Algebraic Geometry in Positive Characteristic

Petr Somberg

Contents

1 Introduction into Algebraic Geometry **2**

1. Algebraic set, Algebraic variety and Algebraic curve 2

    1.1 The Frobenious morphism 10

2 The Theory of Algebraic Function Fields **12**

1. Places, Valuation rings, Valuations 12
2. The Rational Function Fields 20
3. Independence of Valuations 23
4. Divisors 26
5. The Riemann-Roch Theorem 34
6. The Concequences of the Riemann-Roch Theorem 40

3 Examples of Algebraic Function Fields **42**

1. Elliptic Function Fields 42
2. Hyperelliptic Function Fields 47
3. Tame Cyclic Extensions of the Rational Function Fields 49

4 Function Fields over Finite Constant Field **50**

1. The Zeta Function of a Function Field 50
2. The Hasse-Weil Theorem 61

Chapter 1

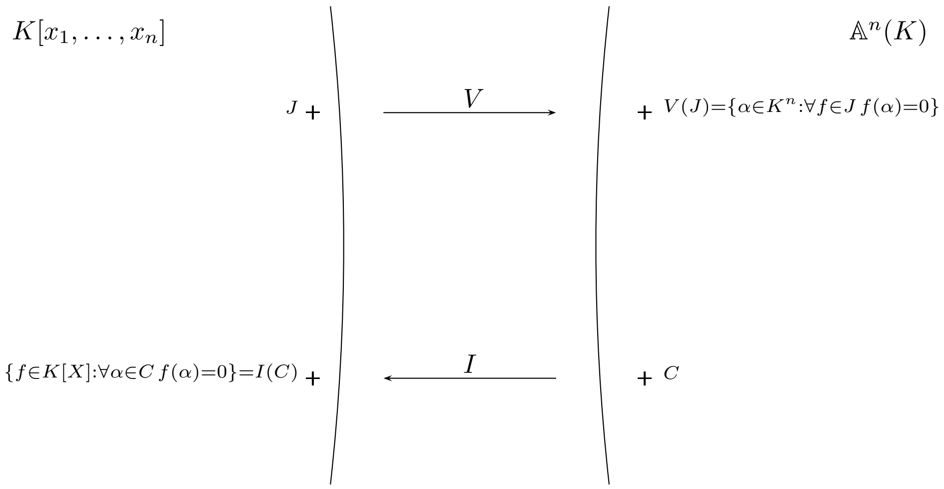
Introduction into Algebraic Geometry

1. Algebraic set, Algebraic variety and Algebraic curve

We shall introduce firstly the affine version and then use the projective completion. Let K be a (commutative) field and $\overline{K}$ its algebraic closure.

Definition 1 *$\mathbb{A}^n(K)$ denotes affine space of dimension n over K, i.e. the set of n-tuples $(a_1, \ldots, a_n)$ of elements of K.*

There is a relation between the set of points of n-dimensional affine space and the set of polynomials in n-variables. Let $K[x_1, \ldots, x_n]$ be a commutative ring of polynomials in n variables over K.
We shall investigate the relation $R = \{(f, \alpha) : f(\alpha) = 0\} \subseteq K[x_1, \ldots, x_n] \times K^n$



where C is a finite subset of n-tuples of $\mathbb{A}^n(K)$ and $J \subseteq K[x_1, \ldots, x_n]$ is an ideal of $K[x_1, \ldots, x_n]$.

Every set of polynomials of the form $I(C)$ is an ideal of the ring $K[x_1, \ldots, x_n]$. These ideals are called closed. The subsets of $\mathbb{A}^n(K)$ of the form $V(J)$, for some $J \subseteq K[x_1, \ldots, x_n]$ are called algebraic sets.

For example, for $\mathbb{R}, \mathbb{C}$, the algebraic sets are closed in usual (analytic) topology. We have $V(I) = \cap_{p \in I} V_p$, where $V_p = V(\{p\})$ is the finite set of n-tuples of zeroes of a polinomial p, i.e. $V(I)$ is closed in usual topology. As we shall prove, the algebraic sets form topology (of closed sets) on $\mathbb{A}^n(K)$ called Zariski topology. It is coarser than the usual (analytic) topology.

Lemma 2

1. *The system of all algebraic sets is closed on finite unions and all intersections. If $V_\alpha = V(J_\alpha)$, $\alpha \in S$, are algebraic sets labelled by the set S, we have*
$$\bigcap_{\alpha \in S} V_\alpha = V(\bigcup_{\alpha \in S} J_\alpha).$$
If $\#S < \infty$, then
$$\bigcup_{\alpha \in S} V_\alpha = V(\prod_{\alpha \in S} J_\alpha).$$
2. *The intersection of any number of closed ideals is closed ideal.*

Proof: The proof of the first part is straight forward. The set $\prod_{\alpha \in S} J_\alpha$ is the product of sets J_α element-wise. Concerning the second part, let J_α, $\alpha \in S$, be closed ideals. We shall show that, for $J = \cap_{\alpha \in S} J_\alpha$ it holds $J = IV(J)$. For p a trivial polynomial on $V(J)$ we get p is trivial on any $V(J_\alpha) \subseteq V(J)$ for all $\alpha \in S$. This means $p \in IV(J_\alpha) = J_\alpha$ for all $\alpha \in S$ and so $p \in J$. ■

Remark 3 *In the previous proof we have used the notion the product of the sets of polynomials. For $J_1, J_2 \subseteq K[x_1, \ldots, x_n]$ we define*
$$(J_1 \cdot J_2) := \left\{ \sum_{i=0,\ldots,m} a_i b_i : m \in \mathbb{N}, a_i \in J_1, b_i \in J_2 \right\}.$$
It is the closure of the set of all products of elements of J_1 with elements of J_2 on the operation of addition. If J_1, J_2 are ideals, then $J_1 \cdot J_2 \subseteq J_1 \cup J_2$ is an ideal. The additive closure has an impact on the underlying algebraic set.

We have shown that the intersection of (infinite system of) closed ideals is closed ideal. However, this ideal doesn't correspond to the union of corresponding algebraic sets, so generally
$$V(\bigcup_{\alpha \in S} J_\alpha) \neq \bigcap_{\alpha \in S} V(J_\alpha)$$
for closed ideals J_α, i.e. infinite union of algebraic sets need not be an algebraic set. But it is true that $V(\bigcap_{\alpha \in S} J_\alpha)$ is the closure of $\bigcup_{\alpha \in S} V(J_\alpha)$ in Zariski topology.

Definition 4 *The commutative ring R is noetherian if it doesn't contain an infinite descending string of proper ideals. The topology is noetherian if it doesn't contain an infinite descending string of closed subsets.*

It is well known that $\mathcal{R} = K[x_1, \ldots, x_n]$ is noetherian ring and so Zariski topology is noetherian.

Theorem 5 *(Hilbert's basis Theorem) If R is a commutative noetherian ring and x is transcendental over R, the ring $\mathcal{R}[x]$ is noetherian.*

Proof: We associate to an ideal $J \subseteq \mathcal{R}[x]$ and a natural number $n \in \mathbb{N}_0$ a set $J^{(n)} = \{r \in R \mid r \text{ is the leading of a polynomial } p \in J,\ \deg(p) = n\} \cup \{0\}$. It follows $J^{(n)} \subseteq R$ is an ideal, $J^{(n)} \subseteq I^{(n)}$ for $J \subseteq I$ and also $J^{(n)} \subseteq J^{(m)}$ for $n \le m$ (corresponding to the multiplication by $x^{m-n} \in R[x]$). Let us consider the string of ideals J_i, $i \in \mathbb{N}$, $J_i \subseteq J_j$ for $i \le j$ of the ring $R[x]$. If $p \in J_j \setminus J_i$, $i < j$, the polynomial of lowest possible degree, it must be $J_i^{(k)} \neq J_j^{(k)}$ for $k = \deg p$. If it was not the case there should exist $q \in J_i$, $\deg(q) = k$, with the same leading coefficient as p and we would get $(p - q) \in J_j \setminus J_i$, $\deg(p - q) < k$, a contradiction.
Thanks to the noetherian property of R $\forall n \in \mathbb{N}_0$, there exists in such that $J_i^{(n)} = J_{in}^{(n)}$ for all $i \ge i_n$. Moreover we have the sequence $J_{i1}^{(1)} \subseteq J_{i2}^{(2)} \subseteq \ldots$ There exists $n_0 \ge 0$ such that $J_{in}^{(n)} = J_{in_0}^{(n_0)}$ for all $n \ge n_0$. The choice $l \gg 0$, $l \ge i_{n_0}$ and $l \ge i_n$ for all $n \le n_0$, leads to

$$J_l^{(n)} = J_i^{(n)} \qquad \forall n \ge 0,\ \forall i \ge l.$$

Following the previous paragraph, $J_i = J_l$ for all $i \ge l$; which is desired noetherian property of $R[x]$. ∎

Inductive application of Hilbert's basis Theorem implies that $K[x_1, \ldots, x_n]$ is noetherian ring. This means that there does not exist infinite descending string of proper ideals, i.e. the same holds for algebraic sets. In other words, Zariski topology is noetherian.

