j(x) \in K[x] \subseteq \mathcal{O}$ and $x \in P$, so that $a_j = \varphi_j(x) - xg_j(x) \in P \cap K$. Since $a_j \neq 0$ by definition, we have a contradiction to Proposition 1(c). Hence, $x_1, \ldots, x_n$ are linearly independent over $K(x)$. □

Proof of Theorem 1. (a) Assume P is not principal and choose $x_1 \in P^*$. There exists $x_2 \in P \backslash x_1\mathcal{O}$. Then $x_2x_1^{-1} \notin \mathcal{O}$, implying $x_2^{-1}x_1 \in P$ by Proposition 1(b), so $x_1 \in x_2P$. By induction, we can produce a sequence $x_1, x_2, x_3, \ldots$ of elements of P such that $x_i \in x_{i+1}P$ for all $i \geqslant 1$, contradicting Lemma 1.

(b) Since z or z^{-1} is in $\mathcal{O}$, we can assume $z \in \mathcal{O}$. If $z \in \mathcal{O}^\times$, $z = t^0 z$. If $z \in P$, there is a maximal $m \geqslant 1$ such that $z \in t^m\mathcal{O}$, because the length of the sequence

$$x_1 = z,\ x_2 = t^{m-1}, \ldots, x_m = t$$

is bounded by Lemma 1. Let $z = t^m u$ with $u \in \mathcal{O}$. Note that u has to be invertible, since otherwise, $u \in P = t\mathcal{O}$ and $u = tw$ with $w \in \mathcal{O}$, implying $z = t^{m+1}w \in t^{m+1}\mathcal{O}$, which contradicts the maximality of m.

As for uniqueness, suppose $z = t^n u = t^m v$ with $m, n \in \mathbb{Z}$ and $u, v \in \mathcal{O}^\times$. We have

$$\begin{aligned} t^n u - t^m v &= 0 \\ t^n(u - t^{m-n}v) &= 0 \\ t^{m-n}v &= u \\ t^{m-n} &= uv^{-1} \in \mathcal{O}^\times. \end{aligned}$$

If $m \neq n$, then $t \in \mathcal{O}^\times$ and $t \notin P$, a contradiction. Hence, $m = n$ and by extension, $u = v$.

(c) Let $I \subseteq \mathcal{O}$ be a non-zero ideal. The set $A := \{r \in \mathbb{N} : t^r \in I\}$ is non-empty, because if $x \in I^*$, then $x = t^r u$, $u \in \mathcal{O}^\times$ and $t^r = xu^{-1} \in I$. Set $n := \min(A)$. We claim that $I = t^n\mathcal{O}$. Since $t^n \in I$, the inclusion $I \subseteq t^n\mathcal{O}$ follows. Now suppose $y \in I^*$. We know $y = t^s w$ with $w \in \mathcal{O}^\times$ and $s \geqslant$, which means $t^s \in I$ and $s \geqslant n$. It follows that $y = t^n \cdot t^{s-n}w \in t^n\mathcal{O}$.

□

Definition 3. *(a) A place P of the function field $F|K$ is the maximal ideal of some valuation ring $\mathcal{O}$ of $F|K$. An element $t \in P$ such that $P = t\mathcal{O}$ is called a prime element of P.*

(b) $\mathbb{P}_F := \{P : P \text{ is a place of } F|K\}$.

If $\mathcal{O}$ is a valuation ring of $F|K$ and P its maximal ideal, then $\mathcal{O}$ is uniquely defined by P by using Proposition 1: $\mathcal{O} = \{z \in F : z^{-1} \notin P\}$. This means we can write $\mathcal{O}_P := \mathcal{O}$ is called the valuation ring of the place P. We can also describe places in terms of certain functions called valuations.

Definition 4. *A discrete valuation of $F|K$ is a function $v : F \to \mathbb{Z} \cup \{\infty\}$ satisfying the following properties for all $x, y \in F$:*

1. $v(x) = \infty \iff x = 0$.
2. $v(xy) = v(x) + v(y)$.
3. $v(x + y) \geqslant \min\{v(x), v(y)\}$.
4. *There exists an element* $z \in F$ *such that* $v(z) = 1$.
5. $v(a) = 0$ *for all* $a \in K^*$.

The symbol ∞ denotes an element not in $\mathbb{Z}$ such that $\infty > n$ and $\infty + \infty = \infty + n = n + \infty$ for all $n \in \mathbb{Z}$. Properties 2 and 4 imply v is surjective. Property 3 is called the triangle inequality. A stronger version os this inequality can be derived from the axioms and will be frequently utilized:

Lemma 2 (Strict Triangle Inequality)**.** *If* v *is a discrete valuation of* $F|K$*, let* $x, y \in F$ *with* $v(x) \neq v(y)$*. Then* $v(x + y) = \min\{v(x), v(y)\}$.

Proof. By properties 2 and 5, $v(ay) = v(y)$ for all $a \in K^*$. In particular, $v(-y) = v(y)$. We can assume $v(x) < v(y)$. Suppose $v(x + y) > \min\{v(x), v(y)\}$, so $v(x + y) > v(x)$. We obtain $v(x) = v((x + y) - y) \geqslant \min\{v(x + y), v(y)\} > v(x)$, a contradiction. □

Definition 5. *To a place* $P \in \mathbb{P}_F$*, we can associate a function* $v_P : F \to \mathbb{Z} \cap \{\infty\}$*, which we will prove to be a discrete valuation, in the following way: pick a prime element* t *for* P*. Every* $z \in F^*$ *has a unique representation* $z = t^n u$ *with* $u \in \mathcal{O}_P^\times$ *and* $n \in \mathbb{Z}$*. Define* $v_P(z) := n$ *and* $v_P(0) := \infty$.

This definition depends only on P, and not on the choice of t. Taking s another prime element for P, then $P = t\mathcal{O} = s\mathcal{O}$, so $t = sw$ for $w \in \mathcal{O}_P^\times$. Therefore $t^n u = (sw)^n u = s^n(w^n u)$ with $w^n u \in \mathcal{O}_P^\times$.

Theorem 2. *Let* $F|K$ *be a function field.*

(a) For a place $P \in \mathbb{P}_F$*,* v_P *is a discrete valuation of* $F|K$*. Moreover*

$$\begin{aligned} \mathcal{O}_P &= \{z \in F : v_P(z) \geqslant 0\}, \\ \mathcal{O}_P^\times &= \{z \in F : v_P(z) = 0\}, \\ P &= \{z \in F : v_P(z) > 0\}. \end{aligned}$$

(b) $x \in F$ *is a prime element for* P *if and only if* $v_P(x) = 1$.

(c) Suppose v *a discrete valuation of* $F|K$*. The set* $P := \{z \in F : v(z) > 0\}$ *is a place of* $F|K$*, and* $\mathcal{O}_P = \{z \in F : v(z) \geqslant 0\}$ *is its corresponding valuation ring.*

(d) Every valuation ring of $F|K$ *is a maximal proper subring of* F.

Proof. (a) v_P evidently has properties $1, 2, 4$ and 5. For the triangle inequality, take $x, y \in F$ with $v_P(x) = n,\ v_P(y) = m$. It is safe to assume $n \leqslant m < \infty$, and thus $x = t^n u_1,\ y = t^m u_2$ with $u_1, u_2 \in \mathcal{O}_P^\times$. We have $x + y = t^n(u_1 + t^{m-n}u_2) = t^n z$ with $z \in \mathcal{O}_P$. If $z = 0$, $v_P(x + y) = \infty > \min\{n, m\}$. Otherwise, $z = t^k u$ with $u = \mathcal{O}_P^\times$. Then,

$$v_P(x + y) = v_P(t^{n+k}u) = n + k \geqslant n = \min\{v_P(x), v_P(y)\}.$$

To prove the set equalities, take $z \in \mathcal{O}_P$. If $z = 0$, then $v_P(z) = \infty > 0$. Otherwise, $z = t^n u$ with $u \in \mathcal{O}_P^\times$ and $v_P(z) = n > 0$. Now, if $z \in F$ and $v_P(z) \geqslant 0$, we have $v_P(z) = 0 \iff z \in \mathcal{O}_P^\times \subseteq \mathcal{O}_P$. Also, $v_P(z) = n > 0 \iff z = t^n u,\ u \in \mathcal{O}_P^\times \iff z \in \mathcal{O}_P$. Finally, $v_P(z) = \infty \iff z = 0 \in \mathcal{O}_P$, proving that $\mathcal{O}_P = \{z \in F : v_P(z) \geqslant 0\}$. The fact that $v_P(z) = 0 \iff z \in \mathcal{O}_P^\times$ proves $\mathcal{O}_P^\times = \{z \in F : v_P(z) = 0\}$ and the set equality for P follows directly from the fact that $P = \mathcal{O}_P \backslash \mathcal{O}_P^\times$.

(b) Let $P = t\mathcal{O}$. Since the valuation does not depend on the choice of t, $x \in F$ is another prime element for P if and only if $v_P(x) = v_P(t) = 1$.

(c) Firstly, $\mathcal{O}_P$ as defined by the valuation v is a valuation ring of $F|K$. Take $z \in F$. If $v(z) \geqslant 0$, there is nothing to prove. If $v(z) < 0$, by property 2 of the discrete valuations, $0 = v(1) = v(zz^{-1}) = v(z) + v(z^{-1})$, that is, $v(z^{-1}) = -v(z)$. Hence, $v(z^{-1}) > 0$ and $z^{-1} \in \mathcal{O}_P$. Since $\mathcal{O}_P = \{z \in F : z^{-1} \notin P\}$, it follows that $\{z \in F : v_P(z) > 0\}$ is the maximal ideal of $\mathcal{O}_P$, and hence, a place of $F|K$.

(d) Let $\mathcal{O}$ be a valuation ring of $F|K$, P its maximal ideal, v_P the discrete valuation of P and $z \in F\backslash\mathcal{O}$. We must show that $F = \mathcal{O}[z]$. The inclusion $\mathcal{O}[z] \subseteq F$ is trivial. In order to prove the reverse inclusion, consider any $y \in F$. Since $z \notin \mathcal{O}$, $v_P(z^{-1}) > 0$, which means $v_P(yz^{-k}) \geqslant 0$ for sufficiently large k. Therefore, $w = yz^{-k} \in \mathcal{O}$ and $y = wz^k \in \mathcal{O}[z]$.

□

If P is a place of $F|K$ and $\mathcal{O}_P$ is its valuation ring, the fact P is maximal implies the quotient $\mathcal{O}_P/P$ is a field. For $x \in \mathcal{O}_P$, we define $x(P) \in \mathcal{O}_P/P$ to be the residue class of x modulo P. For $x \in F\backslash\mathcal{O}_P$, we define $x(P) := \infty$. By Proposition 1, we know $K \subseteq \mathcal{O}_P$ and $K \cap P = \{0\}$, so the map $x \mapsto x(P)$ induces a canonical embedding of K into $\mathcal{O}_P/P$. Therefore, from this point onward, we shall consider K a subfield of $\mathcal{O}_P/P$. This reasoning also works for $\tilde{K}$ and we consider it a subfield of $\mathcal{O}_P/P$ as well.

Definition 6. *(a) $F_P := \mathcal{O}_P/P$ is the residue class field of P. The map $x \mapsto x(P)$ from F to F_P is called the residue class map with respect to P. We can also use the notation $x + P = x(P)$ if $x \in \mathcal{O}_P$.*

(b) $\deg P := [F_P : K]$ is called the degree of P. If $\deg P = 1$, P is called a rational place of $F|K$.

The degree of a place is always a finite number. More precisely, we have the following:

Proposition 2. *If P is a place of $F|K$ and $x \in P^*$, then*

$$\deg P \leqslant [F : K(x)] < \infty.$$

Proof. We already know that $[F : K(x)] < \infty$ from Remark 1. So we just need to show that any elements $z_1, \ldots, z_n \in \mathcal{O}_P$ whose residue classes $z_1(P), \ldots, z_n(P)$ are linearly independent over K are linearly independent over $K(x)$. So suppose there is a nontrivial linear combination

$$\sum_{i=1}^{n} \varphi_i(x) z_i = 0 \tag{1.2}$$

with $\varphi_i(x) \in K(x)$. By the same reasoning used previously, we might assume $\varphi_i(x) \in K[x]$ are polynomials not all divisible by x, that is, $\varphi_i(x) = a_i + x g_i(x)$ for $a_i \in K$ and $g_i \in K[x]$, not all $a_i = 0$. Since $x \in P$ and $g_i(x) \in K[x] \subseteq \mathcal{O}_P$:

$$\varphi_i(x)(P) = a_i(P) + x g_i(x)(P) = a_i(P) = a_i.$$

Applying the residue class map to (1.2), we get

$$0 = 0(P) = \sum_{i=1}^{n} \varphi_i(x)(P) z_i(P) = \sum_{i=1}^{n} a_i z_i(P),$$

a contradiction to the linear independence of $z_1(P), \ldots, z_n(P)$ over K. □

Corollary 1. *The field of constants $\tilde{K}$ of $F|K$ is a finite field extension of K.*

Proof. We make use of the fact that $\mathbb{P}_F \neq \varnothing$, which we shall prove shortly. Choose $P \in \mathbb{P}_F$. $\tilde{K}$ is embedded in F_P via the residue class map $\mathcal{O}_P \to F_P$. Therefore, $[\tilde{K} : K] \leqslant [F_P : K] < \infty$. □

Remark 2. *If $\deg P = 1$, then $F_P = K$ and the residue class map sends F_P to $K \cup \{\infty\}$. In particular, if K is algebraically closed, then all places of $F|K$ are rational and we can interpret an element $z \in F$ as a function*

$$\begin{aligned} z : \mathbb{P}_F &\to K \cup \{\infty\} \\ P &\mapsto z(P). \end{aligned} \tag{1.3}$$

This is the reason why $F|K$ is called a function field. The elements of K interpreted as functions in the sense of (1.3), are constant functions. For this reason, K is called the constant field of F. This remark also justifies the following terminology:

Definition 7. *Let $z \in F$ and $P \in \mathbb{P}_F$. P is a zero of order m of z if $v_P(z) = m > 0$, and P is a pole of order m of z if $v_P(z) - m < 0$.*

We shall now prove that $\mathbb{P}_F \neq \varnothing$ for any function field $F|K$.

Theorem 3. *Let $F|K$ be a function field and R a subring of F such that $K \subseteq R \subseteq F$. Suppose $I \subsetneq R$ is a proper ideal of R. Then there exists a place $P \in \mathbb{P}_F$ such that $I \subseteq P$ and $R \subseteq \mathcal{O}_P$.*

Proof. Consider the set

$$\mathcal{F} := \{S : S \text{ is a subring of } F \text{ with } R \subseteq S \text{ and } IS \neq S\},$$

where IS is the set of all finite sums $\sum a_k s_k$ with $a_k \in I,\ s_k \in S$, which is an ideal of S. We wish to use Zorn's Lemma. To this end, note that $\mathcal{F}$ is non-empty as $R \in \mathcal{F}$, and $\mathcal{F}$ is inductively ordered by inclusion. In fact, take $\mathcal{H} \subseteq \mathcal{F}$ a totally ordered subset of $\mathcal{F}$. Then, $T := \bigcup\{S : S \in \mathcal{H}\}$ is a subring of F with $R \subseteq T$. We must prove that $IT \neq T$. Suppose this is false, then $1 = \sum_{k=1}^{n} a_k s_k,\ a_k \in I,\ s_k \in T$. Since $\mathcal{H}$ is totally ordered, there is $S_0 \in \mathcal{H}$ such that $s_1, \ldots, s_n \in S_0$, so $1 = \sum_{k=1}^{n} a_k s_k \in IS_0$, which is a contradiction.

Applying Zorn's Lemma, F contains a maximal element $\mathcal{O} \subseteq F$ such that $R \subseteq \mathcal{O} \subseteq F$, $I\mathcal{O} \neq \mathcal{O}$ and $\mathcal{O}$ is maximal with respect to these properties. It only remains to show that $\mathcal{O}$ is a valuation ring of $F|K$.

As $I \neq \{0\}$ and $I\mathcal{O} \neq \mathcal{O}$, it follows that $\mathcal{O} \subsetneq F$ and $I \subseteq \mathcal{O}\backslash\mathcal{O}^\times$. Suppose there exists $z \in F$ with $z \notin \mathcal{O}$ and $z^{-1}\mathcal{O}$. Then $I\mathcal{O}[z] = \mathcal{O}[z]$ and $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$, and there exists $a_0, \ldots, a_n, b_0, \ldots, b_m \in I\mathcal{O},\ m, n \geqslant 1$ such that

$$1 = a_0 + a_1 z + \cdots + a_n z^n \tag{1.4}$$

$$1 = b_0 + b_1 z^{-1} + \cdots + b_m z^{-m}. \tag{1.5}$$

We can assume m and n are chosen minimally and $m \leqslant n$. Multiplying (1.4) by $1 - b_0$ and (1.5) by $a_n z^n$, we obtain

$$\begin{aligned} 1 - b_0 &= (1 - b_0)a_0 + (1 - b_0)a_1 z + \cdots + (1 - b_0)a_n z^n \\ 0 &= (b_0 - 1)a_n z^n + b_1 a_n z^{n-1} + \cdots + b_m a_n z^{n-m}. \end{aligned}$$

Adding these equations produces $1 = c_0 + c_1 z + \cdots + c_{n-1} z^{n-1}$ with coefficients $c_i \in I\mathcal{O}$, contradicting the minimality of n. This proves $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$, which means $\mathcal{O}$ is a valuation ring of $F|K$. □

Corollary 2. *Let $F|K$ be a function field, and $z \in F$ transcendental over K. Then z has at leas one zero and one pole in F. In particular, $\mathbb{P}_F \neq \varnothing$.*

Proof. Consider the ring $R = K[z]$ and the ideal $I = zK[z]$. By Theorem 3, there is a place $P \in \mathbb{P}_F$ with $z \in P$, hence P is a zero of z. The same reasoning proves z^{-1} has a zero $Q \in \mathbb{P}_F$, which means Q is a pole of z. □

The preceding corollary can be interpreted in the following way: each $z \in F \backslash \tilde{K}$ yields a non-constant function in the sense of Remark 2.

1.2 The Rational Function Field

In order to better understand places and valuations in arbitrary function fields, it is essential to thoroughly understand these concepts in the simplest case, the rational function field $F = K(x)$ for $x \in F$ transcendental over K. Given an irreducible monic polynomial $p(x) \in K[x]$, take the valuation ring

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x],\ p(x) \nmid g(x) \right\}$$

of $K(x)|K$ whose maximal ideal is

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x],\ p(x) \mid f(x),\ p(x) \nmid g(x) \right\}.$$

In the case where $p(x)$ is linear, that is, $p(x) = x - \alpha$ with $\alpha \in K$, we write $P_\alpha := P_{x-\alpha} \in \mathbb{P}_{K(x)}$.

There is another valuation ring of $K(x)|K$, namely

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x],\ \deg f(x) \leqslant \deg g(x) \right\}$$

with maximal ideal

$$P_\infty := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x],\ \deg f(x) < \deg g(x) \right\}.$$

This place is called the infinite place of $K(x)$. These labels depend on the choice of the generating element x of $K(x)$. For example, $K(x) = K(1/x)$, but the infinite place of $K(1/x)$ is equal to P_0 in $K(x)$.

Proposition 3. *Let $F = K(x)$ be the rational function field.*

(a) Let $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ with $p(x) \in K[x]$ an irreducible polynomial. Then $p(x)$ is a prime element of P, and the corresponding valuation v_P is given as follows: if $z \in K(x)^*$ is written in the form $z = p(x)^n \cdot (f(x)/g(x))$ with $n \in \mathbb{Z}$ and $f(x), g(x) \in K[x]$, then $v_P(z) = n$. The residue class field $K(x)_P = \mathcal{O}_P/P$ is isomorphic to $K[x]/\langle p(x) \rangle$ with isomorphism given by

$$\begin{aligned} \phi : K[x]/\langle p(x) \rangle &\to K(x)_P \\ f(x) \pmod{p(x)} &\mapsto f(x)(P). \end{aligned}$$

Consequently, $\deg P = \deg p(x)$.

(b) If $p(x) = x - \alpha$ with $\alpha \in K$, the degree of $P = P_\alpha$ is 1, and the residue class map is given by $z(P) = z(\alpha)$ for $z \in K(x)$. We define $z(\alpha)$ in the following way: if $z = f(x)/g(x)$ with $f(x), g(x) \in K[x]$ relatively prime polynomials, then $z(\alpha) = f(\alpha)/g(\alpha)$ if $g(\alpha) \neq 0$ and $z(\alpha) = \infty$ if $g(\alpha) = 0$.

(c) If $P = P_\infty$ is the infinite place of $K(x)$, then $\deg P_\infty = 1$ and $t = 1/x$ is a prime element for P_∞. The discrete valuation v_∞ is given by

$$v_\infty(f(x)/g(x)) = \deg g(x) - \deg f(x)$$

where $f(x), g(x) \in K[x]$. The residue class map is defined by $z(P_\infty) = z(\infty)$ for $z \in K(x)$ in the following way: if

$$z = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0},\ a_n, b_m \neq 0,$$

then

$$z(\infty) = \begin{cases} \dfrac{a_n}{b_m} \text{ if } n = m \\ 0 \text{ if } n < m \\ \infty \text{ if } n > m. \end{cases}$$

(d) K is the full constant field of $K(x)|K$.

Proof. (a) The fact that $p(x) \mid f(x)$ directly implies P is generated by $p(x)$, hence it is a prime element for P. To prove the claim about the residue class map, first consider the ring homomorphism

$$\begin{aligned} \varphi : K[x] &\to K(x)_P \\ f(x) &\mapsto f(x)(P). \end{aligned}$$

Notice that $f(x) \in \ker\varphi \iff p(x) \mid f(x) \iff f(x) \in \langle p(x)\rangle$, meaning $\ker\varphi = \langle p(x)\rangle$. φ is also surjective: take $z \in \mathcal{O}_{p(x)}$ and write $z = u(x)/v(x)$ with $u(x), v(x) \in K[x]$ such that $p(x) \nmid v(x)$. Since $p(x)$ and $v(x)$ are coprime, there are $a(x), b(x) \in K[x]$ such that $a(x)p(x) + b(x)v(x) = 1$, therefore

$$z = 1 \cdot z = \frac{a(x)u(x)}{v(x)}p(x) + b(x)u(x),$$

and $z(P) = (b(x)u(x))(P)$ is in the image of φ. Hence, φ induces an isomorphism from $K[x]/\langle p(x)\rangle$ to $K(x)_P$. Seeing as $[K(x)_P : K] = [K[x]/\langle p(x)\rangle : K] = \deg p(x)$, we conclude $\deg P = \deg p(x)$.

(b) Let $P = P_\alpha,\ \alpha \in K$. For $f(x) \in K[x]$, we have $(x - \alpha) \mid (f(x) - f(\alpha))$. Hence $f(x)(P) = (f(x) - f(\alpha))(P) + f(\alpha)(P) = f(\alpha)$. An arbitrary $z \in \mathcal{O}_P$ can be written as $z = f(x)/g(x)$ with $f(x), g(x) \in K[x]$ and $(x - \alpha) \nmid g(x)$, therefore $g(x)(P) = g(\alpha) \neq 0$ and

$$z(P) = \frac{f(x)(P)}{g(x)(P)} = \frac{f(\alpha)}{g(\alpha)} = z(\alpha).$$

(c) If $P = P_\infty$, it is clear that $1/x \in P$. Consider an element $z = f(x)/g(x) \in P_\infty$. We have $\deg f(x) < \deg g(x)$, then

$$z = \frac{1}{x} \cdot \frac{xf(x)}{g(x)}, \text{ with } \deg(xf(x)) \leqslant \deg g(x).$$

This proves $z \in (1/x)\mathcal{O}_\infty$, hence $1/x$ generates P_∞ and is a P_∞-prime element. Finally, since P_∞ with respect to x is P_0 with respect to $1/x$, we have $K(x)_{P_\infty} \simeq K(1/x)_{P_0} \simeq K[1/x]/\langle x \rangle$, implying $\deg P_\infty = \deg P_0 = 1$.

(d) Choose a rational place P of $K(x)|K$. The field $\tilde{K}$ of constants of $K(x)$ is embedded into the residue class field $K(x)_P$, meaning $K \subseteq \tilde{K} \subseteq K(x)_P = K$.

□

Theorem 4. *All places of the rational function field are either of type $P_{p(x)}$ or P_∞.*

Proof. Let P be a place of $K(x)|K$. We split the proof into two cases:

Case 1. Assume $x \in \mathcal{O}_P$. Then, $K[x] \subseteq \mathcal{O}_P$. Define $I := K[x] \cap P$. This is a prime ideal of $K[x]$. The residue class map induces an embedding $K[x]/I \hookrightarrow K(x)_P$, consequently, $I \neq \{0\}$ by Proposition 1. It follows there is a unique irreducible monic polynomial $p(x) \in K[x]$ such that $I = K[x] \cap P = p(x) \cdot K[x]$. Every $g(x) \in K[x]$ with $p(x) \nmid g(x)$ is not in I, so $g(x) \notin P$ and $1/g(x) \in \mathcal{O}_P$ by Proposition 1. Thus we conclude

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x],\ p(x) \nmid g(x) \right\} \subseteq \mathcal{O}_P.$$

Since valuation rings are maximal proper subrings of $K(x)$ (Theorem 2), we see that $\mathcal{O}_P = \mathcal{O}_{p(x)}$.

Case 2. Now assume $x \notin \mathcal{O}_P$. We conclude $K[x^{-1}] \subseteq \mathcal{O}_P,\ x^{-1} \in P \cap K[x^{-1}]$ and $P \cap K[x^{-1}] = x^{-1}K[x^{-1}]$. Like in the previous case,

$$\begin{aligned}
\mathcal{O}_P &\supseteq \left\{ \frac{f(x^{-1})}{g(x^{-1})} : f(x^{-1}), g(x^{-1}) \in K[x^{-1}],\ x^{-1} \nmid g(x^{-1}) \right\} \\
&= \left\{ \frac{a_0 + a_1 x^{-1} + \cdots + a_n x^{-n}}{b_0 + b_1 x^{-1} + \cdots + b_m x^{-m}} : b_0 \neq 0 \right\} \\
&= \left\{ \frac{a_0 x^{m+n} + \cdots + a_n x^m}{b_0 x^{m+n} + \cdots + b_m x^n} : b_0 \neq 0 \right\} \\
&= \left\{ \frac{u(x)}{v(x)} : u(x), v(x) \in K[x],\ \deg u(x) \leqslant \deg v(x) \right\} = \mathcal{O}_\infty.
\end{aligned}$$

Thus $\mathcal{O}_P = \mathcal{O}_\infty$ and $P = P_\infty$. □

Corollary 3. *The rational places of $K(x)|K$ are in a $1-1$ correspondence with $K \cup \{\infty\}$. In particular, if $K = \mathbb{F}_q$, then $|\mathbb{P}_F| = q + 1$.*

1.3 Independence of Valuations

In this section, we shall prove the Weak Approximation Theorem, which intuitively states that given $v_1, \ldots, v_n$ pairwise distinct discrete valuations of $F|K$ and $z \in F$, knowing the values $v_1(z), \ldots, v_{n-1}(z)$ does not give us any information regarding $v_n(z)$. This result will be significantly improved in later sections and will be used when discussing function field extensions.

Theorem 5 (Weak Approximation Theorem)**.** *Let $F|K$ be a function field, $P_1, \ldots, P_n \in \mathbb{P}_F$ pairwise distinct places of $F|K$, $x_1, \ldots, x_n \in F$ and $r_1, \ldots, r_n \in \mathbb{Z}$. Then, there exists some $x \in F$ such that*

$$v_{P_i}(x - x_i) = r_i \text{ for } i = 1, \ldots, n.$$

Proof. In order to simplify notation, we write v_i instead of v_{P_i}. First, we will prove there exists some $u \in F$ such that $v_1(u) > 0$ and $v_i(u) < 0$ for $i = 2, \ldots, n$. By induction, for $n = 2$ we observe $\mathcal{O}_{P_1} \nsubseteq \mathcal{O}_{P_2}$ and vice-versa, since valuation rings are maximal proper subrings of F (Theorem 2). This means we can find $y_1 \in \mathcal{O}_{P_1} \backslash \mathcal{O}_{P_2}$ and $y_2 \in \mathcal{O}_{P_2} \backslash \mathcal{O}_{P_1}$. Then $v_1(y_1) \geqslant 0, v_2(y_1) < 0, v_1(y_2) < 0$, and $v_2(y_2) \geqslant 0$. Considering $u = y_1/y_2$, we have $v_1(u) > 0$ and $v_2(u) < 0$.

For $n > 2$, by the induction hypothesis, we have an element y such that $v_1(y) > 0$ and $v_i(y) < 0$ for $i = 2, \ldots, n-1$. If $v_n(y) < 0$, there is nothing to prove. If $v_n(y) \geqslant 0$, we choose z with $v_1(z) > 0$ and $v_n(z) < 0$ (whose existence is guaranteed by the $n = 2$ case) and define $u := y + z^r$, where $r \geqslant 1$ is any integer such that $r \cdot v_i(z) \neq v_i(y)$ for $i = 1, \ldots, n-1$. It follows that $v_1(u) \geqslant \min\{v_1(y), r \cdot v_1(z)\} > 0$ and by the Strict Triangle Inequality, $v_i(u) = \min\{v_i(y), r \cdot v_i(z)\} < 0$ for $i = 2, \ldots, n$, proving our first claim.

Now we show there exists some $w \in F$ such that $v_1(w - 1) = r_1$ and $v_i(w) > r_i$ for $i = 2, \ldots, n$. In order to prove this, first take $u \in F$ with $v_1(u) > 0$ and $v_i(u) < 0$ for $i = 2, \ldots, n$ and put $w := (1 + u^s)^{-1}$. Given a sufficiently large $s \in \mathbb{N}$, we have

$$v_1(w - 1) = v_1\left(-\frac{u^s}{1 + u^s}\right) = s \cdot v_1(u) - \min\{v_1(1), v_1(u^s)\} = s \cdot v_1(u) > r_1$$

and

$$v_i(w) = -s \cdot v_i(u) > r_i \text{ for } i = 2, \ldots, n.$$

Finally, we prove that given $y_1, \ldots, y_n \in F$, there exists $z \in F$ such that $v_i(z - y_i) > r_i$ for $i = 1, \ldots, n$. First, choose $s \in \mathbb{N}$ such that $v_i(y_j) \geqslant s$ for all $i, j = 1, \ldots, n$. Previously, we proved there are $w_1, \ldots, w_n$ with

$$v_i(w_i - 1) > r_i - s \text{ and } v_j(w_j) > r_i - s \text{ for } j \neq i.$$

The element $z := \sum_{j=1}^{n} y_j w_j$ has the desired property:

$$v_i(z - y_i) = v_i\left(\sum_{\substack{j=1 \\ j\neq i}}^{n} y_j w_j + y_i(w_i - 1)\right) > r_i \text{ for } i = 1, \ldots, n.$$

We are now ready to finish the proof. We take $z \in F$ such that $v_i(z - x_i) > r_i,\ i = 1, \ldots, n$. If t_i is a P_i-prime element, set $z_i := t_i^{r_i}$, meaning $v_i(z_i) = r_i$. Again, we can take z' such that $v_i(z' - z_i) > r_i$ for $i = 1, \ldots, n$. It follows that

$$v_i(z) = v_i((z' - z_i) + z_i) = \min\{v_i(z' - z_i), v_i(z_i) = r_i\}.$$

Setting $x := z + z'$:

$$v_i(x - x_i) = v_i((z - x_i) + z') = \min\{v_i(z - x_i), v_i(z')\} = r_i. \qquad \square$$

Corollary 4. *Every function field has infinitely many places.*

Proof. Suppose a function field $F|K$ has only finitely many places $P_1, \ldots, P_n$. By Theorem 5, we find a non-zero element $x \in F$ such that $v_{P_i}(x) > 0$ for all $i = 1, \ldots, n$. Since x has zeroes, it is transcendental over K. However, it has no poles, contradicting Corollary 2. $\square$

Proposition 4. *Let $F|K$ be a function field and $P_1, \ldots, P_r$ be the zeros of the element $x \in F$. Then*

$$\sum_{i=1}^{r} v_{P_i}(x) \cdot \deg P_i \leqslant [F : K(x)].$$

Proof. We write v_i in place of v_{P_i} and set $f_i := \deg P_i,\ e_i := v_i(x)$. Theorem 5 guarantees for every i, there is an element t_i such that $v_i(t_i) = 1$ and $v_k(t_i) = 0$ for $k \neq i$. Newt, take $s_{i1}, \ldots, s_{if_i} \in \mathcal{O}_{P_i}$ such that $s_{i1}(P_i), \ldots, s_{if_i}(P_i)$ form a basis of F_{P_i} over K. Applying Theorem 5, we find $z_{ij} \in F$ such that for all i, j:

$$v_i(s_{ij} - z_{ij}) > 0 \text{ and } v_k(z_{ij}) \geqslant e_k \text{ for } k \neq i.$$

We claim the elements

$$t_i^a \cdot z_{ij},\ 1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant f_i,\ 0 \leqslant a < e_i$$

are linearly independent over $K(x)$. There are $\sum_{i=1}^{r} f_i e_i = \sum_{i=1}^{r} v_{P_i}(x) \cdot \deg P_i$ of these elements, so proving the linear independence will finish the proof.

Suppose there is a non-trivial linear combination

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=1}^{e_i - 1} \varphi_{ija}(x) t_i^a z_{ij} = 0 \tag{1.6}$$

over $K(x)$. Without loss of generality, we can assume $\varphi_{ija}(x) \in K[x]$ and not all are divisible by x. Then there are indices $k \in \{1, \dots, r\}$ and $c \in \{0, \dots, e_i - 1\}$ such that

$$\begin{aligned} &x \mid \varphi_{kja}(x) \text{ for all } a < c \text{ and all } j \in \{1, \dots, f_k\}, \text{ and} \\ &x \nmid \varphi_{kjc}(x) \text{ for some } j \in \{1, \dots, f_k\}. \end{aligned} \tag{1.7}$$

Multiplying (1.6) by t_k^{-c}:

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=1}^{e_i-1} \varphi_{ija}(x) t_i^a t_k^{-c} z_{ij} = 0. \tag{1.8}$$

Note that for all $i \neq k$, all summands of (1.8) are elements of P_k seeing as

$$v_k(\varphi_{ija}(x) t_i^a t_k^{-c} z_{ij}) = v_k(\varphi_{ija}(x)) + a \cdot v_k(t_i) - c \cdot v_k(t_k) + v_k(z_{ij}) \geqslant -c + e_k > 0.$$

For $i = k$ and $a < c$

$$v_k(\varphi_{ija}(x) t_k^{a-c} z_{kj}) \geqslant e_k + a - c \geqslant e_k - c > 0,$$

since $x \mid \varphi_{kja}(x)$ and therefore $v_k(\varphi_{kja}(x)) \geqslant e_k$. For $i = k$ and $a > c$,

$$v_k(\varphi_{ija}(x) t_k^{a-c} z_{kj}) \geqslant a - c > 0.$$

Combining these observations with (1.8) produces

$$\sum_{j=1}^{f_k} \varphi_{kjc}(x) z_{kj} \in P_k. \tag{1.9}$$

Notice that $\varphi_{kjc}(x)(P_k) \in K$ and not all $\varphi_{kjc}(x)(P_k) = 0$ by (1.7) so (1.9) yields a non-trivial linear combination

$$\sum_{j=1}^{f_k} \varphi_{kjc}(x)(P_k) \cdot z_{kj}(P_k) = 0$$

over K, which leads to a contradiction, as $z_{k1}(P_k), \dots, z_{kf_k}(P_k)$ is a basis for $F_{P_k}|K$. □

Corollary 5. *In a function field $F|K$, every $x \in F^*$ has only finitely many zeros and poles.*

Proof. If x is constant, it has neither zeros nor poles. If it is transcendental over K, its number of zeros is bounded above by $[F : K(x)]$ in accordance with Proposition 4. Applying the same argument, x^{-1} also has finitely many zeros, and thus, x has only finitely many poles. □

1.4 Divisors

The field of constants $\tilde{K}$ of $F|K$ is a finite extension of K, as we have shown and F can be regarded as a function field over $\tilde{K}$. Therefore, making the assumption that K is always the full constant field of F will not limit the generality of the subsequent theory.

Definition 8. *The divisor group of $F|K$ is defined as the additively written free abelian group generated by the places of $F|K$. It is denoted by* $\mathrm{Div}(F)$ *and its elements are called divisors of $F|K$. A divisor is a formal sum*

$$D = \sum_{P \in \mathbb{P}_F} n_P P, \text{ with } n_P \in \mathbb{Z}, \text{ almost all } n_P = 0.$$

The support of the divisor D is defined as $\mathrm{supp}(D) := \{P \in \mathbb{P}_F : n_P \neq 0\}$. *We shall often write*

$$D = \sum_{P \in S} n_P P,$$

where S is a finite set with $\mathrm{supp}(D) \subseteq S$. *A divisor $D = P$ with $P \in \mathbb{P}_F$ is called a prime divisor of $F|K$. The addition of divisors is done coefficient-wise: if $D = \sum n_P P$ and $D' = \sum n'_P P$, then $D + D' = \sum (n_P + n'_P) P$. The zero element of the group is simply the divisor where all coefficients are* 0.