Definition 6 *Algebraic set $V \subseteq \mathbb{A}^n(K)$ is indecomposable, if it is not the union of two proper algebraic subsets.*

Lemma 7 *Let K be a field. If I is a maximal ideal of the ring $K[x_1, \ldots, x_n]$, then $\dim_K(K[x_1, \ldots, x_n]/I) < \infty$.*

Proof: Let us denote $R = K[x_0, \ldots, x_n]/I$ and $a_i = x_i + I$, $i = 1, \ldots, n$. Then $R = K[x_1, \ldots, x_n]$ and $\dim_K R < \infty$ iff a_i is $(\forall_i)$ algebraic over K (R is a field!). Let us renumber the elements a_i in such a way that a_i, $i = 1, \ldots, r+1$ are transcendental over $K(a_1, \ldots, a_{i-1})$ (a subfield of R) and remaining elements $a_{r+2}, \ldots, a_n$ are algebraic over $\widetilde{K} = K(a_1, \ldots, a_{r+1})$.
From the algebraicity of elements $a_{r+2}, \ldots, a_n$ it follows the existence of polynomials $p_i \in \widetilde{K}[x_{r+2}, \ldots, x_i] = (\widetilde{K}[x_{r+1}, \ldots, x_{i-1}])[x_i]$, $i = r+2, \ldots, n$, monic of degree d_i in variable x_i such that

$$\widetilde{K}[a_{r+2}, \ldots, a_n] \simeq \widetilde{K}[x_{r+2}, \ldots, x_n] / \langle p_{r+1}, \ldots, p_n \rangle,$$

where $\langle p_{r+1}, \dots, p_n \rangle$ is the ideal of $\widetilde{K}[x_{r+2}, \dots, x_n]$ generated by $p_{r+2}, \dots, p_n$. The polynomials p_i correspond to minimal polynomials of a_i $(i = r+2, \dots, n)$ over the field $\widetilde{K}[a_{r+1}, \dots, a_{i-1}]$, i.e. $d_i = \dim_{\widetilde{K}[a_{r+1},\dots,a_{i-1}]} \widetilde{K}[a_{r+1}, \dots, a_i]$.
There exists a polynomial $q \neq 0,\ q \in K[a_1, \dots, a_{r+1}]$ such that
$qp_i \in (K[a_1, \dots, a_r])[x_{r+2}, \dots, x_n]\ \forall i = r+2, \dots, n$ (multiply by denominators of the quotients of $K(a_0, \dots, a_{r+1})$). Let us denote by $S = K[a_1, \dots, a_{r+1}, q^{-1}]$ the subring of $\widetilde{K}$, i.e.

$$p_i \in S[x_{r+2}, \dots, x_n], \qquad i = r+2, \dots, n.$$

We assert that R is free S-module with basis

$$\left\{ \prod_{i=r+2,\dots,n} a_i^{k_i} \mid 0 \leq k_i < d_i \right\}.$$

Because $R = S[a_{r+2}, \dots, a_n]$, the elements of R can be written in the form $p(a_{r+2}, \dots, a_n)$ for $p \in S[x_{r+2}, \dots, x_n]$. If we regard p as a polynomial in the variable x_n, we can divide it in the ring $S[x_{r+2}, \dots, x_n]$ with the remainder given by polynomial p_{n-1}. In conclusion, the degree of p in x_n will be less than d_n. We now proceed by induction in i, the index of x_i. As a result we get a polynomial, whose degree is less than d_i in x_i $(i = r+2, \dots, n)$ and which is congruent modulo the ideal $\langle p_{r+2}, \dots, p_n \rangle$ with p . This means that the set $\left\{ \prod_{i=r+2,\dots,n} a_i^{k_i} \mid 0 \leq k_i < d_i \right\}$ generates the ring R (over S). The independence of $\left\{ \prod_{i=r+2,\dots,n} a_i^{k_i} \mid 0 \leq k_i < d_i \right\}$ follows from the minimality of polynomials $p_i,\ i = r+2, \dots, n$.
Let us assume $r \geq 0$. Then S cannot be a field, because the ring $K[a_1, \dots, a_{r+1}]$ is Gauss (the ring of polynomials in $(r+1)$-variables) and if $b \in K[a_1, \dots, a_{r+1}]$ is an element with property $b \not| q$, then $b^{-1} \notin S$. We shall prove that in this case also R is not a field. We have proved that R is free S-module with finite basis, i.e. $R \simeq S^m,\ 0 < m \in \mathbb{N}$. The ring S is not the field and so there is a proper ideal $I \subset S$. It gives an ideal $I' := IR \subset R$ of R. We have $I \cdot R \simeq I \cdot S^m = I^m$, and because $0 \neq I^m \neq S^m$, $I' := IR$ is a proper ideal of R and so R is not a field. ■

Theorem 8 *(Hilbert's Nullstellensatz)*
Let K is algebraically closed field and let $p_1, \dots, p_n \in K[x_1, \dots, x_n]$. If the polynomials $p_1, \dots, p_k$ have no common root, there exist $q_1, \dots, q_k \in K[x_1, \dots, x_n]$ such that $\sum_{i=1,\dots,k} p_i q_i = 1$.

Proof: If we denote by $I \subset K[x_1, \dots, x_n]$ the ideal generated by $p_1, \dots, p_n$, the assumption is that $V_I = \{\emptyset\}$. We must prove that $1 \in I$ (and the fact that this element is generated by $\{q_1, \dots, q_k\}$). Let us assume $1 \notin I$. Then we shall prove that I, proper ideal contained in some maximal ideal J, fullfils $V_J \neq \{\emptyset\}$. By Lemma 7, $\dim_K(K[x_1, \dots, x_n]/J) < \infty$. Let us denote $t_i = x_i + J,\ i = 1, \dots, n$. In the field $K[x_1, \dots, x_n]/J = K[t_1, \dots, t_n]$ are $t_i,\ i = 1 \dots, n$, algebraic over K. The (algebraic) closedness of K implies $t_i \in K,\ i = 1, \dots, n$. The natural projection

$$K[x_1, \dots, x_n] \longrightarrow K[x_1, \dots, x_n]/J$$

corresponds to

$$P \longmapsto p\,(t_1, \ldots, t_n).$$

This implies $(t_1, \ldots, t_n) \in \mathbb{A}^n(K)$ is the point of V_J, i.e. $V_J \neq \{\emptyset\}$. ■

Hilbert's Nullstellensatz can be also reformulated as:
Maximal ideals of the ring $K[x_1, \ldots, x_n]$, for algebraically closed field K, are closed ideals.
In fact, if J is a maximal ideal in $K[x_1, \ldots, x_n]$, we have $V_J \neq \{\emptyset\}$. From the maximality of J it follows that V_J is one-point set. In other words, maximal ideals of $K[x_1, \ldots, x_n]$, for K algebraically closed, correspond to the points of $\mathbb{A}^n(K)$.
Other closed ideals, over algebraically closed field K, are prime ideals.

Definition 9 *The ideal $P \subset R$ is prime ideal if $\forall p, q \in R$:*

$$p\,q \in P \Longrightarrow p \in P \vee q \in P.$$

Maximal ideals are prime ideals. Trivial ideal 0 in an integral domain is prime ideal.

Theorem 10 *Let K be an algebraically closed field. Then the prime ideals of the ring $K[x_1, \ldots, x_n]$ are closed ideals.*

Proof: Let P be a prime ideals. Let us denote by I the intersection of all maximal ideals containing P. Maximal ideals containing P correspond to the points of algebraic set V_P, i.e. for $p \in I$ it holds that p is zero on V_P. Moreover, we have $P \subseteq I$ and I is closed ideal given by intersection of (finite number of) closed ideals. We shall prove the second inclusion, $I \subseteq P$, and the assertion of the Theorem follows.
Let $0 \neq p \in I$. Let us denote by I_1 the ideal of $K[x_1, \ldots, x_{n+1}]$ generated by $\langle P, 1 - x_{n+1}p \rangle$. Obviously $V_{I_1} \subseteq V_P \subseteq \mathbb{A}^{n+1}(K)$. The polynomial $(1 - x_{n+1}p) \in K[x_1, \ldots, x_{n+1}]$ is nonzero on V_P, i.e. $V_{I_1} = \{\emptyset\}$. It follows from Theorem 8 $I_1 = K[x_1, \ldots, x_{n+1}]$, and so:

$$1 = \sum_i q_i p_i + r(1 - x_n p), \qquad p_i \in P,\ r, q_i \in K[x_1, \ldots, x_{n+1}]. \tag{1.1}$$

The substitution of $\frac{1}{p}$ for x_n and multiplication of both sides by suitable power of p in Equation(1.1) it follows $p^m \in P$. Because P is prime ideal $p \in P$ and we are done. ■

The prime ideals correspond to indecomposable algebraic sets. On the one hand we can verify that $I(V)$ must be prime ideal for indecomposable algebraic set V. For $p, q \in R$ such elements that $p\,q \in I(V)$, we can define ideals $I_1 = \langle I(V), p \rangle$ (the ideal generated by $I(V) \cup \{p\}$) and $I_2 = \langle I(V), q \rangle$ (the ideal generated by $I(V) \cup \{q\}$). Algebraic subsets V_{I_1} and V_{I_2} are the subsets of V and $V_{I_1} \cup V_{I_2} = V$ because $p(v) = 0$ or $q(v) = 0$ for every $v \in V$. It follows from indecomposability of V that either $V_{I_1} = V$ or $V_{I_2} = V$, i.e. $p \in I(V)$ or $q \in I(V)$.
Starting with prime ideal P, it is easy to prove that V_P must be indecomposable. If $V_P = V_1 \cup V_2$ is a non trivial decomposition on irreducible algebraic subsets,

then $I(V_1) \supsetneq P$ and $I(V_2) \supsetneq P$. For any couple of elements $p \in I(V_1) \smallsetminus P$, $q \in I(V_2) \smallsetminus P$ we have $p\,q \in P$, i.e. P is not a prime ideal.
Note that a prime ideal P fulfills $P = I(V_P)$, which is only a reformulation of the property of its closedness.

Example 11 *Let V be an algebraic set defined by polynomial p. p is indecomposable then V is indecomposable algebraic set. In fact, in the Gauss domain is the ideal, generated by incecomposable p, prime ideal and so $V = V_P = V_{\langle p \rangle}$ is indecomposable.*

Note that the indecomposability of an algebraic set is investigated over an algebraically closed field K (resp. over algebraic closured of a given field). An algebraic set in $\mathbb{A}^n(K)$ can be also defined over non-algebraically closed field. However, any geometric property will be investigated over algebraic closure $\overline{K}$. As an example, let $V \subseteq \mathbb{A}^n(\mathbb{C})$ the set determined by polynomial $x^2 + y^2$. We have $V \cap \mathbb{A}^n(\mathbb{R}) = \{(0, 0)\}$, i.e. one-point irreducible set. On the other hand, $V \subseteq \mathbb{A}^n(\mathbb{C})$ is reducible, $V = V_{I_1} \cup V_{I_2}$ for $I_1 = x + iy$, $I_2 = x - iy$.

Definition 12 *For an algebraic set $V \subseteq \mathbb{A}^n(\overline{K})$, the set $V \cap \mathbb{A}(K) =: V(K)$ is called the set of K-rational points of V. If V is defined by a polynomial with coefficients in K, we say that V is defined over K.*

Example 13 *Let us consider a quadric defined by ideal $I = x^2 + y^2 - 1$ in $K[x, y]$. We shall prove that V_I is indecomposable algebraic set defined over $\mathbb{Q}$ (or $\overline{\mathbb{Q}} \subseteq \mathbb{C}$). If V_I would be decomposable, i.e.*

$$x^2 + y^2 - 1 = (\alpha x + \beta y + \gamma)(\alpha' x + \beta' y + \gamma'), \qquad \alpha, \beta, \gamma, \alpha', \beta', \gamma'?$$

This would imply

$$\begin{aligned} \alpha\alpha' &= 1, \\ \beta\beta' &= 1, \\ \gamma\gamma' &= -1, \\ \alpha\beta' + \beta\alpha' &= 0, \\ \alpha\gamma' + \gamma\alpha' &= 0, \\ \beta\gamma' + \gamma\beta' &= 0, \end{aligned}$$

which yields

$$\begin{aligned} \alpha^2 + \beta^2 &= 0, \\ \alpha^2 + \gamma^2 &= 0, \\ \beta^2 + \gamma^2 &= 0, \end{aligned}$$

and

$$\alpha' = \frac{1}{\alpha},\ \beta' = \frac{1}{\beta},\ \gamma' = -\frac{1}{\gamma}.$$

These equations have only trivial solution, $\alpha = \alpha' = \beta = \beta' = \gamma = \gamma' = 0$ and the result follows.

Indecomposable algebraic sets are called algebraic varieties. For algebraic variety $V \subseteq \mathbb{A}^n(\overline{K})$ is I_V prime ideal, i.e. the ring

$$\overline{K}[V] := \overline{K}[x_1, \ldots, x_n]/I_V$$

is integral domain. This ring is called coordinate ring (or the ring of regular functions) of V. The quotient field of $\overline{K}[V]$, denoted by $\overline{K}(V)$, is called the field of rational functions on V.
Let V be a nontrivial algebraic variety. The degree of transcendence $\mathrm{trdeg}_{\overline{K}}(\overline{K}(V))$ of field extension $\overline{K} \subset \overline{K}(V)$ is called the dimension of variety V, $\dim_K(V)$. Obviously $0 \leq \mathrm{trdeg}_{\overline{K}}\overline{K}(V) \leq n$.

Example 14 *One-point algebraic set is indecomposable, i.e. variety. Its ideal I_V is maximal i.e. $\overline{K}[V]$ is a field. By Lemma 7 and algebraic closedness of $\overline{K}$ it follows $\overline{K}[V] = \overline{K}$. Note that regarding the dimension it is not necessary to work with algebraically closed fields, because the degree of transcendence doesn't change by passing to the algebraic closure.*
For $V = \mathbb{A}^n(\overline{K})$ is $I_V = \{\emptyset\}$. It is prime ideal, i.e. V is algebraic variety. We have $\overline{K}[\mathbb{A}^n(\overline{K})] = \overline{K}[x_1, \ldots, x_n]$ and $\dim_{\overline{K}} \mathbb{A}^n(\overline{K}) = n$.

Algebraic varieties of dimension one are called algebraic curves.

Projective varieties

Definition 15 *Projective space of dimension n is the set of lines in $(\overline{K})^{n+1}$ passing throught $0 \in (\overline{K})^{n+1}$.*

$$\mathbb{P}^n(\overline{K}) := \left\{[l] \mid 0 \neq l \in (\overline{K})^{n+1}\right\}.$$

The subspaces of $\mathbb{P}^n(\overline{K})$ correspond to linear subspaces of $(\overline{K})^{n+1}$. For example, for the plane $N(\overline{K}) \subseteq (\overline{K})^{n+1}$ passing through $0 \in (\overline{K})^{n+1}$ is

$$\mathbb{P}^n(\overline{K}) \cap N(\overline{K}) = \left\{[l] \mid 0 \neq l \subset N(\overline{K})\right\}$$

projective line. Projective algebraic sets are defined by polynomials from $K[x_1, \ldots, x_{n+1}]$ restricted by the condition of independence of the zero locus on the choice of a point in a given line (passing through the ? of the vector space).

Definition 16 *A polynomial is called homogeneous if the sum of degrees by all variables in every monomial is the same natural number.*

Example 17 *The polynomial*

$$x^2 + z^6x + z^3x + 3 \tag{1.2}$$

is not homogeneous, but

$$x^2y^5 + z^6x + z^3xy^3 + 3y^7$$

is homogeneous and is called homogeneation of (1.2).

Definition 18 *The homogenization of polynomial $p \in \overline{K}[x_1 \dots, x_n]$ is the map*

$$\begin{array}{rcl} \overline{K}[x_1 \dots, x_n] & \longmapsto & \overline{K}[x_1 \dots, x_{n+1}] \\ p \equiv p(x_1, \dots, x_n) & \longmapsto & p^*(x_1, \dots, x_{n+1}) = x_{n+1}^d p\left(\dfrac{x_1}{x_{n+1}}, \dots, \dfrac{x_n}{x_{n+1}}\right) \end{array}$$

where $d \in \mathbb{N} \cup \{\emptyset\}$ is the smallest integer such that p^* is polynomial.

The projective completion $\mathbb{P}^n(\overline{K})$ of n-dimensional affine space $\mathbb{A}^n(\overline{K})$ is a map

$$\begin{array}{rcl} \mathbb{A}^n(\overline{K}) & \longmapsto & \mathbb{P}^n(\overline{K}) \\ (x_1, \dots, x_n) & \longmapsto & [(x_1, \dots, x_n, 1)]. \end{array}$$

If $V_I \subset \mathbb{A}^n(\overline{K})$ is an affine algebraic variety, we can homogenize corresponding ideal I_V:

$$I_V^* = \left\{p^* \in \overline{K}[x_1, \dots, x_{n+1}] \mid p \in I_V\right\},$$

where I_V^* is ideal generated by homogenized polynomials from I_V. We define the projective completion $\overline{V}$ of affine algebraic variety V by

$$\overline{V}_I = \left\{[l] \mid l \neq 0,\ l \in \overline{K}^{n+1},\ p^*(l) = 0\ \forall p^* \in I_V^*\right\}.$$

The subset $V \hookrightarrow \overline{V}$ is called affine part of $\overline{V}$. The points of $\overline{V} \setminus V$ are of the form $[(x_1, \dots, x_n, 0)]$ because for $(x_1, \dots, x_n, x_{n+1})$, $x_{n+1} \neq 0$, we have

$$[(x_1, \dots, x_n, x_{n+1})] = \left[\left(\frac{x_1}{x_{n+1}}, \dots, \frac{x_n}{x_{n+1}}, 1\right)\right].$$

After the substitution of 1 for x_{n+1} into homogenized polynomial p^* we get the former polynomial p.

1.1 The Frobenious morphism

Let K be a field of characteristic $\mathrm{char}\,(K) = p > 0$.

Lemma 19 *The map*

$$\begin{array}{cccc} \sigma: & K & \longrightarrow & K \\ & a & \longrightarrow & a^p \end{array}$$

is a homomorphism (called Frobenious homomorphism).

Proof: The proof follows from the binomial formula

$$(a+b)^p = \sum_{j=0}^{p} \binom{p}{j} a^j b^{p-j},$$

i.e.

$$(a+b)^p = a^p + b^p \mathrm{mod}\, p.$$

The rest of field homomorphism axioms is trivial. ■

Fix a power $q = p^r (r \geq 1)$ of p. For a polynomial $f(x) = \sum_\alpha b_\alpha x^\alpha \in K[x]$ we define $f^{(q)}(x) := \sum_\alpha c_\alpha^q x^\alpha \in K[x]$. As $f(x)^q = f^{(q)}(x^q)$, it follows that

$$\text{if } a \in \overline{K} \text{ is a root of } f(x) \Rightarrow a^q \in K \text{ is a root of } f^{(q)}(x).$$

Similar properties hold for polynomials in several variables.

- <u>A naive definition</u>
  For X affine algebraic set over K given by the polynomials

  $$f_1(x) = \cdots = f_N(x) = 0, \qquad f_j \in K[x] = K[x_1, \ldots, x_n],$$

  we denote by $X^{(q)}$ affine space over K given by the polynomials

  $$f_1^{(q)}(x) = \cdots = f_N^{(q)}(x) = 0.$$

  This means that the ring of regular functions on X resp. $X^{(q)}$ is

  $$A = K[x_1, \ldots, x_n]/(f_1, \ldots, f_N), \qquad A^{(q)} = K[x_1, \ldots, x_n]/\left(f_1^{(q)}, \ldots, f_N^{(q)}\right).$$

  The morphism of K-algebras

  $$\begin{array}{cccc} \varphi_q^*: & A^{(q)} & \longrightarrow & A \\ & \sum_\alpha b_\alpha x^\alpha & \longmapsto & \sum_\alpha b_\alpha x^{q\alpha} \end{array} \tag{1.3}$$

  defines a morphism (over K)

  $$\begin{array}{cccc} \varphi_q: & x & \longrightarrow & x^{(q)}, \\ & a \equiv (a_1, \ldots, a_n) & \longmapsto & \varphi_q(a) = (a_1^q, \ldots, a_n^q). \\ & X(\overline{K}) & & X^{(q)}(\overline{K}) \end{array}$$

- An intrinsic definition

Definition 20 *For any K-algebra A (commutative), put $A^{(q)} = A \underset{K,\sigma^r}{\otimes} K$. This is a K-algebra via the map*

$$k \longrightarrow 1 \otimes k.$$

This definition means that an element of $A^{(q)}$ is a finite sum of expressions $a \otimes k (a \in A, k \in K)$ satisfying a $k \otimes k' = a \otimes k^q k'$ $(a \in A,\ k, k' \in K)$.
The map

$$\begin{array}{rcll} f(x) \otimes k & \longrightarrow & k f^{(q)}(x), & k \in K,\ f(x) \in K[x_1, \ldots, x_n] \\ \sum\limits_{\alpha} b_\alpha x^\alpha \otimes k & \longmapsto & \sum\limits_{\alpha} b_\alpha^q k x^\alpha & \end{array} \tag{1.4}$$

defines an isomorphism of K-algebras

$$K[x_1, \ldots, x_n] \underset{K,\sigma^r}{\otimes} K \overset{\sim}{\longmapsto} K[x_1, \ldots, x_n],$$

which induces an isomorphism of K-algebras

$$K[x_1, \ldots, x_n]/(f_1, \ldots, f_N) \underset{K,\sigma^r}{\otimes} K \overset{\sim}{\longmapsto} K[x_1, \ldots, x_n]/\left(f_1^{(q)}, \ldots, f_N^{(q)}\right).$$

Under this isomorphism, the map 1.3 corresponds to 1.4. In other words, Definition 20 gives the functorial description of $A^{(q)}$. In the language of schemes this means that $X^{(q)}$ can be defined for an arbitrary K-scheme X as the fiber product

Example 21 *For $A = K[x]$, i.e. X is the affine K-line, we get $A^{(q)} = K[x]$ and the morphism of K-algebras*

$$\widetilde{\varphi}_q : A^{(q)} = K[x] \longrightarrow A = K[x]$$

corresponding to $\widetilde{\varphi}_q^* : x \to x^{(q)}$ is given by

$$\widetilde{\varphi}_q(x) = x^q,\ \widetilde{\varphi}_q(k) = k\ (\forall k \in K).$$

Chapter 2

The Theory of Algebraic Function Fields

Remark 22 *In this chapter K denotes an arbitrary field.*

1. Places, Valuation rings, Valuations

Definition 23 *An algebraic functin field F/K of one variable over K is an extension field $F \supseteq K$ such that F is a finite algebraic extension of $K(x)$ for $x \in F$ transcendental over K.*

We refer to F/K as a function field. The set $K := \{z \in F : z$ is algebraic over $K\}$ is a subfield of F (sums, products and inverses of algebraic elements are algebraic elements). $\widetilde{K}$ is so called field of constants of F/K and we have $K \subseteq \widetilde{K} \subset F$. One easily verifies that $F/\widetilde{K}$ is a function field over $\widetilde{K}$. We say that K is algebraically closed in F (i.e. K is the full constant field of F) if $\widetilde{K} = K$. It is clear that the elements $z \in F$ transcendental over K are characterized by $[F : K(z)] < \infty$.