We can also define the discrete valuation of a divisor: for $Q \in \mathbb{P}_F$ and $D = \sum n_P P \in \mathrm{Div}(F)$, we define $v_Q(D) = n_Q$. This allows us to rewrite

$$\mathrm{supp}(D) = \{P \in \mathbb{P}_F : v_P(D) \neq 0\} \text{ and } D = \sum_{P \in \mathrm{supp}(D)} v_P(D) \cdot P.$$

A partial ordering can be defined in $\mathrm{Div}(F)$ *by*

$$D_1 \leqslant D_2 \iff v_P(D_1) \leqslant v_P(D_2) \text{ for all } P \in \mathbb{P}_F.$$

If $D_1 \leqslant D_2$ and $D_1 \neq D_2$, we write $D_1 < D_2$. A divisor $D \geqslant 0$ is called effective. The degree of a divisor is defined as

$$\deg D := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot \deg P,$$

which yields a homomorphism from $\mathrm{Div}(F)$ *to $\mathbb{Z}$ due to the way addition was defined.*

Corollary 5 assures an element $x \in F^*$ has only finitely many zeros and poles in $\mathbb{P}_F$, thus allowing us to define the following:

Definition 9. *Let $x \in F^*$. Denote by $Z \subseteq \mathbb{P}_F$ the set of zeros of x and by $N \subseteq \mathbb{P}_F$ the set of poles of x. We define*

$$\begin{aligned}(x)_0 &:= \sum_{P \in Z} v_P(x) P, \text{ the zero divisor of } x,\\ (x)_\infty &:= \sum_{P \in N} -v_P(x) P, \text{ the pole divisor of } x,\\ (x) &:= (x)_0 - (x)_\infty, \text{ the principal divisor of } x.\end{aligned}$$

It follows from the definitions that $(x)_0 \geqslant 0,\ (x)_\infty \geqslant 0$ and

$$(x) = \sum_{P \in \mathbb{P}_F} v_P(x)P.$$

From Corollary 2, the constant elements $x \in F^*$ are characterized by

$$x \in K \iff (x) = 0.$$

Definition 10. *The set*

$$\mathrm{Princ}(F) := \{(x) : x \in F^*\}$$

is called the group of principal divisors of $F|K$. It is a subgroup of $\mathrm{Div}(F)$ *since for $x, y \in F^*$:*

$$(xy) = \sum_{P \in \mathbb{P}_F} v_P(xy)P = \sum_{P \in \mathbb{P}_F} (v_P(x) + v_P(y))P = (x) + (y).$$

The factor group $\mathrm{Cl}(F) := \mathrm{Div}(F)/\mathrm{Princ}(F)$ *is called the divisor class group of F. For a divisor $D \in \mathrm{Div}(F)$, its corresponding element in* $\mathrm{Cl}(F)$ *is denoted by $[D]$, the divisor class of D. Two divisors D, D' are said to be linearly equivalent, denoted by $D \sim D'$, if $[D] = [D']$, that is $D = D' + (x)$ for some $x \in F^*$. This is an equivalence relation.*

Remark 3. *We shall prove shortly that all principal divisors have degree 0. Thus, considering the subgroup* $\mathrm{Div}^0(F)$ *of degree 0 divisors, we obtain the quotient group* $\mathrm{Cl}^0(F) := \mathrm{Div}^0(F)/\mathrm{Princ}(F)$ *whose order $h := |\mathrm{Cl}^0(F)|$ is called the class number of F. We shall later prove that if K is a finite field, then the class number h is always finite.*

The next definition will play an important role in both the further study of function fields and the construction of lattices.

Definition 11. *For a divisor $A \in \mathrm{Div}(F)$, we define the Riemann-Roch space associated to A as*

$$\mathcal{L}(A) = \{x \in F : (x) \geqslant -A\} \cup \{0\}.$$

We can interpret this definition in the following way: if

$$A = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$$

with $n_i, m_j > 0$, then $\mathcal{L}(A)$ is the set of elements of F such that

- x has zeros of order bounded below by m_j at Q_j for $j = 1, \ldots, s$, and
- x has poles only at $P_1, \ldots, P_r$ with the order at P_i bounded above by n_i for $i = 1, \ldots, r$.

Remark 4. *If $A \in \mathrm{Div}(F)$, then*

(a) $x \in \mathcal{L}(A) \iff v_P(x) \geqslant -v_P(A)$ *for all* $P \in \mathbb{P}_F$.

(b) $\mathcal{L}(A) \neq \{0\} \iff \exists A' \in \mathrm{Div}(F)$ *such that* $A' \geqslant 0$ *and* $A' \sim A$.

These observations, although simple, will often be quite useful when discussing Riemann-Roch spaces.

Lemma 3. *(a)* $\mathcal{L}(A)$ *is a vector space over* K.

(b) If $A' \in \mathrm{Div}(F)$ *is such that* $A' \sim A$, *then* $\mathcal{L}(A)$ *and* $\mathcal{L}(A')$ *are isomorphic as vector spaces over* K.

Proof. (a) Let $x, y \in \mathcal{L}(A)$ and $a \in K$. For all $P \in \mathbb{P}_F$:

$$v_P(x + ay) \geqslant \min\{v_P(x), v_P(ay)\} = \min\{v_P(x), v_P(y)\} \geqslant -v_P(A),$$

thus $x + ay \in \mathcal{L}(A)$ by Remark 4(a).

(b) By hypothesis $A = A' + (z)$ with $Z \in F^*$. Consider the map

$$\begin{aligned} \varphi : \mathcal{L}(A) &\to F \\ x &\mapsto xz. \end{aligned}$$

This is a K-linear map. Also, $\varphi(\mathcal{L}(A)) \subseteq \mathcal{L}(A')$ since $v_P(x) \geqslant -v_P(A' + (z)) = -v_P(A') - v_P(z)$ implies

$$v_P(xz) = v_P(x) + v_P(z) \geqslant -v_P(A') - v_P(z) + v_P(z) = -v_P(A')$$

and $xz \in \mathcal{L}(A')$. In the same way, we can define

$$\begin{aligned} \varphi' : \mathcal{L}(A') &\to F \\ x &\mapsto xz^{-1}, \end{aligned}$$

which is another K-linear map. Its image is contained in $\mathcal{L}(A)$. Since these two maps are inverses of each other, φ is the desired isomorphism between $\mathcal{L}(A)$ and $\mathcal{L}(A')$.

□

Lemma 4. *(a)* $\mathcal{L}(0) = K$.

(b) If $A < 0$, *then* $\mathcal{L}(A) = \{0\}$.

Proof. (a) We know $(x) = 0$ for $x \in K^*$, which implies $K \subseteq \mathcal{L}(0)$. On the other hand, if $x \in \mathcal{L}(0)$ is a non-zero element, then $(x) \geqslant 0$. This means x has no poles, and thus $x \in K$ by Corollary 2.

(b) Suppose there exists a non-zero $x \in \mathcal{L}(A)$. Then $(x) \geqslant -A > 0$, meaning x has at least one zero, but no pole, which is impossible.

□

Our next objective will be to show that the dimension of $\mathcal{L}(A)$ as a K-vector spaces is always finite.

Lemma 5. *Let $A, B \in \mathrm{Div}(F)$ with $A \leqslant B$. Then $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ and*

$$\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leqslant \deg B - \deg A.$$

Proof. If $x \in \mathcal{L}(A)$, then $(x) \geqslant -A \geqslant -B$, and thus $\mathcal{L}(A) \subseteq \mathcal{L}(B)$. In order to prove the other result, we may assume $B = A + P$ for some prime divisor $P \in \mathbb{P}_F$. Since we can reach B from A by adding a finite number of prime divisors, the general case will then follow by induction. Pick an element $t \in F$ such that $v_P(t) = v_P(B) = v_P(A) + 1$. For $x \in \mathcal{L}(B)$: $v_P(x) \geqslant -v_P(B) = -v_P(t)$, so $v_P(xt) \geqslant 0$ and $xt \in \mathcal{O}_P$. Thus, we have a K- linear map

$$\begin{aligned} \psi : \mathcal{L}(B) &\to F_P \\ x &\mapsto (xt)(P). \end{aligned}$$

Note that $x \in \ker\psi \iff xt \in P \iff v_P(xt) > 0 \iff v_P(x) \geqslant -v_P(A)$, since

$$v_P(xt) = v_P(A) + 1 + v_P(x) > 0 \iff v_P(x) > -v_P(A) - 1 \iff v_P(x) \geqslant -v_P(A),$$

meaning $\ker\psi = \mathcal{L}(A)$. Therefore, ψ induces an injective K-linear map from $\mathcal{L}(B)/(A)$ to F_P, therefore

$$\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leqslant \dim F_P = \deg P = \deg B - \deg A. \qquad \square$$

Proposition 5. *For each $A \in \mathrm{Div}(F)$, $\mathcal{L}(A)$ is a finite-dimensional vector space over K. More precisely, if $A = A_+ - A_-$ with positive divisors A_+ and A_-, then $\dim\mathcal{L}(A) \leqslant \deg A_+ + 1$.*

Proof. Since $A \leqslant A_+$, $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$ and it is sufficient to show that $\dim\mathcal{L}(A_+) \leqslant \deg A_+ + 1$. A_+ being a positive divisor, we have $0 \leqslant A_+$ and Lemma 5 yields $\dim(\mathcal{L}(A_+)/\mathcal{L}(0)) \leqslant \deg A_+$. Since $\mathcal{L}(0) = K$, we conclude

$$\dim\mathcal{L}(A_+) = \dim(\mathcal{L}(A_+)/\mathcal{L}(0)) + 1 \leqslant \deg A_+ + 1. \qquad \square$$

Definition 12. *For $A \in \mathrm{Div}(F)$ the integer $\ell(A) := \dim\mathcal{L}(A)$ is called the dimension of the divisor A.*

Calculating the dimension of a divisor is a very important problem both in algebraic function field theory and lattice construction. In order to build up to a result which will allow us to compute this dimension, the Riemann-Roch Theorem, we start by proving the following fact: an element $x \in F^*$ has the same number of zeros and poles counted with their multiplicities.

Theorem 6. *All principal divisors have degree zero. More precisely, if $x \in F\backslash K$, then* $\deg(x)_0 = \deg(x)_\infty = [F : K(x)]$.

Proof. Take $n := [F : K(x)]$ and

$$B := (x)_\infty = \sum_{i=1}^{r} -v_{P_i}(x) \deg P_i,$$

where $P_1, \ldots, P_r$ are the poles of x. Then

$$\deg B = \sum_{i=1}^{r} v_{P_i}(x^{-1}) \cdot \deg P_i \leqslant [F : K(x)] = n$$

by Proposition 4. It only remains to show $n \leqslant \deg B$. To this effect, choose a basis $u_1, \ldots, u_n$ of $F|K(x)$ and a divisor $C \geqslant 0$ such that $(u_i) \geqslant -C$ for all $i = 1, \ldots, n$. Given an integer $l > 0$, consider the elements $x^i u_j$ for $0 \leqslant i \leqslant l$ and $1 \leqslant j \leqslant n$. From $(u_j) \geqslant -C$ and $(x) \geqslant -B$, we have

$$(x^i u_j) = i \cdot (x) + (u_j) \geqslant -iB - C \geqslant -(lB + C) \implies x^i u_j \in \mathcal{L}(lB + C).$$

Furthermore, all $x^i u_j$ are linearly independent over K, since $u_1, \ldots, u_n$ are linearly independent over $K(x)$. Thus, $\ell(lB + C) \geqslant n(l + 1)$. Setting $c := \deg C$ and applying Proposition 5, we get $n(l + 1) \leqslant \ell(lB + C) \leqslant l \cdot \deg B + c + 1$, meaning

$$l(\deg B - n) \geqslant n - c - 1 \tag{1.10}$$

for all $l \in \mathbb{N}$. Since the right side is independent of l, (1.10) is only possible when $\deg B \geqslant n$. This proves that $\deg(x)_\infty = [F : K(x)]$, but since $(x)_0 = (x^{-1})_\infty$, we conclude $\deg(x)_0 = \deg(x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)]$. □

Definition 13. *The degree of a function $z \in F\backslash K$ is defined as*

$$\deg(z) := \deg(z)_0 = \deg(z)_\infty$$

and can be computed in the following ways:

$$\deg(z) = \sum_{\substack{P \in \mathbb{P}_F \\ v_P(z) > 0}} v_P(z) \cdot \deg P = \frac{1}{2} \sum_{P \in \mathbb{P}_F} |v_P(z)| \cdot \deg P.$$

Definition 14. *The positive integer $\gamma := \min\{[F : K(x)] : x \in F\}$ is called the gonality of $F|K$.*

In light of Theorem 6, the gonality can also be interpreted as the smallest degree of a non-constant function of F.

Corollary 6. *(a) Let $A, A' \in \mathrm{Div}(F)$ with $A \sim A'$. Then $\ell(A) = \ell(A')$ and $\deg A = \deg A'$.*

(b) If $\deg A < 0$, then $\ell(A) = 0$.

(c) For $A \in \mathrm{Div}(F)$ with $\deg A = 0$, the following are equivalent

1. *A is a principal divisor.*
2. *$\ell(A) \geqslant 1$.*
3. *$\ell(A) = 1$.*

Proof. (a) $\ell(A) = \ell(A')$ follows from the fact that $\mathcal{L}(A) \simeq \mathcal{L}(A')$, as proved in Lemma 3. And from Theorem 6, for some $x \in F^*$: $A = A' + (x) \implies \deg A = \deg A' + \deg((x)) = \deg A'$.

(b) Suppose $\ell(A) > 0$. Remark 4 implies there exists some divisor $A' \geqslant 0$ such that $A' \sim A$, hence $\deg A = \deg A' \geqslant 0$.

(c) (1) $\Rightarrow$ (2): if $A = (x)$, then $(x^{-1}) = -A$ and $x^{-1} \in \mathcal{L}(A)$, so $\ell(A) \geqslant 1$.
(2) $\Rightarrow$ (3): suppose $\deg A = 0$ and $\ell(A) \geqslant 1$. By Remark 4(b), $A \sim A'$ for some $A' \geqslant 0$. The conditions $A' \geqslant 0$ and $\deg A' = 0$ imply $A' = 0$. Therefore, $\ell(A) = \ell(A') = \ell(0) = 1$.
(3) $\Rightarrow$ (1): Suppose $\deg A = 0$ and $\ell(A) = 1$. Take a non-zero $z \in \mathcal{L}(A)$, then $(z) + A \geqslant 0$. Seeing as $\deg((z) + A) = \deg((z)) + \deg A = 0$, it follows that $(z) + A = 0$ and $A = -(z) = (z^{-1})$ and A is principal. □

Example 2. *Consider the rational function field $F = K(x)$. For a non-zero $z \in K(x)$, we have $z = a \cdot f(x)/g(x)$ with $a \in K^*$, $f(x), g(x) \in K[x]$ monic ans relatively prime with*

$$f(x) = \prod_{i=1}^{r} p_i(x)^{r_i}, \ g(x) = \prod_{j=1}^{s} q_j(x)^{m_j}$$

where $p_i(x), q_j(x) \in K[x]$ are pairwise distinct, irreducible and monic. Then $(z) \in \mathrm{Div}(F)$ has the form

$$(z) = \sum_{i=1}^{r} n_i P_{p_i(x)} - \sum_{j=1}^{s} m_j P_{q_j(x)} + (\deg g(x) - \deg f(x)) P_\infty.$$

Therefore, in arbitrary function fields, the principal divisors can be considered as substitutes for the decomposition into irreducible polynomials from the rational function field.

For an arbitrary function field $F|K$, in Proposition 5 we have showed that

$$\ell(A) \leqslant 1 + \deg A \tag{1.11}$$

for all $A \geqslant 0$. However, (1.11) in fact holds for every divisor of positive degree. To verify this, we may assume $\ell(A) > 0$. Then $A \sim A'$ for some $A' \geqslant 0$ by Remark 4, so $\ell(A) = \ell(A') \leqslant 1 + \deg A' = 1 + \deg A$ by Corollary 6.

Proposition 6. *For all $A \in \mathrm{Div}(F)$ there is a constant $\gamma \in \mathbb{Z}$, independent of A, such that $\deg A - \ell(A) \leqslant \gamma$.*

Proof. Firstly, we observe that applying Lemma 5 for $A_1 \leqslant A_2$ yields

$$\deg A_1 - \ell(A_1) \leqslant \deg A_2 - \ell(A_2). \tag{1.12}$$

Fix $x \in F\backslash K$ and set $B := (x)_\infty$. Like in the proof of Theorem 6, there exists a divisor $C \geqslant 0$ depending on x such that $\ell(lB + C) \geqslant (l+1) \cdot \deg B$ for all $l \geqslant 0$. On the other hand, $\ell(lB + C) \leqslant \ell(lB) + \deg C$ according to Lemma 5. Combining these inequalities produces

$$\ell(lB) \geqslant (l+1)\deg B - \deg C = \deg(lB) + [F : K(x)] - \deg C.$$

In other words, $\deg(lB) - \ell(lB) \leqslant \gamma$ for all $l > 0$ with some $\gamma \in \mathbb{Z}$. We wish to prove that this inequality still holds if we substitute lB for any $A \in \mathrm{Div}(F)$ with the same γ.

In order to achieve this, we first show that given $A \in \mathrm{Div}(F)$, there exists $A_1, D \in \mathrm{Div}(F)$ and an integer $l \geqslant 0$ such that $A \leqslant A_1$, $A_1 \sim D$ and $D \leqslant lB$. Choose a positive divisor A_1 with $A_1 \geqslant A$. Then, for sufficiently large l,

$$\ell(lB - A_1) \geqslant \ell(lB) - \deg A_1 \geqslant \deg(lB) - \gamma - \deg A_1 > 0,$$

where the first inequality follows from Lemma 5. Thus there is some non-zero $z \in \mathcal{L}(lB - A_1)$. Setting $D := A_1 - (z)$, we have proved the claim, since $A_1 \sim D$ and $D \leqslant A_1 - (A_1 - lB) = lB$.

Using this auxiliary result, the proposition follows:

$$\deg A - \ell(A) \overset{(1.12)}{\leqslant} \deg A_1 - \ell(A_1) \overset{\text{Cor.6}}{=} \deg D - \ell(D) \overset{(1.12)}{\leqslant} \deg(lB) - \ell(lB) \leqslant \gamma.$$

□

Definition 15. *The genus g of a function field $F|K$ is defined as*

$$g := \max\{\deg A - \ell(A) + 1 : A \in \mathrm{Div}(F)\}.$$

Proposition 6 assures this definition makes sense. In fact, the genus is the single most important invariant of a function field.

Corollary 7. *The genus g of $F|K$ is a non-negative integer.*

Proof. Taking $A = 0$ in the definition of g produces $g \geqslant \deg(0) - \ell(0) + 1 = 0$. □

Theorem 7 (Riemann's Theorem)**.** *Let $F|K$ be a function field of genus g. Then*

(a) For all $A \in \mathrm{Div}(F)$, $\ell(A) \geqslant \deg A + 1 - g$.

(b) There is $c \in \mathbb{Z}$ depending only on the function field such that $\ell(A) = \deg A + 1 - g$ if $\deg A \geqslant c$.

Proof. (a) Follows directly from the definition of the genus.

(b) Choose $A_0 \in \mathrm{Div}(F)$ with $g = \deg A_0 - \ell(A_0) + 1$ and set $c := \deg A_0 + g$. If $\deg A \geqslant c$, then

$$\ell(A - A_0) \geqslant \deg(A - A_0) + 1 - g \geqslant c - \deg A_0 + 1 - g = 1,$$

which means there is a non-zero $z \in \ell(A - A_0)$. Take $A' := A + (z)$, then $A' \geqslant A_0$ and

$$\deg A - \ell(A) \overset{\text{Cor. 6}}{=} \deg A' - \ell(A') \overset{\text{Lemma 5}}{\geqslant} \deg A_0 - \ell(A_0) = g - 1.$$

Therefore $\ell(A) \leqslant \deg A + 1 - g$.

□

Example 3. *We will show the rational function field $F = K(x)$ has genus $g = 0$. Take P_∞ the pole divisor of x and consider for $r \geqslant 0$ the vector space $\mathcal{L}(rP_\infty)$. For $0 \leqslant i \leqslant r$ we have $(x^i) = i \cdot (x) \geqslant -iP_\infty \geqslant -rP_\infty$, thus $1, x, \ldots, x^r \in \mathcal{L}(rP_\infty)$. This observation yields*

$$r + 1 \leqslant \ell(rP_\infty) = \deg(rP_\infty) + 1 - g = r + 1 - g$$

if r is sufficiently large, implying $g \leqslant 0$, and finally $g = 0$.

1.5 Functions Fields of Algebraic Curves

Up until now, we have studied functions fields as completely independent and abstract mathematical objects. This section aims to establish the connection between the theories of function fields and algebraic curves and provide different interpretations for previously discussed concepts which will assist us during the construction of the Fermat Function Field Lattice.

We begin by presenting some basic definitions from algebraic geometry.

Definition 16. *Let K be a field. The n-dimensional affine space $\mathbb{A}^n = \mathbb{A}^n(K)$ is the set of n-tuples of elements of K.*

If $K[X_1, \ldots, X_n]$ is the ring of polynomials in n variables over K, a subset $V \subseteq \mathbb{A}^n$ is algebraic if there exists a set of polynomials $M \subseteq K[X_1, \ldots, X_n]$ such that

$$V = \{P \in \mathbb{A}^n : F(P) = 0 \text{ for all } F \in M\}.$$

Given an algebraic set $V \subseteq \mathbb{A}^n$, the set of polynomials

$$I(V) = \{F \in K[X_1, \ldots, X_n] : F(P) = 0 \text{ for all } P \in V\}$$

is called the ideal of V. Evidently, it is an ideal of $K[X_1, \ldots, X_n]$, and can be generated by finitely many polynomials $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$. Thus

$$V = \{P \in \mathbb{A}^n : F_1(P) = \cdots = F_r(P) = 0\}.$$

We denote the zero locus of these polynomials as $V = V(F_1, \ldots, F_r)$. V is said to be irreducible if it cannot be written as $V = V_1 \cup V_2$ with V_1, V_2 proper algebraic subsets of V. This corresponds to $I(V)$ being a prime ideal. An irreducible algebraic set $V \subseteq \mathbb{A}^n$ is called an affine variety.

Given an affine variety V, the residue class ring $\Gamma(V) : K[X_1, \ldots, X_n]/I(V)$ is called the coordinate ring of V. Every $f = F + I(V) \in \Gamma(V)$ induces a function $f : V \to K$ by setting $f(P) := F(P)$. Since $I(V)$ is a prime ideal, $\Gamma(V)$ is an integral domain and one can consider the quotient field

$$K(V) := \mathrm{Quot}(\Gamma(V)),$$

called the function field of V. It contains K as a subfield and the dimension of V is the transcendence degree of the field extension $K(V)|K$.

For a point $P \in V$, define

$$\mathcal{O}_P(V) = \{f \in K(V) : f = g/h \text{ for } g, h \in \Gamma(V) \text{ and } h(P) \neq 0\}.$$

This is a local ring whose quotient field is $K(V)$, and unique maximal ideal is

$$M_P(V) = \{f \in K(V) : f = g/h \text{ for } g, h \in \Gamma(V),\ h(P) \neq 0 \text{ and } g(P) = 0\}.$$

$\mathcal{O}_P(V)$ is called the local ring of V at P. For $f = g/h \in \mathcal{O}_P(V)$, the value of f at P is defined as $f(P) := g(P)/h(P)$.

Definition 17. *Take the set $\mathbb{A}^{n+1} \backslash \{(0, \ldots, 0)\}$ and define the equivalence relation $\sim$ as*

$$(a_0, \ldots, a_n) \sim (b_0 \ldots, b_n) \iff b_i = \lambda a_i \text{ for some } \lambda \in K^*.$$

The equivalence class of $(a_0, \ldots, a_n)$ with respect to $\sim$ is denoted by $(a_0 \colon \ldots : a_n)$. The n-dimensional projective space is the set of all equivalence classes

$$\mathbb{P}^n = \{(a_0 \colon \ldots : a_n) : a_i \in K,\ \text{not all } a_i = 0\}.$$

A polynomial $F \in K[X_0, \ldots, X_n]$ is said to be homogeneous of degree d if it is a sum of monomials of the same degree d. An ideal $I \subseteq K[X_0, \ldots, X_n]$ generated by homogeneous polynomials is called a homogeneous ideal.

Let $P = (a_0 \colon \ldots \colon a_n) \in \mathbb{P}^n$ and let $F \in K[X_0, \ldots, X_n]$ be a homogeneous polynomial with $\deg F = d$. We say that $F(P) = 0$ if $F(a_0, \ldots, a_n) = 0$, which makes sense given that

$$F(\lambda a_0, \ldots, \lambda a_n) = \lambda^d \cdot F(a_0, \ldots, a_n),$$

and thus $F(a_0, \ldots, a_n) = 0 \iff F(\lambda a_0, \ldots, \lambda a_n) = 0$.

Projective algebraic sets, irreducibility and projective varieties are defined as in the affine case.

Given a non-empty projective variety $V \subseteq \mathbb{P}^n$, its homogeneous coordinate ring is

$$\Gamma_H(V) := K[X_0, \ldots, X_n]/I(V),$$

which is an integral domain containing K. An element $f \in \Gamma_H(V)$ is called a form of degree d if $f = F + I(V)$ for some homogeneous $F \in K[X_0, \ldots, X_n]$ with $\deg F = d$. The function field of V is defined as

$$K(V) = \{g/h : g, h \in \Gamma_H(V) \text{ are forms of the same degree and } h \neq 0\}.$$

Once again, the dimension of V is defined as the transcendence degree of $K(V)|K$. Given $f = g/h \in K(V)$, we can evaluate f at $P = (a_0 \colon \ldots \colon a_n) \in \mathbb{P}^n$ by making $f = (G + I(V))/(H + I(V))$, where G, H are polynomials of the same degree and setting $f(P) = G(a_0, \ldots, a_n)/H(a_0, \ldots, a_n)$ if $H(P) \neq 0$, since

$$\frac{G(\lambda a_0, \ldots, \lambda a_n)}{H(\lambda a_0, \ldots, \lambda a_n)} = \frac{\lambda^d \cdot G(a_0, \ldots, a_n)}{\lambda^d \cdot H(a_0, \ldots, a_n)} = \frac{G(a_0, \ldots, a_n)}{H(a_0, \ldots, a_n)}.$$

The ring

$$\mathcal{O}_P(V) = \{f \in K(V) : f \text{ is defined at } P\}$$

is a local ring with maximal ideal

$$M_P(V) = \{f \in \mathcal{O}_P(V) : f(P) = 0\}.$$

Given the two previous definitions, we notice that any projective variety can be covered by affine varieties such that some properties are preserved. We do this in the following way: for $0 \leqslant i \leqslant n$, consider the mapping $\varphi_i : \mathbb{A}^n \to \mathbb{P}^n$ given by

$$\varphi_i(a_0 \colon \ldots \colon a_n) = (a_0 \colon \ldots \colon a_{i-1} \colon 1 \colon a_{i+1} \colon \ldots \colon a_n).$$

This is a bijection from $\mathbb{A}^n$ to $U_i = \{(c_0 \colon \ldots \colon c_n) \in \mathbb{P}^n : c_i \neq 0\}$, and $\mathbb{P}^n = \bigcup_{i=0}^{n} U_i$, meaning the n-dimensional projective space is covered (with overlap) by $n + 1$ copies of the affine space $\mathbb{A}^n$.

Let $V \subseteq \mathbb{P}^n$ be a projective variety, then $V = \bigcup_{i=0}^{n}(V \cap U_i)$. Suppose $V \cap U_i \neq \varnothing$ and define

$$V_i := \varphi_i^{-1}(V \cap U_i) \subseteq \mathbb{A}^n.$$

V_i is an affine variety whose ideal $I(V_i)$ is given by

$$I(V_i) = \{F(X_0, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n) : F \in I(V)\}.$$

For convenience, we restrict ourselves to the case $i = n$ and $V \cap U_n \neq \varnothing$. The set $H_n = \mathbb{P}^n \backslash U_n = \{(a_0 \colon \ldots \colon a_n) \in \mathbb{P}^n : a_n = 0\}$ is called the hyperplane at infinity.

A notable consequence of this construction is that the function fields of the projective variety V and the affine variety V_n are isomorphic. Let $f = g/h \in K(V)$, where $g, h \in \Gamma_H(V)$ are forms of the same degree and $h \neq 0$. Choose homogeneous polynomials $G, H \in K[X_0, \ldots, X_n]$ such that $g = G + I(V)$ and $h = H + I(V)$. Define $G_* := G(X_0, \ldots, X_{n-1}, 1),\ H_* := H(X_0, \ldots, X_{n-1}, 1) \in K[X_0, \ldots, X_{n-1}]$ and denote their residue classes in $\Gamma(V_n)$ by g_* and h_*, respectively. The isomorphism is given by

$$\begin{aligned} \alpha : K(V) &\to K(V_n) \\ \frac{g}{h} &\mapsto \frac{g_*}{h_*}. \end{aligned}$$

Under α, the local ring of a point $P \in V \cap U_n$ is mapped onto the local ring of $\varphi_n^{-1}(P) \in V_n$, hence the local rings are also isomorphic.

We can also construct the projective closure of an affine variety. In order to do that, first consider a polynomial $F = F(X_0, \ldots, X_{n-1}) \in K[X_0, \ldots, X_{n-1}]$ of degree d. We can turn it into a homogeneous polynomial of degree d in $n+1$ variables by setting

$$F^* := X_n^d \cdot F(X_0/X_n, \ldots, X_{n-1}/X_n) \in K[X_0, \ldots, X_n].$$

Now consider an affine variety $V \subseteq \mathbb{A}^n$ and its corresponding ideal $I(V) \subseteq K[X_0, \ldots, X_{n-1}]$. Define the projective variety $\bar{V}$ as:

$$\bar{V} := \{P \in \mathbb{P}^n : F^*(P) = 0 \text{ for all } F \in I(V)\}.$$

The variety $\bar{V}$ is called the projective closure of V. It is possible to recover V from $\bar{V}$ by the process we just outlined:

$$V = \varphi_n^{-1}(\bar{V} \cap U_n) = \bar{V}_n.$$

It follows that the function fields of V and $\bar{V}$ are isomorphic, and both varieties have the same dimension.

We now turn our attention to a specific class of maps between varieties.

Definition 18. *Let $V \subseteq \mathbb{P}^m$ and $W \subseteq \mathbb{P}^n$ be projective varieties. If $F_0, \ldots, F_n \in K[X_0, \ldots, X_m]$ are homogeneous polynomials such that*

(a) $F_0, \ldots, F_n$ have the same degree

(b) not all F_i are in $I(V)$

(c) $H(F_0, \ldots, F_n) \in I(V)$ for all $H \in I(W)$.

Take a point $Q \in V$ such that $F_i(Q) \neq 0$ for at least one $i \in \{0, \ldots, n\}$ (by (b), such point exists). Then, the point $(F_0(Q) \colon \ldots \colon F_n(Q)) \in \mathbb{P}^n$ lies in W by (c). If $(G_0, \ldots, G_n)$ is another n-tuple of polynomials satisfying (a), (b) and (c), we say that $(F_0, \ldots, F_n)$ and $(G_0, \ldots, G_n)$ are equivalent if

(d) $F_iG_j - F_jG_i \in I(V)$ for all $0 \leqslant i, j \leqslant n$.

The equivalence class of $(F_0, \ldots F_n)$ with respect to this equivalence relation is $\phi = (F_0 \colon \ldots \colon F_n)$ and ϕ is called a rational map from V to W.

A rational map $\phi = (F_0 \colon \ldots \colon F_n)$ is regular at the point $P \in V$ if there exist homogeneous polynomials $G_0, \ldots, G_n \in K[X_0, \ldots, X_m]$ such that $\phi = (G_0 \colon \ldots \colon G_n)$ and $G_i(P) \neq 0$ for at least one i. Then we can set

$$\phi(P) = (G_0(P), \ldots, G_n(P)) \in W,$$

which is well-defined by (a) and (d).

Two varieties V_1 and V_2 are birationally equivalent if there are rational maps $\phi_1 : V_1 \to V_2$ and $\phi_2 : V_2 \to V_1$ such that $\phi_1 \circ \phi_2$ and $\phi_2 \circ \phi_1$ are the identity maps on the points at which they are regular. Moreover, V_1 and V_2 are birationally equivalent if and only if the function fields $K(V_1)$ and $K(V_2)$ are K-isomorphic.

A rational map $\phi : V \to W$ which is regular at all points $P \in V$ is called a morphism. It is called an isomorphism if there is a morphism $\psi : W \to V$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity maps on W and V, respectively. In this case, the varieties V and W are said to be isomorphic.

Definition 19. *A projective (affine) algebraic curve V is a projective (affine) variety of dimension 1. This implies that the field $K(V)$ is an algebraic function field of one variable.*

A point $P \in V$ is non-singular if the local ring $\mathcal{O}_P(V)$ is a discrete valuation ring, that is, a principal ideal domain with exactly one maximal ideal. In a given curve, there are only finitely many singular points. The curve V is called non-singular if all of its points are non-singular.

A plane affine curve is an affine curve $V \subseteq \mathbb{A}^2$. Its ideal $I(V) \subseteq K[X_0, X_1]$ is generated by a unique irreducible polynomial $G \in K[X_0, X_1]$. Conversely, given an irreducible polynomial $G \in K[X_0, X_1]$, the set $V = \{P \in \mathbb{A}^2 : G(P) = 0\}$ is a plane affine curve, and G generates $I(V)$. A point $P \in V$ is non-singular if and only of

$$\frac{\partial G}{\partial X_0}(P) \neq 0 \text{ or } \frac{\partial G}{\partial X_1}(P) \neq 0.$$

Similarly, the ideal of a plane projective curve $V \subseteq \mathbb{P}^2$ is generated by an irreducible homogeneous polynomial $H \in K[X_0, X_1, X_2]$. A point $P \in V$ is non-singular if at least one of the partial derivatives of H at P is not zero.

If $V = \{P \in \mathbb{A}^2 : G(P) = 0\}$ is a plane affine curve with $G \in K[X_0, X_1]$ an irreducible polynomial of degree d, then the projective closure of $\bar{V} \subseteq \mathbb{P}^2$ is the zero locus of the homogeneous polynomial $G_* = X_2^d \cdot G(X_0/X_2, X_1/X_2)$.

If we consider rational maps $\phi : V \to W$ between two projective curves, the following hold

(a) ϕ is regular at all non-singular points of V. In particular, if V is non-singular, ϕ is a morphism.

(b) If V is non-singular and ϕ is non-constant, then ϕ is surjective.

Singular points may present a problem when studying certain properties algebraic curves. For this reason, we often make use of the non-singular model of a curve: given V a projective curve, there exists a non-singular projective curve V' and a birational morphism $\phi' : V' \to V$, that is, every projective curve is birationally equivalent to a non-singular projective curve. The pair (V', ϕ') is unique in the sense that if given another non-singular curve V'' and birational morphism $\phi'' : V'' \to V$, there exists a unique isomorphism $\phi : V' \to V''$ such that $\phi' = \phi'' \circ \phi$. Therefore, the pair (V', ϕ') is called the non-singular model of V.

This is particularly useful when studying function fields. Since V and V' are birationally equivalent, they have isomorphic function fields. This means one can always consider the non-singular model of any given curve, eliminating the problem of singular points.

The following theorem establishes a very important link between the theory of algebraic curves and the theory of algebraic function fields.

Theorem 8. *Let $F|K$ be an algebraic function field of one variable. There exists a non-singular projective curve V such that $K(V)$ is (K-isomorphic to) F.*

Proof. One can construct V as follows: choose $x, y \in F$ such that $F = K(x, y)$ (every algebraic function field is an extension of the rational function field). Let $G(X, Y) \in K[X, Y]$ be the irreducible polynomial with $G(x, y) = 0$. Let $W = \{P \in \mathbb{A}^2 : G(P) = 0\}$ and $\bar{W} \subseteq \mathbb{P}^2$ be the projective closure of W. Then, denoting by V the non-singular model of $\bar{W}$, it follows that $K(V) \simeq F$. □

Let V be a non-singular projective curve with $K(V) = F$. There is a $1-1$ correspondence between the points $P \in V$ and the places of $F|K$, given by $P \mapsto M_P(V)$, the maximal ideal of the local ring $\mathcal{O}_P(V)$. In particular, the points in the set

$$V(K) = V \cap \mathbb{P}^n(K) = \{(a_0 \colon \ldots \colon a_n) \in V : a_i \in K \text{ for all } i = 0, \ldots, n\},$$

called K-rational points of V each correspond to a rational place of F.

These correspondences allow us to translate some concepts of function fields over to algebraic curves and vice versa. For example

- The genus g of an algebraic curve is the same as the genus of its function field.
- If V is non-singular, a divisor of V is a formal sum of points $D = \sum_{P \in V} n_P P$, where $n_P \in \mathbb{Z}$, almost all $n_P = 0$. The degree of D is $\deg D = \sum_{P \in V} n_P$.
- The order of a function $f \in K(V)$ at a point $P \in V$ is defined to be $v_P(f)$, where v_P denotes the discrete valuation of $K(V)$ corresponding to the valuation ring $\mathcal{O}_P(V)$.
- The principal divisor (f) of a non zero function $f \in K(V)$ is $(f) = \sum_{P \in V} v_P(f) P$. The degree of a principal divisor is 0.
- For $D \in \mathrm{Div}(V)$, the space $\mathcal{L}(D)$ is defined as in the function field case

  $$\mathcal{L}(D) = \{f \in K(V) : (f) \geqslant -D\} \cup \{0\}.$$

  It is a finite-dimensional K-vector space, whose dimension $\ell(D)$ will be the main focus of the next section.