Example 24 *(Rational function field) F/K is called rational if $F = K(x)$ for some $x \in F$ transcendental over K iff $[F : K(x)] < \infty$. The field $K(x)$ is UFD, i.e. $\forall z \neq 0 \in F$ has a unique representation*

$z = a \prod_i p_i(x)^{n_i}$, $a \neq 0 \in K,\ p_i(x) \in K[x]$ are monic, pair wise distinc irreducible polynomials, $n_i \in \mathbb{Z}\ \forall\, i$.

An arbitrary function field F/K is often represented as field extension of rational function field $K(x)$, i.e. $F = K(x, y) : \varphi(y)$ for irreducible polynomial $\varphi(\mathcal{T}) \in K(x)[\mathcal{T}]$.

Questions 25 *What is the factorization of non-rational function field F/K into irreducibles?*

What is an irreducible element of F/K?
How to find an element $z \in F/K$ with prescribed zeros and (or) poles in $\alpha_1, \ldots, \alpha_n \in K$?

Definition 26 *A valuation ring of the function field F/K is a ring $\mathcal{O} \subseteq F$ with the following properties:*

1. *$K \subseteq \mathcal{O} \subseteq F$,*
2. *$\forall z \in F : z \in \mathcal{O} \vee z^{-1} \in \mathcal{O}$.*

This definition is motivated by the following observation in the case of rational function field $F = K(x)$. Let $p(x) \in K[x]$ be an irreducible polynomial and consider a valuation ring of $K(x)/K$:

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \not| \, g(x) \right\}.$$

Note that if $q(x) \neq p(x)$ is another irreducible polynomial, then $\mathcal{O}_{p(x)} \neq \mathcal{O}_{q(x)}$.

Lemma 27 *Let $\mathcal{O}$ be a valuation ring of the function field F/K. Then*

1. *$\mathcal{O}$ is a local ring, i.e. $\mathcal{O}$ has a unique maximal ideal $P = \mathcal{O} \setminus \mathcal{O}^*$, where $\mathcal{O}^* := \{z \in \mathcal{O} \mid \exists w \in \mathcal{O} : zw = 1\}$ is the group of units of $\mathcal{O}$,*
2. *for $0 \neq x \in F : x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$,*
3. *for the field of constants $\widetilde{K}$ of F/K we have $\widetilde{K} \subseteq \mathcal{O}$, $\widetilde{K} \cap P = \{\emptyset\}$.*

Proof:

1. We Claim $P := \mathcal{O}/\mathcal{O}^*$ is an ideal of $\mathcal{O}$. From this assertion it follows at once that P is the unique maximal ideal since a proper ideal of $\mathcal{O}$ cannot contain a unit of $\mathcal{O}$.
   (a) Let $x \in P$, $z \in \mathcal{O}$. Then $xz \notin \mathcal{O}^*$ (otherwise x would be a unit and so $x \notin P$), consequently $xz \in P$.
   (b) Let $x, y \in P$. Without loss of generality we can assume $\frac{x}{y} \in \mathcal{O}$ (else $x \to y$, $y \to x$ and $\frac{y}{x} \in \mathcal{O}$). Then $\left(1 + \frac{x}{y}\right) \in \mathcal{O}$ and $x + y = y\left(1 + \frac{x}{y}\right) \in P$ by (a).

   Hence $P \subset \mathcal{O}$ is an ideal.
2. Follows from the Definition 26.
3. Let $z \in \widetilde{K}$ and suppose $z \notin \mathcal{O}$. Then $z^{-1} \in \mathcal{O}$ by Definition 26. Since z^{-1} is algebraic over K ($\widetilde{K}/K$ is an algebraic extension) there are elements $a_1, \ldots, a_r \in K$ with

$$a_r \left(z^{-1}\right)^r + \cdots + a_1 z^{-1} + 1 = 0,$$

i.e.

$$z^{-1}\left(a_r\left(z^{-1}\right)^{r-1}+\cdots+a_1\right)=-1.$$

Therefore

$$z=-\left(a_r\left(z^{-1}\right)^{r-1}+\cdots+a_1\right)\in K\left[z^{-1}\right]\subseteq\mathcal{O},$$

i.e. $z\in\mathcal{O}$. The part $\widetilde{K}\cap P=\{0\}$ is trivial. ■

Theorem 28 *Let $\mathcal{O}$ be a valuation ring of the function field $F/K, P\subseteq\mathcal{O}$ its maximal ideal. Then*

1. *P is principal ideal.*
2. *If $P=t\mathcal{O}$ then any $0\neq z\in F$ has a unique representation of the form $z=t^n u$ for some $n\in\mathbb{Z},\ u\in\mathcal{O}^*$.*
3. *$\mathcal{O}$ is PID, i.e. 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 with these properties is called a **discrete valuation ring**.

Lemma 29 *Let $\mathcal{O}$ be a valuation ring of the algebraic function field F/K, P its maximal ideal and $0\neq x\in P$. Let $x_1,\ldots,x_n\in P$ be such that $x_1=x,\ x_i\in x_{i+1}P$ for $i=1,\ldots,n-1$. Then $n\leq[F:K(x)]<\infty$.*

Proof: It follows from Definition 23 and Lemma 27 that $[F:K(x)]<\infty$, so it is sufficient to prove that $x_1,\ldots,x_n$ are linearly independent over $K(x)$. Suppose there is a non-trivial linear combination $\sum_{i=1}^n\varphi_i x_i=0,\ \varphi_i\in K(x)\ (\forall\, i)$. We can assume $\varphi_i\in K[x]\ (\forall\, i)$ and $(\exists\, i)\ x\nmid\varphi_i(x)$. Put $a_i:=\varphi_i(0)$ and define $j\in\{1,\ldots,n\}$ by the condition $a_j\neq 0$, but $a_i=0\ \ \forall\, i>j$. We obtain

$$-\varphi_j x_j=\sum_{i\neq j}\varphi_i x_i$$

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

$$-\varphi_j=\sum_{i<j}\varphi_i\frac{x_1}{x_j}+\sum_{i>j}\frac{x}{x_j}g_i x_i.$$

Because $\frac{x_i}{x_j}$ (for $i<j$) belongs to P and $\frac{x}{x_j}=\frac{x_i}{x_j}$ belongs to P, $\varphi_i\in P$. On the other hand, $\varphi_j=a_j+xg_j,\ g_j\in K[x]\subseteq\mathcal{O}$. Because $a_j=\varphi_j-xg_j$ and both $\varphi_j\in P,\ xg_j\in P$, we get $a_j\in K\cap P$. Since $a_j\neq 0$, this contradicts Lemma 27, 3. ■

Proof (Theorem 28):

1. Assume $P\subseteq\mathcal{O}$ is not principal and choose $0\neq x_1\in P$. Because $P\neq x_1\mathcal{O}$, there is $x_2\in P\smallsetminus x_1\mathcal{O}$ fulfilling $x_2x_1^{-1}\notin\mathcal{O}$ (otherwise $x_2\in x_1\mathcal{O}$ would contradict with $x_2\in P\smallsetminus x_1\mathcal{O}$) and by Lemma 27 par 2. $x_2^{-1}x_1\in P$, i.e. $x_1\in x_2P$. By induction we obtain an infinite sequence $x_1,x_2,x_3,\ldots$, in P such that $x_i\in x_{i+1}P\ (\forall\, i\geq 1)$, a contradiction to Lemma 29.

2. The uniqueness of the representation $z = t^n u,\ u \in \mathcal{O}^*$, is trivial. Let us show the existence of this decomposition. As $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$, we can assume $z \in \mathcal{O}$. If $z \in \mathcal{O}$ then $z = t^0 z$. In the case $z \in P \subset \mathcal{O}$ there is a maximal $m \geq 1$ with $z \in t^m\mathcal{O}$, since the length of the sequence $x_1 = z,\ x_2 = t^{m-1},\ x_3 = t^{m-2}, \ldots,\ x_m = t$ is bounded by Lemma 29. Write $z = t^m u,\ u \in \mathcal{O}$. Then $u \in \mathcal{O}^*$, otherwise $u \in P = t\mathcal{O}$ and so $u = tw,\ w \in \mathcal{O},\ z = t^{m+1}w \in t^{m+1}\mathcal{O}$, a contradiction to the maximality of $m \in \mathbb{N}$.

3. Let $\{0\} \neq I \subset \mathcal{O}$ be an ideal. The set $A := \{r \in \mathbb{N} \mid t^r \in I\}$ is non-empty. In fact, if $0 \neq x \in I$ then $x = t^r u,\ u \in \mathcal{O}^*$, and $t^r = xu^{-1} \in I$. Put $n := \min(A)$. We claim that $I = t^n\mathcal{O}$. The inclusion $I \supseteq t^n\mathcal{O}$ is trivial since $t^n \in I$. Conversely, let $y \in I,\ y \neq 0$. We have $y = t^s w,\ w \in \mathcal{O}^*,\ s \geq 0$, and so $t^s \in I$ and $s \geq n$. Therefore $y = t^s w = t^n t^{s-n} w \in t^n\mathcal{O}$. ∎

Definition 30

1. *A place P of the function field F/K is the maximal ideal of some valuation ring $\mathcal{O}$ of F/K. Any element $t \in P : P = t\mathcal{O}$, is called a prime element for P (uniformization variable, local parameter).*

2. $\mathbb{P}_F := \{P \mid P$ *is a place of* $F/K\}$

3. *If $\mathcal{O} \subset F/K$ is valuation ring of F/K and P its maximal ideal, then $\mathcal{O}$ is uniquely determined by P, i.e. $\mathcal{O} = \left\{z \in F \mid z^{-1} \notin P\right\}$. Hence $\mathcal{O}_P := \mathcal{O}$ is called the valuation ring of the place $P \in \mathbb{P}_F$.*

A place can be equivalently described by valuation.

Definition 31 *A discrete valuation of F/K is a function $v : F \to \mathbb{Z} \cup \{\infty\}$ fulfilling:*

1. $v(x) = \infty \Leftrightarrow x = 0$,

2. $v(xy) = v(x) + v(y),\ \forall x, y \in F$,

3. $v(x + y) \geq \min\{v(x), v(y)\},\ \forall x, y \in F$,

4. $\exists z \in F : v(z) = 1$,

5. $v(a) = 0\ \forall\, 0 \neq a \in K$.

The symbol "∞" means some element not in $\mathbb{Z}$, such that $\infty + \infty = \infty = \infty + n = n + \infty,\ \infty > m\ \forall m, n \in \mathbb{Z}$.
From 2., 4. it follows that v is surjective. The property 3. is called Triangle inequality.

Remark 32 *The notions of valuation and triangle inequality are justified by the following relation: let v be a discrete valuation of F/K in the sense of previous Definition 31. Then for any real number $c \in (0, 1)$ we can define the function $|\ |_v : F \to \mathbb{R}$ by*

$$|z|_v := \begin{cases} c^{v(x)} & \text{if } z \neq 0, \\ 0 & \text{if } z = 0. \end{cases}$$

One then easily verifies that this function has the properties of an ordinary absolute value, e.g. the ordinary triangle inequality $|x + y|_v \leq |x|_v + |y|_v$ is the consequence of Definition 31, 3.

Lemma 33 *(Strict Triangle Inequality) Let v be a discrete valuation of F/K and $x, y \in F$ with $v(x) \neq v(y)$. Then $v(x + y) = \min\{v(x), v(y)\}$.*

Proof: By Definition 31, 2., 5. we have $v(ay) = v(y)\ \forall a \in K^*$, e.g. $v(-y) = v(y)$. Since $v(x) \neq v(y)$ we can assume $v(x) < v(y)$. Suppose that $v(x + y) \neq \min\{v(x), v(y)\}$, i.e. $v(x + y) > v(x)$ by Definition 31, 3. From this we obtain

$$v(x) = v((x + y) - y) \geq \min\{v(x + y), v(y)\} > v(x),$$

a contradiction. ■

Definition 34 *To any place $P \in \mathbb{P}_F$ we associate a function $v_P : F \to \mathbb{Z} \cup \{\infty\}$ that will turn out to be a discrete valuation of F/K. Choose a prime element t for P. Then $\forall z \in F,\ z \neq 0\ \exists!\ n \in \mathbb{Z}\ u \in \mathcal{O}_P^* : z = ut^n$. Define $v_P(z) := n,\ v_P(0) := \infty$.*

The definition depends only on the choice of the place P, not on the uniformizing element t. If t' is another prime element for P then $P = t\mathcal{O} = t'\mathcal{O}$, i.e. $t = t'w$ for some $w \in \mathcal{O}_P^*$. Therefore $t^n u = (t'^n w^n)u = t'^n(w^n u)$ with $w^n u \in \mathcal{O}_P^*$.

Theorem 35 *Let F/K be a function field. Then*

1. *For any place $P \in \mathbb{P}_F$, the function $v_P : F \to \mathbb{Z} \cup \{\infty\}$ defined in Definition 34 is a discrete valuation of F/K. We have*

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

   An element $x \in F$ is a prime element for P iff $v_P(x) = 1$.

2. *Suppose that v is a discrete valuation of F/K. Then the set $P := \{z \in F \mid v(z) > 0\}$ is a place of F/K, and $\mathcal{O}_P := \{z \in F \mid v(z) \geq 0\}$ is the corresponding valuation ring.*

3. *Any valuation ring $\mathcal{O}$ of F/K is a maximal proper subring of F.*

Proof: Obviously v_P has the properties Definition 31, 1., 2., 4., 5. In order to prove the Triangle Inequality Definition 31, 3., consider $x, y \in F$ with $v_P(x) = n,\ v_P(g) = m$. We can assume that $n \leq m < \infty$, i.e. $x = t^n u_1$ and $y = t^m u_2$ with $u_1, u_2 \in \mathcal{O}_P^*$. Then $x + y = t^n(u_1 + t^{m-n}u_2) = t^n z$ with $z \in \mathcal{O}_P$. If $z = 0$ we have $v_P(x+y) = \infty > \min(m, n)$, otherwise $z = t^k u$ with $k \geq 0$ and $u \in \mathcal{O}_P^*$. Then

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

and so v_P is discrete valuation of F/K. The rest of 1. and 2. are trivial.
3. Let $\mathcal{O}$ be a valuation ring of F/K, P its maximal ideal, v_P the discrete

valuation associated to P and $z \in F \setminus \mathcal{O}$. We have to show $F = \mathcal{O}[z]$. Let us consider an arbitrary $y \in F$. We have then $v_P(yz^{-k}) \geq 0$ for sufficiently large $k \geq 0$ (note that $v_P\left(z^{-1}\right) > 0$ since $z \notin \mathcal{O}$). Consequently $w := yz^{-k} \in \mathcal{O}$ and so $y = wz^k \in \mathcal{O}[z]$. ■

In other words, we have proved for function fields that

1. places,
2. valuation rings,
3. discrete valuations

amount to the same thing.
Let P be a place of F/K and $\mathcal{O}_P$ be its valuation ring. Since P is a maximal ideal, the residue class ring $\mathcal{O}_P/P$ is a field. For $x \in \mathcal{O}_P$ we define $x(P) \in \mathcal{O}_P/P$ to be the residue class of $x \bmod P$, for $x \in F \setminus \mathcal{O}_P$ we define $x(P) := \infty$. By Lemma 27 we know $K \subseteq \mathcal{O}_P$ and $K \cap P = \{0\}$, so the residue class map $\mathcal{O}_P \twoheadrightarrow \mathcal{O}_P/P$ induces canonical embedding $K \hookrightarrow \mathcal{O}_P/P$. We shall always understand K embedded in $\mathcal{O}_P/P$ via this canonical map. The same applies to $\widetilde{K} \supset K$.

Definition 36 *Let $P \in \mathbb{P}_F$.*

1. *$F_P := \mathcal{O}_P/P$ is the residue class field of P. The map $x \to x(P)$ from F to $F_P \cup \{\infty\}$ is called the residue class map w. r. to P. Sometimes we shall use the notation $x + P := x(P)$ for $x \in \mathcal{O}_P$.*
2. *$\deg P := [F_P : K]$ is called the degree of P.*

Proposition 37 *If P is a place of F/K, $0 \neq x \in P$. Then*

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

Proof: By Example 24, $[F : K(x)] < \infty$. Thus it is sufficient to show that for any set of elements $\{z_1, \ldots, z_n\} \in \mathcal{O}_P$, whose residue classes $z_1(P), \ldots, z_n(P) \in F_P$ are linearly independent over K, are linearly independent over $K(x)$. Suppose there is a non-trivial linear combination

$$\sum_{i=1}^{n} \varphi_i z_i = 0$$

with $\varphi_i \in K(x)$. Without lost of generality we can assume that the φ_i are polynomials ($\varphi_i \in K[x] (\forall\, i)$) and not all of them are divisible by x, i.e. $\varphi_i = a_i + xg_i,\ a_i \in K,\ g_i \in K[x] : \exists i\ a_i \in K^*$. Since $x \in P$ and $g_i \in \mathcal{O}_P,\ \varphi_i(P) = a_i(P) = a_i$. The residue class map implies

$$O = O(P) = \sum_{i=1}^{n} \varphi_i(P) z_i(P) = \sum_{i=1}^{n} a_i z_i(P).$$

This contradicts K-linear independence of the set $\{z_1(P), \ldots, z_n(P)\}$. ■

Lemma 38 *The field $\widetilde{K}$ of constants of F/K is a finite field extension of K.*

Proof: In the Lemma 42 we shall prove the fact that $\mathbb{P}_F \neq 0$. Choose some $P \in \mathbb{P}_F$. Since $\widetilde{K} \hookrightarrow F_P$ via residue class map $\mathcal{O}_P \to F_P$, it follows that $[\widetilde{K} : K] \leq [F_P : K] < \infty$. ■

Remark 39 *In the case when* $\deg(P) = 1$ *we have $F_P = K$, and the residue class map maps F to $K \cup \{\infty\}$. In particular, if K is an algebraically closed field, any place has degree one and so we understand an element $z \in F$ as a function*

$$z : \left\{ \begin{array}{ccc} \mathbb{P}_F & \longmapsto & K \cup \{\infty\}, \\ P & \longmapsto & z(P). \end{array} \right.$$

This is the reason for F/K to be called a function field. The elements of $K \subset F$, interpreted as functions in the previous sense, are constant functions, sometimes K is called the field of constants.

Definition 40 *Let $z \in F$, $P \in \mathbb{P}_F$. We say that P is a zero of z iff $v_P(z) > 0$; P is a pole of z iff $v_P(z) < 0$. If $v_p(z) = m > 0$, P is a zero of z of order m; if $v_P(z) = -m < 0$, P is a pole of z of order m.*

Theorem 41 *Let F/K be a function field and R be a subring of F with $K \subseteq R \subseteq F$. Suppose that $\{0\} \neq I \subsetneq R$ is a proper ideal of R. Then there is a place $P \in \mathbb{P}_F$ such that $I \subseteq P$ and $R \subseteq \mathcal{O}_P$.*