1.6 The Riemann-Roch Theorem

For this section, we always assume $F|K$ is an algebraic function field with genus g.

Definition 20. *For $A \in \mathrm{Div}(F)$, the integer $i(A) := \ell(A) - \deg A + g - 1$ is called the index of specialty of A.*

Theorem 7 states $i(A)$ is a non-negative integer and $i(A) = 0$ if $\deg A$ is sufficiently large.

Definition 21. *An adele of $F|K$ is a mapping*

$$\begin{aligned} \alpha : \mathbb{P}_F &\to F \\ P &\mapsto \alpha_P, \end{aligned}$$

such that $\alpha_P \in \mathcal{O}_P$ for almost all $P \in \mathbb{P}_F$. We consider an adele an element of the direct product $\prod_{P \in \mathbb{P}_F} F$ and use the notations $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ or $\alpha = (\alpha_P)$. The set

$$\mathcal{A}_F := \{\alpha : \alpha \text{ is an adele of } F|K\}$$

is called the adele space of $F|K$. Is will always be regarded as a vector space over K with operations defined in the usual way.

The principal adele of an element $x \in F$ is the adele where all components are equal to x. Since x has only finitely many poles, only finitely many components of the adele will not be in $\mathcal{O}_P$, hence this definition makes sense. This gives us an embedding $F \hookrightarrow \mathcal{A}_F$. Valuations from F are also naturally extended to $\mathcal{A}_F$ by setting $v_P(\alpha) = v_P(\alpha_P)$, where α_P is the P-component of the adele α. From the definition, $v_P(\alpha) \geqslant 0$ for almost all $P \in \mathbb{P}_F$.

Definition 22. *For $A \in \mathrm{Div}(F)$, we define the adele space of A as*

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F : v_P(\alpha) \geqslant -v_P(A) \text{ for all } P \in \mathbb{P}_F\}.$$

This is a K-subspace of $\mathcal{A}_F$.

Theorem 9. *For every $A \in \mathrm{Div}(F)$, the index of specialty is*

$$i(A) = \dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)).$$

Note that even though F, $\mathcal{A}_F$ and $\mathcal{A}_F(A)$ are infinite-dimensional vector spaces over K, the theorem states the dimension of the quotient space $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$ over K is finite.

Proof. First we prove that given $A_1, A_2 \in \mathrm{Div}(F)$ with $A_1 \leqslant A_2$, then $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ and

$$\dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) = \deg A_2 - \deg A_1. \tag{1.13}$$

The first claim is evident, since $\alpha \in \mathcal{A}_F(A_1)$ implies for all $P \in \mathbb{P}_F$:

$$v_P(\alpha) \geqslant -v_P(A_1) \geqslant -v_P(A_2) \implies \alpha \in \mathcal{A}_F(A_2).$$

For the second claim, as in the proof of Lemma 5, we only need to establish a proof for the case $A_2 = A_1 + P$, $P \in \mathbb{P}_F$ and the general case will follow by induction. Choose $t \in F$

such that $v_P(t) = v_P(A_2) = v_P(A_1) + 1$ and consider the K-linear map

$$\begin{aligned} \varphi : \mathcal{A}_F(A_2) &\to F_P \\ \alpha &\mapsto (t\alpha_P)(P). \end{aligned}$$

Note that $\alpha \in \ker\varphi \iff v_P(t\alpha_P) > 0 \iff v_P(\alpha) \geqslant -v_P(A_1)$, since

$$v_P(t\alpha_P) = v_P(A_1)+1+v_P(\alpha_P) > 0 \iff v_P(\alpha_P) > -v_P(A_1)-1 \iff v_P(\alpha) \geqslant -v_P(A_1),$$

meaning $\ker\varphi = \mathcal{A}_F(A_1)$. Furthermore, φ is surjective: take $x \in \mathcal{O}_P$ and define the adele

$$\alpha_Q = \begin{cases} t_Q^{-v_Q(A_2)+1}, \text{ if } Q \neq P \\ \dfrac{x}{t}, \text{ if } Q = P \end{cases}$$

where t_Q is a Q-prime element. For $Q \neq P$, we have

$$v_Q(\alpha_Q) = v_Q\left(t_Q^{-v_Q(A_2)+1}\right) = -v_Q(A_2) + 1 \geqslant -v_Q(A_2),$$

and for $Q = P$

$$v_P(\alpha_P) = v_P(x) - v_P(t) = v_P(x) - v_P(A_2) \geqslant -v_P(A_2),$$

since $v_P(x) \geqslant 0$. Thus, $\alpha \in \mathcal{A}_F(A_2)$ and $\varphi(\alpha) = x(P)$. We then conclude that $\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \simeq F_P$ and $\dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) = \deg P = \deg A_2 - \deg A_1$.

Now we prove that if $A_1, A_2 \in \mathrm{Div}(F)$ and $A_1 \leqslant A_2$, then

$$\dim((\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F)) = (\deg A_2 - \ell(A_2)) - (\deg A_1 - \ell(A_1)). \tag{1.14}$$

In order to prove this, consider the following sequence of linear mappings

$$0 \to \mathcal{L}(A_2)/\mathcal{L}(A_1) \xrightarrow{\sigma_1} \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \xrightarrow{\sigma_2} (\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F) \to 0, \tag{1.15}$$

where

$$\begin{aligned} \sigma_1 : \mathcal{L}(A_2)/\mathcal{L}(A_1) &\to \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \\ x + \mathcal{L}(A_1) &\mapsto x + \mathcal{A}_F(A_1) \end{aligned}$$

and

$$\begin{aligned} \sigma_2 : \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) &\to (\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F) \\ x + \mathcal{A}_F(A_1) &\mapsto x + (\mathcal{A}_F(A_1) + F). \end{aligned}$$

It follows directly from the definitions that σ_1 is injective and σ_2 is surjective. We now wish to show that $\mathrm{Im}(\sigma_1) = \ker(\sigma_2)$.

Take $\alpha \in \mathcal{A}_F(A_2)$ with $\sigma_2(\alpha + \mathcal{A}_F(A_1)) = 0$. Then $\alpha \in \mathcal{A}_F(A_1) + F$ and there is some $x \in F$ with $\alpha - x \in \mathcal{A}_F(A_1)$. Since $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$, we conclude $x \in \mathcal{A}_F(A_2) \cap F = \mathcal{L}(A_2)$.

Therefore, $\alpha + \mathcal{A}_F(A_1) = x + \mathcal{A}_F(A_1) = \sigma_1(x + \mathcal{L}(A_1))$ and $\alpha \in \mathrm{Im}(\sigma_1)$. On the other hand, if $y \in \mathrm{Im}(\sigma_1)$, then $y = x + \mathcal{A}_F(A_1)$, but $x + \mathcal{A}_F(A_1) \in \mathcal{A}_F(A_1) + F$. Thus $\sigma_2(y) = 0$ and $\mathrm{Im}(\sigma_1) = \ker(\sigma_2)$. This means the sequence (1.15) is exact and by using (1.13), we conclude

$$\begin{aligned}\dim((\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F)) &= \dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) - \dim(\mathcal{L}(A_2)/\mathcal{L}(A_1)) \\ &= (\deg A_2 - \deg A_1) - (\ell(A_2) - \ell(A_2)).\end{aligned}$$

Next we prove that if B is a divisor with $\ell(B) = \deg B + 1 - g$, then $\mathcal{A}_F = \mathcal{A}_F(B) + F$. Observe that for $B_1 \geqslant B$, Lemma 5 yields

$$\ell(B_1) \leqslant \deg B_1 + \ell(B) - \deg B = \deg B_1 + 1 - g.$$

Riemann's Theorem then shows that

$$\ell(B_1) = \deg B_1 + 1 - g \text{ for each } B_1 \geqslant B. \tag{1.16}$$

Let $\alpha \in \mathcal{A}_F$. We can find a divisor $B_1 \geqslant B$ such that $\alpha \in \mathcal{A}_F(B_1)$. By (1.14) and (1.16)

$$\begin{aligned}\dim((\mathcal{A}_F(B_1) + F)/(\mathcal{A}_F(B) + F)) &= (\deg B_1 - \ell(B_1)) - (\deg B - \ell(B)) \\ &= (g - 1) - (g - 1) = 0.\end{aligned}$$

This means $\mathcal{A}_F(B_1) + F = \mathcal{A}_F(B) + F$, and thus, $\alpha \in \mathcal{A}_F(B)$, proving our claim.

We are now ready to finish the proof. Take an arbitrary divisor A. By Theorem 7(b), there exists some $A_1 \geqslant A$ such that $\ell(A_1) = \deg A_1 + 1 - g$, then $\mathcal{A}_F = \mathcal{A}_F(A_1) + F$. Applying (1.14)

$$\begin{aligned}\dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)) &= \dim((\mathcal{A}_F(A_1) + F)/(\mathcal{A}_F(A) + F)) \\ &= (\deg A_1 - \ell(A_1)) - (\deg A - \ell(A)) \\ &= (g - 1) + \ell(A) - \deg A = i(A).\end{aligned}$$

□

This theorem can be restated as follows: for all $A \in \mathrm{Div}(F)$

$$\ell(A) = \deg A + 1 - g + \dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)).$$

As a corollary, we obtain another characterization for the genus.

Corollary 8. $g = \dim(\mathcal{A}_F/(\mathcal{A}_F(0) + F))$.

Proof. $i(0) = \ell(0) - \deg(0) + g - 1 = 1 - 0 + g - 1 = g$. □

We now introduce the concept of Weil differentials, which will provide a second interpretation of the index of specialty of a divisor.

Definition 23. *A Weil differential of $F|K$ is a K-linear map $\omega : \mathcal{A}_F \to K$ that vanishes on $\mathcal{A}_F(A) + F$ for some divisor $A \in \mathrm{Div}(F)$. The set*

$$\Omega_F := \{\omega : \omega \text{ is a Weil differential of } F|K\}$$

is called the module of Weil differentials of $F|K$. For $A \in \mathrm{Div}(F)$ let

$$\Omega_F(A) := \{\omega \in \Omega_F : \omega \text{ vanishes on } \mathcal{A}_F(A) + F\}.$$

We observe that Ω_F is a K-vector space. Indeed, if ω_1 vanishes on $\mathcal{A}_F(A_1) + F$ and ω_2 vanishes on $\mathcal{A}_F(A_2) + F$, the $\omega_1 + \omega_2$ vanishes on $\mathcal{A}_F(A_3) + F$ for any $A_3 \in \mathrm{Div}(F)$ with $A_3 \leqslant A_1$ and $A_3 \leqslant A_2$. Also, $a\omega_1$, $a \in K$ vanishes on $\mathcal{A}_F(A_1) + F$. With this, we regard $\Omega_F(A)$ a K-subspace of Ω_F.

Lemma 6. *For $A \in \mathrm{Div}(F)$, we have $\dim \Omega_F(A) = i(A)$.*

Proof. Let L denote the set of K-linear maps from $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$ to K and define

$$\begin{aligned} \psi : \Omega_F(A) &\to L \\ \omega &\mapsto \omega', \end{aligned}$$

where $\omega'(\alpha + (\mathcal{A}_F(A) + F)) = \omega(\alpha)$ for $\alpha \in \mathcal{A}_F$. From the definition of $\Omega_F(A)$, ψ is K-linear and bijective. Thus, $\Omega_F(A) \simeq L$. Since $\dim \Omega_F(A) = \dim L = \dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)) = i(A)$ by Theorem 9, our lemma follows. □

A direct consequence of this lemma is that $\Omega_F \neq \varnothing$. Choose $A \in \mathrm{Div}(F)$ with $\deg A \leqslant -2$. Then

$$\dim \Omega_F(A) = i(A) = \ell(A) - \deg A + g - 1 = 0 + 2 + g - 1 = g + 1 \geqslant 1,$$

hence $\Omega_F(A) \neq \varnothing$.

Definition 24. *For $x \in F$ and $\omega \in \Omega_F$, we define $x\omega : \mathcal{A}_F \to K$ by $(x\omega)(\alpha) := \omega(x\alpha)$.*

$x\omega$ is indeed a Weil differential of $F|K$, since if ω vanishes on $\mathcal{A}_F(A) + F$, then $x\omega$ vanishes on $\mathcal{A}_F(A + (x)) + F$. This definition gives Ω_F the structure of a vector space over F.

Proposition 7. *Ω_F is a one-dimensional vector space over F.*

Proof. Choose a non-zero $\omega_1 \in \Omega_F$. We must show that for any non-zero $\omega_2 \in \Omega_F$ there exists some $z \in F$ such that $\omega_2 = z\omega_1$. Choose $A_1, A_2 \in \mathrm{Div}(F)$ such that $\omega_1 \in \Omega_F(A_1)$ and $\omega_2 \in \Omega_F(A_2)$. For a divisor B, consider the K-linear injective maps

$$\begin{aligned} \varphi_i : \mathcal{L}(A_i + B) &\to \Omega_F(-B) \\ x &\mapsto x\omega_i. \end{aligned}$$

We claim that for an appropriate choice of B, $\mathrm{Im}(\varphi_1) \cap \mathrm{Im}(\varphi_2) \neq \{0\}$. From linear algebra, we know that if U_1, U_2 are subspaces of a finite-dimensional vector space V, then

$$\dim(U_1, \cap U_2) \geqslant \dim U_1 + \dim U_2 - \dim V. \tag{1.17}$$

Applying Riemann's Theorem, let $B > 0$ be of sufficiently large degree such that

$$\ell(A_i + B) = \deg(A_i + B) + 1 - g.$$

Set $U_i := \mathrm{Im}(\varphi_i) \subseteq \Omega_F(-B)$. From the fact that

$$\dim \Omega_F(-B) = i(-B) = \ell(-B) - \deg(-B) + g - 1 = \deg B - 1 + g,$$

we obtain

$$\begin{aligned}\dim U_1 + \dim U_2 - \dim \Omega_F(-B) &= \deg(A_1 + B) + \deg(A_2 + B) - \deg B + 3(1-g) \\ &= \deg B + (\deg A_1 + \deg A_2 + 3(1-g)).\end{aligned}$$

Thus, if $\deg B$ is sufficiently large, $\dim U_1 + \dim U_2 - \dim \Omega_F(-B) > 0$. By (1.17), it follows that $U_1 \cap U_2 \neq \{0\}$, proving the claim.

Having proved this intermediate result, the proposition now easily follows: choose $x_1 \in \mathcal{L}(A_1 + B)$ and $x_2 \in \mathcal{L}(A_2 + B)$ such that $x_1\omega_1 = x_2\omega_2 \neq 0$. Then $\omega_2 = (x_1 x_2^{-1})\omega_1$ as desired. □

We now wish to attach a divisor to each non-zero Weil differential. To this end, for a fixed $\omega \in \Omega_F$, define the set of divisors

$$M(\omega) := \{A \in \mathrm{Div}(F) : \omega \text{ vanishes on } \mathcal{A}_F(A) + F\}.$$

Lemma 7. *Let $0 \neq \omega \in \Omega_F$. There is a uniquely determined divisor $W \in M(\omega)$ such that $A \leqslant W$ for all $A \in M(\omega)$.*

Proof. Riemann's Theorem states there is a constant c depending only on the function field $F|K$ such that $i(A) = 0$ for all $A \in \mathrm{Div}(F)$ with $\deg A \geqslant c$. Since $i(A) = \dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F))$, we have that $\deg A < c$ for all $A \in M(\omega)$. This means we can choose a divisor $W \in M(\omega)$ of maximal degree.

Suppose W does not have the desired property. Then there exists a divisor $A_0 \in M(\omega)$ with $A_0 \nleqslant W$, that is, $v_Q(A_0) > v_Q(W)$ for some $Q \in \mathbb{P}_F$. We claim that if this is the case, then $W + Q \in M(\omega)$, which would contradict the maximality of W. Indeed, consider the adele $\alpha = (\alpha_P) \in \mathcal{A}_F(W + Q)$. Writing $\alpha = \alpha' + \alpha''$ with

$$\alpha'_P = \begin{cases} \alpha_P \text{ for } P \neq Q \\ 0 \text{ for } P = Q \end{cases} \quad \text{and} \quad \alpha''_P = \begin{cases} 0 \text{ for } P \neq Q \\ \alpha_Q \text{ for } P = Q. \end{cases}$$

Then $\alpha' \in \mathcal{A}_F(W)$ and $\alpha'' \in \mathcal{A}_F(A_0)$, therefore $\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0$. Hence ω vanishes on $\mathcal{A}_F(W + Q) + F$, proving that $W + Q \in M(\omega)$. The uniqueness of W is a direct consequence of its properties. □

The preceding lemma now allows us to make the following definitions:

Definition 25. *(a) The divisor (ω) of a Weil differential $\omega \neq 0$ is the uniquely determined divisor of $F|K$ such that*

1. *ω vanishes on $\mathcal{A}_F((\omega)) + F$*
2. *if ω vanishes on $\mathcal{A}_F(A) + F$, then $A \leqslant (\omega)$.*

(b) For $0 \neq \omega \in \Omega_F$ and $P \in \mathbb{P}_F$, we define $v_P(\omega) := v_P((\omega))$.

(c) A place P is a zero of ω if $v_P(\omega) > 0$, and it is a pole of ω if $v_P(\omega) < 0$. The Weil differential is said to be regular at P if $v_P(\omega) \geqslant 0$, and ω is said to be regular if it is regular for all $P \in \mathbb{P}_F$.

(d) A divisor W is called a canonical divisor of $F|K$ if $W = (\omega)$ for some $\omega \in \Omega_F$.

Remark 5. *From the preceding definitions, it follows that*

$$\Omega_F(A) = \{\omega \in \Omega_F : \omega = 0 \text{ or } (\omega) \geqslant A\} \text{ and } \Omega_F(0) = \{\omega \in \Omega_F : \omega \text{ is regular}\}.$$

As a consequence of Lemma 6 and the definition of the index of specialty, we have

$$\dim \Omega_F(0) = g.$$

Proposition 8. *(a) For $x \in F^*$ and $0 \neq \omega \in \Omega_F$ we have $(x\omega) = (x) + (\omega)$.*

(b) Any two canonical divisors of $F|K$ are equivalent.

Proof. (a) If ω vanishes on $\mathcal{A}_F(A)+F$, then $x\omega$ vanishes on $\mathcal{A}_F(A+(x))+F$, consequently $(\omega) + (x) \leqslant (x\omega)$. In the same manner, $(x\omega) + (x^{-1}) \leqslant (x^{-1}x\omega) = (\omega)$. Combining these inequalities:

$$(\omega) + (x) \leqslant (x\omega) \leqslant -(x^{-1}) + (\omega) = (\omega) + (x).$$

(b) Given $\omega_1, \omega_2 \in \Omega_F$ two non-zero Weil differentials, Proposition 7 implies $\omega_2 = x\omega_1$ for some $x \in F$. By item (a): $(\omega_2) = (x) + (\omega_1)$ and $(\omega_1) \sim (\omega_2)$.

□

From this proposition we conclude that all the canonical divisors of $F|K$ are in the same class $[W]$ in the divisor class group $\mathrm{Cl}(F)$. Such class is called the canonical class of $F|K$.

Theorem 10 (Duality Theorem)**.** *Let A be any divisor of $F|K$ and $W = (\omega)$ be a canonical divisor of $F|K$. The mapping*

$$\begin{aligned} \mu : \mathcal{L}(W - A) &\to \Omega_F(A) \\ x &\mapsto x\omega \end{aligned}$$

is an isomorphism of K-vector spaces. In particular, $\ell(W - A) = i(A)$.

Proof. For $x \in \mathcal{L}(W - A)$, we have $(x\omega) = (x) + (\omega) \geqslant -(W - A) + W = A$, hence $x\omega \in \Omega_F(A)$ by Remark 5 and μ is well-defined. It is evident that μ is K-linear and injective. In order to prove it is also surjective, take $\omega_1 \in \Omega_F(A)$. By Proposition 7, $\omega_1 = x\omega$ for some $x \in F$. Since

$$(x) + W = (x) + (\omega) = (x\omega) = (\omega_1) \geqslant A,$$

we get $(x) \geqslant -(W - A)$, so $x \in \mathcal{L}(W - A)$ and $\omega_1 = \mu(x)$. We have thus proved that $\dim \mathcal{L}(W - A) = \dim \Omega_F(A)$. Applying Lemma 6, the result follows. □

A direct implication of the Duality Theorem is the Riemann-Roch Theorem, the most important theorem in the theory of algebraic function fields.

Theorem 11 (Riemann-Roch Theorem)**.** *If W is a canonical divisor of $F|K$ and $A \in \mathrm{Div}(F)$, then*

$$\ell(A) = \deg A + 1 - g + \ell(W - A).$$

Corollary 9. *For a canonical divisor W, $\deg W = 2g - 2$ and $\ell(W) = g$.*

Proof. Applying the Riemann-Roch Theorem for $A = 0$, Lemma 4 yields

$$1 = \ell(0) = \deg 0 + 1 - g + \ell(W - 0) \implies \ell(W) = g.$$

Setting $A = W$, we obtain

$$g = \ell(W) = \deg W + 1 - g + \ell(W - W) = \deg W + 2 - g \implies \deg W = 2g - 2.$$

□

Riemann's Theorem shows the existence of some constant c such that $i(A) = 0$ whenever $\deg A \geqslant c$. We can now give a more precise description of this constant.

Theorem 12. *If $A \in \mathrm{Div}(F)$ is such that $\deg A \geqslant 2g - 1$, then $\ell(A) = \deg A + 1 - g$.*

Proof. Since $\deg A \geqslant 2g - 1$ and $\deg W = 2g - 2$ for a canonical divisor W, we have

$$\deg(W - A) = \deg W - \deg A \leqslant 2g - 2 - (2g - 1) = -1 < 0.$$

By Corollary 6, we conclude that $\ell(W - A) = 0$. Applying the Riemann-Roch Theorem, it follows that $\ell(A) = \deg A + 1 - g$. □

It is worth noting that the bound $2g-1$ is the best possible, as for a canonical divisor W

$$\ell(W) > \deg W + 1 - g$$

by Corollary 9.

We shall now explore several consequences of the Riemann-Roch Theorem. Our first aim is to show that this theorem characterizes both the genus and the canonical class of $F|K$.

Proposition 9. *If $g_0 \in \mathbb{Z}$ and $W_0 \in \mathrm{Div}(F)$ satisfy*

$$\ell(A) = \deg A + 1 - g_0 + \ell(W_0 - A) \tag{1.18}$$

for all $A \in \mathrm{Div}(F)$, then $g_0 = g$ and W_0 is a canonical divisor.

Proof. Setting $A = 0$ in (1.18) yields $\ell(W_0) = g_0$, and setting $A = W_0$, $\deg W_0 = 2g_0 - 2$. Let W be a canonical divisor of $F|K$ and choose $A \in \mathrm{Div}(F)$ such that $\deg A > \max\{2g-2, 2g_0-2\}$. Theorem 12 implies $\ell(A) = \deg A + 1 - g$. Since $\deg(W_0 - A) < 0$, we have $\ell(W_0 - A) = 0$ and by (1.18): $\ell(A) = \deg A + 1 - g_0$. Thus, $g = g_0$. Finally, substituting $A = W$ in (1.18):

$$g = (2g-2) + 1 - g + \ell(W_0 - W) \implies \ell(W_0 - W) = 1.$$

Since $\deg(W_0 - W) = (2g_0 - 2) - (2g - 2) = 0$, $W_0 - W$ is principal according to Corollary 6, so $W_0 \sim W$ and W_0 is canonical. □

Proposition 10. *A divisor B is canonical if and only if $\deg B = 2g-2$ and $\ell(B) \geqslant g$.*

Proof. The forward direction has already been proven. Now suppose $\deg B = 2g-2$ and $\ell(B) \geqslant g$. Choose a canonical divisor W, then

$$g \leqslant \ell(B) = \deg B + 1 - g + \ell(W - B) = g - 1 + \ell(W - B).$$

Thus, $\ell(W - B) \geqslant 1$. The fact that $\deg(W - B) = 0$ now implies $W \sim B$ by Corollary 6. □

Proposition 11. *A function field $F|K$ is rational if and only if $F|K$ has genus 0 and there is some $A \in \mathrm{Div}(F)$ with $\deg A = 1$.*

Proof. ($\Rightarrow$): proven in Example 3.
($\Leftarrow$): Let $g = 0$ and $\deg A = 1$. Then $\deg A \geqslant 2g - 1$ and $\ell(A) = \deg A + 1 - g = 2$ by Theorem 12. Thus $A' \sim A$ for some $A' \geqslant 0$ by Remark 4(b). Since $\ell(A') = 2$, there exists some $x \in \mathcal{L}(A') \backslash K$, so $(x) \neq 0$ and $A' + (x) \geqslant 0$. As $A' \geqslant 0$ and $\deg A' = 1$, this is only possible if $A' = (x)_\infty$. Now

$$[F : K(x)] = \deg(x)_\infty = \deg A' = 1$$

by Theorem 6, so $F = K(x)$. □

Remark 6. *There exist non-rational function fields of genus* 0*, although these cannot have a divisor of degree* 1 *by the preceding proposition. However, if* K *is algebraically closed or finite, there will always exist a divisor of degree* 1*. Hence, in these cases,* $g = 0$ *is equivalent to* $F|K$ *being rational.*

Next, we give an improved version of the Weak Approximation Theorem.

Theorem 13 (Strong Approximation Theorem)**.** *Let* $S \subsetneq \mathbb{P}_F$ *and* $P_1, \dots, P_r \in S$*. Given* $x_1, \dots, x_r \in F$ *and* $n_1, \dots, n_r \in \mathbb{Z}$*, there is an element* $x \in F$ *such that* $v_{P_i}(x - x_i) = n_i$ *for* $i = 1, \dots, r$ *and* $v_P(x) \geqslant 0$ *for* $P \in S \backslash \{P_1, \dots, P_r\}$*.*

Proof. Take the adele $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ with

$$\alpha_P = \begin{cases} x_i \text{ for } P = P_i \\ 0 \text{ otherwise.} \end{cases}$$

Choose $Q \in \mathbb{P}_F \backslash S$. For a sufficiently large $m \in \mathbb{N}$

$$\mathcal{A}_F = \mathcal{A}_F\left(mQ - \sum_{i=1}^{r}(n_i + 1)P_i\right) + F$$

by Theorems 9 and 12. So there is an element $z \in F$ with $z - \alpha \in \mathcal{A}_F\left(mQ - \sum_{i=1}^{r}(n_i + 1)P_i\right)$. This means

$$\begin{aligned} v_{P_i}(z - x_i) > n_i \text{ for } i = 1, \dots, r \text{ and} \\ v_P(z) \geqslant 0 \text{ for } P \in S \backslash \{P_1, \dots, P_r\}. \end{aligned} \tag{1.19}$$

Now we choose $y_1, \dots, y_r \in F$ with $v_{P_i}(y_i) = n_i$. In the same manner we construct $y \in F$ with

$$v_{P_i}(z - x_i) > n_i \text{ for } i = 1, \dots, r \text{ and} \tag{1.20}$$

$$v_P(z) \geqslant 0 \text{ for } P \in S \backslash \{P_1, \dots, P_r\}. \tag{1.21}$$

Then for $i = 1, \dots, r$

$$v_{P_i}(y) = v_{P_i}((y - y_i) + y_i) = n_i \tag{1.22}$$

by (1.20) and the Strict Triangle Inequality. Setting $x =: y + z$, we get

$$v_{P_i}(x - x_i) = v_{P_i}(y + (z - x_i)) = n_i$$

by (1.22). For $P \in S \backslash \{P_1, \dots, P_r\}$, $v_P(x) = v_P(y + z) \geqslant 0$ by (1.19) and (1.21). □

Proposition 12. *Let* $P \in \mathbb{P}_F$ *and* $n \in \mathbb{N}$ *with* $n \geqslant 2g$*. There exists an element* $x \in F$ *such that* $(x)_\infty = nP$*.*

Proof. By Theorem 12, we know $\ell((n-1)P) = (n-1)\deg P + 1 - g$ and $\ell(nP) = n \cdot \deg P + 1 - g$ hence, $\mathcal{L}((n-1)P) \subsetneq \mathcal{L}(nP)$. Thus every element $x \in \mathcal{L}(nP) \backslash \mathcal{L}((n-1)P)$ has pole divisor nP. □

Definition 26. *Let $P \in \mathbb{P}_F$. An integer $n \geqslant 0$ is called a pole number of P if there is an element $x \in F$ such that $(x)_\infty = nP$. Otherwise, n is called a gap number of P.*

From the previous proposition, n is a pole number of P if and only if $\ell(nP) > \ell((n-1)P)$. Moreover, the set of pole numbers of P is a sub-semigroup of the additive semigroup $\mathbb{N}$, since $(x_1 x_2)_\infty = (n_1 + n_2)P$ if $(x)_\infty = n_1 P$ and $(x_2)_\infty = n_2 P$.

Theorem 14 (Weierstrass Gap Theorem)**.** *Let $F|K$ be a function field of genus $g > 0$ and $P \in \mathbb{P}_F$ with $\deg P = 1$. Then there are exactly g gap numbers $i_1 < \cdots < i_g$ of P where $i_1 = 1$ and $i_g \leqslant 2g - 1$.*

Proof. By Proposition 12, each gap number of P is bounded above by $2g-1$ and 0 is a pole number. We can characterize gap number by the following equivalence

$$i \text{ is a gap number of } P \iff \mathcal{L}((i-1)P) = \mathcal{L}(iP).$$

Take the sequence of vector spaces

$$K = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \cdots \subseteq \mathcal{L}((2g-1)P), \tag{1.23}$$

where $\dim \mathcal{L}(0) = 1$ and $\dim \mathcal{L}((2g-1)P) = g$ according to Theorem 12. Applying Lemma 5, we observe that for all i

$$\dim \mathcal{L}(iP) \leqslant \dim \mathcal{L}((i-1)P) + 1,$$

so in (1.23) there are exactly $g-1$ numbers $1 \leqslant i \leqslant 2g-1$ such that $\mathcal{L}((i-1)P) \subsetneq \mathcal{L}(iP)$. The remaining g numbers are the pole numbers of P. In order to show that 1 is a gap number, suppose the converse, that is, 1 is a pole number of P. But since the pole numbers form an additive subgroup, this would imply every $n \in \mathbb{N}$ is a pole number of P and there are no gaps, a contradiction since $g > 0$. □

Remark 7. *If K is algebraically closed, it can be shown that almost all places of $F|K$ have the same gap sequence. Such places are called ordinary places of $F|K$. The non-ordinary places are called Weierstrass points of $F|K$. If $g \geqslant 2$, there exists at least one Weierstrass point.*

If A is a divisor of negative degree, we know that $\mathcal{L}(A) = \{0\}$ and $\ell(A) = 0$. On the other hand, if $\deg A > 2g - 2$ then $\ell(A) = \deg A + 1 - g$. So $\ell(A)$ depends on $\deg A$ and g in these cases. We shall now consider the case where $0 \leqslant \deg A \leqslant 2g - 2$, which is significantly more complex.

Definition 27. *A divisor $A \in \mathrm{Div}(F)$ is called non-special if $i(A) = 0$. Otherwise A is called special.*

Remark 8. *(a) A is non-special $\iff \ell(A) = \deg A + 1 - g$.*

(b) $\deg A > 2g - 2 \implies A$ is non-special.

(c) A being special or non-special depends only on the class $[A]$ on the divisor class group.

(d) Canonical divisors are special.

(e) Every divisor A with $\ell(A) > 0$ and $\deg A < g$ is special.

(f) If A is non-special and $B \geqslant A$, then B is non-special.

Proof. (a) Direct consequence of the definition of $i(A)$.

(b) This is a restatement of Theorem 12.

(c) Follows from the fact if $A' \sim A$, then $\deg A = \deg A'$ and $\ell(A) = \ell(A')$.

(d) For a canonical divisor W, $i(W) = \ell(W - W) = 1$ from the Duality Theorem, hence W is special.

(e) $1 \leqslant \ell(A) = \deg A + 1 - g + i(A) \implies i(A) \geqslant g - \deg A > 0$, since $\deg A < g$.

(f) Bt Theorem 9, A is non-special $\iff \mathcal{A}_F = \mathcal{A}_F(A) + F$. If $B \geqslant A$, we know $\mathcal{A}_F(A) \subseteq \mathcal{A}_F(B)$, so the claim follows.

□

Proposition 13. *Suppose $T \subseteq \mathbb{P}_F$ is a set of rational places with $|T| \geqslant g$. Then there exists a non-special divisor $B \geqslant 0$ with $\deg B = g$ and $\operatorname{supp} B \subseteq T$.*

Proof. First we prove that given g distinct places $p_1, \ldots, p_g \in T$ and a divisor $A \geqslant 0$ with $\ell(A) = 1$ and $\deg A \leqslant g - 1$, there is an index $j \in \{1, \ldots, g\}$ such that $\ell(A + P_j) = 1$.

Suppose the claim is false, that is, $\ell(A + P_j) > 1$ for all j. Then there are elements $z_j \in \mathcal{L}(A + P_j) \backslash \mathcal{L}(A)$. Since

$$v_{P_j}(z_j) = -v_{P_j}(A) - 1 \text{ and } v_{P_i}(z_j) \geqslant -v_{P_i}(A) \text{ for } i \neq j,$$

the Stirct Triangle Inequality implies there are $g + 1$ elements $1, z_1, \ldots, z_g$ are linearly independent over K. Pick a divisor $D \geqslant A + P_1 + \cdots + P_g$ with $\deg D = 2g - 1$. Then $1, z_1, \ldots, z_g \in \mathcal{L}(D)$, hence $\ell(D) \geqslant g + 1$. On the other hand, $\ell(D) = \deg D + 1 - g = g$ by the Riemann-Roch Theorem, a contradiction.

Using this claim we find divisors $0 < P_{i1} < P_{i1} + P_{i2} < \cdots < P_{i1} + \cdot + P_{ig} := B$ with $i_v \in \{1, \ldots, g\}$ not necessarily distinct such that $\ell(P_{i1} + \cdots + P_{ij}) = 1$ for $j = 1, \ldots, g$. In particular $\ell(B) = 1$. The divisor B is non-special since

$$\deg B + 1 - g = g + 1 - g = 1 = \ell(B)$$

according to Remark 8(a). □

Lemma 8. *If A and B are divisors with $\ell(A) > 0$ and $\ell(B) > 0$, then*

$$\ell(A) + \ell(B) \leqslant 1 + \ell(A + B).$$

Proof. Since $\ell(A) > 0$ and $\ell(B) > 0$, we can find $A_0, B_0 \geqslant 0$ with $A \sim A_0$ and $B \sim B_0$. Consider the set

$$X := \{D \in \mathrm{Div}(F) : D \geqslant A_0 \text{ and } \mathcal{L}(D) = \mathcal{L}(A_0)\}.$$

We have $X \neq \varnothing$ since $A_0 \in X$. Furthermore, $\deg D \geqslant 0$ for all $D \in X$, so there must be $D_0 \in X$ of minimal degree. It follows that

$$\ell(D_0 - P) < \ell(D_0) \text{ for all } P \in \mathbb{P}_F. \tag{1.24}$$

We wish to show that

$$\ell(D_0) + \ell(B_0) \leqslant 1 + \ell(D_0 + B_0), \tag{1.25}$$

since the lemma follows immediately from this:

$$\begin{aligned} \ell(A) + \ell(B) = \ell(D_0) + \ell(B_0) &\leqslant 1 + \ell(D_0 + B_0) \\ &\leqslant 1 + \ell(A_0 + B_0) \\ &\leqslant 1 + \ell(A + B). \end{aligned}$$

In order to prove (1.25), we make the additional assumption that K is infinite. It will later be shown in this text that the lemma still holds for finite fields. Let $\operatorname{supp} B_0 = \{P_1, \ldots, P_r\}$. Then $\mathcal{L}(D_0 - P_i)$ is a proper subspace of $\mathcal{L}(D_0)$ for every $i = 1, \ldots, r$. Since a vector space over an infinite field is not the union of finitely many proper subspaces, we find an element

$$z \in \mathcal{L}(D_0) \backslash \bigcup_{i=1}^{r} \mathcal{L}(D_0 - P_i).$$

Consider the K-linear map

$$\begin{aligned} \varphi : \mathcal{L}(B_0) &\to \mathcal{L}(D_0 + B_0)/\mathcal{L}(A_0) \\ x &\mapsto xz + \mathcal{L}(A_0). \end{aligned}$$

We wish to show that $\ker \varphi = K$. The inclusion $K \subseteq \ker \varphi$ follows directly from the fact that $\mathcal{L}(D_0) = \mathcal{L}(A_0)$ is a K-vector space. In order to show $\ker \varphi \subseteq K$, we first prove that

$v_{P_i}(z) = -v_{P_i}(D_0)$ for all $i = 1, \dots, r$. Indeed, $z \in \mathcal{L}(D_0) \implies v_P(z) \geqslant -v_P(D_0)$ for all $P \in \mathbb{P}_F$. In particular,

$$v_{P_i}(z) \geqslant -v_{P_i}(D_0) \text{ for all } i = 1, \dots, r.$$

Supposing that $v_{P_k}(z) > -v_{P_k}(D_0)$ for some $k = 1, \dots, r$, we get:

$$v_{P_k}(z) > -v_{P_k}(D_0) \implies v_{P_k}(z) \geqslant -v_{P_k}(D_0) + 1 = -(v_{P_k}(D_0) - 1) = -v_{P_k}(D_0 - P_k).$$

Since $v_Q(D_0) = v_Q(D_0 - P_k)$ for $Q \neq P_k$, it follows that $z \in \mathcal{L}(D_0 - P_k)$, which contradicts our choice of z.