Proof: Consider the set

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

By definition, IS is the set of all finite sums $\sum_\nu a_\nu s_\nu$ with $a_\nu \in I,\ s_\nu \in S$, and it is an ideal of S. The set $\mathcal{F}$ is non empty ($R \in \mathcal{F}$), and $\mathcal{F}$ is inductively ordered by inclusion. In fact, if $\mathcal{H} \subset \mathcal{F}$ is a totally ordered subset of $\mathcal{F}$ then $\mathcal{T} := \bigcup\{S \mid S \in \mathcal{H}\}$ is a subring of F with $R \subseteq \mathcal{T}$. We have to verify that $I\mathcal{T} \neq \mathcal{T}$. Suppose the contrary, i.e. $1 = \sum_{\nu=1}^n a_\nu s_\nu$ with $a_\nu \in I,\ s_\nu \in \mathcal{T}$. Since $\mathcal{H}$ is totally (=linearly) ordered there is an S_0 such that $s_1, \ldots, s_n \in S_0$, so $1 = \sum_{\nu=1}^n a_\nu s_\nu \in IS_0$, i.e. $S_0 = IS_0$ a contradiction. By Zorn's Lemma $\mathcal{F}$ contains a maximal element, i.e. there is a ring $\mathcal{O} \subseteq F$ such that $R \subseteq \mathcal{O} \subseteq F,\ I\mathcal{O} \neq \mathcal{O}$, and $\mathcal{O}$ is maximal with respect to these properties. We shall show that $\mathcal{O}$ is a valuation ring of F/K. As $I \neq \{0\}$ and $I\mathcal{O} \neq \mathcal{O}$ we have $\mathcal{O} \subsetneq F$ and $I \subseteq \mathcal{O} \smallsetminus \mathcal{O}^*$. Suppose there exists $z \in F$ with $z \notin \mathcal{O} \wedge z^{-1} \notin \mathcal{O}$. Then $I\mathcal{O}[z] = \mathcal{O}[z]$ and $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$. Then it holds $I\mathcal{O}[z] = \mathcal{O}[z]$ and $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$, and we can find $\left.\begin{array}{c} a_0, \ldots, a_n \\ b_0, \ldots, b_m \end{array}\right\} \in I\mathcal{O}$ with

$$1 = a_0 + a_1 z + \cdots + a_n z^n, \tag{2.1}$$

$$1 = b_0 + b_1 z^{-1} + \cdots + b_m z^{-m}, \tag{2.2}$$

where $m \geq 1,\ n \geq 1$. Let us assume that $m, n \in \mathbb{Z}$ are minimal integers and $m \leq n$. Multiplying (2.1) by $1 - b_0$ and (2.2) by $a_n z^n$, we obtain

$$1 - b_0 = (1 - b_0)a_0 + (1 - b_0)a_1 z + \cdots + (1 - b_0)a_n z^n, \tag{2.3}$$

$$0 = (b_0 - 1)a_n z^n + b_1 a_n z^{n-1} + \cdots + b_m a_n z^{n-m} \tag{2.4}$$

(2.3)+(2.4) yields

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

for $c_i \in I\mathcal{O}(\forall\, i = 0, \ldots, n-1)$. This contradicts the minimality of n, i.e. we have proved that either $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$ for any $z \in F$, hence $\mathcal{O}$ is a valuation ring of F/K. ∎

Lemma 42 *Let F/K be a function field, $z \in F$ a transcendental element over K. Then z has at least one zero and one pole. In particular, $\mathbb{P}_F \neq \emptyset$.*

Proof: Consider the ring $R = K[z]$ and the ideal $I = zK[z]$. By Theorem 41, there is a place $P \in \mathbb{P}_F$ with $z \in P$, i.e. P is a zero of z. The same argument shows that z^{-1} has a zero $Q \in \mathbb{P}_F$. Then Q is a pole of z. ∎

Remark 43 *The result of Lemma 42 can be interpreted as follows: any $z \in F$, which is not in the field of constant $\widetilde{K} \subset F/K$, yields a non-constant function in the sense of Remark 39.*
Note that $\mathbb{P}_F$ is in fact infinite.

2. The Rational Function Fields

We shall investigate, as an example, the previous concepts in the case of the rational function field $F = K(x)$, where x is transcendental over K. Given a monic, irreducible polynomial $p(x) \in K[x]$ consider the valuation ring

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \not| \, g(x) \right\}$$

of $K[x]/K$ with maximal ideal

$$P_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \mid f(x), p(x) \not| \, g(x) \right\} \subsetneq \mathcal{O}_{p(x)}. \tag{2.5}$$

In particular, when $p(x)$ is linear, i.e. $p(x) = x - a$ with $a \in K$, we abbreviate and write $P_a := P_{x-a} \in \mathbb{P}_{K(x)}$.
There is another valuation ring of $K(x)/K$, namely

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

with maximal ideal

$$P_\infty := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \deg f(x) \leq \deg g(x) \right\}. \tag{2.6}$$

This is called infinite place of $K(x)$. Note that the places depend on the specific choice of the generating element x of $K(x)/K$ (for example, take $x \mapsto \frac{1}{x}$, i.e. $K(x) = K(\frac{1}{x})$, then $P_0 \to P_\infty$ and $P_\infty \to P_0$).

Lemma 44 *Let $F = K(x)$ be the rational function field.*

1. *Let $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ be the place defined by monic irreducible polynomial $p(x) \in K[x]$. Then $p(x)$ is a prime element for P, and the corresponding discrete valuation v_P can be described as follows: if $z \in K[x] \setminus \{\emptyset\}$ is written in the form $z = p^n(x) \left(\frac{f(x)}{g(x)}\right)$ with $n \in \mathbb{Z}$, $f(x), g(x) \in K[x]$, $p(x) \not| \, f(x)$ and $p(x) \not| \, g(x)$, then $v_P(z) = n$. The residue class field $K(x)_P \equiv \mathcal{O}_P/P$ is isomorphic to $K[x]/(p(x))$. An isomorphism is given by*

   $$\begin{array}{rccc} \varphi : & K[x]/(p(x)) & \xrightarrow{\sim} & K(x)_P, \\ & f(x) \bmod p(x) & \longmapsto & f(x)(P). \end{array}$$

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

2. *In the special case $p(x) = x - a$, $a \in K$, the degree at $P = P_a$ is one, and the residue class map is given by*

   $$z(P) = z(a) \qquad \text{for } z \in K(x),$$

   where $z(a)$ is defined as follows: write $z = \frac{f(x)}{g(x)}$ with relatively prime polynomials $f(x), g(x) \in K[x]$. Then

   $$z(a) = \begin{cases} \frac{f(a)}{g(a)} & \text{if } g(a) \neq 0, \\ \infty & \text{if } g(a) = 0. \end{cases}$$

3. *Finally, let $P = P_\infty$ be the infinite place of $K(x)/K$. Then $\deg P_\infty = 1$, and the prime element for P_∞ is $t = \frac{1}{x}$. The corresponding discrete valuation v_∞ is given by*

$$v_\infty\left(\frac{f(x)}{g(x)}\right) = \deg g(x) - \deg f(x),$$

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

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

then

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

4. *K is the full constant field of $K(x)/K$.*

Proof: We prove only some essentials of this proposition; the remaining parts of the proof are straight forward.

1. Let $P = P_{p(x)}$, $p(x) \in K[x]$ irreducible. The ideal $P_{p(x)} \subseteq \mathcal{O}_{p(x)}$ is obviously generated by $p(x)$, hence $p(x)$ is a prime element for P. Let us consider the ring homomorphism

$$\begin{array}{rccc} \varphi: & K[x] & \longrightarrow & K(x)_P, \\ & f(x) & \longmapsto & f(x)(P). \end{array}$$

The kernel of φ is clearly the ideal generated by $p(x)$. Moreover φ is surjective because if $z \in \mathcal{O}_{p(x)}$, we can write $z = \frac{u(x)}{v(x)}$ with $u(x), v(x) \in K[x]$ such that $p(x) \not| v(x)$. Thus by Euclid algorithm there are $a(x), b(x) \in K[x]$ with $a(x)p(x) + b(x)v(x) = 1(x)$, therefore

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

and so $z(P) = (b(x)u(x))(P)$ is in the image of φ. Thus φ induces isomorphism $K[x]/(p(x)) \xrightarrow{\sim} K(x)_P$.

2. We have $P = P_a$ with $a \in K$. If $f(x) \in K[x]$ then $(x - a) \mid (f(x) - f(a))$, hence $f(x)(P) = (f(x) - f(a))(P) + f(a)(P) = f(a)$. An arbitrary element $z \in \mathcal{O}_P$ can be written as $z = \frac{f(x)}{g(x)}$ with polynomials $f(x), g(x) \in K[x]$ and $(x - a) \mid g(x)$, therefore $g(x)(P) = g(a) \neq 0$ and

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

3. We want to show that $\frac{1}{x}$ is a prime element for P_∞. Consider some element $z = \frac{f(x)}{g(x)} \in P_\infty$, i.e. $\deg f < \deg g$. Then

$$z = \frac{1}{x} \frac{x f(x)}{g(x)},$$

with $\deg(xf) = 1 + \deg f \leq \deg g$. This proves that $z \in \left(\frac{1}{x}\right)\mathcal{O}_\infty$, i.e. $\frac{1}{x}$ is a P_∞-prime element.

4. Choose a place P of $K(x)/K$, $\deg P = 1$ (e.g. $P = P_a$ with $a \in K$). The field $\widetilde{K}$ of constants of $K(x)$ is embedded into the residue class field $K(x)_P$, hence $K \subseteq \widetilde{K} \subseteq K(x)_P = K$. ■

Theorem 45 *There are no places of the rational function field $K(x)/K$ other than the places $P_{p(x)}$ and P_∞, defined by Equations (2.5) and (2.6).*

Proof: We show that given a place $P \in \mathbb{P}_{K(x)}$, $P \neq P_\infty$, there is an irreducible polynomial $p(x) \in K[x]$ such that $\mathcal{O}_{p(x)} = \mathcal{O}_P$.

a) Assume that $x \in \mathcal{O}_P$. Then $K[x] \subseteq \mathcal{O}_P$. Set $I := K[x] \cap P$; this is a prime ideal of $K[x]$. The residue class map induces an embedding $K[x]/I \hookrightarrow K(x)_P$, and by Proposition 37. $I \neq \{\emptyset\}$. It follows that there is a uniquely determined irreducible monic polynomial $p(x) \in K[x]$ such that $I = K[x] \cap P = p(x)K[x]$. Any $g(x) \in K[x]$ with $p(x) \not| \, g(x)$ is not in I, so $g(x) \notin P$ and $\frac{1}{g(x)} \in \mathcal{O}_P$ by Definition 26. We conclude that

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \not| \, g(x) \right\} \subseteq \mathcal{O}_P.$$

As valuation rings are maximal proper subrings of $K[x]$ (Theorem 35), we see that $\mathcal{O}_P = \mathcal{O}_{p(x)}$.

b) Assume that $x \notin \mathcal{O}_P$. We conclude that $K[x^{-1}] \subseteq \mathcal{O}_P$, $x^{-1} \in P \cap K[x^{-1}]$ and $P \cap K[x^{-1}] = x^{-1}K[x^{-1}]$. As in the case a),

$$\begin{aligned}
\mathcal{O}_P \quad &\supseteq \quad \left\{ \frac{f(x^{-1})}{g(x^{-1})} \mid f(x^{-1}), g(x^{-1}) \in K[x^{-1}], x^{-1} \not| \, g(x^{-1}) \right\} \\
&= \quad \left\{ \frac{a_0 + a_1x^{-1} + \cdots + a_nx^{-n}}{b_0 + b_1x^{-1} + \cdots + b_mx^{-m}} \mid b_0 \neq 0 \right\} \\
&= \quad \left\{ \frac{a_0x^{m+n} + \cdots + a_nx^m}{b_0x^{m+n} + \cdots + b_mx^n} \mid b_0 \neq 0 \right\} \\
&= \quad \left\{ \frac{u(x)}{v(x)} \mid u(x), v(x) \in K[x], \deg u(x) \leq \deg v(x) \right\} = \mathcal{O}_\infty.
\end{aligned}$$

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

The consequence of the Lemma 44 and Theorem 45 is

Corollary 46 *The places of $K(x)/K$ of degree one are in bijection with $K \cup \{\infty\}$.*

In other words, the set of places of $K(x)/K$ is in bijection with the set of K-points of K-projective line $\mathbb{P}^1(K)$.