Now, given $x \in \mathcal{L}(B_0) \backslash K$, we show that $xz \notin \mathcal{L}(A_0)$. If $x \in \mathcal{L}(B_0)$, we know that $v_P(x) \geqslant 0$ for all $P \notin \operatorname{supp}(B_0)$. And seeing as $x \notin K$, x has at least one pole $P' \in \mathbb{P}_F$ where $v_{P'}(x) < 0$. Combining these two observations, we conclude that $P' \in \operatorname{supp}(B_0)$, that is, $P' = P_j$ for some $j = 1, \dots, r$. Therefore,

$$v_{P_j}(xz) = v_{P_j}(x) + v_{P_j}(z) < v_{P_j}(z) = -v_{P_j}(D_0),$$

which implies $xz \notin \mathcal{L}(D_0) = \mathcal{L}(A_0)$. Hence, $\ker \varphi = K$ and

$$\ell(B_0) - 1 \leqslant \ell(D_0 - B_0) - \ell(A_0),$$

proving (1.25) an our lemma. □

Theorem 15 (Clifford's Theorem)**.** *For all divisors A with $0 \leqslant \deg A \leqslant 2g - 2$*

$$\ell(A) \leqslant 1 + \frac{1}{2} \cdot \deg A.$$

Proof. If $\ell(A)$, the theorem follows immediately. Likewise, if $\ell(W - A) = 0$ for some canonical divisor W, then

$$\ell(A) = \deg A + 1 - g = 1 + \frac{1}{2} \deg A + \frac{1}{2}(\deg A - 2g) < 1 + \frac{1}{2} \deg A,$$

since $\deg A \leqslant 2g - 2$. Finally, if $\ell(A) > 0$ and $\ell(W - A) > 0$, we apply Lemma 8 to obtain

$$\ell(A) + \ell(W - A) \leqslant 1 + \ell(W) = 1 + g.$$

On the other hand,

$$\ell(A) - \ell(W - A) = \deg A + 1 - g.$$

Adding these equations finishes the proof. □

1.7 Equivalent Formulations of the Riemann-Roch Problem

This section is mostly based on chapter 3 of (GOPPA, 1988), although some results are stated slightly differently in order to facilitate their use in later chapters.

Having studied the Riemann-Roch space of a divisor in the case of algebraic function fields, we now use the definitions and results of Section 1.5 to re-frame the problem of describing this vector space in the context of algebraic curves and present some results that will be helpful when constructing the Fermat Function Field Lattice.

Up until now, we have studied how to compute the dimension $\ell(D)$ of the Riemann-Roch space associated with a divisor D. There are, however, two problems equivalent to this which when investigated will not only yield different ways to compute $\ell(D)$, but produce an explicit base for $\mathcal{L}(D)$ in some cases.

Let $\mathcal{F}$ be a projective curve over a field K and D a divisor of $\mathcal{F}$. The Riemann-Roch problem is equivalent to finding all effective divisors D' which are linearly equivalent to D: $D' = D + (f)$ for some $f \in K(\mathcal{F})$. Since D' is effective, $D + (f) \geqslant 0$ and hence $(f) \geqslant -D$. The set of functions f whose divisors satisfy this inequality is exactly $\mathcal{L}(D)$.

The other formulation of the problem deals with intersections of algebraic curves. In order to state it, we first define the intersection divisor of two curves:

Definition 28. *Let $\mathcal{F}$, $\mathcal{G}$ be two algebraic curves and Q be a non-singular point on both curves. The positive integer $I(\mathcal{F} \cap \mathcal{G}, Q)$ denotes the intersection multiplicity of $\mathcal{F}$ and $\mathcal{G}$ at Q. In addition, if $\mathcal{F}$ is not a component of $\mathcal{G}$, then $\mathcal{F} \cap \mathcal{G} = \{Q_1, \ldots, Q_m\}$ and*

$$\mathcal{F} \cdot \mathcal{G} := \sum_{i=1}^{m} I(\mathcal{F} \cap \mathcal{G}, Q_i) \cdot Q_i$$

is the intersection divisor of $\mathcal{F}$ and $\mathcal{G}$. In this case, we say that $\mathcal{F}$ 'cuts out' the divisor $\mathcal{F} \cdot \mathcal{G}$ on $\mathcal{G}$.

Let $f_0, \ldots, f_{r-1}$ be linearly independent forms of the same degree, $\lambda_0, \ldots, \lambda_{r-1} \in K$ and consider the following equation, called a linear system of curves

$$\lambda_0 f_0(X, Y, Z) + \cdots + \lambda_{r-1} f_{r-1}(X, Y, Z) = 0. \tag{1.26}$$

By the preceding definition, all the curves of the linear system cut out effective divisors on the initial curve $\mathcal{C}$. The set of these divisors with $\lambda_0, \ldots, \lambda_{r-1}$ running over the field K is called a linear series.

We note that $\mathcal{C}$ and the curves $f_0, \ldots, f_{r-1}$ may pass through a common set of points (a divisor). Apart from this, the remaining divisors are all distinct, since if two divisors of the linear series coincided, the corresponding curves would differ only by a constant multiplier, contradicting the assumption that $f_0, \ldots, f_{r-1}$ are linearly independent.

Therefore, all divisors of the linear series are in a $1-1$ correspondence with the points of $\mathbb{P}^{r-1}$. It is evident that all divisors of a linear series are linearly equivalent, and thus have the same degree. We use the notation g_n^r to refer to a linear series whose divisors have degree n.

Dividing (1.26) by f_0, for example, we obtain a linear system of functions

$$\lambda_0 + \lambda_1\phi_1 + \cdots + \lambda_{r-1}\phi_{r-1} = 0.$$

If D is the divisor of f_0, then all functions of this system belong to $\mathcal{L}(D)$. If the system coincides with $\mathcal{L}(D)$, the system is said to be complete. In this case, $\{1, \phi_1, \ldots, \phi_{r-1}\}$ is a base for $\mathcal{L}(D)$.

Thus, the notions of Riemann-Roch space of a divisor and of the complete linear system are equivalent. We now examine how one may construct such a linear system.

Theorem 16 (Bézout's Theorem)**.** *Let $\mathcal{F}$ and $\mathcal{G}$ be plane algebraic curves of degree m and n, respectively. If $\mathcal{F}$ is not a component of $\mathcal{G}$, then*

$$\sum_{P \in \mathcal{F} \cap \mathcal{G}} I(\mathcal{F} \cap \mathcal{G}, P) \leqslant mn.$$

Definition 29. *Let $\mathcal{F}$ be an algebraic curve of degree m whose singular points are $Q_1, \ldots, Q_s$ with respective multiplicities $r_1, \ldots, r_s$. A curve $\mathcal{G}$ of degree n is said to be an adjoint curve of $\mathcal{F}$ if*

$$I(\mathcal{F} \cap \mathcal{G}, Q_i) \geqslant r_i - 1 \text{ for all } i = 1, \ldots, s.$$

In the case that $\mathcal{F}$ is non-singular, any curve is an adjoint curve of $\mathcal{F}$ and by Bézout's Theorem, the intersection divisor consists of mn distinct points. This is the only case we consider going forward. Under this condition, we have the following theorem:

Theorem 17 (Noether's Theorem)**.** *Let $\mathcal{F} = V(F)$ and $\mathcal{G} = V(G)$ be curves of degree m and n, respectively such that all mn intersection points are different. Then, all curves of degree d that pass through the divisor $\mathcal{F} \cdot \mathcal{G}$ can be written as*

$$D = AF + BG,$$

where $A, B \in K[X, Y, Z]$ with $\deg A = d - m$ and $\deg B = d - n$.

Let $\mathcal{F} = V(F)$ be a non-singular algebraic curve of degree m. If two divisors D and D' of $\mathcal{C}$ are linearly equivalent, there exist two forms H and H' of the same degree such that $D + (H) = D' + (H')$. Let $\mathcal{G} = V(G)$ be an adjoint curve of $\mathcal{F}$ of degree n. We have

$$(GH) = (G) + (H) = D' + (H') - D + (G).$$

If $\mathcal{G}$ also passes through D, that is, $(G) = D + R$ for some divisor R, then $(GH) - (H') = D' + R$. The curve GH passes through the intersection divisor of F and H', so by Noether's Theorem, it can be represented as

$$GH = FF' + G'H'$$

for some forms F', G'. Since $(FF') = 0$, it follows that

$$(G') = (GH) - (H') = D' + R.$$

Hence G' is an adjoint curve of $\mathcal{F}$ of the same degree as $\mathcal{G}$. We have thus proved the following:

Theorem 18. *Let D be a divisor of the curve $\mathcal{F}$ and $D \sim D'$. If $\mathcal{G} = V(G)$ is an adjoint of $\mathcal{F}$ of degree n such that $(G) = D + R$, where R is called the residue divisor, then there exists an adjoint curve $\mathcal{H} = V(H)$ of degree m such that*

$$(H) = D' + R.$$

This gives another way to compute the dimension of a Riemann-Roch space. Given D a divisor of $\mathcal{F}$, find an adjoint curve $\mathcal{G} = V(G)$ of degree m passing through the divisor D, that is, $(G) = D + R$. Now, find all adjoint curves of degree m that pass through the residue divisor R. The complete linear system g_n^r of divisors cut out on $\mathcal{F}$ by the adjoint curves found correspond to the space $\mathcal{L}(D)$. This is because all the curves we found pass through the common set of points defined by R, thus this divisor can be omitted and g_n^r contains D and all of its equivalent divisors.

We can summarize our findings with the following lemma:

Lemma 9. *Let $\mathcal{F}$ be a non-singular curve, D an effective divisor of $\mathcal{F}$, and $\mathcal{G}$ an adjoint curve of $\mathcal{F}$ of degree m such that*

$$\mathcal{G} \cdot \mathcal{F} = D + R.$$

Then, the dimension $\ell(D)$ is the dimension of the linear system of adjoint curves of degree m passing through R.

Finally, we give another useful interpretation for the index of specialty of a divisor.

Definition 30. *Let $\mathcal{F}$ be an algebraic curve of degree m. The adjoint curves of $\mathcal{F}$ that have degree $m - 3$ are called canonical adjoints of $\mathcal{F}$.*

Given D an effective divisor of $\mathcal{F}$, the number of linearly independent canonical adjoints of $\mathcal{F}$ passing through D is the index of specialty of D, denoted by $i(D)$. This allows us to present an alternative formulation for the Rieman-Roch theorem discussed previously

Theorem 19 (Riemann-Roch)**.** *Let D be an effective divisor of $\mathcal{F}$, then*

$$\ell(D) = \deg D - g + 1 + i(D),$$

where g is the genus of $\mathcal{F}$, which is the same as the genus of $K(\mathcal{F})$.

1.8 Algebraic Extensions of Function Fields

In order to study function field extensions, in the following sections we assume that given a function field $F|K$, the base field K is perfect, that is, every finite extension of K is separable. Furthermore, we fix $\bar{F}$ an algebraic closure of F and consider only extensions $F' \supseteq F$ such that $F' \subseteq \bar{F}$.

Definition 31. *(a) An algebraic function field $F'|K'$ is an algebraic extension of $F|K$ if $F'|F$ is an algebraic extension and $K \subseteq K'$.*

(b) The algebraic extension $F'|K'$ of $F|K$ is a constant field extension if $F' = FK'$.

(c) The algebraic extension $F'|K'$ of $F|K$ is finite if $[F' : F] < \infty$.

Lemma 10. *If $F'|K'$ is an algebraic extension of $F|K$, then*

(a) $K'|K$ is algebraic and $F \cap K' = K$.

(b) $F'|K'$ is a finite extension of $F|K$ if and only if $[K' : K] < \infty$.

(c) $FK'|K'$ is a constant field extension of $F|K$, and $F'|K'$ is a finite extension of $FK'|K'$ with the same field of constants.

Definition 32. *Given an algebraic extension $F'|K'$ of $F|K$, a place $P' \in \mathbb{P}_{F'}$ lies over $P \in \mathbb{P}_F$ if $P \subseteq P'$. We also say that P' extends P and write $P'|P$.*

Proposition 14. *Let $F'|K'$ be an algebraic extension of $F|K$. If $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$, denote by $\mathcal{O}_P \subset F$ and $\mathcal{O}_{P'} \subseteq F'$ the respective valuation rings and by v_P and $v_{P'}$ the respective discrete valuations. The following are equivalent:*

1. *$P'|P$.*
2. *$\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.*
3. *There exists an integer $e \geqslant 1$ such that $v_{P'}(x) = e \cdot v_P(x)$ for all $x \in F$.*

Besides that, if $P'|P$, then $P = P' \cap F$ and $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$.

Proof. 1. $\Rightarrow$ 2. : Suppose $P'|P$ and $\mathcal{O}_P \nsubseteq \mathcal{O}_{P'}$. Then there is some $u \in F$ with $v_P(u) \geqslant 0$ and $v_{P'}(u) < 0$. Since $P \subseteq P'$, we have $v_P(u) = 0$. Choose $t \in F$ a P-prime element, then $t \in P'$ and $r := v_{P'}(t) > 0$. Consequently,

$$v_P(u^r t) = r \cdot v_P(u) + v_P(t) = 1,\ v_{P'}(u^r t) = r \cdot v_{P'}(u) + v_{P'}(t) = 1 \leqslant -r + r = 0.$$

Thus $u^r t \in P \backslash P'$, contradicting $P \subseteq P'$.
2. $\Rightarrow$ 1. : First we show that

$$\mathcal{O}_P \subset \mathcal{O}_{P'} \implies \mathcal{O}_P = F \cap \mathcal{O}_{P'}. \tag{1.27}$$

We see that $F \cap \mathcal{O}_{P'}$ is a subring of F with $\mathcal{O}_P \subseteq F \cap \mathcal{O}_{P'}$, therefore $F \cap \mathcal{O}_{P'} = \mathcal{O}_{P'}$ or $F \cap \mathcal{O}_{P'} = F$ by Theorem 2(c). Assume $F \cap \mathcal{O}_{P'} = F$, that is, $F \subseteq \mathcal{O}_{P'}$. Choose $z \in F' \backslash \mathcal{O}_{P'}$. As $F'|F$ is algebraic, there is an equation

$$z^n + c_{n-1} z^{n-1} + \cdots + c_1 z + c_0 = 0$$

with $c_i \in F$. We have $v_{P'}(z^n) = n \cdot v_{P'}(z) < 0$ since $z \notin \mathcal{O}_{P'}$, therefore

$$v_{P'}(z) < v_{P'}(c_i z^i) \text{ for } i = 1, \ldots, n-1.$$

By the Strict Triangle Inequality

$$v_{P'}(z^n + c_{n-1} z^{n-1} + \cdots + c_1 z + c_0) = n \cdot v_{P'}(z) \neq v_{P'}(0),$$

contradicting the original equation and proving (1.27). Now, assuming $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$, let $y \in P$. Then $y^{-1} \notin \mathcal{O}_P$ by Proposition 1, therefor $y^{-1} \notin P'$ by (1.27). Using Proposition 1 again yields $y = (y^{-1})^{-1} \in P$ and hence $P \subseteq P'$.
2. $\Rightarrow$ 3. : Let $u \in F$ be such that $v_P(u) = 0$. Then $u, u^{-1} \in \mathcal{O}_P$ by 2., so $v_{P'}(u) = 0$. Now choose t a P-prime element and set $e := v_{P'}(t)$. The inclusion $P \subseteq P'$ implies $e \geqslant 1$. Let $x \in F^*$ and $r := v_P(x) \in \mathbb{Z}$, then $v_P(xt^{-r}) = 0$ and

$$v_{P'}(x) = v_{P'}(xt^{-r}) + v_{P'}(t^{-r}) = 0 + r \cdot v_{P'}(t) = e \cdot v_P(x).$$

3. $\Rightarrow$ 2. : This follows from Theorem 2(a) and the fact that $e \geqslant 1$.
Finally, $P = P' \cap F$ since given $x \in P$, we know $x \in P'$, and given $x \in P' \cap F$, using 3. shows that $x \in P$. □

If $P'|P$, this proposition implies there is a canonical embedding between the residue class fields $F_P = \mathcal{O}_P/P$ and $F'_{P'} = \mathcal{O}_{P'}/P'$ given by $x(P) \mapsto x(P')$ for $x \in \mathcal{O}_P$. We thus consider F_P as a subfield of $F'_{P'}$.

Definition 33. *Let $F'|K'$ be an algebraic extension of $F|K$ and $P'|P$.*

(a) The integer $e(P'|P) := e$ such that $v_{P'}(x) = e \cdot v_P(x)$ for all $x \in F$ is called the ramification index of P' over P. We say the extension $P'|P$ is ramified if $e(P'|P) > 1$ and unramified if $e(P'|P) = 1$.

(b) $f(P'|P) := [F'_{P'} : F_P]$ *is called the relative degree of* P' *over* P.

Proposition 15. *Let* $F'|K'$ *be an algebraic extension of* $F|K$ *and* $P'|P$.

(a) $f(P'|P) < \infty \iff [F' : F] < \infty$.

(b) If $F''|K''$ *is an algebraic extension of* $F'|K'$ *with* $P'' \in \mathbb{P}_{F''}$ *lying over* P', *then*

$$e(P''|P) = e(P''|P') \cdot e(P'|P) \text{ and } f(P''|P) = f(P''|P') \cdot f(P'|P).$$

Proposition 16. *Let* $F'|K'$ *be an algebraic extension of* $F|K$.

(a) For each $P' \in \mathbb{P}_{F'}$, *there is exactly one* $P \in \mathbb{P}_F$ *such that* $P'|P$, *namely* $P = P' \cap F$.

(b) Every place $P \in \mathbb{P}_F$ *has at least one, but only finitely many extensions* $P' \in \mathbb{P}_{F'}$.

Proof. (a) First we prove there is some $z \in F^*$ with $v_{P'}(z) \neq 0$. Assume it is false and choose $t \in F'$ with $v_{P'}(t) > 0$. $F'|F$ being algebraic means

$$c_n t^n + \cdots + c_1 t + c_0 = 0$$

for some $c_i \in F$, $c_0 \neq 0$ and $c_n \neq 0$. By assumption, $v_{P'}(c_0) = 0$ and $v_{P'}(c_i t^i) = v_{P'}(c_i) + i \cdot v_{P'}(t) > 0$ for $i = 1, \ldots, n$, contradicting the Strict Triangle inequality. We now set $\mathcal{O} := \mathcal{O}_{P'} \cap F$ and $P := P' \cap F$. $\mathcal{O}$ is a valuation ring of $F|K$ by what was just shown and P is its corresponding place. Since P is a maximal ideal, the uniqueness follows.

(b) Given $P \in \mathbb{P}_F$, choose $x \in F \backslash K$ such that the only zero of x is P (possible by Proposition 12). For $P' \in \mathbb{P}_{F'}$, we show that $P'|p \iff v_{P'}(x) > 0$. If $P'|P$, $v_{P'}(x) = e(P'|P) \cdot v_P(x) > 0$. Conversely, if $v_{P'}(x) > 0$, denote by Q the place lying under P'. Then $v_Q(x) > 0$, meaning $Q = P$ given that P is the only zero of x. Since x has at least one, but only finitely many zeros in $F|K$, the claim follows.

□

This propositions gives us the final tool we need to prove that the class number, as defined in Remark 3, is always finite if K is a finite field. To this end, we first prove the following lemma:

Lemma 11. *Let* $F|\mathbb{F}_q$ *be an algebraic function field of genus* g. *For every* $n \geqslant 0$, *there exist only finitely many positive divisors of degree* n.

Proof. Since every positive divisor is a sum of prime divisors, it suffices to prove that the set $S := \{P \in \mathbb{P}_F : \deg P \leqslant n\}$ is finite. Take $x \in F \backslash \mathbb{F}_q$ and consider $S_0 := \{P_0 \in \mathbb{P}_{\mathbb{F}_q(x)} : \deg P_0 \leqslant n\}$. By Proposition 16, we know that $P \cap \mathbb{F}_q(x) \in S_0$ for all $P \in S$ and each

$P_0 \in S_0$ has only finitely many extensions in F, meaning it suffices to show that S_0 is finite. Aside from the pole of x, every place of $\mathbb{F}_q(x)$ corresponds to an irreducible monic polynomial $p(x) \in \mathbb{F}_q$ of the same degree. Thus, the finiteness of $\mathbb{F}_q$ implies S_0 is also finite, finishing the proof. □

Proposition 17. *Under the same conditions as Lemma 11, the order* $h := h_F := |\operatorname{Cl}^0(F)|$ *is finite.*

Proof. Choose a divisor $B \in \operatorname{Div}(F)$ such that $n := \deg B \geqslant g$ and consider the set of divisor classes

$$\operatorname{Cl}^n(F) := \{[C] \in \operatorname{Cl}(F) : \deg[C] = n\}.$$

The map

$$\begin{aligned} \psi : \operatorname{Cl}^0(F) &\to \operatorname{Cl}^n(F) \\ [A] &\mapsto [A + B] \end{aligned}$$

is a bijection, since

- for some $x \in F \backslash \mathbb{F}_q$, $[A_1 + B] = [A_2 + B] \implies A_1 + B = A_2 + B + (x) \implies A_1 = A_2 + (x) \implies [A_1] = [A_2]$, and
- given $[D] \in \operatorname{Cl}^n(F)$, $[D - B] \in \operatorname{Cl}^0(F)$ and $\psi([D - B]) = [D]$.

So we only need to verify that $\operatorname{Cl}^n(F)$ is finite. In order to do this, we prove that for each $[C] \in \operatorname{Cl}^n(F)$, there exists a divisor $A \in [C]$ with $A \geqslant 0$. Indeed, since $\deg C = n \geqslant g$, the Riemann-Roch Theorem implies

$$\ell(C) = \ell([C]) \geqslant n + 1 - g \geqslant 1,$$

proving our claim. By Lemma 11, there are only finitely many divisors $A \geqslant 0$ of degree n, so our claim implies $\operatorname{Cl}^n(F)$ is finite. □

We now define a homomorphism between the divisor groups of F and F'.

Definition 34. *Let $F'|K'$ be an algebraic extension of $F|K$. For a place $P \in \mathbb{P}_F$, its conorm with respect to $F'|F$ is defined as*

$$\operatorname{Con}_{F'|F}(P) := \sum_{P'|P} e(P'|P) \cdot P'.$$

This map extends to a homomorphism between $\operatorname{Div}(F)$ *and* $\operatorname{Div}(F')$ *by setting*

$$\operatorname{Con}\left(\sum n_P \cdot P\right) := \sum n_P \cdot \operatorname{Con}_{F'|F}(P).$$

By Proposition 15(b), the conorm behaves well in towers of function fields $F'' \supseteq F' \supseteq F$, that is,

$$\mathrm{Con}_{F''|F}(A) = \mathrm{Con}_{F''|F'}(\mathrm{Con}_{F'|F}(A))$$

for every $A \in \mathrm{Div}(F)$. The conorm also preserves principal divisors:

Proposition 18. *Let $F'|K'$ be an algebraic extension of $F|K$. Then*

$$\mathrm{Con}_{F'|F}((x)_0^F) = (x)_0^{F'},\ \mathrm{Con}_{F'|F}((x)_\infty^F) = (x)_\infty^{F'} \text{ and } \mathrm{Con}_{F'|F}((x)^F) = (x)^{F'},$$

where the superscripts F and F' denote under which divisor group the divisor is considered.

Proof. From the definition of the principal divisor:

$$\begin{aligned}(x)^{F'} &= \sum_{P' \in \mathbb{P}_{F'}} v_{P'}(x) \cdot P' = \sum_{P' \in \mathbb{P}_{F'}} \sum_{P'|P} e(P'|P) \cdot v_P(x) \cdot P' \\ &= \sum_{P' \in \mathbb{P}_{F'}} v_P(x) \cdot \mathrm{Con}_{F'|F}(P) = \mathrm{Con}_{F'|F}\left(\sum_{P \in \mathbb{P}_F} v_P(x) \cdot P\right) \\ &= \mathrm{Con}_{F'|F}((x)^F).\end{aligned}$$

Considering only the positive or negative components of the principal divisor, the other assertions follow. □

This proposition means the conorm also induces a homomorphism between divisor class groups

$$\mathrm{Con}_{F'|F} : \mathrm{Cl}(F) \to \mathrm{Cl}(F').$$

Lemma 12. *Let $K'|K$ be a finite extension and x transcendental over K. Then*

$$[K'(x) : K(x)] = [K' : K].$$

Using this lemma, we can now prove the most important result of this section:

Theorem 20 (Fundamental Equality)**.** *Let $F'|K'$ be a finite extension of $F|K$. Given $P \in \mathbb{P}_F$, let $P_1, \ldots, P_m$ be all places of F' lying over P. If $e_i := e(P_i|P)$ and $f_i := f(P_i|P)$, then*

$$\sum_{i=1}^{m} e_i f_i = [F' : F].$$

Proof. Take $x \in F$ such that P is the only zero of x in $F|K$ and set $r := v_P(x) > 0$. The places $P_1, \ldots, P_m \in \mathbb{P}_{F'}$ are the zeros of x in $F'|K'$. We compute $[F' : K(x)]$ in two

different ways:

$$\begin{aligned}
[F' : K(x)] &= [F' : K'(x)][K'(x) : K(x)] \\
&= \left(\sum_{i=1}^{m} v_{P_i}(x) \cdot \deg P_i \right) \cdot [K' : K] \\
&= \sum_{i=1}^{m} (e_i \cdot v_P(x)) \cdot [F'_{P_i} : K'] \cdot [K' : K] \\
&= r \cdot \sum_{i=1}^{m} e_i \cdot [F'_{P_i} : F_P] \cdot [F_P : K] \\
&= r \cdot \deg P \cdot \sum_{i=1}^{m} e_i f_i.
\end{aligned}$$

On the other hand,

$$[F' : K(x)] = [F' : F][F : K(x)] = [F' : F] \cdot r \cdot \deg P,$$

since $(x)_0^F = rP$. Comparing the two equalities yields the result. □

Corollary 10. *Let $F'|K'$ be a finite extension of $F|K$ and $P \in \mathbb{P}_F$. Then*

(a) $|\{P' \in \mathbb{P}_{F'} : P' \supseteq P\}| \leqslant [F' : F]$.

(b) If $P'|P$, then $e(P'|P) \leqslant [F' : F]$ and $f(P'|P) \leqslant [F' : F]$.

We can now give the following definition

Definition 35. *Let $F'|K'$ be an extension of $F|K$ with $n := [F' : F]$ and $P \in \mathbb{P}_F$.*

(a) P splits completely in $F'|F$ if there are exactly n distinct places of F' lying over P.

(b) P is totally ramified in $F'|F$ if there is a place $P' \in \mathbb{P}_{F'}$ with $P'|P$ and $e(P'|P) = n$.

The Fundamental equality implies that $P \in \mathbb{P}_F$ splits completely in $F'|F$ if and only if $e(P'|P) = f(P'|P) = 1$ for all $P'|P$. And if P is totally ramified, there is only one place $P' \in \mathbb{P}_F$ that extends it.

Corollary 11. *Let $F'|K'$ be a finite extension of $F|K$. For each $A \in \mathrm{Div}(F)$*

$$\deg \mathrm{Con}_{F'|F}(A) = \frac{[F' : F]}{[K' : K]} \cdot \deg A.$$

Proof. It suffices to prove the result for a prime divisor $A = P \in \mathbb{P}_F$. We have

$$\begin{aligned}
\deg \mathrm{Con}_{F'|F}(P) &= \sum_{P'|P} e(P'|P) \cdot [F'_{P'} : K'] \\
&= \sum_{P'|P} e(P'|P) \cdot \frac{[F'_{P'} : K]}{[K' : K]} \\
&= \frac{1}{[K' : K]} \cdot \left(\sum_{P'|P} e(P'|P) \cdot [F'_{P'} : F_P] \right) \cdot [F_P : K] \\
&= \frac{[F' : F]}{[K' : K]} \cdot \deg P.
\end{aligned}$$

□

Finally, we present a criterion for polynomial irreducibility.

Proposition 19 (Eisenstein Criterion)**.** *Let $F|K$ be an algebraic function field and*

$$\varphi(T) = a_n T^n + \cdots + a_1 T + a_0$$

be a polynomial with $a_i \in F$. Assume there is a place $P \in \mathbb{P}_F$ such that one of the following conditions hold

1. *$v_P(a_n) = 0$, $v_P(a_i) \geqslant v_P(a_0) > 0$ for $i = 1, \ldots, n-1$, and $\gcd(n, v_P(a_0)) = 1$.*
2. *$v_P(a_n) = 0$, $v_P(a_i) \geqslant 0$ for $i = 1, \ldots, n-1$, $v_P(a_0) < 0$, and $\gcd(n, v_P(a_0)) = 1$.*

Then $\varphi(T)$ is irreducible in $F[T]$. If $F' = F(y)$ with $\varphi(y) = 0$, then P has a unique extension $P' \in \mathbb{P}_{F'}$ and $e(P'|P) = n$, $f(P'|P) = 1$.

1.9 Subrings and Integral Bases

Definition 36. *A subring of a function field $F|K$ is a ring R such that $K \subseteq R \subseteq F$ and R is not a field. In particular, $K \subsetneq R \subsetneq F$.*

Some examples of subrings are the valuation ring $\mathcal{O}_P$ of a place $P \in \mathbb{P}_F$ and the polynomial ring $K[x_1, \ldots, x_n]$ with $x_1, \ldots, x_n \in F \backslash K$.

Definition 37. *Given $\varnothing \neq S \subsetneq \mathbb{P}_F$, let $\mathcal{O}_S := \{z \in F : v_P(z) \geqslant 0 \text{ for all } P \in S\}$ be the intersection of all valuation rings $\mathcal{O}_P$ with $P \in S$. A ring of the form $R = \mathcal{O}_S$ is called a holomorphy ring of $F|K$.*

For example, $K[x]$ is a holomorphy ring of $K(x)|K$ since $K[x] = \bigcap_{P \neq P_\infty} \mathcal{O}_P$.

Lemma 13. *(a) Every valuation ring $\mathcal{O}_P$ is a holomorphy ring: $\mathcal{O}_P = \mathcal{O}_S$ for $S = \{P\}$.*

(b) Every holomorphy ring $\mathcal{O}_S$ is a subring of $F|K$.

(c) For $P \in \mathbb{P}_F$ and $\emptyset \neq S \subsetneq \mathbb{P}_F$, $\mathcal{O}_S \subseteq \mathcal{O}_P \iff P \in S$. Consequently, $\mathcal{O}_S = \mathcal{O}_T \iff S = T$.

Definition 38. *Let R be a subring of $F|K$.*

(a) An element $z \in F$ is said to be integral over R if $f(z) = 0$ for some monic polynomial $f(T) \in R[T]$. The equation $f(z) = 0$ is called the integral equation of z over R.

(b) The set $\mathrm{ic}_F(R) := \{z \in F : z \text{ is integral over } R\}$ is called the integral closure of R in F.

(c) If $F_0 \subseteq F$ is the quotient field of R, then the ring R is called integrally closed if $\mathrm{ic}_{F_0}(R) = R$.

Proposition 20. *If $\mathcal{O}_S$ is a holomorphy ring of $F|K$, then*

(a) F is the quotient field of $\mathcal{O}_S$.

(b) $\mathcal{O}_S$ is integrally closed.

Theorem 21. *Let R be a subring of $F|K$ and $S(R) := \{p \in \mathbb{P}_F : R \subseteq \mathcal{O}_P\}$. Then $\emptyset \neq S(R) \subsetneq \mathbb{P}_F$ and the integral closure of R in F is $\mathcal{O}_{S(R)}$.*

Corollary 12. *A subring R of $F|K$ with quotient field F is integrally closed if and only if it is a holomorphy ring.*

Proposition 21. *If $\mathcal{O}_S$ is a holomorphy ring of $F|K$, there is a bijection between S and the set of maximal ideals of $\mathcal{O}_S$ given by $P \mapsto M_P := P \cap \mathcal{O}_S$ for $P \in S$. Furthermore, the following map is an isomorphism*

$$\begin{aligned} \varphi : \mathcal{O}_S/M_P &\to F_P \\ x + M_P &\mapsto x + P. \end{aligned}$$

Proposition 22. *If $\emptyset \neq S \subseteq \mathbb{P}_F$ is finite, then $\mathcal{O}_S$ is a principal ideal domain.*

We now consider $F|K$ a function field with K its full constant field and $F'|K'$ a finite field extension of $F|K$.

Proposition 23. *Let R be a holomorphy ring of F. For $z \in F'$, if $\varphi(T) \in F[T]$ denotes its minimal polynomial over F, then z is integral over R if and only if $\varphi(T) \in R[T]$.*

Corollary 13. *Let $\mathrm{Tr}_{F'|F} : F' \to F$ denote the trace map from F' to F and $x \in F'$ be an integral element over R. Then $\mathrm{Tr}_{F'|F}(x) \in R$.*

Proposition 24. *Let $M|L$ be a separable finite field extension with basis $\{z_1, \ldots, z_n\}$. Then there are unique elements $z_1^*, \ldots, z_n^* \in M$ such that $\mathrm{Tr}_{M|L}(z_i z_j^*) = \delta_{ij}$, where δ_{ij} denotes the Kronecker delta. The set $\{z_1^*, \ldots, z_n^*\}$ is also a base for $M|L$ called the dual base of $\{z_1, \ldots, z_n\}$ with respect to the trace.*

Theorem 22. *Let R be an integrally closed subring of $F|K$ with quotient field F and $F'|F$ be a separable field extension of degree n. If R' denotes the integral closure of R in F', then*

(a) For every base $\{x_1, \ldots, x_n\}$ of $F'|F$ there are elements $a_i \in R^*$ such that $a_1 x_1 + \cdots + a_n x_n \in R'$. It follows that there are bases of $F'|F$ which are contained in R'.

(b) If $\{z_1, \ldots, z_n\} \subseteq R'$ is a base of $F'|F$ and $\{z_1^*, \ldots, z_n^*\}$ is its dual with respect to the trace, then

$$\sum_{i=1}^{n} Rz_i \subseteq R' \subseteq \sum_{i=1}^{n} Rz_i^*.$$

(c) If R is also a principal ideal domain, there exists a base $\{u_1, \ldots, u_n\}$ of $F'|F$ such that $R' = \sum_{i=1}^{n} Ru_i$.

Corollary 14. *If $F'|F$ is a finite separable extension of and P is a place of F, then the integral closure $\mathcal{O}'_P$ of $\mathcal{O}_P$ is $\mathcal{O}'_P = \bigcap_{P'|P} \mathcal{O}_P$. Also, since $\mathcal{O}_P$ is a principal ideal domain, there is a base $\{u_1, \ldots, u_n\}$ of $F'|F$ such that $\mathcal{O}'_P = \sum_{i=1}^{n} \mathcal{O}_P \cdot u_i$. In this case, $\{u_1, \ldots, u_n\}$ is called an integral base of P or of $\mathcal{O}'_P$ over $\mathcal{O}_P$.*

Theorem 23. *Let $F'|F$ be a finite separable extension. Then each base $\{z_1, \ldots, z_n\}$ of $F'|F$ is an integral base for all but finitely many places.*

We will now prove a theorem that will help with determining all the extensions of a place $P \in \mathbb{P}_F$ in an extension $F'|F$. In the sequel, we use the notation $\bar{F} := F_P$ for the residue class field of P, $\bar{a} := a(P) \in \bar{F}$ the residue class of $a \in \mathcal{O}_P$ and if $\psi(T) = \sum c_i T^i \in \mathcal{O}_P[T]$, we set $\bar{\psi}(T) := \sum \bar{c}_i T^i \in \bar{F}[T]$. Also, we can represent every polynomial $\gamma(T) \in \bar{F}[T]$ as $\gamma(T) = \bar{\psi}(T)$ with $\psi(T) \in \mathcal{O}_P[T]$ and $\deg \psi = \deg \gamma$.

Theorem 24 (Kummer)**.** *Suppose $F' = F(y)$ for some y integral over $\mathcal{O}_P$, and consider the minimal polynomial $\varphi(T) \in \mathcal{O}_P[T]$ of y over F. Let $\bar{\psi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\varepsilon_i}$ be the decomposition of $\bar{\psi}$ into irreducible factors over $\bar{F}$. Choose monic polynomials $\psi_i(T) \in \mathcal{O}_P[T]$ with $\bar{\psi}_i(T) = \gamma_i(T)$ and $\deg \psi_i = \deg \gamma_i$. Then, for $1 \leqslant i \leqslant r$, there are places $P_i \in \mathbb{P}_{F'}$ such that $P_i|P$, $\psi_i(y) \in P_i$ and $f(P_i|P) \geqslant \deg \gamma_i$. Moreover $P_i \neq P_j$ if $i \neq j$.*

If we suppose at least one of the following conditions is satisfied

(i) $\varepsilon_i = 1$ *for* $i = 1, \ldots, r$.

(ii) $\{1, y, \ldots, y^{n-1}\}$ *is an integral basis for* P.