3. Independence of Valuations

The result of the following Theorem be summarized as follows. If $v_1, \ldots, v_n$ are pairwise distinct discrete valuations of F/K and $z \in F$, and if we know the values $v_1(z), \ldots, v_{n-1}(z)$, then we cannot conclude anything about $v_n(z)$.

Theorem 47 *(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 $x \in F$, such that*

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

Proof: We shall write v_i instead of v_{p_i}. The proof is divided into several steps.

a) There is some $u \in F$ with $v_1(u) > 0$ and $v_i(u) < 0$ for $i = 2, \ldots, n$.
Proof: By induction. For $n = 2$ we observe that $\mathcal{O}_{P_1} \subsetneq \mathcal{O}_{P_2}$ and vice versa, since valuation rings are maximal proper subrings of F (Theorem 35). Therefore $\exists y_1 \in \mathcal{O}_{P_1} \setminus \mathcal{O}_{P_2}$, $y_2 \in \mathcal{O}_{P_1} \setminus \mathcal{O}_{P_2}$. Then $v_1(y_1) \geq 0$, $v_2(y_1) < 0$, $v_2(y_2) \geq 0$ and $v_1(y_2) < 0$. The element $u := y_1 y_2^{-1}$ has the property $v_1(u) > 0$, $v_2(u) < 0$ as desired.
For $n > 2$ we have by induction hypothesis an element g with $v_1(y) > 0, v_2(y) < 0, \ldots, v_{n-1}(y) < 0$. If $v_n(y) < 0$ the proof is finished. If $v_n(y) \geq 0$, we choose $z \in F$ with $v_1(z) > 0$, $v_n(z) < 0$ and put $u := y + z^r$. There $r \geq 1$ is chosen in such a manner that $rv_i(z) \neq v_i(y)$ for $i = 1, \ldots, n-1$ (this is obviously possible). It follows that $v_1(u) \geq \min\{v_1(y), rv_1(z)\} > 0$ and $v_i(u) = \min\{v_i(y), rv_i(z)\} < 0$ for $i = 2, \ldots, n$ (Strict Triangle Inequality applies).

b) There is some $w \in F$ such that $v_1(v - 1) > r_1$ and $v_i(w) > r_i$ for $i = 2, \ldots, n$.
Proof: Choose u as in a) and put $w := (1 + u^s)^{-1}$. We have, for sufficiently large $s \in \mathbb{N}$, $v_1(w - 1) = v_1\left(-u^s\left(1 + u^s\right)^{-1}\right) = sv_1(u) > r_1$ and $v_i(w) = -v_i\left(1 + u^s\right) = -sv_i(u) > r_i$ for $i = 2, \ldots, n$ (note $v_i(u) < 0$ for $i = 2, \ldots, n$).

c) Given $y_1, \ldots, y_n \in F$ there is an element $z \in F$ with $v_i(z - y_i) > r_i$ for $i = 1, \ldots, n$.
Proof: Choose $s \in \mathbb{Z}$ such that $v_j(y_j) \geq s$ for all $i, j \in \{1, \ldots, n\}$. By b) there are $w_1, \ldots, w_n$ such that $v_i(w_i - 1) > r_i - s$, $v_i(w_j) > r_i - s$ for $j \neq i$. Then $z := \sum_{j=1}^{n} y_j w_j$ has desired properties.

The proof of Theorem goes as follows. By c) we can find $z \in F$ with $v_i(z - x_i) > r_i$, $i = 1, \ldots, n$.Next choose $z_i \in F : v_i(z_i) = r_i$ (this is trivial). By c) there is z' with $v_i(z' - z_i) > r_i$, $i = 1, \ldots, n$. It follows

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

Let $x := z + z'$. Then

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

■

Corollary 48 *Any function field has infinitely many places.*

Proof: Assume there are finitely many places $P_1, \dots, P_n$. By Theorem 47 we find a non-zero element $x \in F$ with $v_{p_i}(x) > 0$, for $i = 1, \dots, n$. Then x is transcendental over K since it has zeros, but x has no pole. This contradicts Lemma 42. ■

Lemma 49 *Let F/K be a function field and $P_1, \dots, P_n$ be zeros of the element $x \in F$. Then*

$$\sum_{i=1}^{n} v_{P_i}(x) \deg P_i \leq [F : K(x)]$$

Proof: We set $v_i := v_{P_i}$, $f_i := \deg P_i$, $e_i := v_i(x)$. The Weak Approximation Theorem implies for any i the existence of $t_i \in F$ such that $v_i(t_j) = \delta_{ij}$. Let us choose $s_{ij}(P_i) \in F_{P_i}$ $j \in \{1, \dots, f_i\}$ the K basis of F_{P_i}. We designate $s_{i1}, \dots, s_{if_i} \in \mathcal{O}_{P_i}$ the correspondent representans. Again by the Weak Approximation Theorem we can find $z_{ij} \in F$ such that $(\forall i, j)$:

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

We claim that the elements $t_i^a z_{ij}$, $1 \leq i \leq r$, $1 \leq j \leq f_i$, $0 \leq a \leq e_i - 1$ are linearly independent over $K(x)$. Their number is equal to

$$\#\{\, t_i^a z_{ij}\} = \sum_{i=1}^{n} f_i e_i = \sum_{i=1}^{n} v_{P_i}(x) \deg P_i \leq [F : K(x)],$$

so the proposition follows from this claim.

To finish the proof we have to show the last claim. Let us assume, that $t_i^a z_{ij}$ are $K(x)$ lineary dependent, i.e. there is a non-trivial $K(x)$ linear combination

$$\sum_{i=1}^{n} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija}(x) t_i^a z_{ij} = 0. \tag{2.7}$$

W.l.o.g. $\varphi_{ija}(x) \in K[x]$ and there is a multiindex $i_0 j_0 a_0$ such that $x \not| \varphi_{ija}(x)$. In other words there is $k \in \{1, \dots, n\}$ and $c \leq e_{k-1}$ such that $\forall j \in \{1, \dots, f_k\}$ and $\forall a \in \{0, \dots, c-1\}$ $\; x \mid \varphi_{kja}$. There is $j_0 \in \{1, \dots, f_k\}$ such that $x \not| \varphi_{kj_0c}$. Multiplying (2.7) by t_k^{-c} we obtain

$$\sum_{i=1}^{n} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija}(x) t_i^a t_k^{-c} z_{ij} = 0. \tag{2.8}$$

For $i \neq k$
$v_k(\varphi_{ija}(x) t_i^a t_k^{-c} z_{ij}) = v_k(\varphi_{ija} + a v_k(t_i) - c v_k(t_k) + v_k(z_{ij}) \geq 0 + 0 - c + e_k > 0.$
For $i = k$, $a < c$
$v_k(\varphi_{kja} t_k^{a-c} z_{kj}) = v_k(\varphi_{kja} + a - c + v(z_{kj}) > e_k + a - c \geq e_k - c > 0.$
For $i = k$, $a > c$
$v_k(\varphi_{kja} t_k^{a-c} z_{kj}) = v_k(\varphi_{kja} + a - c + 0 > 0.$

Hence

$$\sum_{j=1}^{f_k} \varphi_{kjc} z_{kj} = \sum_{i=1}^{n} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i - 1} \varphi_{ija}(x) t_i^a t_k^{-c} z_{ij} - \sum_{j=1}^{f_k} \varphi_{kjc} z_{kj} \in P_k. \tag{2.9}$$

We project onto F_{P_k} and we obtain

$$\sum \varphi_{kjc}(P_k) z_{ij}(P_k) = 0$$

We observe $\varphi_{kjc}(P_k) \in K$ and $\varphi_{kj_0c}(P_k) \neq 0$.

So $z_{k1}(P_k), \ldots, z_{kf_k} \in F_{P_k}$ are K lineary dependent. Since $v_k(z_{kj} - s_{kj}) > 0$ we have $z_{kj}(P_k) = s_{kj}(P_k)$. And this is a contradiction. ∎

Corollary 50 *In a function field F/K, any element $0 \neq x \in F$ has only finitely many zeros and poles.*

Proof: If x is constant ($x \in K$), x has neither zeros nor poles. If x is transcendental over K, the number of zeros is $\leq [F : K(x)]$ by Lemma 49. The same argument shows that x^{-1} has only a finite number of zeros. ∎

4. Divisors

We shall make the following (non-critical) assumption: F/K will always denote an algebraic function field of one variable such that K is the full constant field of F/K. In other words, in our situation $\widetilde{K} = K$, i.e. K does not extend.

Definition 51 *The free abelian group, generated by places of F/K, is denoted by D_F and called divisor group of F/K. The elements of D_F are called divisors of F/K.*

In other words, a divisor is a formal sum

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

The support of D is defined by

$$\operatorname{supp}(D) := \{P \in \mathbb{P}_F \mid n_p \neq 0\}.$$

We shall usually write

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

where $S \subseteq \mathbb{P}_F$ is finite set with $S \supseteq \operatorname{supp}(D)$.
A divisor of the form $D = P$ with $P \in \mathbb{P}_F$ is called a prime divisor. The structure of abelian groupi is defined by

$$D + D' := \sum_{P \in \mathbb{P}_F} (n_P + n'_P)P, \quad D = \textstyle\sum_{P \in \mathbb{P}_F} n_P P$$
$$D' = \textstyle\sum_{P \in \mathbb{P}_F} n'_P P.$$

The zero element of this divisor group is the divisor

$$0 := \sum_{P \in \mathbb{P}_F} r_P P, \qquad \text{all } r_p = 0.$$

For $Q \in \mathbb{P}_F$ and $D = \sum n_P P \in D_F$ we define $v_Q(D) := n_Q$, therefore

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

A partial order on D_F is defined by

$$D_1 \leq D_2 \Longleftrightarrow v_P(D_1) \leq v_P(D_2) \qquad \text{for any } P \in \mathbb{P}_F.$$

A divisor $D \geq 0$ is called positive (or effective). The degree of a divisor is defined by

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

and it yields a homomorphism $\deg : D_F \to \mathbb{Z}$. By Corollary 50, any $x \neq 0$, $x \in F$, has only finitely many zeros and poles in $\mathbb{P}_F$. Thus it makes sense:

Definition 52 *Let $x \neq 0$, $x \in F$, and denote by Z resp. N the set of zeros resp. poles of x in $\mathbb{P}_F$. Then we define*

$$(x)_0 := \sum_{P \in Z} v_P(x)P, \text{ the divisor of zeros of } x$$

$$(x)_\infty := \sum_{P \in N} (-v_P(x))P, \text{ the divisor of poles of } x$$

$$(x) := (x)_0 - (x)_\infty, \text{ the principal divisor of } x$$

Clearly $(x)_0 \geq 0$, $(x)_\infty \geq 0$ and

$$(x) = \sum_{P \in \mathbb{P}_F} v_P(x)P. \tag{2.10}$$

The elements $0 \neq x \in F$ which are constants are characterized by

$$x \in K \Longleftrightarrow (x) = 0,$$

which follows immediately from Lemma 42 and Proposition ((?)) (recall the assumption that K is algebraically closed in F).