Then there exists, for $1 \leqslant i \leqslant r$, *exactly one place* $P_i \in \mathbb{P}_{F'}$ *with* $P_i | P$ *and* $\varphi_i(y) \in P_i$. *The places* $P_1, \ldots, P_r$ *are all the places of* F' *lying over* P *and we have*

$$\mathrm{Con}_{F'|F}(P) = \sum_{i=1}^{r} \varepsilon_i P_i,$$

that is, $\varepsilon_i = e(P_i|P)$. *The residue class field* F'_{P_i} *is isomorphic to* $\bar{F}[T]/\langle \gamma_i(T) \rangle$, *hence* $f(P_i|P) = \deg \gamma_i$.

Proof. Set $\bar{F}_i := \bar{F}[T]/\langle \gamma_i(T) \rangle$. Since γ_i is irreducible, $\bar{F}_i | \bar{F}$ has degree

$$[\bar{F}_i : \bar{F}] = \deg \gamma_i. \tag{1.28}$$

Consider the ring $\mathcal{O}_P[y] = \sum_{j=0}^{n-1} \mathcal{O}_P \cdot y^j$, where $n = \deg \varphi = [F' : F]$. There are ring homomorphisms

$$\begin{aligned} \rho : \mathcal{O}_P[T] &\to \mathcal{O}_P[y] \\ \textstyle\sum c_j T^j &\mapsto \textstyle\sum c_j y^j \end{aligned}$$

and

$$\begin{aligned} \pi_i : \mathcal{O}_P[T] &\to \bar{F}_i \\ \textstyle\sum c_j T^j &\mapsto \textstyle\sum \bar{c}_j T^j \mod \gamma_i(T). \end{aligned}$$

We see that $\ker \rho = \langle \varphi(T) \rangle$. Since $\pi_i(\varphi(T)) = \bar{\varphi}(T) \mod \gamma_i(T) = 0$, it follows that $\ker \rho \subseteq \ker \pi_i$. Therefore, there is a unique homomorphism $\sigma_i : \mathcal{O}_P[y] \to \bar{F}_i$ with $\pi_i = \sigma_i \circ \rho$, given explicitly by

$$\begin{aligned} \sigma_i : \mathcal{O}_P[y] &\to \bar{F}_i \\ \sum_{j=0}^{n-1} c_j y^j &\mapsto \sum_{j=0}^{n-1} \bar{c}_j y^j \mod \gamma_i(T), \end{aligned}$$

which is also surjective. We show that

$$\ker \sigma_i = P \cdot \mathcal{O}_P[y] + \varphi_i(y) \cdot \mathcal{O}_P[y]. \tag{1.29}$$

From the definition of σ_i, the inclusion $P \cdot \mathcal{O}_P[y] + \varphi_i(y) \cdot \mathcal{O}_P[y] \subseteq \ker \sigma_i$ follows. Conversely, take $\sum_{j=0}^{n-1} c_j y^j \in \ker \sigma_i$. Then $\sum_{j=0}^{n-1} \bar{c}_j T^j = \bar{\varphi}_i(T) \cdot \bar{\psi}(T)$ for some $\psi(T) \in \mathcal{O}_P[T]$, hence

$$\sum_{j=0}^{n-1} c_j T^j - \varphi_i(T) \cdot \psi(T) \in P \cdot \mathcal{O}_P[T].$$

Setting $T = y$ yields

$$\sum_{j=0}^{n-1} c_j y^j - \varphi_i(y) \cdot \psi(y) \in P \cdot \mathcal{O}_P[y],$$

proving (1.29).

Using Theorem 3, there exists a place $P_i \in \mathbb{P}_F$ such that $\ker \sigma_i \subseteq P_i$ and $\mathcal{O}_P[Y] \subseteq \mathcal{O}_{P_i}$, implying $P_i|P$ and $\varphi_i(y) \in P_i$. The residue class field $\mathcal{O}_{P_i}/P_i$ contains $\mathcal{O}_P[y]/\ker \sigma_i$, which is isomorphic to $\bar{F}_i$ via σ_i. From (1.28), we see that

$$f(P_i|P) \geqslant [\bar{F}_i : \bar{F}] = \deg \gamma_i.$$

For $i \neq j$, the polynomials $\gamma_i(T) = \bar{\varphi}_i(T)$ and $\gamma_j(T) = \bar{\varphi}_j(T)$ are coprime in $\bar{F}[T]$, meaning there exists $\lambda_i(T), \lambda_j(T) \in \mathcal{O}_P[T]$ such that

$$1 = \bar{\varphi}_i(T) \cdot \bar{\lambda}_i(T) + \bar{\varphi}_j(T) \cdot \bar{\lambda}_j(T),$$

and thus

$$\varphi_i(T) \cdot \lambda_i(T) + \varphi_j(T) \cdot \lambda_j(T) - 1 \in P \cdot \mathcal{O}_P[y].$$

This means $1 \in \ker \sigma_i + \ker \sigma_j$ by (1.29). Since $P_i \supseteq \ker \sigma_i$ and $P_j \supseteq \ker \sigma_j$, it is proved that $P_i \neq P_j$ for $i \neq j$.

Now, assume that condition (i) is fulfilled, that is, $\bar{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T)$. Then

$$\begin{aligned}
[F' : F] = \deg \varphi &= \sum_{i=1}^{r} \deg \varphi_i \\
&\leqslant \sum_{i=1}^{r} f(P_i|P) \leqslant \sum_{i=1}^{r} e(P_i|P) \cdot f(P_i|P) \\
&\leqslant \sum_{P'|P} e(P'|P) \cdot f(P'|P) = [F' : F]
\end{aligned}$$

by the Fundamental Equality. This is only possible if $e(P_i|P) = 1$, $f(P_i|P) = \deg \varphi_i$ and the only places that extend P are $P_1, \ldots, P_r$.

If condition (ii) is satisfied, choose $P_i \in \mathbb{P}_{F'}$ such that $P_i|P$ and $\varphi_i(y) \in P_i$. First we show that $P_1, \ldots, P_r$ are the only extensions of P in F'. Take $P' \in \mathbb{P}_{F'}$ with $P'|P$. Since

$$0 = \varphi(y) \equiv \prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \mod P \cdot \mathcal{O}_P[y],$$

we have

$$\prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \in P' \tag{1.30}$$

P' is a prime ideal of $\mathcal{O}_{P'}$, so $\varphi_i(y) \in P'$ for some $i \in \{1, \ldots, r\}$ and

$$P \cdot \mathcal{O}_P[y] + \varphi_i(y) \cdot \mathcal{O}_P[y] \subseteq P' \cap \mathcal{O}_P[y] \tag{1.31}$$

by (1.30). The left side is a maximal ideal of $\mathcal{O}_P[y]$ by (1.29), meaning equality holds in (1.31). Since we also know that

$$P \cdot \mathcal{O}_P[y] + \varphi_i(y) \cdot \mathcal{O}_P[y] \subseteq P_i \cap \mathcal{O}_P[y],$$

it follows that

$$P' \cap \mathcal{O}_P[y] = P_i \cap \mathcal{O}_P[y] = P \cdot \mathcal{O}_P[y] + \varphi_i(y) \cdot \mathcal{O}_P[y]. \tag{1.32}$$

Since $\mathcal{O}_P[y]$ is the integral closure of $\mathcal{O}_P$ in F' by condition (ii), Proposition 21 implies $P' = P_i$ and our claim is proved. Having showed this, an immediate consequence of applying 14 is

$$\mathcal{O}_P[y] = \bigcap_{i=1}^{r} \mathcal{O}_{P_i}. \tag{1.33}$$

Using the Approximation Theorem, we find elements $t_1, \ldots, t_r \in F'$ such that

$$v_{P_i}(t_i) = 1 \text{ and } v_{P_j}(t_i) = 0 \text{ for } i \neq j.$$

Choose a P-prime element $t \in F$, then

$$t_i \in \mathcal{O}_P[y] \cap P_i = \varphi_i(y) \cdot \mathcal{O}_P[y] + t \cdot \mathcal{O}_P[y]$$

by (1.32) and (1.33). Thus, there exists $a_i(y), b_i(y) \in \mathcal{O}_P[y]$ such that

$$t_i = \varphi_i(y) \cdot a_i(y) + t \cdot b_i(y).$$

From this we get

$$\prod_{i=1}^{r} t_i^{\varepsilon_i} = a(y) \cdot \prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} + t \cdot b(y) \tag{1.34}$$

for some $a(y), b(y) \in \mathcal{O}_P[y]$. Since

$$\prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \equiv \varphi(y) \mod t \cdot \mathcal{O}_P[y]$$

and $\varphi(y) = 0$, (1.34) implies that

$$\prod_{i=1}^{r} t_i^{\varepsilon_i} = t \cdot u(y) \text{ for some } u(y) \in \mathcal{O}_P[y]. \tag{1.35}$$

Therefore

$$\varepsilon_i = v_{P_i}\left(\prod_{j=1}^{r} t_j^{\varepsilon_j}\right) \geqslant v_{P_i}(t) = e(P_i|P). \tag{1.36}$$

On the other hand,

$$f(P_i|P) = \deg \gamma_i \tag{1.37}$$

by (1.28), (1.29), (1.32) and Proposition 21. Finally, applying the Fundamental Equality yields

$$\begin{aligned}[F' : F] &= \sum_{i=1}^{r} e(P_i|P) \cdot f(P_i|P) \\ &\leqslant \sum_{i=1}^{r} \varepsilon_i \cdot \deg \gamma_i = \deg \varphi = [F' : F],\end{aligned}$$

proving that $\varepsilon_i = e(P_i|P)$ for all $i = 1, \ldots, r$. □

Corollary 15. *Let $\varphi(T) = T^n + f_{n-1}(x)T^{n-1} + \cdots + f_0(x) \in K(x)[T]$ be an irreducible polynomial over the rational function field $K(x)$. Consider the extension $K(x,y)|K$ where $\varphi(y) = 0$ and an element $\alpha \in K$ with $f_j(\alpha) \neq \infty$ for all $j = 0, \ldots, n-1$. Suppose the polynomial*

$$\varphi_\alpha(T) := T^n + f_{n-1}(\alpha)T^{n-1} + \cdots + f_0(\alpha) \in K[T]$$

decomposes as $\prod_{i=1}^{r} \psi_i(T)$ over $K[T]$ with irreducible, monic and pairwise distinct polynomials $\psi_i(T) \in K[T]$. Then the following hold

(a) For every $i = 1, \ldots, r$ there is a unique place $P_i \in \mathbb{P}_{K(x,y)}$ such that $x - \alpha \in P_i$ and $\psi_i(y) \in P_i$. The element $x - \alpha$ is a prime element of P_i, that is, $e(P_i|P_\alpha) = 1$ and the residue class field of P_i is K-isomorphic to $K[T]/\langle \psi_i(T) \rangle$, hence $f(P_i|P_\alpha) = \deg \psi_i$.

(b) If $\deg \psi_i = 1$ for at least one $i \in \{1, \ldots, r\}$, then K is the full constant field of $K(x,y)$.

(c) If $\varphi_\alpha(T)$ has $\deg \varphi$ distinct roots β in K, then there is for each β a unique place $P_{\alpha,\beta} \in \mathbb{P}_{K(x,y)}$ such that $x - \alpha \in P_{\alpha,\beta}$ and $y - \beta \in P_{\alpha,\beta}$. Also, $P_{\alpha,\beta}$ is a rational place of $K(x,y)$.

Proof. Set $F := K(x)$ and $F' := K(x,y)$. The assumption $f_j(\alpha) \neq \infty$ means y is integral over $\mathcal{O}_{P_\alpha}$, and $\varphi_\alpha(T)$ is merely $\bar{\varphi}(T)$ using the notation from Kummer's Theorem. Therefore, condition (i) is satisfied and the corollary follows. □

1.10 The Hurwitz Genus Formula

This most important result of this section is the Hurwitz formula for the genus of a function field extension. In order to prove this, we first introduce the notions of the cotrace of a Weil differential, as well as the different of a function field extension.

Definition 39. *For $P \in \mathbb{P}_F$, let $\mathcal{O}'_P$ denote the integral closure of $\mathcal{O}_P$ in F'. The set*

$$\mathcal{C}_P := \{z \in F' : \mathrm{Tr}_{F'|F}(z \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P\}$$

is called the complementary module over $\mathcal{O}_P$.

Proposition 25. *(a) $\mathcal{C}_P$ is an $\mathcal{O}_P$-module with $\mathcal{O}'_P \subseteq \mathcal{C}_P$.*

(b) If $\{z_1, \ldots, z_n\}$ is an integral basis of $\mathcal{O}'_P$ over $\mathcal{O}_P$, then

$$\mathcal{C}_P = \sum_{i=1}^{n} \mathcal{O}_P \cdot z_i^*,$$

where $\{z_1^*, \ldots, z_n^*\}$ is the dual basis of $\{z_1, \ldots, z_n\}$ with respect to the trace.

(c) There is an element $t \in F'$ depending on P such that $\mathcal{C}_P = t \cdot \mathcal{O}'_P$. Moreover, $v_{P'}(t) \leqslant 0$ for all $P'|P$ and for every $t' \in F'$, $\mathcal{C}_P = t' \cdot \mathcal{O}'_P$ if and only if $v_{P'}(t') = v_{P'}(t)$ for all $P'|P$.

(d) $\mathcal{C}_P = \mathcal{O}'_P$ for almost all $P \in \mathbb{P}_F$.

Definition 40. *Let P be a place of F and $\mathcal{O}'_P$ be its integral closure in F'. If $\mathcal{C}_P = t \cdot \mathcal{O}_P$', then the different exponent of $P'|P$ is $d(P'|P) := -v_{P'}(t)$. By Proposition 25, $d(P'|P)$ is well-defined and non-negative. And since $\mathcal{C}_P = 1 \cdot \mathcal{O}'_P$, $d(P'|P) = 0$ for almost all $P \in \mathbb{P}_F$. This means the following divisor, called the different of $F'|F$ is well-defined:*

$$\mathrm{Diff}(F'|F) := \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P) \cdot P'.$$

Remark 9. *From the definitions, we can characterize the complementary module by the following equivalence*

$$z \in \mathcal{C}_P \iff v_{P'}(z) \geqslant -d(P'|P) \text{ for all } P'|P.$$

Definition 41. *The adele space of a function field extension $F'|F$ is*

$$\mathcal{A}_{F'|F} := \{\alpha \in \mathcal{A}_{F'} : \alpha_{P'} = \alpha_{Q'} \text{ if } P' \cap F = Q' \cap F\}.$$

This is an F'-subspace of $A_{F'}$. We can also extend the trace map $\mathrm{Tr}_{F'|F} : F' \to F$ to an F-linear map from $\mathcal{A}_{F'|F}$ to $\mathcal{A}_F$ setting

$$(\mathrm{Tr}_{F'|F}(\alpha))_P := \mathrm{Tr}_{F'|F}(\alpha_{P'}) \text{ for } \alpha \in \mathcal{A}_{F'|F}$$

where P' is any place of F' that extends P. We notice that $\alpha_{P'} \in \mathcal{O}_{P'}$ for almost all $P' \in \mathbb{P}_{F'}$, meaning $\mathrm{Tr}_{F'|F}(\alpha_{P'}) \in \mathcal{O}_P$ for almost all $P \in \mathbb{P}_F$ by Corollary 13. Hence $\mathrm{Tr}_{F'|F}(\alpha)$ is an adele of $F|K$. Furthermore, the trace of a principal adele $z \in F'$ is the principal adele of $\mathrm{Tr}_{F'|F}(z)$. Given a divisor $A' \in \mathrm{Div}(F')$, we set $\mathcal{A}_{F'|F}(A') = \mathcal{A}_{F'}(A') \cap \mathcal{A}_{F'|F}$.

Theorem 25. *For every Weil differential of $F|K$, there exists a unique Weil differential ω' of $F'|K'$ such that*

$$\mathrm{Tr}_{K'|K}(\omega'(\alpha)) = \omega(\mathrm{Tr}_{F'|F}(\alpha))$$

for all $\alpha \in \mathcal{A}_{F'|F}$. This is called the cotrace of ω in $F'|F$, denoted by $\mathrm{Cotr}_{F'|F}(\omega)$. If $\omega \neq 0$ and (ω) is the divisor of ω, then

$$(\mathrm{Cotr}_{F'|F}(\omega)) = \mathrm{Con}_{F'|F}((\omega)) + \mathrm{Diff}(F'|F).$$

A particularly noteworthy case of this theorem is

Corollary 16. *Let $F|K$ be a function field and $x \in F$ be an element such that $F|K(x)$ is separable. If η is the Weil differential of the rational function field with $(\eta) = -2P_\infty$ ($-2P_\infty$ is canonical by Proposition 10), then*

$$(\mathrm{Cotr}_{F|K(x)}(\eta)) = -2(x)_\infty + \mathrm{Diff}(F|K(x)).$$

Some useful properties of the cotrace are

Proposition 26. *If ω, η are Weil differentials of $F|K$ and $x \in F$, then*

(a) $\mathrm{Cotr}_{F'|F}(\omega + \eta) = \mathrm{Cotr}_{F'|F}(\omega) + \mathrm{Cotr}_{F'|F}(\eta)$.

(b) $\mathrm{Cotr}_{F'|F}(x\omega) = x \cdot \mathrm{Cotr}_{F'|F}(\omega)$.

Corollary 17. *If $F'' \supseteq F' \supseteq F$ are finite separable extensions, then*

(a) $\mathrm{Diff}(F''|F) = \mathrm{Con}_{F''|F'}(\mathrm{Diff}(F'|F)) + \mathrm{Diff}(F''|F')$.

(b) $d(P''|P) = e(P''|P') \cdot d(P'|P) + d(P''|P)$, *if* $P \in \mathbb{P}_F$, $P' \in \mathbb{P}_{F'}$ *and* $P'' \in \mathbb{P}_{F''}$.

Finally, we can prove the main result of this section:

Theorem 26 (Hurwitz Genus Formula)**.** *If $F|K$ is a function field of genus g and $F'|K'$ is a finite seperable extension of F with genus g'. If K' is the full constant field of F', then*

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg \mathrm{Diff}(F'|F).$$

Proof. Take $\omega \neq 0$ a Weil differential of $F|K$. From Theorem 25:

$$\mathrm{Cotr}_{F'|F}(\omega) = \mathrm{Con}_{F'|F}((\omega)) + \mathrm{Diff}(F'|F).$$

The canonical divisors of F and F' have degree $2g - 2$ and $2g' - 2$, respectively. Applying Corollary 11 to the above equation yields

$$\begin{aligned} 2g' - 2 &= \deg \mathrm{Con}_{F'|F}((\omega)) + \deg \mathrm{Diff}(F'|F) \\ &= \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg \mathrm{Diff}(F'|F). \end{aligned}$$

□

Since every function field can be regarded as a finite extension of the rational function field, this special case of the Hurwitz genus formula is of great utility:

Corollary 18. *Let $F|K$ be a function field of genus g and $x \in F \backslash K$ be an element such that the extension $F|K(x)$ is separable. Then*

$$2g - 2 = -2[F : K(x)] + \deg \mathrm{Diff}(F|K(x)).$$

1.11 The Different

Given the Hurwitz genus formula discussed previously, a more in-depth investigation of the different divisor of an extension is warranted. The main result of this section is Dedekind's Different Theorem, which gives a more precise characterization to the different exponent of a place extension.

In order to prove the theorem, we make use of two lemmas:

Lemma 14. *Let $F'|F$ be an algebraic extension of function fields and $P \in \mathbb{P}_F$, $P' \in \mathbb{P}_{F'}$ such that $P'|P$. If σ is an automorphism of $F'|F$, then $\sigma(P') := \{\sigma(z) : z \in P'\}$ is a place of F' and*

(a) $v_{\sigma(P')}(y) = v_{P'}(\sigma^{-1}(y))$ *for all* $y \in F'$.

(b) $\sigma(P')|P$.

(c) $e(\sigma(P')|P) = e(P'|P)$ *and* $f(\sigma(P')|P) = f(P'|P)$.

Proof. First we notice that $\sigma(\mathcal{O}_{P'})$ is a valuation ring of F' with $\sigma(P')$ being its maximal ideal. Therefore, a place of F' with corresponding valuation ring $\mathcal{O}_{\sigma(P')} = \sigma(\mathcal{O}_{P'})$. If t' is a P'-prime element, then $\sigma(P') = \sigma(t') \cdot \sigma(\mathcal{O}_{P'})$, meaning $\sigma(t')$ is a $\sigma(P')$-prime element.

(a) Take a non-zero element $y \in F'$, say $y = \sigma(z)$. Then $z = t'^r u$ with $r := v_{P'}(z)$ and $u \in \mathcal{O}_{P'} \backslash P'$, thus $y = \sigma(t')^r \cdot \sigma(u)$ with $\sigma(U) \in \mathcal{O}_{\sigma(P')} \backslash \sigma(P')$ and $\sigma(t')$ is a prime element for $\sigma(P')$. We then conclude that $v_{\sigma(P')}(y) = r = v_{P'}(z) = v_{P'}(\sigma^{-1}(y))$.

(b) Since $P' \supseteq P$ and $\sigma(P) = P$, it follows that $\sigma(P') \supseteq \sigma(P) = P$, meaning $\sigma(P')|P$.

(c) Take x a P-prime element. Then

$$e(\sigma(P')|P) = v_{\sigma(P')}(x) = v_{P'}(\sigma^{-1}(x)) = v_{P'}(x) = e(P'|P).$$

The automorphism σ induces an automorphism $\bar{\sigma}$ between the residue class fields $F'_{P'}$ and $F'_{\sigma(P')}$ given by $\bar{\sigma}(z + P') = \sigma(z) + \sigma(P')$. This application is the identity over F_P, hence $f(P'|P) = f(\sigma(P')|P)$.

□

Lemma 15. *Let $P \in \mathbb{P}_F$ and $P_1, \ldots, P_r \in \mathbb{P}_{F'}$ be all extensions of P in $F'|F$. Consider the residue class fields $F_P := \mathcal{O}_P/P$, $F'_{P_i} := \mathcal{O}_{P_i}/P_i \supseteq F_P$ and their respective residue class maps $\pi : \mathcal{O}_P \to F_P$ and $\pi_i : \mathcal{O}_{P_i} \to F'_{P_i}$. Then, for every $u \in \mathrm{ic}_{F'}(\mathcal{O}_P)$, we have*

$$\pi(\mathrm{Tr}_{F'|F}(u)) = \sum_{i=1}^{r} e(P_i|P) \cdot \mathrm{Tr}_{F'_{P_i}|F_P}(\pi_i(u)).$$

Theorem 27 (Dedekind's Different Theorem)**.** *Given $F'|K'$ a finite separable extension of $F|K$, for all $P \in \mathbb{P}_F$, $P' \in \mathbb{P}'_F$ such that $P'|P$, the following are valid*

(a) $d(P'|P) \geqslant e(P'|P) - 1$.

(b) $d(P'|P) = e(P'|P) - 1$ *if and only if* $e(P'|P)$ *is not divisible by* $\operatorname{char} K$. *In particular, if* $\operatorname{char}(K) = 0$, *then* $d(P'|P) = e(P'|P) - 1$.

Proof. (a) Let $\mathcal{O}'_P$ denote the integral closure of $\mathcal{O}_P$ on F' and $\mathcal{C}_P$ denote its complementary module. We wish to prove that

$$\operatorname{Tr}_{F'|F}(t \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P \tag{1.38}$$

for all $t \in F'$ such that

$$v_{P'}(t) = 1 - e(P'|P) \text{ for all } P'|P. \tag{1.39}$$

The inclusion (1.38) implies $t \in \mathcal{C}_P$ and the characterization of $\mathcal{C}_P$ given in Remark 9 yields $1 - e(P'|P) \geqslant -d(P'|P)$, implying $d(P'|P) \geqslant e(P'|P) - 1$.

In order to prove (1.38), take a finite Galois extension $F''|F$ such that $F \subseteq F' \subseteq F''$ and choose $n = [F' : F]$ automorphisms $\sigma_1, \ldots, \sigma_n$ of $F''|F$ who are all distinct when restricted to F'. For $z \in \mathcal{O}'_P$:

$$\operatorname{Tr}_{F'|F}(tz) = \sum_{i=1}^{n} \sigma_i(tz). \tag{1.40}$$

Fix a place P'' of F'' lying over P. Set $P''_i := \sigma_i^{-1}(P'')$ and $P'_i := P''_i \cap F'$. We see that $\sigma_i(z)$ is integral over $\mathcal{O}_P$, since $z \in \mathcal{O}'_P$, and thus $v_{P''}(\sigma_i(z)) \geqslant 0$. Then

$$\begin{aligned} v_{P''}(\sigma_i(tz)) &= v_{P''}(\sigma_i(t)) + v_{P''}(\sigma_i(z)) \\ &\geqslant v_{P''}(\sigma_i(t)) \overset{14(a)}{=} v_{P''_i}(t) \\ &\overset{(1.39)}{=} e(P''_i|P'_i)(1 - e(P'_i|P)) \\ &> -e(P''_i|P'_i) \cdot e(P'_i|P) \\ &= -e(P''_i|P) \overset{14(c)}{=} -e(P''|P). \end{aligned}$$

Using (1.40) we conclude

$$-e(P''|P) < v_{P''}(\operatorname{Tr}_{F'|F}(tz)) = e(P''|P) \cdot v_P(\operatorname{Tr}_{F'|F}(tz)),$$

meaning $v_P(\operatorname{Tr}_{F'|F}(tz)) \geqslant 0$, and hence (1.38).

(b) Using the notation of Lemma 15, set $e_i := e(P_i|P)$, $P' := P_1$ and $e := e(P'|P)$. We must prove that

$$d(P'|P) = e - 1 \iff \operatorname{char} K \text{ does not divide } e. \tag{1.41}$$

First suppose e is not divisible by $\operatorname{char} K$ and $d(P'|P) \geqslant e$. Then there exists some $w \in F'$ with

$$v_{P'}(w) \leqslant -e \text{ and } \operatorname{Tr}_{F'|F}(w \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P. \tag{1.42}$$

Since K is a perfect field, the extension $F'_{P_i}|F_P$ is separable, and we can find $y_0 \in \mathcal{O}_{P'}$ with $\operatorname{Tr}_{F'_{P_i}|F_P}(\pi_1(y_0)) \neq 0$. By the Approximation Theorem, there is some $y \in F'$ such that $v_{P'}(y - y_0) > 0$ and

$$v_{P_i}(y) \geqslant \max\{1, e_i + v_{P_i}(w)\} \text{ for } 2 \leqslant i \leqslant r. \tag{1.43}$$

Then $y \in \mathcal{O}'_P$ and applying Lemma 15 yields

$$\begin{aligned}\pi(\operatorname{Tr}_{F'|F}(y)) &= e \cdot \operatorname{Tr}_{F'_{P_1}|F_P}(\pi_1(y)) + \sum_{i=2}^{r} e_i \cdot \operatorname{Tr}_{F'_{P_i}|F_P}(\pi_i(y)) \\ &= e \cdot \operatorname{Tr}_{F'_{P_1}|F_P}(\pi_1(y_0)) \neq 0,\end{aligned}$$

since $\operatorname{char} K$ not dividing e implies $e \neq 0$ in F_P. We conclude that $v_P(\operatorname{Tr}_{F'|F}(y)) = 0$. Now take $x \in F$ a P-prime element. Then

$$\operatorname{Tr}_{F'|F}(x^{-1}y) = x^{-1} \cdot \operatorname{Tr}_{F'|F}(y) \notin \mathcal{O}_P. \tag{1.44}$$

On the other hand, $x^{-1}yw^{-1} \in \mathcal{O}'_P$, since

$$v_{P'}(x^{-1}yw^{-1}) = -e + v_{P'}(y) - v_{P'}(w) \geqslant 0$$

and

$$v_{P_i}(x^{-1}yw^{-1}) = v_{P_i}(y) - (e_i + v_{P_i}(w)) \geqslant 0$$

for $i = 2, \ldots, r$ by (1.42) and (1.43). Thus, $x^{-1}y \in w \cdot \mathcal{O}'_P$ and $\operatorname{Tr}_{F'|F}(x^{-1}y) \in \mathcal{O}_P$ by (1.42), which contradicts (1.44). This proves the reverse implication of (1.41).

In order to prove the direct implication, assume $\operatorname{char} K$ divides e and we must show that $d(P'|P) \geqslant e$. Choose $u \in F'$ such that

$$v_{P'}(u) = -e \text{ and } v_{P_i}(u) \geqslant -e_i + 1 \text{ for } i = 2, \ldots, r. \tag{1.45}$$

If $x \in F$ is a P-prime element, for every $z \in \mathcal{O}'_P$, we have $v_{P'}(xuz) \geqslant 0$ and $v_{P_i}(xuz) > 0$ for $i = 2, \ldots, r$. Therefore, $xuz \in \mathcal{O}'_P$, and by Lemma 15:

$$\begin{aligned}\pi(\operatorname{Tr}_{F'|F}(xuz)) &= e \cdot \operatorname{Tr}_{F'_{P_1}|F_P}(\pi_1(xuz)) + \sum_{i=2}^{r} e_i \cdot \operatorname{Tr}_{F'_{P_i}|F_P}(\pi_i(xuz)) \\ &= e \cdot \operatorname{Tr}_{F'_{P_1}|F_P}(\pi_1(xuz)) = 0.\end{aligned}$$

We conclude that $x \cdot \operatorname{Tr}_{F'|F}(uz) = \operatorname{Tr}_{F'|F}(xuz) \in P = x \cdot \mathcal{O}_P$, implying $\operatorname{Tr}_{F'|F}(uz) \in \mathcal{O}_P$ for all $z \in \mathcal{O}'_P$. Thus, $u \in \mathcal{C}_P$ and $-e = v_{P'}(u) \geqslant -d(P'|P)$ by (1.45) and Remark 9. □

Definition 42. *Let $F'|F$ be an algebraic extension of function fields and $P \in \mathbb{P}_F$.*

(a) An extension P' of P is said to be tamely ramified if $e(P'|P) > 1$ and $\operatorname{char} K \nmid e(P'|P)$. If $\operatorname{char} K \mid e(P'|P)$, the extension is wildly ramified.

(b) P is said to be ramified in $F'|F$ if there exists some $P' \in \mathbb{P}_{F'}$ for which $P'|P$ is ramified. P is unramified otherwise. Furthermore, P is tamely ramified if no extension of P in F' is wildly ramified. If there is at least one wildly ramified extension $P'|P$, P is said to be wildly ramified.

(c) P is totally ramified in $F'|F$ if there is only one extension $P' \in \mathbb{P}_{F'}$ of P in F' and the ramification index is $e(P'|P) = [F' : F]$.

(d) $F'|F$ is ramified if at least one place $P \in \mathbb{P}_F$ is ramified in $F'|F$. Otherwise, $F'|F$ is said to be unramified.

(e) The extension $F'|F$ is tame if no $P \in \mathbb{P}_F$ is wildly ramified in $F'|F$.

Corollary 19. *If $F'|F$ is a finite separable extension*

(a) The extension $P'|P$ is ramified if and only if $P' \leqslant \operatorname{Diff}(F'|F)$. If $P'|P$ is ramified, then $d(P'|P) = e(P'|P) - 1$ if and only if $P'|P$ is tamely ramified, and $d(P'|P) \geqslant e(P'|P)$ if and only if $P'|P$ is wildly ramified.

(b) Almost all places $P \in \mathbb{P}_F$ are unramified in $F'|F$.

Corollary 20. *If $F'|F$ is a finite separable extension such that K is the full constant field of F and F', denoting their respective genera by g and g', we have*

$$2g' - 2 \geqslant [F' : F] \cdot (2g - 2) + \sum_{P \in \mathbb{P}_F} \sum_{P'|P} (e(P'|P) - 1) \cdot \deg P',$$

where equality holds if and only $F'|F$ is tame.

Corollary 21. *If $F'|F$ is a finite separable extension of function fields with the same constant field. Then $g \leqslant g'$.*

Corollary 22. *Let $F|K(x)$ be a finite separable extension of the rational function field of degree $[F : K(x)] > 1$ such that K is the full constant field of F. Then $F|K(x)$ is ramified.*

Theorem 28. *Suppose $F' = F(y)$ is a finite separable extension of F with $[F' : F] = n$. Let $P \in \mathbb{P}_F$ be such that the minimal polynomial $\varphi(T)$ of y has coefficients in $\mathcal{O}_P$, and let $P_1, \ldots, P_r \in \mathbb{P}_F$ be all extensions of P. The following hold*

(a) $d(P_i|P) \leqslant v_{P_i}(\varphi'(y))$ for $1 \leqslant i \leqslant r$, where φ' denotes the formal derivative of φ in the polynomial ring $F[T]$.

(b) $\{1, y, \ldots, y^{n-1}\}$ *is an integral base of* $F'|F$ *at* P *if and only if* $d(P_i|P) = v_{P_i}(\varphi'(y))$ *for* $1 \leqslant i \leqslant r$.

Corollary 23. *Let* $F' = F(y)$ *be a finite separable extension of* F *with* $[F'|F] = n$. *If* $\varphi(T) \in F[T]$ *is the minimal polynomial of* y *over* F *and* $P \in \mathbb{P}_F$ *is such that* y *is integral over* $\mathcal{O}_P$ *and* $v_{P'}(\varphi'(y)) = 0$ *for all* $P'|P$, *then* P *is unramified in* $F'|F$ *and* $\{1, y, \ldots, y^{n-1}\}$ *is an integral base of* $F'|F$ *at* P.

Proposition 27. *Let* $F'|F$ *be a finite separable extension of function fields and* $P \in \mathbb{P}_F$, $P' \in \mathbb{P}_{F'}$ *be such that* $P'|P$. *If* $P'|P$ *is totally ramified, that is,* $e(P'|P) = [F' : F] = n$ *and* $t \in F'$ *is a* P'*-prime element with minimal polynomial* $\varphi(T) \in F[T]$ *over* F, *then* $d(P'|P) = v_{P'}(\varphi'(t))$ *and* $\{1, t, \ldots, t^{n-1}\}$ *is an integral base of* $F'|F$ *at* P.

1.12 Galois Extensions

We now study a particularly useful case of algebraic function field extensions. An extension $M|L$ is said to be Galois if the automorphism group

$$\mathrm{Aut}(M|L) = \{\sigma : M \to M \mid \sigma \text{ is an automorphism with } \sigma_{|L} = \mathrm{id}\}$$

has order $[M : L]$. In this case, $\mathrm{Aut}(M|L)$ is called the Galois group of $M|L$ and denoted by $\mathrm{Gal}(M|L)$. We shall restrict our study to Galois extensions of finite degree.

Let $F'|F$ be a Galois extension of function fields of finite degree. Given a place $P \in \mathbb{P}_F$, the group $\mathrm{Gal}(F'|F)$ acts on the set of all extensions $\{P' \in \mathbb{P}_{F'} : P'|P\}$ via $\sigma(P') = \{\sigma(x) : x \in P'\}$, and we have proved in Lemma 14 that the valuation $v_{\sigma(P')}$ is given by

$$v_{\sigma(P')}(y) = v_{P'}(\sigma^{-1}(y)) \text{ for } y \in F'.$$

Theorem 29. *Let* $F'|K'$ *be a Galois extension of* $F|K$ *and* $P_1, P_2 \in \mathbb{P}_{F'}$ *be place extensions of* $P \in \mathbb{P}_F$. *Then* $P_2 = \sigma(P_1)$ *for some* $\sigma \in G := \mathrm{Gal}(F'|F)$. *In other words,* G *acts transitively on the set of extensions of* P.

Proof. Suppose the assertion is false, that is, $P_2 \neq \sigma(P_1)$ for all $\sigma \in G$. By the Approximation Theorem, there is some $z \in F'$ such that $v_{P_2}(z) > 0$ and $v_Q(z) = 0$ for all other $Q \in \mathbb{P}_{F'}$ with $Q|P$. Let $N_{F'|F} : F' \to F$ be the norm map, then

$$\begin{aligned} v_{P_1}(N_{F'|F}(z)) &= v_{P_1}\left(\prod_{\sigma \in G} \sigma(z)\right) = \sum_{\sigma \in G} v_{P_1}(\sigma(z)) \\ &= \sum_{\sigma \in G} v_{\sigma^{-1}(P_1)}(z) = \sum_{\sigma \in G} v_{\sigma(P_1)}(z) = 0, \end{aligned} \tag{1.46}$$

since by assumption, P_2 is not equal to any $\sigma(P_1)$. On the other hand,

$$v_{P_2}(N_{F'|F}(z)) = \sum_{\sigma \in G} v_{\sigma(P_2)}(z) > 0. \tag{1.47}$$

But $N_{F'|F}(z) \in F$, thus $v_{P_1}(N_{F'|F}(z)) = 0 \Leftrightarrow v_P(N_{F'|F}(z)) = 0 \Leftrightarrow v_{P_2}(N_{F'|F}(z)) = 0$, which contradicts (1.46) and (1.47). □

Corollary 24. *With the same notation as in Theorem 29, let $P_1, \ldots, P_r$ be all place extensions of P in F'. Then*

(a) $e(P_i|P) = e(P_j|P)$ and $f(P_i|P) = f(P_j|P)$ for all i, j. Therefore, we set $e(P) := e(P_i|P)$, $f(P) := f(P_i|P)$, and call them the ramification index and relative degree of P, respectively.

(b) $e(P) \cdot f(P) \cdot r = [F' : F]$.

(c) $d(P_i|P) = d(P_j|P)$ for all i, j.

Proof. (a) This is a direct consequence of Theorem 29 and Lemma 14(c).

(b) Follows from (a) and the Fundamental Equality.

(c) Consider the integral closure

$$\mathcal{O}'_P = \bigcap_{i=1}^{r} \mathcal{O}_{P_i}$$

of $\mathcal{O}_P$ in F' and the complementary module

$$\mathcal{C}_P = \{z \in F' : \mathrm{Tr}_{F'|F}(z \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P\}.$$

Let $\sigma \in \mathrm{Gal}(F'|F)$. We know that $\mathrm{Tr}_{F'|F}(\sigma(u)) = \mathrm{Tr}_{F'|F}(u)$ for $u \in F'$, so $\sigma(\mathcal{O}'_P) = \mathcal{O}'_P$ and $\sigma(\mathcal{C}_P) = \mathcal{C}_P$. Writing $\mathcal{C}_P = t \cdot \mathcal{O}'_P$, we get $\sigma(t) \cdot \mathcal{O}'_P = \sigma(\mathcal{C}_P) = \mathcal{C}_P = t \cdot \mathcal{O}'_P$, so

$$-d(P_i|P) = v_{P_i}(t) = v_{P_i}(\sigma(t)) \text{ for } 1 \leqslant i \leqslant r$$

by Proposition 25(c). Now take two places P_i, P_j lying over P and take an automorphism $\sigma \in \mathrm{Gal}(F'|F)$ such that $\sigma(P_j) = P_i$. Then

$$-d(P_i|P) = v_{P_i}(\sigma(t)) = v_{\sigma^{-1}(P_i)}(t) = v_{P_j}(t) = -d(P_j|P).$$ □

We now discuss a class of Galois extensions called Kummer extensions.

Proposition 28 (Kummer Extensions)**.** *Let $F|K$ be an algebraic function field such that K contains a primitive n-th root of unity, where $n > 1$ is coprime with* char K*. If $u \in F$ satisfies*

$$u \neq w^d \text{ for all } w \in F \text{ and } d \mid n,\ d > 1. \tag{1.48}$$

Let

$$F' = F(y), \text{ with } y^n = u. \tag{1.49}$$

The extension $F'|F$ is called a Kummer extension of F. It has the following properties:

(a) $\Phi(T) = T^n - u$ *is the minimal polynomial of* y *over* F*. The extension* $F'|F$ *is Galois of degree* $[F' : F] = n$*. Its Galois group is cyclic generated by* $\sigma(y) = \zeta y$*, where* $\zeta \in K$ *is a primitive root of unity.*

(b) Let $P \in \mathbb{P}_F$ *and* $P' \in \mathbb{P}_{F'}$ *be an extension of* P*. Then*

$$e(P'|P) = \frac{n}{r_P} \text{ and } d(P'|P) = \frac{n}{r_P} - 1,$$

where $r_P = \gcd(n, v_P(u)) > 0$*.*

(c) If K' *is the constant field of* F' *and* g, g' *are the genera of* F *and* F'*, respectively, than*

$$g' = 1 + \frac{n}{[K' : K]} \left(g - 1 + \frac{1}{2} \sum_{P \in \mathbb{P}_F} \left(1 - \frac{r_P}{n}\right) \cdot \deg P \right).$$

Proof. (a) This is a well-known fact from Galois Theory.

(b) If $r_P = 1$, (1.49) implies $n \cdot v_{P'}(y) = v_{P'}(y^n) = v_{P'}(u) = e(P'|P) \cdot v_P(u)$, which means $e(P'|P) = n$, because n and $v_P(u)$ are coprime. Since $\operatorname{char} K \nmid n$, Dedekind's Different Theorem yields $d(P'|P) = n - 1$. If $r_P = n$ take $l \in \mathbb{Z}$ such that $v_P(u) = l \cdot n$, choose $t \in F$ with $v_P(t) = l$ and set $y_1 := t^{-1}y$, $u_1 := t^{-n}u$. Then $y_1^n = u_1$, $v_{P'}(y_1) = v_P(u_1)$ and the minimal polynomial of y_1 over F is $\psi(T) = T^n - u_1 \in F[T]$, thus y_1 is integral over $\mathcal{O}_P$ and Theorem 28 yields

$$0 \leqslant d(P'|P) \leqslant v_{P'}(\psi'(y_1)).$$

Since $\psi'(y_1) = n y_1^{n-1}$, $v_{P'}(\psi'(y_1)) = (n-1) \cdot v_{P'}(y_1) = 0$ and $d(P'|P) = 0$. By Dedekind's Theorem, $e(P'|P) = 1$, finishing the proof of this case.

Finally, if $1 < r_P < n$, consider the intermediate field $F_0 := F(y_0)$ where $y_0 := y^{n/r_P}$. Then $[F' : F_0] = n/r_P$ and $[F_0 : F] = r_P$. The element y_0 satisfies

$$y_0^{r_P} = u \tag{1.50}$$

over F. Set $P_0 := P' \cap F_0$. The second applies to $F_0|F$, and thus $e(P_0|P) = 1$. By (1.50), $v_{P_0}(y_0) = v_P(u)/r_P$, which is coprime with n/r_P, so the first case applies to $F' = F_0(y)$. Consequently, $e(P'|P_0) = n/r_P$ and

$$e(P'|P) = e(P'|P_0) \cdot e(P_0|P) = \frac{n}{r_P}.$$

(c) The degree of $\operatorname{Diff}(F'|F)$ is

$$\deg \operatorname{Diff}(F'|F) = \sum_{P \in \mathbb{P}_F} \left(\frac{n}{r_P} - 1 \right) \cdot \sum_{P'|P} \deg P'. \tag{1.51}$$

Since the ramification index $e(P)$ depends only on P, we have

$$\begin{aligned}\sum_{P'|P} \deg P' &= \frac{1}{e(P)} \cdot \deg \left(\sum_{P'|P} e(P'|P) \cdot P' \right) \\ &= \frac{1}{e(P)} \cdot \deg \mathrm{Con}_{F'|F}(P) = \frac{r_P}{n} \cdot \frac{n}{[K' : K]} \cdot \deg P \\ &= \frac{r_P}{[K' : K]} \cdot \deg P\end{aligned}$$

by (b) and Corollary 11. Substituting this into (1.51) proves that

$$\begin{aligned}\deg \mathrm{Diff}(F'|F) &= \sum_{P \in \mathbb{P}_F} \frac{n - r_P}{r_P} \cdot \frac{r_P}{[K' : K]} \cdot \deg P \\ &= \frac{n}{[K' : K]} \cdot \sum_{P \in \mathbb{P}_F} \left(1 - \frac{r_P}{n}\right) \cdot \deg P.\end{aligned}$$

Applying the Hurwitz Genus Formula finishes the proof. □

Corollary 25. *Let $F|K$ be a function field and $F' = F(y)$ with $y^n = u \in F$, where* $\mathrm{char}\, K \nmid n$ *and K contains a primitive n-th root of unity. If there is a place $Q \in \mathbb{P}_F$ such that* $\gcd(n, v_Q(u)) = 1$*, then K is the full constant field of F', the extension $F'|F$ is cyclic of degree n and*

$$g' = 1 + n(g-1) + \frac{1}{2} \sum_{P \in \mathbb{P}_F} (n - r_P) \cdot \deg P.$$

Example 4. *Let $F = K(x, y)$ with* $\mathrm{char}\, K \neq 2$ *and*

$$y^2 = f(x) = p_1(x) \cdots p_s(x) \in K[x],$$

where $p_1(x), \ldots, p_s(x)$ are distinct irreducible polynomials. Then K is the full constant field of F and if $m := \deg f$, then $F|K$ has genus

$$g = \begin{cases} \dfrac{m-1}{2} & \text{if } m \text{ is odd} \\ \dfrac{m-2}{2} & \text{if } m \text{ is even.} \end{cases}$$

Proof. Note that $F = F_0(y)$, where $F_0 = K(x)$ is the rational function field. If $P_i \in \mathbb{P}_{K(x)}$ denotes the zero of $p_i(x)$ and P_∞ denotes the pole of x in $K(x)$, then $v_{P_i}(f(x)) = 1$ and $v_{P_\infty}(f(x)) = -m$. From Corollary 25, we obtain that $F|F_0$ is cyclic of degree 2 and K is the full constant field of F. The numbers r_P for $P \in \mathbb{P}_{K(x)}$ are

$$\begin{aligned} r_{P_i} &= 1 \text{ for } i = 1, \ldots, s \\ r_{P_\infty} &= 1 \text{ if } m \text{ is odd} \\ r_{P_\infty} &= 2 \text{ if } m \text{ is even.} \end{aligned}$$

Our last claim now follows from Corollary 25. □

1.13 Lattice Theory

In this section we follow chapter 2 of (COSTA et al., 2017) and give the basic definitions and results of lattice theory which will be used for the construction of function field lattices.

Definition 43. *Let $v_1, \ldots, v_m$ be linearly independent over $\mathbb{R}^n$. A lattice Λ with basis $\{v_1, \ldots, v_m\}$ is defined as*

$$\Lambda := \{a_1 v_1 + \cdots + a_m v_m : a_1, \ldots, a_m \in \mathbb{Z}\}.$$

The integer m is called the rank of Λ, denoted by $\mathrm{rank}(\Lambda)$. *If $m = n$, we say Λ has full rank. Equivalently, a subset of $\mathbb{R}^n$ is a lattice if and only if it is a discrete subgroup of $\mathbb{R}^n$ with respect to vector addition.*

Definition 44. *A generator matrix B for the lattice Λ is a matrix whose columns are the basis vectors of Λ:*

$$B = \left[v_1 | \cdots | v_m\right].$$

It is clear from these two definitions that the rank of the matrix B is m. Also, this matrix is not unique, as multiple basis can generate the same lattice.

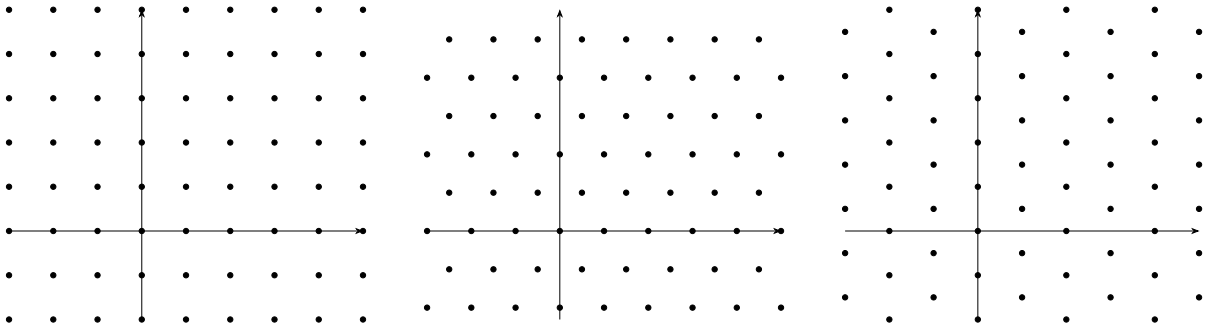
Example 5. *Two of the simplest examples of lattices in the plane are the square lattice and the hexagonal lattice, displayed below. The square lattice is nothing more than $\mathbb{Z}^2$:*

$$\mathbb{Z}^2 = \{(a_1, a_2) : a_1, a_2 \in \mathbb{Z}\}.$$

A natural basis for this lattice is the canonical basis $\{e_1 = (1, 0), e_2 = (0, 1)\}$. The hexagonal lattice has a basis $\{(1, 0), (1/2, \sqrt{3}/2)\}$. We can also visualize different examples of lattices simply by coming up with basis for them. For example, the lattice with basis $\mathcal{B} = \{(1, 1/2), (2, 0)\}$ is also shown below.

Figure 1 – Examples of lattices in the plane

(a) Square lattice (b) Hexagonal lattice (c) Lattice generated by $\mathcal{B}$



Definition 45. *The volume of the lattice Λ, denoted by $V(\Lambda)$ is the positive real number*

$$V(\Lambda) := \sqrt{\det(B^T B)},$$

where B is a generator matrix of Λ.

Definition 46. *The minimum distance of a lattice is the minimum norm among its non-zero vectors, that is*

$$d(\Lambda) := \min_{0 \neq x \in \Lambda} ||x||,$$

where $||\cdot||$ denotes the euclidean norm.

Definition 47. *The kissing number $K(\Lambda)$ is defined as the number of lattice vectors that attain the minimum distance*

$$K(\Lambda) := |\{x \in \Lambda : ||x|| = d(\Lambda)\}|.$$

Definition 48. *If Λ is a lattice of rank n, we say it is well-rounded if it contains n linearly independent minimum length vectors over $\mathbb{R}$.*

Note that the previous definition asks for linear independence over $\mathbb{R}$. This means that well-roundedness is not equivalent to having a base of minimum length vectors. The equivalence holds for lower dimensions, but for all other cases, being generated by minimum length vectors is a strictly stronger condition.

Example 6. *Another example of a lattice that will be quite useful is the root lattice in $\mathbb{R}^n$, denoted by A_{n-1}. It is defined as*

$$A_{n-1} := \left\{ (x_1, \ldots, x_n) \in \mathbb{Z}^n : \sum_{i=1}^{n} x_i = 0 \right\}.$$

Considering the vectors $v_i = e_1 - e_i$ for $i = 2, \ldots, n$, we have a basis for A_{n-1}. Hence, $\operatorname{rank}(A_{n-1}) = n - 1 < n$ and A_{n-1} is not a full-rank lattice. Taking $B = [v_2 | \cdots | v_n]$, we find

$$V(A_{n-1}) = \sqrt{\det(B^T B)} = \begin{vmatrix} 2 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 2 \end{vmatrix}^{1/2} = \sqrt{n}.$$

The vectors of A_{n-1} achieving minimum distance are of the form $e_i - e_j$ for $i, j \in \{1, \ldots, n\}$, $i \neq j$. Hence the minimum vector length is $d(A_{n-1}) = \sqrt{2}$. From this characterization of minimum length vectors, we can also conclude

$$K(A_{n-1}) = n(n-1).$$

Finally, since $||v_i|| = \sqrt{2}$ for all $i = 1, \ldots, n$, A_{n-1} has a basis of minimum length vectors, implying is it also well-rounded.

Theorem 30. *Let Λ be a lattice of rank n and Λ' a sublattice of Λ of the same rank. Then the quotient group Λ/Λ' has finite order given by*

$$|\Lambda/\Lambda'| = \frac{V(\Lambda')}{V(\Lambda)}.$$

This positive integer is called the index of Λ' in Λ.

2 Function Field Lattices

Having laid out all the essentials, we now finally turn our attention to the topic of function field lattices. We start by presenting the method used for all constructions and outline some essential properties every function field lattice must satisfy. After that, we explore a couple of known examples and their properties.

2.1 Construction and Basic Properties

The general results of this section are taken from (ATEŞ, 2017).

Let F be a function field over the finite field $\mathbb{F}_q$, where $q = p^h$ for some prime number p and $h \geqslant 1$. Denote its genus by $g(F) = g$ and its set of places by $\mathbb{P}_F$. Take n distinct degree 1 (rational) places of F, form the set of places

$$\mathcal{P} = \{P_1, \ldots, P_n\} \subseteq \mathbb{P}_F$$

and define the set of functions

$$O_{\mathcal{P}}^* := \{z \in F^* : \operatorname{supp}(z) \subseteq \mathcal{P}\}.$$

Proposition 29. *$O_{\mathcal{P}}^*$ is an abelian group with respect to multiplication.*

Proof. Multiplication is evidently commutative since F is a field.

- $1 \in O_{\mathcal{P}}^*$, since $\operatorname{supp}(1) = \varnothing \subseteq \mathcal{P}$
- Given $x, y \in O_{\mathcal{P}}^*$, we know $(xy) = (x)+(y)$. Hence $\operatorname{supp}(xy) \subseteq \operatorname{supp}(x) \cup \operatorname{supp}(y) \subseteq \mathcal{P}$ and $xy \in O_{\mathcal{P}}^*$.
- Since $(x^{-1}) = -(x)$, it follows that $\operatorname{supp}(x^{-1}) = \operatorname{supp}(x) \subseteq \mathcal{P}$ and $x^{-1} \in O_{\mathcal{P}}^*$. □

Define the map

$$\begin{aligned} \varphi_{\mathcal{P}} : (O_{\mathcal{P}}^*, \cdot) &\to (\mathbb{Z}^n, +) \\ z &\mapsto (v_{P_1}(z), \ldots, v_{P_n}(z)). \end{aligned}$$

The following proposition will allow us to properly define function field lattices:

Proposition 30. *$\varphi_{\mathcal{P}}$ is a group homomorphism.*

Proof. This is an immediate consequence of the fact that $v_P(xy) = v_P(x) + v_P(y)$ for any $P \in \mathbb{P}_F$:

$$\begin{aligned}\varphi_{\mathcal{P}}(xy) &= (v_{P_1}(xy), \ldots, v_{P_n}(xy)) \\ &= (v_{P_1}(x) + v_{P_1}(y), \ldots, v_{P_n}(x) + v_{P_n}(y)) \\ &= (v_{P_1}(x), \ldots, v_{P_n}(x)) + (v_{P_1}(y), \ldots, v_{P_n}(y)) \\ &= \varphi_{\mathcal{P}}(x) + \varphi_{\mathcal{P}}(y).\end{aligned}$$

□

Definition 49. *The set $\Lambda_{\mathcal{P}} := \mathrm{Im}(\varphi_{\mathcal{P}})$ is a discrete additive subgroup of $\mathbb{R}^n$ by the previous proposition and thus is called the function field lattice of F generated by $\mathcal{P}$.*

For an element $z \in O_{\mathcal{P}}^*$, the fact that $\mathrm{supp}(z) \subseteq \mathcal{P}$ implies we can identify its principal divisor (z) with its image $\varphi_{\mathcal{P}}(z) \in \Lambda_{\mathcal{P}}$ in the natural way. In addition, we define the length of z as the vector length of $\varphi_{\mathcal{P}}(z)$:

$$||z|| := ||\varphi_{\mathcal{P}}(z)||.$$

We now discuss some general properties of function field lattices regarding first rank and volume, followed by minimum distance, kissing number and well-roundedness.

Proposition 31. *If h is the class number of $F|\mathbb{F}_q$, then*

(a) $\Lambda_{\mathcal{P}}$ is a sublattice of the root lattice A_{n-1}.

(b) $\mathrm{rank}(\Lambda_{\mathcal{P}}) = n - 1$.

(c) The index $|A_{n-1}/\Lambda_{\mathcal{P}}|$ is equal to some positive integer h_0 that divides h.

(d) The volume of $\Lambda_{\mathcal{P}}$ is $V(\Lambda_{\mathcal{P}}) = \sqrt{n} \cdot h_0$.

Proof. (a) By Theorem 6, all principal divisors have degree 0, thus

$$\deg((z)) = \sum_{i=1}^{n} v_{P_i}(z) = 0 \implies \varphi_{\mathcal{P}}(z) \in A_{n-1}.$$

(b) Consider the degree 0 divisors of F given by $P_1 - P_i$ for $i = 2, \ldots, n$. Since h is the class number of F, $hP_1 - hP_i \in \mathrm{Princ}(F)$ and $hP_1 - hP_i = (z_i)$ for some $z_i \in O_{\mathcal{P}}^*$. The corresponding images of these functions are

$$\begin{aligned}\varphi_{\mathcal{P}}(z_2) &= (h, -h, 0, \ldots, 0) \\ \varphi_{\mathcal{P}}(z_3) &= (h, 0, -h, \ldots, 0) \\ &\vdots \\ \varphi_{\mathcal{P}}(z_n) &= (h, 0, \ldots, 0, -h).\end{aligned}$$

Thus, we find $n-1$ vectors of $\Lambda_{\mathcal{P}}$ which are linearly independent over $\mathbb{R}$. Hence, $\operatorname{rank}(\Lambda_{\mathcal{P}}) \geqslant n-1$. But seeing as $\operatorname{rank}(\Lambda_{\mathcal{P}}) \leqslant \operatorname{rank}(A_{n-1}) = n-1$ from (a), our claim follows.

(c) Seeing as A_{n-1} and $\Lambda_{\mathcal{P}}$ have the same rank, Theorem 30 implies the index $h_0 = |A_{n-1}/\Lambda_{\mathcal{P}}|$ is finite. In order to prove that $h_0 \mid h$, consider the group homomorphism

$$\begin{aligned} \psi : A_{n-1} &\to \mathrm{Cl}^0(F) \\ (x_1, \ldots, x_n) &\mapsto [x_1 P_1 + \cdots + x_n P_n] \end{aligned}$$

and notice that

$$\begin{aligned} (x_1, \ldots, x_n) \in \ker \psi &\iff x_1 P_1 + \cdots + x_n P_n \in \mathrm{Princ}(F) \\ &\iff x_1 P_1 + \cdots + x_n P_n = (z),\ z \in O_{\mathcal{P}}^* \\ &\iff (x_1, \ldots, x_n) = \varphi_{\mathcal{P}}(z),\ z \in O_{\mathcal{P}}^*. \end{aligned}$$

Thus $\ker \psi = \Lambda_{\mathcal{P}}$ and $h_0 \mid h$.

(d) Applying Theorem 30 and Example 6 yields

$$V(\Lambda_{\mathcal{P}}) = V(A_{n-1}) \cdot |A_{n-1}/\Lambda_{\mathcal{P}}| = \sqrt{n} \cdot h_0. \qquad \square$$

Remark 10. *Since the value of h_0 is often unknown, the previous proposition serves to establish at least an upper bound for the volume of all function field lattices:*

$$V(\Lambda_{\mathcal{P}}) \leqslant \sqrt{n} \cdot h,$$

where h is the class number of F.

Example 7. *As a first example, let us examine the lattice from a rational function field $F = \mathbb{F}_q(z)$. Take*

$$\mathcal{P} = \{P_1, \ldots, P_{n-1}, P_\infty\},$$

where P_∞ is the pole of z and $P_i := P_{z-a_i}$ for $a_i \in \mathbb{F}_q$, $i = 1, \ldots, n-1$. We have the vectors

$$\begin{aligned} \varphi_{\mathcal{P}}(z - a_1) &= (1, 0, \ldots, 0, -1) \\ \varphi_{\mathcal{P}}(z - a_2) &= (0, 1, \ldots, 0, -1) \\ &\vdots \\ \varphi_{\mathcal{P}}(z - a_{n-1}) &= (0, \ldots, 0, 1, -1) \end{aligned}$$

in $\Lambda_{\mathcal{P}}$. By Proposition 31, $\Lambda_{\mathcal{P}}$ can have no more than these $n-1$ linearly independent vectors. Since we know from Example 6 that these vectors generate A_{n-1}, it follows that $\Lambda_{\mathcal{P}} = A_{n-1}$.

Proposition 32. *(a) If $z \in O_{\mathcal{P}}^* \backslash \mathbb{F}_q$, then $||z|| \geqslant \sqrt{2\deg(z)}$. Equality holds if and only if the zero and pole of z in $\mathbb{F}_q(z)$ split completely in the extension $F|\mathbb{F}_q(z)$.*

(b) $d(\Lambda_{\mathcal{P}}) \geqslant \sqrt{2\gamma}$, where γ is the gonality of F.

(c) Let $z \in O_{\mathcal{P}}^* \backslash \mathbb{F}_q$. Then $||z|| = \sqrt{2\gamma}$ if and only if $\deg(z) = \gamma$ and the zero and pole of z in $\mathbb{F}_q(z)$ split completely in $F|\mathbb{F}_q(z)$.

Proof. (a) Since z is transcendental over $\mathbb{F}_q$, $\deg(z)$ is finite. Let the principal divisor of z be

$$(z) = (b_1 Q_1 + \cdots + b_s Q_s) - (c_1 R_1 + \cdots + c_t R_t),$$

where $Q_i, R_j \in \mathcal{P}$ are distinct places and $b_i, c_j \in \mathbb{N}$ for $i = 1 \ldots, s$ and $j = 1 \ldots, t$. Then

$$||z||^2 = \sum_{i=1}^{s} b_i^2 + \sum_{j=1}^{t} c_j^2 \geqslant \sum_{i=1}^{s} b_i + \sum_{j=1}^{t} c_j = 2\deg(z).$$

Equality holds if and only if $b_i = c_j = 1$ for all i, j, which is equivalent to saying the zero and pole of z split completely in the extension $F|\mathbb{F}_q(z)$.

(b) Since $\gamma \leqslant \deg(z)$ for all $z \in F \backslash \mathbb{F}_q$ by definition, it follows from (a) that $||z|| \geqslant \sqrt{2\gamma}$ for all $z \in O_{\mathcal{P}}^* \backslash \mathbb{F}_q$ and thus

$$d(\Lambda_{\mathcal{P}}) \geqslant \sqrt{2\gamma}.$$

(c) This follows directly from part (a). □

As a consequence of this proposition, we can now precisely determine the conditions under which a function field lattice attains the lower bound $\sqrt{2\gamma}$ for the minimum distance:

Corollary 26. *$d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$ if and only if there exists a rational subfield $E \subseteq F$ with $[F : E] = \gamma$ and at least two places P and Q of E such that:*

1. *P and Q split completely in $F|E$.*
2. *$\mathcal{P} \subseteq \mathbb{P}_F$ contains all extensions of P and Q.*

Proof. ($\Rightarrow$): If $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$, there exists $z \in O_{\mathcal{P}}^*$ with $||z|| = \sqrt{2\gamma}$. Setting $E := \mathbb{F}_q(z)$ and applying Proposition 32(c) implies first $[F : E] = \deg(z) = \gamma$, and also P_0, P_∞ the zero and pole of z in E, respectively, split completely in $F|E$. Since $\mathrm{supp}(z) \subseteq \mathcal{P}$, all the extensions of P_0 and P_∞ must be contained in $\mathcal{P}$.
($\Leftarrow$): Let $P, Q \in \mathbb{P}_E$ be distinct rational places that satisfy conditions 1 and 2. We can find an element $z \in E$ such that P is the zero of z in E and Q is the pole of z in E. Condition 1 yields $[F : \mathbb{F}_q(z)] = \gamma = [F : E]$, and thus $E = \mathbb{F}_q(z)$. Since all extensions of P and Q are contained in $\mathcal{P}$ by condition 2, it follows that $\mathrm{supp}(z) \subseteq \mathcal{P}$ and $z \in O_{\mathcal{P}}^*$. Proposition 32(c) now assures $||z|| = \sqrt{2\gamma}$ and $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$. □

Lemma 16. *Let E be a rational subfield of F with $[F : E] = \gamma$ and $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$. Define the set $S(E) \subseteq \mathbb{P}_E$ as the set of rational places of E satisfying conditions 1 and 2 of Corollary 26. If $m := |S(E)| \geqslant 2$, then:*

(a) If $z \in E \cap O_{\mathcal{P}}^*$, the vectors $\varphi_{\mathcal{P}}(z) \in \Lambda_{\mathcal{P}}$ of minimum length span a sublattice $\Delta_{\mathcal{P}}$ of $\Lambda_{\mathcal{P}}$ such that $\operatorname{rank}(\Delta_{\mathcal{P}}) = m - 1$.

(b) The number of minimum length vectors $\varphi_{\mathcal{P}}(z) \in \Lambda_{\mathcal{P}}$ with $z \in E \cap O_{\mathcal{P}}^*$ is $m(m-1)$.

Proof. By Corollary 26, there exists a rational subfield $E \subseteq F$ with $[F : E] = \gamma$ and $|S(E)| \geqslant 2$. Let $S(E) = \{P_1, \ldots, P_m\}$.

(a) If $z \in E \cap O_{\mathcal{P}}^*$ with $||z|| = \sqrt{2\gamma}$, Proposition 32 implies $[F : \mathbb{F}_q(z)] = \gamma$, and thus $E = \mathbb{F}_q(z)$ and the zero and pole of z satisfy conditions 1 and 2. Denoting by $(z)^E$ the principal divisor of z in E, we have

$$(z)^E = P_i - P_j \text{ for } i, j \in \{1, \ldots, m\},\ i \neq j.$$

Denoting z by $z_{i,j}$ if $(z)^E = P_i - P_j$, we have

$$(z_{i,j})^E = P_i - P_j = (P_i - P_1) - (P_j - P_1) = (z_{i,1})^E - (z_{j,1})^E \text{ for } i, j \in \{2, \ldots, m\}.$$

Also notice that $(z_{1,j})^E = P_1 - P_j = -(P_j - P_1) = -(z_{j,1})^E$. Identifying principal divisors with images via $\varphi_{\mathcal{P}}$ yields

$$\varphi_{\mathcal{P}}(z_{i,j}) = \varphi_{\mathcal{P}}(z_{i,1}) - \varphi_{\mathcal{P}}(z_{j,1}) \text{ and } \varphi_{\mathcal{P}}(z_{1,j}) = -\varphi_{\mathcal{P}}(z_{j,1}).$$

Therefore, all vectors $\varphi_{\mathcal{P}}(z_{i,j})$, $i, j \in \{1, \ldots, m\}$, $i \neq j$ are spanned by the set

$$\{\varphi_{\mathcal{P}}(z_{j,1}) : j = 2, \ldots, m\}.$$

Notice that $v_P(z_{j,1}) = -1$ for all $P \in \mathbb{P}_F$ such that $P|P_1$, $v_Q(z_{j,1}) = 1$ for all $Q \in \mathbb{P}_F$ such that $Q|P_j$ and all other valuations are zero. Since every place of F extends exactly one place of E by Proposition 16(a), no other vector besides $\varphi_{\mathcal{P}}(z_{j,1})$ will have non-zero entries at the places corresponding to the extensions of P_j. Therefore, the generating set of $\Delta_{\mathcal{P}}$ obtained previously is linearly independent and $\operatorname{rank}(\Delta_{\mathcal{P}}) = m - 1$.

(b) Using part (a), we simply have to count the elements $z_{i,j}$ for $i, j \in \{1, \ldots, m\}$ and $i \neq j$. This number is $m(m-1)$. □

We now consider multiple rational subfields of F and give an interval on which $\operatorname{rank}(\Delta_{\mathcal{P}})$ must lie.

Theorem 31. *Let E_i be rational subfields of F with $[F : E_i] = \gamma$ for $i = 1, \ldots, s$ and $d(\Lambda_{\mathcal{P}}) = \sqrt{2\gamma}$. Define the set $S(E_i) \subseteq \mathbb{P}_{E_i}$ in the same way as Lemma 16. Setting $m_i := |S(E_i)|$ and $m := \max_{1 \leqslant i \leqslant s} m_i$, the following statements hold:*

(a) $m \geqslant 2$.

(b) $\operatorname{rank} \Lambda_{\mathcal{P}} \geqslant m\gamma - 1$.

(c) $m - 1 \leqslant \operatorname{rank}(\Delta_{\mathcal{P}}) \leqslant s(m-1)$.

Proof. (a) Since the lower bound for the minimum distance is attained, Corollary 26 guarantees at least one of the $S(E_i)$ has 2 or more places, hence $m \geqslant 2$.

(b) From Proposition 31(b), $\operatorname{rank}(\Lambda_{\mathcal{P}}) = |\mathcal{P}| - 1$. By condition 1, every place of $S(E_i)$ splits completely in the extension $F|E_i$, thus there are $\gamma = [F : E_i]$ rational places of F lying over each one. From condition 2, all these extensions are contained in $\mathcal{P}$, therefore

$$|\mathcal{P}| \geqslant m\gamma \implies \operatorname{rank}(\Lambda_{\mathcal{P}}) \geqslant m\gamma - 1.$$

(c) Let $\varphi_{\mathcal{P}}(z)$ be a minimal vector. Applying Corollary 26, we get $\mathbb{F}_q(z) = E_i$ for some $i = 1, \ldots, s$ and $m_i \geqslant 2$. Thus, $z \in E_i \cap O_{\mathcal{P}}^*$. Lemma 16(a) now implies there are $m_i - 1$ linearly independent vectors $\varphi_{\mathcal{P}}(z)$ of minimal length. This means the number of linearly independent minimal length vectors in $\Lambda_{\mathcal{P}}$ must satisfy

$$m_i - 1 \leqslant m - 1 \leqslant \operatorname{rank}(\Delta_{\mathcal{P}}) \leqslant \sum_{i=1}^{s} (m_i - 1) \leqslant s(m-1). \qquad \square$$

Corollary 27. *If the hypothesis of Theorem 31 hold along with $g > 0$ and $s \leqslant \gamma$, then $\Lambda_{\mathcal{P}}$ is not well-rounded.*

Proof. First notice that $g > 0$ implies $\gamma > 1$, since if $\gamma = 1$, then F would be rational and its genus would be 0. Thus,

$$\operatorname{rank}(\Delta_{\mathcal{P}}) \leqslant s(m-1) \leqslant \gamma(m-1) = \gamma m - \gamma < \gamma m - 1 \leqslant \operatorname{rank}(\Lambda_{\mathcal{P}}),$$

meaning there are less linearly independent minimal length vectors than the rank of $\Lambda_{\mathcal{P}}$. Therefore, it cannot be well-rounded. $\square$

Example 8. *Let $F|\mathbb{F}_q$ be a hyperelliptic function field, that is, an extension of $\mathbb{F}_q(x)$ with $[F : \mathbb{F}_q(x)] = 2 = \gamma$ and $g \geqslant 2$, where $\mathbb{F}_q(x)$ is the unique rational subfield of F of degree 2, thus $s = 1$. If at least two places of $\mathbb{F}_q(x)$ split completely in $F|\mathbb{F}_q$, then we are under the hypothesis of Corollary 27 and the function field lattice associated to F is never well-rounded.*

Finally, we can give an exact expression for the kissing number:

Corollary 28. *Under the same assumptions as Theorem 31, the kissing number of* $\Lambda_{\mathcal{P}}$ *is*

$$K(\Lambda_{\mathcal{P}}) = \sum_{i=1}^{s} m_i(m_i - 1).$$

Proof. Applying Corollary 26 shows that any minimal length vector must be the image of some $z \in E_i \cap O_{\mathcal{P}}^*$ such that $m_i \geqslant 2$. By Lemma 16(b), there are $m_i(m_i - 1)$ such vectors, hence

$$K(\Lambda_{\mathcal{P}}) = \sum_{i=1}^{s} m_i(m_i - 1). \qquad \square$$

2.2 Known Examples

This section is dedicated to examining the existing examples of function field lattices with particular emphasis being placed on the minimum distance, kissing number and well-roundedness. The first part is based on (FUKSHANSKY; MAHARAJ, 2014) and the second part on (BÖTTCHER et al., 2016) with some needed properties regarding function fields taken from chapter 6 of (STICHTENOTH, 2009).

2.2.1 Elliptic Function Fields

Definition 50. *An Algebraic function field* $F|K$ *with* K *the full constant field of* F *is said to be elliptic if its genus is* $g = 1$ *and there exists some* $A \in \mathrm{Div}(F)$ *with* $\deg A = 1$.

Elliptic function fields can be characterized explicitly via the following proposition:

Proposition 33. *Let* $F|K$ *be an elliptic function field.*

(a) If $\mathrm{char}\, K \neq 2$, *there exist* $x, y \in F$ *such that* $F = K(x, y)$ *and* $y^2 = f(x)$ *for some square-free polynomial* $f(x) \in K[x]$ *of degree* 3.

(b) If $\mathrm{char}\, K = 2$, *there exist* $x, y \in F$ *such that* $F = K(x, y)$ *and* $y^2 + y = f(x) \in K[x]$ *with* $\deg f = 3$ *or* $y^2 + y = x + \dfrac{1}{ax + b}$ *where* $a, b \in K$ *and* $a \neq 0$.

We now present some results that allow us to induce a group structure on the set of rational places of an elliptic function field.

Proposition 34. *Let* $F|K$ *be an elliptic function field. If* $\mathcal{P}$ *denotes the set of all rational places of* F, *then*

(a) For each divisor $A \in \mathrm{Div}(F)$ *with* $\deg A = 1$, *there is a unique place* $P \in \mathcal{P}$ *with* $A \sim P$. *In particular,* $\mathcal{P} \neq \varnothing$.

(b) Given a fixed place $P_0 \in \mathcal{P}$, the following map is a bijection

$$\begin{aligned} \Phi : \mathcal{P} &\to \mathrm{Cl}^0(F) \\ P &\mapsto [P - P_0]. \end{aligned}$$

Proof. (a) Let $A \in \mathrm{Div}(F)$ with $\deg A = 1$. Since $\deg A > 2g - 2$, the Riemann-Roch Theorem implies $\ell(A) = \deg A + 1 - g > 0$ and by Remark 4(b), there is a divisor $A_1 \sim A$ with $A_1 > 0$. Since $\deg A = \deg A_1 = 1$, it follows that $A_1 = P \in \mathcal{P}$. To prove uniqueness, suppose $A \sim P$ and $A \sim Q$ for distinct places $P, Q \in \mathcal{P}$. Then, $P \sim Q$ and there exists $x \in F$ with $P - Q = (x)$. Applying Theorem 6:

$$[F : K(x)] = \deg(x)_\infty = \deg Q = 1,$$

hence $F = K(x)$, which is impossible, since $F|K$ is elliptic.

(b) First suppose $\Phi(P) = \Phi(Q)$ for $P, Q \in \mathcal{P}$. Then $P - P_0 \sim Q - P_0$, and hence $P \sim Q$. If $P \neq Q$, Theorem 6 produces a contradiction, so $P = Q$ and Φ is injective. To show that it is surjective, take $[B] \in \mathrm{Cl}^0(F)$. We know that $\deg(B + P_0) = 1$, so (a) implies the existence of a unique $P \in \mathcal{P}$ with $B + P_0 \sim P$. Hence, $[B] = [P - P_0] = \Phi(P)$. □

Using the bijection Φ, we can carry over the group structure from $\mathrm{Cl}^0(F)$ to $\mathcal{P}$ by defining, for $P, Q \in P$:

$$P \oplus Q := \Phi^{-1}(\Phi(P) + \Phi(Q)). \tag{2.1}$$

This definition has the following properties:

Proposition 35. *Let $F|K$ be an elliptic function field. Then:*

(a) $\mathcal{P}$ with the operation $\oplus$ as defined in (2.1) is an abelian group.

(b) The place P_0 is the zero element of the group $(\mathcal{P}, \oplus)$.

(c) For $P, Q, R \in \mathcal{P}$: $P \oplus Q = R \iff P + Q \sim R + P_0$.

(d) The map $\Phi : \mathcal{P} \to \mathrm{Cl}^0(F)$ is a group isomorphism.

The group law of $\mathcal{P}$ is dependent on the choice of P_0. Since we will represent an elliptic function field $F|K$ as $F = K(x, y)$ according to Proposition 33, we set $P_0 := Q_\infty$, the common pole of x and y, which is a rational place. We also note that if $P, Q \in \mathcal{P}$, then $P - Q$ is a principal divisor if and only if $P = Q$. Hence $\ell(P - Q) > 0 \iff P = Q$.

Let E be a curve over $\mathbb{F}_q$ such that $\mathbb{F}_q(E) = F$ (Theorem 8). Each $\mathbb{F}_q$-rational point of E corresponds to a rational place of F, so we denote a place by P and its corresponding point in E by $\mathbf{P}$. This means $P + Q$ is a divisor of F, while $\mathbf{P} + \mathbf{Q}$ is another point of E.

Let the set of rational places of F be $\mathcal{P} = \{P_0 := Q_\infty, P_1, \ldots, P_{n-1}\}$. For a place $P \in \mathcal{P}$, P' will denote the place corresponding to the additive inverse of $\mathbf{P}$, that is, $\mathbf{P} + \mathbf{P}' = \mathbf{Q}_\infty$. In this case, $x(\mathbf{P}) = x(\mathbf{P}')$.

Define $m(\mathbf{P}, \mathbf{Q})$ as the line through $\mathbf{P}$ and $\mathbf{Q}$ if $P, Q \neq Q_\infty$, meaning $m(\mathbf{P}, \mathbf{Q}) = ax + by + c$ for some $a, b, c \in \mathbb{F}_q$. If $P = Q \neq Q_\infty$, then $m(\mathbf{P}, \mathbf{Q})$ is the tangent line of E at the point $\mathbf{P}$. If $Q = P' \neq Q_\infty$ then $m(\mathbf{P}, \mathbf{Q}) = x - x(\mathbf{P}) = x - x(\mathbf{Q})$. If $P = Q_\infty$ or $Q = Q_\infty$, we define $m(\mathbf{P}, \mathbf{Q}) := 1 \in \mathbb{F}_q$.

If $P, Q \neq Q_\infty$ and $\mathbf{P} + \mathbf{Q} = \mathbf{R}$, then $m(\mathbf{P}, \mathbf{Q})$ intersects E at points $\mathbf{P}, \mathbf{Q}$ and $\mathbf{R}'$, and thus has the principal divisor

$$(m(\mathbf{P}, \mathbf{Q})) = P + Q + R' - 3Q_\infty.$$

If $R' = Q_\infty$, then $Q = P'$. In this case,

$$(m(\mathbf{P}, \mathbf{Q})) = P + P' - 2Q_\infty.$$

Therefore, if $\mathbf{P} + \mathbf{Q} = \mathbf{R}$ and $R \neq Q_\infty$, it follows that

$$\left(\frac{m(\mathbf{P}, \mathbf{Q})}{x - x(\mathbf{R})}\right) = (P + Q + R' - 3Q_\infty) - (R + R' - 2Q_\infty) = P + Q - R - Q_\infty.$$

Supposing $\mathbf{P} + \mathbf{Q} = \mathbf{R}$, we define

$$F(\mathbf{P}, \mathbf{Q}) := \begin{cases} \dfrac{x - x(\mathbf{R})}{m(\mathbf{P}, \mathbf{Q})} \text{ if } \mathbf{P}, \mathbf{Q}, \mathbf{R} \neq \mathbf{Q}_\infty \\ \dfrac{1}{m(\mathbf{P}, \mathbf{Q})} \text{ if } \mathbf{P}, \mathbf{Q} \neq \mathbf{Q}_\infty \text{ and } \mathbf{R} = \mathbf{Q}_\infty \\ 1 \text{ if } \mathbf{P} = \mathbf{Q}_\infty \text{ or } \mathbf{Q} = \mathbf{Q}_\infty. \end{cases}$$

In any case, the divisor of $F(\mathbf{P}, \mathbf{Q})$ is

$$(F(\mathbf{P}, \mathbf{Q})) = -P - Q + R + Q_\infty.$$

Lemma 17. *If $F|K$ is a function field, $f \in F$ and $D \in \mathrm{Div}(F)$, then*

$$f\mathcal{L}(D) = \mathcal{L}(D - (f)).$$

Proposition 36. *Let $P, Q, R \in \mathcal{P}$. Then $\boldsymbol{P} + \boldsymbol{Q} = \boldsymbol{R}$ if and only if $\mathcal{L}(P + Q - R - Q_\infty) \neq \{0\}$, in which case*

$$\mathcal{L}(P + Q - R - Q_\infty) = \mathrm{span}_{\mathbb{F}_q}(F(\boldsymbol{P}, \boldsymbol{Q})).$$

Proof. ($\Rightarrow$) : If $\mathbf{P} + \mathbf{Q} = \mathbf{R}$, then $P + Q - R - Q_\infty$ is the principal divisor of $(1/F(\mathbf{P}, \mathbf{Q}))$. Hence $\mathcal{L}(P + Q - R - Q_\infty) \neq \{0\}$ by our previous observation.
($\Leftarrow$) : In order to show that $\mathbf{P} + \mathbf{Q} = \mathbf{R}$, first suppose $P, Q \neq Q_\infty$, then

$$\frac{1}{F(\mathbf{P}, \mathbf{Q})}\mathcal{L}(P + Q - R - Q_\infty) = \mathcal{L}(S - R),$$

where $\mathbf{S}$ is the third point of intersection of the line $m(\mathbf{P}, \mathbf{Q})$ and the curve E. By assumption, $\mathcal{L}(S - R)$ has positive dimension, so $R = S$ and $\mathcal{L}(S - R) = \mathbb{F}_q$, implying

$$\mathcal{L}(P + Q - R - Q_\infty) = \text{span}_{\mathbb{F}_q}(F(\mathbf{P}, \mathbf{Q})).$$

If $P = Q_\infty$, then $\mathbf{P} + \mathbf{Q} = \mathbf{Q}$ and $\mathcal{L}(P + Q - R - Q_\infty) = \mathcal{L}(Q - R) \neq \{0\}$ by assumption and it follows that $P = Q$ and $\mathbf{R} = \mathbf{P} + \mathbf{Q}$. Finally, $\mathcal{L}(P + Q - R - Q_\infty) = \text{span}_{\mathbb{F}_q}(1) = \text{span}_{\mathbb{F}_q}(F(\mathbf{P}, \mathbf{Q}))$. The $Q = Q_\infty$ case is proven in the same manner. □

Theorem 32. *For an integer $i \geqslant 1$, $i\boldsymbol{P} = \boldsymbol{Q}_\infty$ if and only if*

$$\mathcal{L}(iP - iQ_\infty) = \text{span}_{\mathbb{F}_q}(F(\boldsymbol{P}, \boldsymbol{P})F(\boldsymbol{P}, 2\boldsymbol{P}) \cdots F(\boldsymbol{P}, (i-1)\boldsymbol{P})).$$

Proof. For $i = 1$, the result follows immediately. For $k \geqslant 1$, set $\mathbf{P}_k := k\mathbf{P}$. So, if $k \geqslant 1$, $\mathbf{P} + \mathbf{P}_{k-1} = \mathbf{P}_k$ and by Proposition 36:

$$\mathcal{L}(P + P_{k-1} - P_k - Q_\infty) = \text{span}_{\mathbb{F}_q}(F(\mathbf{P}, \mathbf{P}_{k-1})).$$

Now suppose $i\mathbf{P} = \mathbf{Q}_\infty$, meaning $\mathbf{P} + \mathbf{P}_{i-1} = \mathbf{Q}_\infty$ and

$$\mathcal{L}(P + P_{i-1} - 2Q_\infty) = \text{span}_{\mathbb{F}_q}(F(\mathbf{P}, \mathbf{P}_{i-1})).$$

Also, $\mathbf{P} + \mathbf{P}_{i-j-1} = \mathbf{P}_{i-j}$ for $j = 1, \ldots, i-2$, so the following identities hold:

$$\begin{aligned}
\mathcal{L}(P + P_{i-2} - P_{i-1} - Q_\infty) &= \text{span}_{\mathbb{F}_q}(F(\mathbf{P}, \mathbf{P}_{i-2})) \\
\mathcal{L}(P + P_{i-3} - P_{i-2} - Q_\infty) &= \text{span}_{\mathbb{F}_q}(F(\mathbf{P}, \mathbf{P}_{i-3})) \\
&\vdots \\
\mathcal{L}(P + P - P_2 - Q_\infty) &= \text{span}_{\mathbb{F}_q}(F(\mathbf{P}, \mathbf{P})).
\end{aligned}$$

Now, if $\mathcal{L}(D_1) = \text{span}_{\mathbb{F}_q}(f_1)$ and $\mathcal{L}(D_2) = \text{span}_{\mathbb{F}_q}(f_2)$, then $\mathcal{L}(D_1 + D_2) = \text{span}_{\mathbb{F}_q}(f_1 f_2)$. Combining this with the equalities above yields

$$\mathcal{L}(iP - iQ_\infty) = \text{span}_{\mathbb{F}_q}(F(\mathbf{P}, \mathbf{P})F(\mathbf{P}, \mathbf{P}_2) \cdots F(\mathbf{P}, \mathbf{P}_{i-1})).$$

Now assume the above equation holds. The divisor of $g := F(\mathbf{P}, \mathbf{P})F(\mathbf{P}, \mathbf{P}_2) \cdots F(\mathbf{P}, \mathbf{P}_{i-2})$ is

$$(g) = \sum_{j=1}^{i-2}(F(\mathbf{P}, \mathbf{P}_j)) = \sum_{j=1}^{i-2}[-P - P_j + P_{j+1} + Q_\infty] = -(i-1)P + P_{i-1} + (i-2)Q_\infty,$$

so we conclude that

$$\frac{1}{g}\mathcal{L}(iP - iQ_\infty) = \mathcal{L}(P + P_{i-1} - 2Q_\infty) \neq \{0\}.$$

Applying Proposition 36 shows that $\mathbf{P} + \mathbf{P}_{i-1} = \mathbf{Q}_\infty$, that is, $i\mathbf{P} = \mathbf{Q}_\infty$. □

Theorem 33. *Let $D \in \mathrm{Div}(F)$ define as*

$$D := rQ_\infty + \sum_{i=1}^{n-1} a_i P_i$$

be a divisor of degree 0. Then D is a principal divisor if and only if

$$\sum_{i=1}^{n-1} a_i \boldsymbol{P}_i = \boldsymbol{Q}_\infty.$$

In this case, $D = (f)$, where f is a product of functions of the form $F(\boldsymbol{P}, \boldsymbol{Q})$ with $P, Q \in \mathcal{P}$. The group $O^*_{\mathcal{P}}$ of functions with support in $\mathcal{P}$ is generated by the functions $F(\boldsymbol{P}, \boldsymbol{Q})$. Consequently, the lattice $\Lambda_{\mathcal{P}}$ is generated by vectors of the form $P + Q - R - Q_\infty$ where $\boldsymbol{P} + \boldsymbol{Q} = \boldsymbol{R}$.

Proof. First we observe that it may be assumed that $a_i \geqslant 0$ for $1 \leqslant i \leqslant n-1$. Indeed, for a place $P \in \mathcal{P}$ and an integer $k \geqslant 2$, define

$$T_k(\mathbf{P}) := F(\mathbf{P}, \mathbf{P})F(\mathbf{P}, 2\mathbf{P}) \cdots F(\mathbf{P}, (k-1)\mathbf{P}).$$

Suppose $a_j < 0$ and let k_j be such that $k_j \mathbf{P}_j = \mathbf{Q}_\infty$. By Theorem 32: $(T_{K_j}(\mathbf{P}_j)) = -k_j P_j + k_j Q_\infty$. Therefore

$$\left(\frac{1}{T_{k_j}(\mathbf{P}_j)}\right)^l \mathcal{L}(D) = \mathcal{L}(D'),$$

where

$$D' := D + l \cdot (T_{k_j}(\mathbf{P}_j)) = (r - lk_j)Q_\infty + \sum_{\substack{i=1 \\ i \neq j}}^{n-1} a_i P_i + (a_j + lk_j)P_j$$

and $a_j + lk_j \geqslant 0$ for a sufficiently large l. Also, D' is a principal divisor if and only if D is also a principal divisor and

$$\sum_{\substack{i=1 \\ i \neq j}}^{n-1} a_i \mathbf{P}_i + (a_j + lk_j)\mathbf{P}_j = \sum_{i=1}^{n-1} a_i \mathbf{P}_i.$$

Write $D = rQ_\infty + Q_1 + \cdots + Q_t$ with repetitions possibly occurring among the places Q_i and $t = -r$. Define

$$\mathbf{T}_i := \mathbf{Q}_{t-i} + \mathbf{Q}_{t-i+1} + \cdots + \mathbf{Q}_t$$

and

$$f := F(\mathbf{Q}_{t-1}, \mathbf{Q}_t)F(\mathbf{Q}_{t-2}, \mathbf{T}_1)F(\mathbf{Q}_{t-3}, \mathbf{T}_2) \cdots F(\mathbf{Q}_1, \mathbf{T}_{t-2}).$$

Note that

$$\begin{aligned}\left(\frac{1}{f}\right) &= [Q_{t-1} + Q_t - T_1 - Q_\infty] + \sum_{i=1}^{t-2} [Q_{t-i-1} + T_i - T_{i+1} - Q_\infty] \\ &= Q_t + Q_{t-1} + \cdots + Q_1 - T_{t-1} - (t-1)Q_\infty.\end{aligned}$$

And $D - (1/f) = -Q_\infty + T_{t-1}$. So

$$\frac{1}{f}\mathcal{L}(D) = \mathcal{L}(-Q_\infty + T_{t-1}).$$

The result now follows since $-Q_\infty + T_{t-1}$ is principal if and only if $\mathbf{T}_{t-1} = \mathbf{Q}_\infty$, that is, $\mathbf{Q}_1 + \mathbf{Q}_2 + \cdots + \mathbf{Q}_t = \mathbf{Q}_\infty$. Furthermore, $-Q_\infty + T_{t-1}$ is a principal divisor if and only if $\frac{1}{f}\mathcal{L}(-Q_\infty + T_{t-1}) = \mathbb{F}_q$, that is, $\mathcal{L}(D) = \mathrm{span}_{\mathbb{F}_q}(f)$.

For the remaining statement, note that each function $F(\mathbf{P}, \mathbf{Q})$ belongs to $O^*_\mathcal{P}$. Furthermore, $O^*_\mathcal{P}$ is the union of all $\mathcal{L}(D)\backslash\{0\}$ for all principal divisors D with support in P. From what was just proved, $\mathcal{L}(D)$ is spanned by products of functions $F(\mathbf{P}, \mathbf{Q})$ for $P, Q \in \mathcal{P}$, which finishes the proof. □

We can now prove results concerning some parameters of the lattice $\Lambda_\mathcal{P}$ from an elliptic function field.

Theorem 34. *If $n \geqslant 4$, $d(\Lambda_\mathcal{P}) = 2$ and the minimal vectors of $\Lambda_\mathcal{P}$ are of the form $P + Q - R - S$, where $P, Q, R, S \in \mathcal{P}$ are distinct places and $\boldsymbol{P} + \boldsymbol{Q} = \boldsymbol{R} + \boldsymbol{S}$. If $n = 3$ and $\mathcal{P} = \{P, Q, Q_\infty\}$, then $d(\Lambda_\mathcal{P}) = \sqrt{6}$ and the minimal vectors have the form $\pm(P + Q - 2Q_\infty)$, $\pm(P - 2Q + Q_\infty)$ and $\pm(-2P + Q + Q_\infty)$.*

Proof. $P - Q$ is a principal divisor if and only if $P = Q$, so $\gamma > 1$. $F(\mathbf{P}, \mathbf{Q})$ is a function of degree 2, meaning $\gamma = 2$. First assume $n \geqslant 4$. There are two distinct points $\mathbf{P}, \mathbf{Q}$ not equal to $\mathbf{Q}_\infty$ such that $\mathbf{P} \neq \mathbf{Q}'$. This means $\mathbf{P} + \mathbf{Q} = \mathbf{R}$ for $\mathbf{R} \neq \mathbf{P}, \mathbf{Q}, \mathbf{Q}_\infty$. Since $(F(\mathbf{P}, \mathbf{Q})) = -P - Q + R + Q_\infty$, $d(\Lambda_\mathcal{P}) \leqslant 2$. On the other hand, Proposition 32(b) implies $d(\Lambda_\mathcal{P}) \geqslant 2$, so $d(\Lambda_\mathcal{P}) = 2$.

A minimal vector v of $\Lambda_\mathcal{P}$ must have the form $P + Q - R - S$ where $P, Q, R, S \in \mathcal{P}$ are all distinct. Also, $P + Q - R - S$ is a principal divisor. Suppose $\mathbf{P} + \mathbf{Q} = \mathbf{R}_1$, then $P + Q - R_1 - Q_\infty$ is a principal divisor as is $(P + Q - R_1 - Q_\infty) - (P + Q - R - S) = R + S - R_1 - Q_\infty$. It follows from Proposition 36 that $\mathbf{R} + \mathbf{S} = \mathbf{R}_1$. Therefore, the minimal vectors of $\Lambda_\mathcal{P}$ have the form $P + Q - R - S$ where $\mathbf{P} + \mathbf{Q} = \mathbf{R} + \mathbf{S}$.

Finally, if $n = 3$, then $\mathbb{Z}_3 \simeq \mathcal{P} = \{Q_\infty, P, Q\}$, where $\mathbf{P} = 2\mathbf{Q}$. We have the following vectors of $\Lambda_\mathcal{P}$: $3P - 3Q_\infty$, $3Q - 3Q_\infty$, $2P - Q - Q_\infty$, $P - 2Q + Q_\infty$. This means that if $a_1P + b_1Q + c_1Q_\infty$ is a lattice vector, then $a_2P + b_2Q + c_2Q_\infty$ with $a_2 \equiv a_1 \mod 3$, $b_2 \equiv b_1 \mod 3$ and $c_2 = -a_2 - b_2$. A vector with minimal length is obtained when $a_2 = b_2 = 1$ and $c_2 = -2$, implying $d(\Lambda_\mathcal{P}) = \sqrt{6}$. □

We now give a formula for the kissing number of $\Lambda_\mathcal{P}$.

Theorem 35. *If $n \geqslant 4$ and e is the number of points of $\boldsymbol{P}$ such that $2\boldsymbol{P} = \boldsymbol{Q}_\infty$, then*

$$K(\Lambda_\mathcal{P}) = \frac{n}{e} \cdot \frac{(n-e)(n-e-2)}{4} + \left(n - \frac{n}{e}\right) \cdot \frac{n(n-2)}{4}.$$

Proof. Define the homomorphism $\tau : E \to E$ by $\tau(\mathbf{P}) = 2\mathbf{P}$. Then $|\ker \tau| = e$ and $|\operatorname{Im} \tau| = |E/\ker \tau| = n/e$. Fix some point $\mathbf{A}$ of E. We first count the number of solutions to the equation $\mathbf{P} + \mathbf{Q} = \mathbf{A}$ for $\mathbf{P}$ and $\mathbf{Q}$ distinct points of E. Note that $\mathbf{P} = \mathbf{Q}$ if and only if $\mathbf{A} \in \operatorname{Im} \tau$. In the case that $\mathbf{A} \in \operatorname{Im} \tau$, each element of the kernel gives a solution to $2\mathbf{P} = \mathbf{A}$, so there are e of them. Thus, there are $n - e$ points $\mathbf{P}$ such that $\mathbf{Q} := \mathbf{A} - \mathbf{P} \neq \mathbf{P}$, so there are $(n-e)/2$ pairs $\mathbf{P}, \mathbf{Q}$ such that $\mathbf{P} + \mathbf{Q} = \mathbf{A}$ and $\mathbf{P} \neq \mathbf{Q}$. Therefore, the number of pairs $\mathbf{R}, \mathbf{S}$ disjoint from $\mathbf{P}, \mathbf{Q}$ such that $\mathbf{R} + \mathbf{S} = \mathbf{A}$ is $(n - e - 2)/2$. We conclude that the number of minimal vectors $P + Q - R - S$ such that $\mathbf{P} + \mathbf{Q} = \mathbf{A} = \mathbf{R} + \mathbf{S}$ with $\mathbf{A} \in \operatorname{Im} \tau$ is $\dfrac{n}{e} \cdot \dfrac{(n-e)(n-e-2)}{4}$.

If $\mathbf{A} \notin \operatorname{Im} \tau$, there are no solutions to $2\mathbf{P} = \mathbf{A}$. A similar argument shows there are $\left(n - \dfrac{n}{e}\right) \cdot \dfrac{n(n-2)}{4}$ minimal vectors $P + Q - R - S$ such that $\mathbf{P} + \mathbf{Q} \notin \operatorname{Im} \tau$, which concludes the proof. □

Finally, we show that $\Lambda_{\mathcal{P}}$ has a base of minimal vectors.

Theorem 36. *If E has at least 5 points, then $\Lambda_{\mathcal{P}}$ is generated by minimal vectors. In particular, $\Lambda_{\mathcal{P}}$ is well-rounded.*

Proof. From Theorem 33, $\Lambda_{\mathcal{P}}$ is generated by vectors of the form $v := -P - Q + R + Q_\infty$ where $\mathbf{P} + \mathbf{Q} = \mathbf{R}$. We need only to prove that v is generated by minimal vectors. Suppose v does not have minimum length, that is, P, Q, R, Q_∞ are not all distinct. Since v is a nonzero principal divisor, $P, Q \neq Q_\infty$. Also, $P, Q \neq R$, so either $P = Q$ or $R = Q_\infty$.

If $P = Q$, $v = -2P + R + Q_\infty$ and $2\mathbf{P} = \mathbf{R}$. Since E has at least 5 points, we can choose a rational place U such that $\mathbf{U}$ is different from $\mathbf{Q}_\infty, \mathbf{P}, 2\mathbf{P}$ and $-\mathbf{P}$. Set $\mathbf{S} := \mathbf{P} + \mathbf{U}$ and notice that

$$-2P + R + Q_\infty = (-P - U + S + Q_\infty) - (P + S - R - U).$$

We claim $-P - U + S + Q_\infty$ and $P + S - R - U$ are minimal vectors. By choice, $U \neq P, Q_\infty$ and $U \neq S$, otherwise $\mathbf{P} = \mathbf{Q}_\infty$. Also, $S \neq P$ otherwise $U \neq Q_\infty$. Finally, $S \neq Q_\infty$ as equality would imply $\mathbf{P} + \mathbf{U} = \mathbf{Q}_\infty$ and $\mathbf{U} = -\mathbf{P}$, which is false. Thus $-P - U + S + Q_\infty$ is a minimal vector.

Observe that $\mathbf{P} + \mathbf{S} = 2\mathbf{P} + \mathbf{U} = \mathbf{R} + \mathbf{U}$, so $P + S - R - U$ is a lattice vector. We know P, S, U are distinct, so we must show that $S, U \neq R$. If $R = S$, then $\mathbf{U} = \mathbf{P}$, which is impossible. If $R = U$ then $\mathbf{U} = \mathbf{R} = 2\mathbf{P}$, which is also not possible. Therefore, $P + S - R - U$ is a minimal vector. This shows that v is the difference of two minimal vectors if $P = Q$.

Now assume $R = Q_\infty$, meaning $v = -P - Q + 2Q_\infty$ and $\mathbf{P} + \mathbf{Q} = \mathbf{Q}_\infty$. Since E has at least 5 rational points, choose a rational point $\mathbf{U} \neq \mathbf{P}, \mathbf{Q}, 2\mathbf{P}, \mathbf{Q}_\infty$. Set $\mathbf{S} := \mathbf{Q} + \mathbf{U}$ and note

that $U \neq S$ as $Q \neq Q_\infty$. Also, $Q+U-S-Q_\infty$ is a lattice vector and $\mathbf{P}+\mathbf{S} = \mathbf{P}+\mathbf{Q}+\mathbf{U} = \mathbf{U}$ so that $P + S - U - Q_\infty$ is also a lattice vector. Writing v as

$$v = -(Q + U - S - Q_\infty) - (P + S - U - Q_\infty)$$

we notice that it is a sum of two lattice vectors, so we only need to show that $Q+U-S-Q_\infty$ and $P + S - U - Q_\infty$ are minimal vectors.

For the first vector we show that Q, U, S, Q_∞ are all distinct places. By choice, $U \neq Q, Q_\infty$ and we have already observed that $U \neq S$. If Q were equal to S, then $\mathbf{Q} = \mathbf{S} = \mathbf{Q} + \mathbf{U}$, implying $\mathbf{U} = \mathbf{Q}_\infty$ and $U = Q_\infty$, which contradicts the choice of $\mathbf{U}$. Finally, $S \neq Q_\infty$ as otherwise, $\mathbf{U} = -\mathbf{Q} = \mathbf{P}$, another contradiction. Therefore, $Q + U - S - Q_\infty$ is a minimal vector.

Finally, to show that $P + S - U - Q_\infty$ is a minimal vector, we once again prove all of its places are distinct. From the previous argument, S, U, Q_∞ are all distinct. If $P = U$ or $P = Q_\infty$, then the vector $P + S - U - Q_\infty$ would have length 1, contradicting Theorem 34. And if $P = S$, then $\mathbf{U} = \mathbf{P} + \mathbf{S} = 2\mathbf{P}$, contradicting the choice of $\mathbf{U}$. Therefore $P + S - U - Q_\infty$ is a minimal vector and the vectors that generate $\Lambda_\mathcal{P}$ are themselves generated by vectors of minimal length, implying $\Lambda_\mathcal{P}$ is also generated by vectors of minimum length. □

2.2.2 Hermitian Function Fields

Definition 51. *The Hermitian function field over $\mathbb{F}_{q^2}$ is defined as*

$$H := \mathbb{F}_{q^2}(x, y) \text{ where } y^q + y = x^{q+1}.$$

One of the reasons why the Hermitian function field is of particular interest is the fact that it contains many rational places. The following results make this notion more precise:

Theorem 37 (Hasse-Weil bound)**.** *If $F|\mathbb{F}_q$ is a function field of genus g and N is the number of rational places of F, then*

$$|N - (q + 1)| \leqslant 2g\sqrt{q}.$$

Lemma 18. *The Hermitian function field $H|\mathbb{F}_{q^2}$ has the following properties:*

(a) H has genus $g = q(q-1)/2$ and gonality $\gamma = q$.

(b) H has $q^3 + 1$ $\mathbb{F}_{q^2}$-rational places, namely

- *the common pole Q_∞ of x and y, and*

- *for each $\alpha \in \mathbb{F}_{q^2}$, there are q elements $\beta \in \mathbb{F}_{q^2}$ such that $\beta^q + \beta = \alpha^{q+1}$, and for all such pairs (α, β) there is a unique place $P_{\alpha,\beta}$ such that $x(P_{\alpha,\beta}) = \alpha$ and $y(P_{\alpha,\beta}) = \beta$.*

(c) H attains the upper Hasse-Weil bound, that is, $H|\mathbb{F}_{q^2}$ is a maximal function field.

(d) For each pair $(d, e) \in \mathbb{F}_{q^2}^2$ with $e^q + e = d^{q+1}$, there is an automorphism $\sigma \in \mathrm{Aut}(H|\mathbb{F}_{q^2})$ with $\sigma(x) = x + d$ and $\sigma(y) = y + d^q x + e$.

Let $\mathcal{K} := \{(\alpha, \beta) \in \mathbb{F}_{q^2}^2 : \beta^q + \beta = \alpha^{q+1}\}$ and let $\mathcal{P}$ be the set of all rational places of H, that is, the common pole Q_∞ of x and y, and the places $P_{\alpha,\beta}$ indexed by $\mathcal{K}$. For each pair $(\alpha, \beta) \in \mathcal{K}$, define the function

$$\tau_{\alpha,\beta} := y - \beta - \alpha^q(x - \alpha) = y - \alpha^q x + \beta^q,$$

which is the tangent line to the Hermitian curve at the point (α, β).

Interpreting H as a Kummer extension of the rational function field $\mathbb{F}_{q^2}(y)$, the rational places of $\mathbb{F}_{q^2}(y)$ satisfy

- For each $\gamma \in \mathbb{F}_{q^2}$ with $\gamma^q + \gamma = 0$, the place $P_{y-\gamma}$ is totally ramified, and if $\gamma^q + \gamma \neq 0$, the place $P_{y-\gamma}$ splits completely in $H|\mathbb{F}_{q^2}$.
- The pole of y is totally ramified.

We note that

$$\tau_{\alpha,\beta}^q + \tau_{\alpha,\beta} = (x - \alpha)^{q+1}, \tag{2.2}$$

therefore $H = \mathbb{F}_{q^2}(x, y) = \mathbb{F}_{q^2}(\tau_{\alpha,\beta}, x)$ and $H|\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ is a Kummer extension. It follows that

$$(\tau_{\alpha,\beta}) = (q+1)P_{\alpha,\beta} - (q+1)Q_\infty.$$

We denote the rational places of $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ by their corresponding monic irreducible polynomials, except for the place at infinity, denoted by $P_\infty(\tau_{\alpha,\beta})$. For any $\gamma \in \mathbb{F}_{q^2}$ with $\gamma^q + \gamma = 0$, we have $\tau_{\alpha,\beta} - \gamma = \tau_{\alpha,\beta+\gamma}$.

Functions of the type $ax + by + c$ with $a, b, c \in \mathbb{F}_{q^2}$ and $a, b \neq 0$ will be referred to as lines. By points on the line, we mean intersection points between the line and the Hermitian curve. The following lemma allows us to determine the divisor of every line, and thus obtain the points of $\mathcal{K}$ which lie on a line.

Lemma 19. *Let $H|\mathbb{F}_{q^2}$ be the Hermitian function field and $\gamma \in \mathbb{F}_{q^2}$.*

(a) If $\gamma^q + \gamma = 0$, the place $\tau_{\alpha,\beta} - \gamma = \tau_{\alpha,\beta+\gamma}$ is totally ramified in $H|\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ and the divisor of $\tau_{\alpha,\beta} - \gamma$ is

$$(\tau_{\alpha,\beta} - \gamma) = (q+1)P_{\alpha,\beta+\gamma} - (q+1)Q_\infty$$

and the line $\tau_{\alpha,\beta} - \gamma$ is a tangent line.

(b) The pole $P_\infty(\tau_{\alpha,\beta})$ of $\tau_{\alpha,\beta}$ is totally ramified in the extension $H|\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$.

(c) If $\gamma^q + \gamma \neq 0$, the place $\tau_{\alpha,\beta} - \gamma$ of $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ splits completely in $H|\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$, and the divisor of $\tau_{\alpha,\beta} - \gamma$ is

$$(\tau_{\alpha,\beta} - \gamma) = \sum_{i=0}^{q} P_{\alpha+\delta\zeta^i, \beta+\gamma+\alpha^q\delta\zeta^i} - (q+1)Q_\infty \tag{2.3}$$

with ζ a primitive $(q+1)$st root of unity in $\mathbb{F}_{q^2}$ and $\delta \in \mathbb{F}_{q^2}^*$ is such that $\gamma^q + \gamma = \delta^{q+1}$. The points of $\mathcal{K}$ lying on the line $\tau_{\alpha,\beta} - \gamma$ are

$$(\alpha + \delta\zeta^i, \beta + \gamma + \alpha^q\delta\zeta^i),\ 0 \leqslant i \leqslant q.$$

The line $\tau_{\alpha,\beta} - \gamma$ is not a tangent line.

(d) Let $f := y + bx + c$ and $\delta \in \mathbb{F}_{q^2}$ be such that $\delta^{q+1} = b^{q+1} - (c^q + c)$. The points of $\mathcal{K}$ lying on the line f are

$$(-b^q + \delta\zeta^i, b^{q+1} - c - b\delta\zeta^i),\ 0 \leqslant i \leqslant q.$$

In this case, f is a tangent line $\iff \delta = 0 \iff (-b^q, c^q) \in \mathcal{K} \iff (-b, c) \in \mathcal{K}$. If f is a tangent line, then $f = \tau_{-b^q, c^q}$. If $\delta \neq 0$, then f contains exactly $q+1$ points of $\mathcal{K}$.

(e) If $f = x - c$, the divisor of f is

$$(f) = \sum_d P_{c,d} - qQ_\infty, \tag{2.4}$$

where the sum is done over the q solutions $d \in \mathbb{F}_{q^2}$ of $d^q + d = c^{q+1}$.

Proof. One can view H as a Kummer extension of $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$, so parts (a), (b), (e) and the first statement of (c) all follow from Proposition 28.

(c) In order to determine the divisor of $\tau_{\alpha,\beta} - \gamma$, we apply Theorem 24. Over $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$, the minimal polynomial of x is $\phi(T) := (T-\alpha)^{q+1} - \tau_{\alpha,\beta}^q - \tau_{\alpha,\beta} \in \mathbb{F}_{q^2}(\tau_{\alpha,\beta})[T]$. The place $\tau_{\alpha,\beta} - \gamma$ is rational in $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$, so its residue class field is isomorphic to $\mathbb{F}_{q^2}$. Using notation as in Theorem 24, we will study the decomposition of $\bar{\phi}(T) = (T-\alpha)^{q+1} - (\gamma^q + \gamma) \in \mathbb{F}_{q^2}[T]$. The trace map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ is $z \mapsto z^q + z$ and the norm map from $\mathbb{F}_{q^2}^*$ to $\mathbb{F}_q^*$, given by $z \mapsto z^{q+1}$ is surjective, so there exists $\delta \in \mathbb{F}_{q^2}^*$ with $\gamma^q + \gamma = \delta^{q+1}$. If $\zeta \in \mathbb{F}_{q^2}$ is a primitive $(q+1)$st root of unity, using the notation of Theorem 24, we can write

$$\bar{\phi}(T) = (T-\alpha)^{q+1} - \delta^{q+1} = \prod_{i=0}^{q} (T - \alpha - \delta\zeta^i).$$

Therefore, the place $\tau_{\alpha,\beta}-\gamma$ splits completely in the extension $H|\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$, and the function $\tau_{\alpha,\beta}-\gamma$ has $q+1$ zeros in H, say, $Z_0, Z_1, \ldots, Z_q$ with $x-\alpha-\delta\zeta^i \in Z_i$ for $i=0,\ldots,q$. Since

$$\tau_{\alpha,\beta}-\gamma = y-\alpha^q x+\beta^q-\gamma = (y-\beta-\delta\alpha^q\zeta^i)-\alpha^q(x-\alpha-\delta\zeta^i),$$

a common zero of the functions $\tau_{\alpha,\beta}-\gamma$ and $x-\alpha-\delta\zeta^i$ is also a zero of $y-\beta-\delta\alpha^q\zeta^i$. The functions $x-\alpha-\delta\zeta^i$ and $y-\beta-\delta\alpha^q\zeta^i$ have $P_{\alpha+\delta\zeta^i,\beta+\delta\alpha^q\zeta^i}$ as a unique common zero in H, that means $Z_i = P_{\alpha+\delta\zeta^i,\beta+\delta\alpha^q\zeta^i}$ for $i=0,\ldots,q$. From the fact that $\tau_{\alpha,\beta}-\gamma = y-\alpha^q x+\beta^q-\gamma$, any pole of $\tau_{\alpha,\beta}-\gamma$ must be a pole of x or y. This means Q_∞ is the only pole of $\tau_{\alpha,\beta}-\gamma$, with order $q+1$.

(d) Seeing as $b^{q+1}-(c^q+c)\in\mathbb{F}_{q^2}$, there exists $\delta\in\mathbb{F}_{q^2}$ such that $\delta^{q+1}=b^{q+1}-(c^q+c)$. Set $\alpha=-b^q$, then $b=-\alpha^q$. If $\beta\in\mathbb{F}_{q^2}$ is such that $\beta^q+\beta=\alpha^{q+1}=b^{q+1}$, then $f=y-\alpha^q x+c=\tau_{\alpha,\beta}-\gamma$ with $\gamma=\beta^q-c$. Note that $\gamma^q+\gamma=b^{q+1}-(c^q+c)=\delta^{q+1}$. By part (c), the points on f are $(\alpha+\delta\zeta^i,\beta+\gamma+\alpha^q\delta\zeta^i)=(-b^q+\delta\zeta^i, b^{q+1}-c-b\delta\zeta^i)$.

Now, f is a tangent to the Hermitian curve at $(B,C)\in\mathcal{K} \iff f=\tau_{B,C}=y-B^qx+C^q$ for some $(B,C)\in\mathcal{K} \iff (b,c)=(-B^q,C^q)$ for some $(B,C)\in\mathcal{K}$. Since $b=-B^q \iff B=-b^q$ and $c=C^q \iff C=c^q$, f is a tangent $\iff (-b^q,c^q)\in\mathcal{K} \iff (-b,c)\in\mathcal{K} \iff \delta=0$. □

This lemma allows us to find the minimum distance of the lattice.

Theorem 38. *The Hermitian function field lattice $\Lambda_{\mathcal{P}}$ generated by $\mathcal{P}$ attains the lower bound for the minimum distance: $d(\Lambda_{\mathcal{P}})=\sqrt{2q}$.*

Proof. Pick a point $P=(\alpha,\beta)$ on the Hermitian curve and two distinct non-tangent lines f_1, f_2 through P such that neither is of the form $x-\alpha$. These can be constructed by picking two distinct slopes $M_1, M_2\in\mathbb{F}_{q^2}$ which are not equal to $-\alpha^q$. We can find $m_1, m_2\in\mathbb{F}_{q^2}$ with $M_1=m_1^q$ and $M_2=m_2^q$. Defining $f_1 := y-\beta-m_1^q(x-\alpha)$ and $f_2 := y-\beta-m_2^q(x-\alpha)$, we see both lines pass through P and are not the tangent at this point since their slopes are not $-\alpha^q$. Neither can these lines be tangential to the curve at any other point, because every tangent passes only through its point of tangency.

Applying Lemma 19(c), we observe the intersection between the supports of (f_1) and (f_2) consists of only the pole Q_∞ and $P_{\alpha,\beta}$. Therefore $(f_1)=P_{\alpha,\beta}+\sum_{i=1}^{q}Q_i-(q+1)Q_\infty$ and $(f_2)=P_{\alpha,\beta}+\sum_{i=1}^{q}R_i-(q+1)Q_\infty$, meaning

$$\left(\frac{f_1}{f_2}\right)=\sum_{i=1}^{q}Q_i-\sum_{i=1}^{q}R_i$$

and $||f_1/f_2||=\sqrt{2q}$. □

Having attained the lower bound for the minimum distance, we can now easily determine a lower bound for the kissing number.

Theorem 39. $K(\Lambda_{\mathcal{P}}) \geqslant (q^3+1)\cdot q^2 \cdot (q^2-1)$.

Proof. The function x has degree q, so $[H : \mathbb{F}_{q^2}(x)] = q$. There are q^3+1 rational subfields E of H which are conjugate to $\mathbb{F}_q(x)$, meaning $[H : E] = q$. In each of these extensions, all places but the pole of the generating element split completely, that is, q^2 in each one. Applying Corollary 28, we conclude

$$K(\Lambda_{\mathcal{P}}) \geqslant \sum_{i=1}^{q^3+1} q^2(q^2-1) = (q^3+1)\cdot q^2 \cdot (q^2-1). \qquad \square$$

From Lemma 19 and Theorem 38, we have the following characterization for minimal vectors:

Lemma 20. *If f_1, f_2 are distinct lines, then f_1/f_2 and f_2/f_1 are minimal vectors if one of the following conditions hold:*

- *f_1 and f_2 are of the form $x-\alpha$.*
- *One of the lines is of the form $x-\alpha$, the other is a non tangent line $y+bx+c$ and both intersect in exactly one point.*
- *Both lines are non tangent of the form $y+bx+c$ with a point of intersection lying in $\mathcal{K}$.*

Hiss proved in (HISS, 2004) that every function in the set $O^*_{\mathcal{P}}$ can be represented as a product of functions of the form $ax+by+c$ and their inverses. Combining this result with the previous lemma, we can prove that $\Lambda_{\mathcal{P}}$ is not only well-rounded, but also generated by minimal vectors.

Theorem 40. *$\Lambda_{\mathcal{P}}$ is generated by minimal vectors and is, thus, well-rounded.*

Proof. Since $\Lambda_{\mathcal{P}}$ is generated by the divisors of lines, we need only prove that every such divisor is an integer linear combination of minimal vectors. We will call a line good if it is an integer linear combination of minimal vectors. Denoting by $\zeta \in \mathbb{F}_{q^2}$ a primitive $(q+1)$st root of unity, the proof is split into cases.

Case 1: Let $d, e \in \mathbb{F}_{q^2}$ be such that $d^q + d = e^{q+1}$. We first show that $y-d$ and $x-e$ are good. Denote by $d_1 = d, d_2, \ldots, d_q$ the solutions to $y^q + y = e^{q+1}$. Then

$$\prod_{i=1}^{q} y - d_i = y^q + y - e^{q+1} = x^{q+1} - e^{q+1} = \prod_{i=0}^{q} x - \zeta^i e,$$

therefore,

$$x - e = \prod_{i=1}^{q} \frac{y - d_i}{x - \zeta^i e}.$$

The lines $y - d_i$ and $x - \zeta^i e$ have only one point of intersection and $y - d_i$ are non tangent since $d_i^q + d_i = e^{q+1} \neq 0$. By Lemma 20, $\dfrac{y - d_i}{x - \zeta^i e}$ is a minimal vector and $x - e$ is a sum of minimal vectors, proving the line $x - e$ is good. On the other hand,

$$y - d = (x - e)(x - \zeta e) \prod_{i=2}^{q} \frac{x - \zeta^i e}{y - d_i},$$

meaning $y - d$ is also a sum of minimal vectors.

Case 2: We now prove every non tangent line $f = y + bx + c$ is good. Since f is non tangent, from Lemma 19 we get that $(-b, c) \notin \mathcal{K}$, that is $c^q + c \neq (-b)^{q+1} = b^{q+1}$. Set $\alpha = -b^q$ so that $b = -\alpha^q$ and $\alpha^{q+1} = b^{q+1}$. Let $\beta \in \mathbb{F}_{q^2}$ be a solution to $\beta^q + \beta = \alpha^{q+1} = b^{q+1}$. Then

$$f = y - \alpha^q x + \beta^q + c - \beta^q = \tau_{\alpha,\beta} - d \text{ where } d = \beta^q - c.$$

Also, $d^q + d = \beta^q + \beta - (c^q + c) = b^{q+1} - (c^q + c) \neq 0$. Now choose $e \in \mathbb{F}_{q^2}$ such that $d^q + d = e^{q+1}$, so $c^q + c = b^{q+1} - e^{q+1}$. It follows that $e \neq 0$. Defining $d_1 = d, d_2, \ldots, d_q \in \mathbb{F}_{q^2}$ to be the solutions of $y^q + y = e^{q+1}$, we have:

$$\prod_{i=1}^{q} \tau_{\alpha,\beta} - d_i = \tau_{\alpha,\beta}^q + \tau_{\alpha,\beta} - e^{q+1} = (x - \alpha)^{q+1} - e^{q+1} = \prod_{i=1}^{q} x - \alpha\zeta^i e, \tag{2.5}$$

and from this, it follows that

$$x - \alpha - e = \prod_{i=1}^{q} \frac{\tau_{\alpha,\beta} - d_i}{x - \alpha - \zeta^i e}. \tag{2.6}$$

Due to the fact that $d_i^q + d_i = e^{q+1} = d^q + d \neq 0$, we infer from Lemma 19 that the lines $\tau_{\alpha,\beta} - d_i$ are not tangent lines. Moreover, the line $\tau_{\alpha,\beta} - d_i$ intersects $x - \alpha - \zeta^i e$ at exactly one point, namely $(\alpha + \zeta^i e, \beta + d_i + e\alpha^q \zeta^i)$, which belongs to $\mathcal{K}$, since

$$\begin{aligned}(\beta + d_i + e\alpha^q\zeta^i)^q + \beta + d_i + e\alpha^q\zeta^i &= \beta^q + \beta + d_i^q + d_i + e^q\alpha\zeta^{iq} + e\alpha^q\zeta^i \\ &= \alpha^{q+1} + e^{q+1} + e^q\alpha\zeta^{iq} + e\alpha^q\zeta^i \\ &= (\alpha + \zeta^i e)^{q+1}.\end{aligned}$$

Thus, the vectors corresponding to $\dfrac{\tau_{\alpha,\beta} - d_i}{x - \alpha - \zeta^i e}$, $i = 1, \ldots, q$ are minimal vectors. From equation (2.6), the line $x - \alpha - e$ is good. The same argument applies for $x - \alpha - \zeta e$. From equation (2.5):

$$f = \tau_{\alpha,\beta} - d = (x - \alpha - e)(x - \alpha - \zeta e) \prod_{i=2}^{q} \frac{x - \alpha - \zeta^i e}{\tau_{\alpha,\beta} - d_i}, \tag{2.7}$$

meaning f is a sum of minimal vectors and the line defined by f is good.

Case 3: Now, we prove the line $\tau_{0,0} = y$ is good. Firstly, notice that

$$y^{q+1} - x^{q+1} = y^{q+1} - y^q - y = (y-1)^{q+1} - 1 = \prod_{i=0}^{q} y - 1 - \zeta^i.$$

But also $y^{q+1} - x^{q+1} = \prod_{i=0}^{q}(y - \zeta^i x)$, so

$$\prod_{i=0}^{q} y - 1 - \zeta^i = \prod_{i=0}^{q} y - \zeta^i x.$$

Since -1 is a $(q+1)$st root of unity, there is a unique $j \in \{0, \ldots, q\}$ such that $\zeta^j = -1$. Then

$$y = (y - \zeta^j x) \prod_{\substack{i=0 \\ i \neq j}}^{q} \frac{y - \zeta^i x}{y - 1 - \zeta^i}. \tag{2.8}$$

The points of $\mathcal{K}$ on the line $y - (1 + \zeta^i)$ are $((1+\zeta^i)\zeta^k, 1 + \zeta^i)$ for $k = 0, \ldots, q$, meaning the line $y - (1 + \zeta^i)$ for $i \neq j$ intersects $y - \zeta^i x$ in exactly one point of $\mathcal{K}$, that being $((1+\zeta^i)\zeta^{q+1-i}, 1 + \zeta^i)$, which belongs to $\mathcal{K}$ given that

$$\begin{aligned}((1+\zeta^i)\zeta^{q+1-i})^{q+1} = (1+\zeta^i)^{q+1} &= (1+\zeta^{iq})(1+\zeta^i) \\ &= 1 + \zeta^{iq} + \zeta^i + 1 \\ &= (1+\zeta^i)^q + (1+\zeta^i).\end{aligned}$$

The lines $y - \zeta^i x$ are not tangent since $(\zeta^i)^{q+1} = 1 \neq 0$ and thus $(-\zeta^i, 0) \notin \mathcal{K}$. Consequently, the functions $\dfrac{y - \zeta^i x}{y - 1 - \zeta^i}$ for $i = 0, \ldots, q$ and $i \neq j$ correspond to minimal vectors. Since $y - \zeta^j x$ is not a tangent, it is good by case 2, and from equation (2.8), y is good.

Case 4: For every $(\alpha, \beta) \in \mathcal{K}$, the tangent line $\tau_{\alpha,\beta} = y - \alpha^q x + \beta^q$ is good. Note that $(-\alpha, \beta^q) \in \mathcal{K}$. From Lemma 18(d), there is an automorphism $\sigma \in \mathrm{Aut}(H|\mathbb{F}_{q^2})$ with $\sigma(x) = x - \alpha$ and $\sigma(y) = y - \alpha^q x + \beta^q = \tau_{\alpha,\beta}$. Applying σ to equation (2.8):

$$\tau_{\alpha,\beta} = (\tau_{\alpha,\beta} - \zeta^j(x - \alpha)) \prod_{\substack{i=0 \\ i \neq j}}^{q} \frac{\tau_{\alpha,\beta} - \zeta^i(x-\alpha)}{\tau_{\alpha,\beta} - 1 - \zeta^i}. \tag{2.9}$$

By Lemma 14, a place Q is a common zero of $\sigma(y - 1 - \zeta^i)$ and $\sigma(y - \zeta^i x)$ if and only if $\sigma^{-1}(Q)$ is a common zero of $y - 1 - \zeta^i$ and $y - \zeta^i x$. Applying the results from case 3, the line $\tau_{\alpha,\beta} - 1 - \zeta^i = \sigma(y - 1 - \zeta^i)$ intersects $\tau_{\alpha,\beta} - \zeta^i(x - \alpha) = \sigma(y - \zeta^i x)$ at only one point. Again, by Lemma 14, these lines are not tangents, both of the form $y + ax + c$. Applying Lemma 20, the vectors from $\dfrac{\tau_{\alpha,\beta} - \zeta^i(x-\alpha)}{\tau_{\alpha,\beta} - 1 - \zeta^i}$ for $i = 0, \ldots, q$ and $i \neq j$ all have length $\sqrt{2q}$. Since $\tau_{\alpha,\beta} - \zeta^j(x - \alpha)$ is good, we conclude from equation (2.9) that $\tau_{\alpha,\beta}$ is good.

Case 5: Finally, we show that x is good. First we observe

$$y^q + y - (x^q + x) = x^{q+1} - x^q - x = (x-1)^{q+1} - 1 = \prod_{i=0}^{q} x - 1 - \zeta^i.$$

On the other hand

$$y^q + y - (x^q + x) = (y - x)^q + (y - x) = \prod_{i=1}^{q} y - x - \rho_i,$$

with $\rho_1, \ldots, \rho_q \in \mathbb{F}_{q^2}$ are the solutions to $\rho^q + \rho = 0$. Thus

$$\prod_{i=0}^{q} x - 1 - \zeta^i = \prod_{i=1}^{q} y - x - \rho_i. \tag{2.10}$$

Denoting by $z_1, \ldots, z_q$ a numbering of $1 + \zeta^i$ for $i = 0, \ldots, q$ and $i \neq j$, since $\zeta^j = -1$. From equation (2.10):

$$x = \prod_{i=1}^{q} \frac{y - x - \rho_i}{x - z_i}. \tag{2.11}$$

The two lines $x - (1 + \zeta^m)$ and $y - x - \rho_i$ intersect at $(1 + \zeta^m, 1 + \zeta^m + \rho_i)$, which is a point of $\mathcal{K}$, since

$$(1 + \zeta^m + \rho_i)^q + (1 + \zeta^m + \rho_i) = \rho_i + \rho_i^q + 1 + \zeta^{mq} + 1 + \zeta^m = (1 + \zeta^m)^{q+1}.$$

The line $y - x - \rho_i$ is non-tangent since $(1, -\rho_i) \notin \mathcal{K}$. From Lemma 20, the functions $\dfrac{y - x - \rho_i}{x - z_i}$ generate minimal vectors, and from equation (2.11), x is good, finishing the proof. □

3 Fermat Function Field Lattices

Finally, we construct some lattices associated to the Fermat function field. This construction is based on the study made by David Rohrlich on the group of functions with support at the "points at infinity" of the Fermat curve. See (ROHRLICH, 1977).

Techniques from algebraic geometry are employed to prove results concerning the minimum distance, kissing number and well-roundedness of the lattice. We show that the lower bound $\sqrt{2\gamma}$ for the minimum distance is not attained. Furthermore, the kissing number is low and fixed for the Fermat curves of degree $n \geqslant 5$.

Let $\mathcal{F}_n$ denote the Fermat curve of degree $n \geqslant 4$, that is, the non-singular plane algebraic curve given by the projective equation

$$x^n + y^n = z^n.$$

Denote its function field by

$$F_n := \mathbb{F}_q(x, y) \text{ where } x^n + y^n = 1$$

and $q = p^h$ with p an odd prime number and $h \geqslant 1$ such that $2n \mid q - 1$. This implies $\mathbb{F}_q$ contains ζ, a primitive n-th root of unity, and ε, a primitive n-th root of -1. Thus we have $3n$ $\mathbb{F}_q$-rational points on the curve for which exactly one of the coordinates is zero, namely:

$$a_i := (0 : \zeta^i : 1),\ b_i := (\zeta^i : 0 : 1),\ c_i := (\varepsilon\zeta^i : 1 : 0) \text{ for } i = 0, \ldots, n-1.$$

For the sake of simplicity, we put $A := a_0 + \cdots + a_{n-1}$, $B := b_0 + \cdots + b_{n-1}$, $C := c_0 + \cdots + c_{n-1}$. The set $\mathcal{P}$ is the set of the places corresponding to these $3n$ points. Note that all points of type a_i are contained in the line $x = 0$, all points b_i are on the line $y = 0$, and all of the c_i are on $z = 0$. Thus, we refer to them as lying on a triangle where each of the lines corresponds to a side of this triangle.

Denoting by Λ_n the lattice from $F_n|\mathbb{F}_q$ and generated by $\mathcal{P}$, we first investigate the minimum distance $d(\Lambda_n)$ and prove that it exceeds $\sqrt{2\gamma} = \sqrt{2(n-1)}$ for all $n \geqslant 4$.

In order for a function to attain the minimum distance $\sqrt{2(n-1)}$, it, in particular, must have a pole divisor of the form $p_1 + \cdots + p_{n-1}$, where $p_1, \ldots, p_{n-1} \in \mathcal{P}$ are all distinct. Therefore, examining the Riemann-Roch space $\mathcal{L}(p_1 + \cdots + p_{n-1})$ is very useful when determining if the minimum distance lower bound is achieved.

Remark 11. *Suppose notation as in Lemma 9. If D is the sum of j different points and those points lie on k different sides ($k = 2, 3$), then there are at least $n - j + k - 1$ points of R on each side.*

This is easily verifiable, since if $k = 2$, a side must have at least 1 point of D, meaning the other can have at most $j-1$ points of D, and at least $n-(j-1) = n-j+1 = n-j+k-1$ points of R. For $k = 3$, two sides have at least 1 point of D and the other has at most $j-2$, meaning each side has at least $n-(j-2) = n-j+2 = n-j+k-1$ points of R.

We have the following proposition:

Proposition 37. *Let $p_1, \ldots, p_{n-1}$ be any $n-1$ distinct points of $\mathcal{P}$.*

1. *If $p_1, \ldots, p_{n-1}$ lie on one side, then $\ell(p_1 + \cdots + p_{n-1}) = 2$.*
2. *If $p_1, \ldots, p_{n-1}$ lie on two sides, then $\ell(p_1 + \cdots + p_{n-1}) = 1$.*
3. *If $p_1, \ldots, p_{n-1}$ lie on three sides, then $\ell(p_1 + \cdots + p_{n-1}) = 1$.*

Proof. For $n = 4$, consider the effective divisor $D = p_1 + p_2 + p_3$. Its degree is $\deg D = 3$. Furthermore, the genus of $\mathcal{F}_4$ is:

$$g = \frac{(4-1)(4-2)}{2} = 3.$$

Hence, by the Riemman-Roch Theorem 19, we have $\ell(D) = i(D) + 1$. Since the canonical adjoints of $\mathcal{F}_4$ are all lines, we have the cases:

1. If p_1, p_2 and p_3 lie on one side of the triangle, then they determine a unique line that passes through them, which implies $\ell(p_1 + p_2 + p_3) = 2$.

2,3. If p_1, p_2 and p_3 lie on more than one side of the triangle, there doesn't exist a line passing through all three points. Hence $\ell(p_1 + p_2 + p_3) = 1$.

For $n \geqslant 5$ we make use of Lemma 9.

1. Suppose all $n-1$ points lie on one side of the triangle, say, $x = 0$. Take the line $\mathcal{L} = V(x)$. Bezout's Theorem 16 guarantees that

   $$\mathcal{L} \cdot \mathcal{F}_n = A.$$

   The residue divisor R always consists of one point, meaning $\ell(p_1 + \cdots + p_{n-1})$ is the dimension of the pencil of lines through a point, that is, $\ell(p_1 + \cdots + p_{n-1}) = 2$.

2. If $p_1, \ldots, p_{n-1}$ lie on two sides, say, $x = 0$ and $y = 0$, consider the conic $\mathcal{G} = V(xy)$. Then,

   $$\mathcal{G} \cdot \mathcal{F}_n = A + B.$$

R now consists of $n+1$ points. Applying Remark 11 with $j = n-1$ and $k = 2$, we see that at least 2 points of R are on each side. However, if a side has 3 or more residue points, Theorem 16 implies that side must be a component of any conic passing through the residue. If both sides satisfy this condition, the conic is uniquely determined.

If one of the sides, say $x = 0$, contains only 2 residue points then $y = 0$ contains the other $n-1$ points, and thus, is a component of the conic. The 2 remaining points define a unique line. As the conic must also pass through these points, there is only one choice for such a conic.

Finally, observe that if both sides contain only 2 residue points each, the divisor D would have $2n-4$ points. However, $2n-4 > n-1$ for $n \geqslant 5$, so this configuration is impossible and $\ell(p_1 + \cdots + p_{n-1}) = 1$ in all cases.

3. For $p_1, \ldots, p_{n-1}$ lying on all three sides, take the cubic $\mathcal{C} = V(xyz)$, which cuts out on $\mathcal{F}_n$ the divisor

$$\mathcal{C} \cdot \mathcal{F}_n = A + B + C.$$

The residue consists of $2n+1$ points, and according to Remark 11 with $j = n-1$ and $k = 3$, at least 3 of those are on each side. But if a side contains 4 or more residue points, Bezout's Theorem implies that side is a component of any cubic passing through the residue. If all sides satisfy this condition, the cubic is unique.

In the case that only 2 sides have 4 or more residue points, the cubic is still unique, since the 3 residue points on the last side are aligned, and thus define a unique line through them.

Finally, note that two different sides cannot contain only 3 residue points each. If this were the case, the last side would have to contain $2n-5$ residue points. Since $2n-5 \geqslant n$ for $n \geqslant 5$, this is impossible and $\ell(p_1 + \cdots + p_{n-1}) = 1$ in all cases, finishing the proof. □

This proposition shows there are no non-constant functions of degree $\gamma = n-1$ in F_n whose pole divisor has unaligned points of $\mathcal{P}$. Thus, the only remaining possibility for a function to have length $\sqrt{2\gamma}$ is to have a pole divisor with all points aligned. We will prove, however, that no functions in the Riemann-Roch spaces of case 1 of Proposition 37 attain the length $\sqrt{2\gamma}$. In order to prove that, we tabulate some functions and divisors which will be useful:

Function	Divisor
x	$A - C$
y	$B - C$
$x - \zeta^j$	$n \cdot b_j - C$
$y - \zeta^j$	$n \cdot a_j - C$
$x - \varepsilon\zeta^j y$	$n \cdot c_j - C.$

From this table, we notice that

$$\begin{aligned}\left(\frac{y-\zeta^j}{x}\right) &= (n-1)\cdot a_j - (A - a_j)\\ \left(\frac{x-\zeta^j}{y}\right) &= (n-1)\cdot b_j - (B - b_j)\\ \left(x - \varepsilon\zeta^j y\right) &= (n-1)\cdot c_j - (C - c_j)\,.\end{aligned}$$

This gives us explicit bases for the Riemann-Roch spaces of type 1, as described in our proposition:

$$\begin{aligned}\left\{1, \frac{y-\zeta^j}{x}\right\} &\text{ is a base for } \mathcal{L}(A - a_j)\\ \left\{1, \frac{x-\zeta^j}{y}\right\} &\text{ is a base for } \mathcal{L}(B - b_j)\\ \left\{1, x - \varepsilon\zeta^j y\right\} &\text{ is a base for } \mathcal{L}(C - c_j).\end{aligned}$$

We can now prove our first major result concerning the Fermat function field lattice:

Theorem 41. $d(\Lambda_n) > \sqrt{2\gamma} = \sqrt{2(n-1)}$.

Proof. According to Proposition 37, we only need to examine the Riemann-Roch spaces of case 1. Given $f \in \mathcal{L}(A - a_j)$, it has the form

$$f = a + b \cdot \frac{y - \zeta^j}{x}$$

with $a, b \in \mathbb{F}_q$. Note that we may assume $a, b \neq 0$, since if $b = 0$, f is constant, and if $a = 0$, $(f) = \left(\frac{y-\zeta^j}{x}\right)$, which has a zero of order $n-1$ and thus does not have length $\sqrt{2\gamma}$. We have

$$(f) = \left(\frac{ax + b(y - \zeta^j)}{x}\right) = (ax + b(y - \zeta^j)) - (x).$$

Notice that $ax + b(y - \zeta^j) = 0$ defines a line ℓ which is not the tangent at $a_j = (0 : \zeta^j : 1)$. It cannot coincide with $x = 0$ since $b \neq 0$. It also is not $y = 0$ or $z = 0$, given that it passes through a_j.

Therefore, ℓ can only possibly intersect the triangle at one point on each side. This means that for $n \geqslant 5$, ℓ must have at least one zero outside of $\mathcal{P}$. In the case $n = 4$, three

points of intersection is impossible. Indeed, if ℓ intersected all three sides, its zero divisor would have the form $(\ell)_0 = a_i + b_j + c_k$ for some $i, j, k \in \{0, \ldots, n-1\}$. But this means $(1/\ell)_\infty = a_i + b_j + c_k$, and thus $1/\ell$ has three unaligned poles, contradicting Proposition 37. Now, the divisor of x has neither zeros nor poles outside the triangle thus subtracting it means f still has at least one zero outside of $\mathcal{P}$, meaning $f \notin O_{\mathcal{P}}^*$ and f cannot achieve length $\sqrt{2\gamma}$.

For a function $g \in \mathcal{L}(B - b_j)$, the argument is similar. g has the form

$$g = a + b \cdot \frac{x - \zeta^j}{y}$$

with $a, b \in \mathbb{F}_q^*$. Its divisor is

$$(g) = \left(\frac{ay + b(x - \zeta^j)}{y}\right) = (ay + b(x - \zeta^j)) - (y).$$

The line $m : ay + b(x - \zeta^j) = 0$ is not the tangent at $b_j = (\zeta^j : 0 : 1)$. Neither is it $y = 0$, given that $b \neq 0$. It also is not $x = 0$ or $z = 0$, as it passes through b_j. The same argument as the previous case now applies: since (y) has only zeros and poles in the triangle, $g \notin O_{\mathcal{P}}^*$.

Finally, if $h \in \mathcal{L}(C - c_j)$:

$$h = a + b(x - \varepsilon\zeta^j y),$$

$a, b \in \mathbb{F}_q^*$. The line $h = 0$ cannot be $z = 0$, since it does not pass through c_j. It also is not $x = 0$ or $y = 0$, since

$$x = 0 \implies y = \frac{a}{b\varepsilon\zeta^j}$$
$$y = 0 \implies x = -\frac{a}{b},$$

that is, the intersection points are uniquely determined. Once again, our argument applies and the claim is proved. □

Remark 12. *This constitutes the first example known by the authors of a function field lattice with arbitrarily large dimension that does not attain the lower bound for the minimum distance. The only other instance in which this happens is in Theorem 34 if there are only* 3 *places in the set* $\mathcal{P}$.

Corollary 29. $d(\Lambda_n) = \sqrt{2n}$.

Proof: The lower bound $\sqrt{2(n-1)}$ isn't attained, so $d(\Lambda_n) \geqslant \sqrt{2(\gamma+1)} = \sqrt{2n}$. This corresponds to functions with n simple zeros and n simple poles. Some examples of such functions and their divisors are:

Function	Divisor
x	$A - C$
y	$B - C$
$1/x$	$C - A$
$1/y$	$C - B$
x/y	$A - B$
y/x	$B - A$

This also gives a lower bound for the kissing number: $\kappa(\Lambda_n) \geqslant 6$. □

This lower bound turns out to be sharp for every $n \geqslant 5$. In order to prove this, we shall first prove an analogous version of Proposition 37:

Proposition 38. *If $n \geqslant 5$, let $p_1, \ldots, p_n$ be any n points of $\mathcal{P}$.*

1. *If $p_1, \ldots, p_n$ lie on one side, then $\ell(p_1 + \cdots + p_n) = 3$.*
2. *If $p_1, \ldots, p_n$ lie on two sides, then $\ell(p_1 + \cdots + p_n) = 2$ if there is only one unaligned point and $\ell(p_1 + \cdots + p_n) = 1$ otherwise.*
3. *If $p_1, \ldots, p_n$ lie on three sides, then $\ell(p_1 + \cdots + p_n) = 1$.*

Remark 13. *For the third case of this proposition, we must make a key observation about the required number of residue points on a side that guarantees it is a part of the cubic.*

If there is a side with 4 or more residue points, it is a component of the cubic by Bézout's Theorem, as previously established. However, if we have already determined a side to be a component of the cubic, there is only the need to find a conic which passes through the remaining residue points. This means that if a side already has 4 or more points, finding a second component only requires a side to have 3 points. Finally, if two components have already been determined, it suffices for the last side to have only 2 points, which always happens.

Proof: 1. Suppose the points lie on $\mathcal{L} = V(x)$. Then

$$\mathcal{L} \cdot \mathcal{F}_n = A.$$

Hence R is the zero divisor. This means there are no restrictions imposed on the lines of the linear system, that is, $\ell(p_1 + \cdots + p_n)$ is the dimension of the space of all lines in the projective plane, implying $\ell(p_1 + \cdots + p_n) = 3$.

2. If the points lie on sides $x = 0$ and $y = 0$, for example, we consider the conic $V(xy)$ which cuts out the divisor $A + B$ on $\mathcal{F}_n$. The residue R consists of n points with at least 1 of them lying on each side by Remark 11. Thus, the possible distributions for the residue points are:

Side 1	Side 2
$n-1$	1
$n-2$	2
$n-3$	3
$\vdots$	$\vdots$
1	$n-1$

In the first and last lines of the table, since $n-1 \geqslant 4$, one side is always a component of any conic passing through the residue. The other component may be any line that passes through the point lying on the other side, that is, $\ell(p_1 + \cdots + p_n) = 2$.

For the second line, $n-2 \geqslant 3$ and side 1 is a component. The 2 points remaining in side 2 define a unique line, which means $\ell(p_1 + \cdots + p_n) = 1$. For all other lines of the table, side 2 is always a component, and side 1 always has 2 or more points, meaning the conic is always unique and $\ell(p_1 + \cdots + p_n) = 1$ always holds.

3. Considering the cubic $\mathcal{C} = V(xyz)$ which cuts out the divisor $A + B + C$ on $\mathcal{F}_n$, leaving $2n$ points on the residue divisor with at least 2 (Remark 11) and at most $n-1$ on each side, since n residue points on a side means that side has no points of D. The first two possible distributions of residue points are

Side 1	Side 2	Side 3
2	$n-1$	$n-1$
3	$n-1$	$n-2$

If one side has only 2 residue points, the only way to distribute the other $2n-2$ is to have $n-1$ be on each remaining side. The fact that $n-1 \geqslant 4$ then implies these two sides must be components of the cubic. The last component is the line determined by the two points on the first side and the cubic is unique.

Now, if one side has 3 residue points, one of the other sides must have $n-1$ points, and the other, $n-2$. Seeing as $n-1 \geqslant 4$, this side is a component of the cubic. By Remark 13, the side with 3 points now is also a component, implying the cubic is always unique.

Finally, suppose there are $k \geqslant 4$ residue points on the first side, implying it is a component. Evidently, we must have $n \geqslant k+1$. To conclude uniqueness, we will show that at least one of the other sides must always be a component. The distribution of points always has the form

$$k + (n-\alpha) + (n-\beta), \text{ with } \alpha + \beta = k.$$

The most balanced distribution of residue points is

$$k + \left(n - \frac{k}{2}\right) + \left(n - \frac{k}{2}\right), \text{ if } k \text{ is even.}$$
$$k + \left(n - \frac{k-1}{2}\right) + \left(n - \frac{k+1}{2}\right), \text{ if } k \text{ is odd.}$$

Note that if we can prove uniqueness for the case of these distributions, all of the other cases will follow, since other distributions will necessarily have more residue points accumulated on one side. Hence, if that side was a component under the most balanced distribution, it will also be a component under the other distributions.

If k is odd, we need only show that $n - \frac{k-1}{2} \geqslant 3$. We have

$$n - \frac{k-1}{2} \geqslant k + 1 - \frac{k-1}{2} = \frac{k+3}{2} \geqslant 4 > 3$$

for $k \geqslant 5$. And if k is even, we show that $n - \frac{k}{2} \geqslant 3$. We have

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

for $k \geqslant 4$. Hence, uniqueness is always guaranteed and $\ell(p_1 + \cdots + p_n) = 1$ always holds. □

We can now determine the kissing number of the lattice for all $n \geqslant 5$.

Theorem 42. *$K(\Lambda_n) = 6$ for all $n \geqslant 5$.*

Proof: We will show that apart from the 6 functions presented, the minimum length is not achieved by any other function in the Riemann-Roch spaces of Proposition 38 whose the dimension is greater than 1. In case 1, we have the following bases:

$$\mathcal{L}(A) : \left\{1, \frac{1}{x}, \frac{y}{x}\right\}$$
$$\mathcal{L}(B) : \left\{1, \frac{1}{y}, \frac{x}{y}\right\}$$
$$\mathcal{L}(C) : \{1, x, y\}.$$

A function $f \in \mathcal{L}(C)$ has the form $f = a + bx + cy$ with $a, b, c \in \mathbb{F}_q$. Note that at least two of these scalars must be non-zero, since if $b, c = 0$, f is constant, if $a, c = 0$, $(f) = (x)$ and if $a, b = 0$, $(f) = (y)$.

In any case, is it clear that the line defined by f cannot coincide with any side of the triangle. This means the same argument used in the proof of Theorem 41 applies, implying f has at least one zero outside of $\mathcal{P}$. For functions in $\mathcal{L}(A)$ or $\mathcal{L}(B)$, we do the same as

in the previous case, except with the subtraction of (x) or (y) which, as discussed in the proof of Theorem 41, does not change the fact that the functions in these spaces have zeros not in the triangle. Hence, there can be no minimum length functions in $\mathcal{L}(A), \mathcal{L}(B)$ or $\mathcal{L}(C)$, except for the non-constant basis elements.

In case 2 with $p_1, \ldots, p_{n-1}$ lying on one side and p_n on another, the situation is the same as in the first case of Proposition 37. Suppose we take $p_1 + \cdots + p_{n-1} = A - a_j$ for some $j = 0, 1, \ldots, n-1$ and $p_n \neq a_j$, then it is clear that $\dfrac{y - \zeta^j}{x} \in \mathcal{L}(p_1 + \cdots + p_n)$, implying $\left\{1, \dfrac{y - \zeta^j}{x}\right\}$ is a base for $\mathcal{L}(p_1 + \cdots + p_n)$. Note that we can consider $n-1$ aligned points over $y = 0$ or $z = 0$ and construct the same bases as we did for Theorem 41. We have already shown that functions generated by those bases either are not in $O_{\mathcal{P}}^*$ or have length $\sqrt{(n-1)^2 + (n-1)} > \sqrt{2n}$, proving the theorem. □

Corollary 30. *The lattice Λ_n is never well rounded for $n \geqslant 5$.*

Proof. For $n \geqslant 5$, the rank of Λ_n is $\operatorname{rank}(\Lambda_n) = 3n - 1 \geqslant 14$. Since there are only 6 minimal vectors by Theorem 42, our claim follows. □

For $n = 4$, we can apply the Riemann-Roch Theorem 19 to conclude

Proposition 39. *Let $p_1, \ldots, p_4$ be any 4 points of $\mathcal{P}$.*

1. *If $p_1, \ldots, p_4$ lie on one side, then $\ell(p_1 + \cdots + p_4) = 3$.*
2. *If $p_1, \ldots, p_4$ lie on two sides, then $\ell(p_1 + \cdots + p_4) = 2$.*
3. *If $p_1, \ldots, p_4$ lie on three sides, then $\ell(p_1 + \cdots + p_4) = 2$.*

Functions in the Riemann-Roch spaces of case 1 and case 2 with 3 aligned points and 1 unaligned point do not achieve minimum length by the same arguments used in the proof of Theorem 42. However, the remaining cases still require closer investigation, so for Λ_4 there is only the lower bound $K(\Lambda_4) \geqslant 6$ for the kissing number.

Bibliography

ATEŞ, L. *On Lattices from Function Fields*. Tese (Doutorado) — Sabancı University, 2017. Citado 2 vezes nas páginas 10 and 81.

BÖTTCHER, A.; FUKSHANSKY, L.; GARCIA, S. R.; MAHARAJ, H. Lattices from hermitian function fields. *Journal of Algebra*, Elsevier, v. 447, p. 560–579, 2016. Citado 2 vezes nas páginas 10 and 87.

COSTA, S. I.; OGGIER, F.; CAMPELLO, A.; BELFIORE, J.-C.; VITERBO, E. *Lattices Applied to Coding for Reliable and Secure Communications*. [S.l.]: Springer, 2017. Citado 2 vezes nas páginas 10 and 78.

FUKSHANSKY, L.; MAHARAJ, H. Lattices from elliptic curves over finite fields. *Finite Fields and Their Applications*, Elsevier, v. 28, p. 67–78, 2014. Citado 2 vezes nas páginas 10 and 87.

GOPPA, V. D. *Geometry and Codes*. [S.l.]: Springer Science & Business Media, 1988. Citado 2 vezes nas páginas 10 and 52.

HISS, G. Hermitian function fields, classical unitals, and representations of 3-dimensional unitary groups. *Indagationes Mathematicae*, Elsevier Science, v. 15, n. 2, p. 223–243, 2004. Citado na página 98.

ROHRLICH, D. E. Points at infinity on the fermat curves. *Inventiones Mathematicae*, Springer, v. 39, n. 2, p. 95–127, 1977. Citado 2 vezes nas páginas 10 and 102.

STICHTENOTH, H. *Algebraic Function Fields and Codes*. 2. ed. [S.l.]: Springer Science & Business Media, 2009. v. 254. Citado 3 vezes nas páginas 10, 11, and 87.