Definition 53

$$P_F := \{(x) \mid 0 \neq x \in F\}$$

is called the group of principal divisors of F/K. This is a subgroup of D_F, since for $0 \neq x, y \in F$, $(xy) = (x) + (y)$ by Equation (2.10). The quotient group

$$C_F := D_F / P_F$$

is called the **divisor class group**. *For a divisor $D \in D_F$, the corresponding element in the factor group C_F is denoted by $[D]$, the divisor class of D. Two divisors $D, D' \in D_F$ are said to be equivalent, written*

$$D \sim D',$$

if $[D] = [D']$, i.e. $D = D' + (x)$ for some $0 \neq x \in F$ $\left(\Leftrightarrow D' = D - (x) = D + \left(x^{-1}\right),\right.$ where obviously $\left.x^{-1} = -(x)\right)$.
This is easily seen to be an equivalence relation.

The next definiton introduces a basic technical notion appearing in the Riemann-Roch Theorem.

Definition 54 *For a divisor $A \in D_F$ we set $\mathcal{L}(A) := \{x \in F \mid (x) \geq -A\} \cup \{0\}$.*

This definition has the following interpretation - if

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

with $n_i > 0$, $m_j > 0$ $(\forall i, j)$ then $\mathcal{L}(A)$ consists of all elements $x \in F$ such that

1. x has zeros of order $\geq m_j$ at Q_j, for $j = 1, \dots, s$ and
2. x may have poles only at the places $P_1, \dots, P_r$, with the poles of order at P_i bounded by $n_i (i = 1, \dots, r)$.

Remark 55 *Let $A \in D_F$. Then*

1. $x \in \mathcal{L}(A) \Longleftrightarrow v_p(x) \geq -v_P(A) \qquad \forall P \in \mathbb{P}_F$.
2. $\mathcal{L}(A) \neq \{0\} \Longleftrightarrow \exists A', A' \sim A, A' \geq 0$.

The proof is trivial: in the second case 2. take $A' = A + (x)$, $0 \neq x \in \mathcal{L}(A)$.

Lemma 56 *Let $A \in D_F$. Then*

1. *$\mathcal{L}(A)$ is a vector space over K.*
2. *If $A' \sim A$ then $\mathcal{L}(A) \xrightarrow{\sim} \mathcal{L}(A')$ (isomorphic as K-vector spaces).*

Proof:

1. Let $x, y \in \mathcal{L}(A), a \in K$. Then, for any $P \in \mathbb{P}_F$:
$$v_P(x + y) \geq \min\{v_P(x), v_P(y)\} \geq -v_P(A),$$
$$v_P(ax) = v_P(a) + v_P(x) \geq -v_P(A),$$
and so $x + y, ax \in \mathcal{L}(A)$ by 1. of Remark 55.
2. $A' \sim A \Leftrightarrow \exists\ 0 \neq z \in F : A = A' + (z)$. Consider the mapping
$$\varphi : \begin{cases} \mathcal{L}(A) & \longrightarrow & F, \\ x & \longrightarrow & xz. \end{cases}$$
This is K-linear map fulfilling $\operatorname{Im} \varphi \subset \mathcal{L}(A')$. In the same manner,
$$\varphi' : \begin{cases} \mathcal{L}(A') & \longrightarrow & F, \\ x & \longrightarrow & xz^{-1}. \end{cases}$$
is K-linear map such that $\operatorname{Im} \varphi' \subset \mathcal{L}(A)$. The maps φ, φ' are inverse to each other, hence φ is an isomorphism $\mathcal{L}(A) \xrightarrow{\sim} \mathcal{L}(A')$. ■

Lemma 57

1. *$\mathcal{L}(0) = K$.*
2. *if $A < 0$ then $\mathcal{L}(A) = \{0\}$.*

Proof:

1. We have $(x) = 0$ for $0 \neq x \in K$, therefore $K \subseteq \mathcal{L}(0)$. Conversely, if $0 \neq x \in \mathcal{L}(0)$ then $(x) \geq 0$. This means that x has no poles, so $x \in K$ by Corollary (?)

2. Assume there exists an element $0 \neq x \in \mathcal{L}(A)$. Then $(x) \geq -A > 0$, which implies that x has at least one zero and no pole, which is impossible. ■

Let us denote by $\dim V$ the dimension of the K-vector space V. We shall prove the finite dimensionality of $\mathcal{L}(A)$ for all $A \in D_F$.

Lemma 58 *Let $A, B \in D_F$ with $A \leq B$. Then $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ and*

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

Proof: $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ is trivial. In order to prove the second assertion, let us assume $B = A + P$ for some $P \in \mathbb{P}_F$. Choose an element $t \in F$ with $v_P(t) = v_P(B) = v_P(A) + 1$. For $x \in \mathcal{L}(B)$ we have $v_P(x) \geq -v_P(B) = -v_P(t)$, and so $v_P(xt) \geq 0$, i.e. $xt \in \mathcal{O}_P$. Thus we obtain K-linear map

$$\psi : \left\{ \begin{array}{ccc} \mathcal{L}(B) & \longrightarrow & F_P, \\ x & \longrightarrow & (xt)(P). \end{array} \right.$$

The element $x \in \mathrm{Ker}\,(\psi)$ iff $v_P(xt) > 0$, i.e. $v_P(x) \geq -v_P(A)$. Consequently $\mathrm{Ker}\,(\psi) = \mathcal{L}(A)$, and ψ induces a K-linear injective map from $\mathcal{L}(B)/\mathcal{L}(A)$ to F_P. It follows that

$$\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \dim F_P = \deg B - \deg A.$$

The general case follows by induction. ■

Theorem 59 *For any divisor $A \in D_F$, the space $\mathcal{L}(A)$ is a finite-dimesional K-vector space. If $A = A_+ - A_- (A_+ \geq 0, A_- \geq 0)$, then*

$$\dim \mathcal{L}(A) \leq \deg A_+ + 1.$$

Proof: Since $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$, it is sufficient to show

$$\dim \mathcal{L}(A_+) \leq \deg A_+ + 1.$$

Because $0 \leq A_+$, the Lemma 58 yields $\dim(\mathcal{L}(A_+)/\mathcal{L}(0)) \leq \deg A_+$. Since $\mathcal{L}(0) = K$ by Lemma 57, $\dim \mathcal{L}(A_+) = \dim(\mathcal{L}(A_+)/\mathcal{L}(0)) + 1$, and so

$$\dim \mathcal{L}(A_+) = \dim \left(\frac{\mathcal{L}(A_+)}{\mathcal{L}(0)} \right) + 1 \leq \deg A_+ + 1$$

and the proof is complete. ■

Definition 60 *For $A \in D_F$, the integer* $\dim A := \dim \mathcal{L}(A)$ *is called the dimension of the divisor A.*

Now we shall prove an algebraic analog of well known theorem for meromorphic functions of complex variable, that an element $0 \neq x \in F$ has as many zeros as poles counted with multiplicities.

Lemma 61

1. *Let A, A' be divisors with $A \sim A'$. Then we have* $\dim A = \dim A'$ *and* $\deg A = \deg A'$.
2. *If* $\deg A < 0$ *then* $\dim A = 0$.
3. *For a divisor A of degree zero, the following assertions are equivalent:*
   (a) *A is principal.*
   (b) $\dim A \geq 1$.
   (c) $\dim A = 1$.

Proof:

1. It follows from Lemma 56 and Theorem 62.
2. Suppose $\dim A > 0$. By Remark 55 there is some divisor $A' \sim A$ with $A' \geq 0$ (i.e. effective), hence $\deg A = \deg A' \geq 0$.
3. (a) $\Rightarrow$ b
   If $A = (x)$ is principal then $x^{-1} \in \mathcal{L}(A)$, so $\dim A \geq 1$.
   (b) $\Rightarrow$ c
   Assume now that $\dim A \geq 1$ and $\deg A = 0$. Then $A \sim A'$ for some $A' \geq 0$ (Remark 55). The conditions $A' \geq 0$ and $\deg A' = 0$ imply that $A' = 0$, hence $\dim A = \dim A' = \dim 0 = 1$ by Lemma 57.
   (c) $\Rightarrow$ a
   Suppose that $\dim A = 1$ and $\deg A = 0$. Choose $0 \neq z \in \mathcal{L}(A)$, then $(z) + A \geq 0$. Since $\deg((z) + A) = 0$ it follows that $(z) + A = 0$, therefore $A = -(z) = (z^{-1})$ is principal. ■

Theorem 62 *Any principal divisor has degree zero. In particular, let $x \in F \setminus K$ and $(x)_0$ resp. $(x)_\infty$ denote the zero resp. pole divisor of x. Then*

$$\deg(x)_0 = \deg(x)_\infty = [F : K(x)].$$

Proof: Set $n := [F : K(x)]$ and $B := (x)_\infty = \sum_{i=1}^{r} -v_{P_i}(x) P_i$, where $P_1, \ldots, P_r$ are all the poles of x. Then

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

by Lemma (?) and thus it remains to show that $n \leq \deg B$ as well. Choose a basis $\{u_1, \ldots, u_n\}$ of $F/K(x)$ and a divisor $C \geq 0$ such that $u_i \geq -C$ for $i = 1, \ldots, n$. We have

$$\dim(lB + C) \geq n(l + 1) \qquad \text{for all } l \in \mathbb{N}_0,$$

which follows immediately from the fact that $x^i u_j \in \mathcal{L}(lB + C)$ for $0 \leq i \leq l$, $1 \leq j \leq n$ (observe that these elements are linearly independent over K since $u_1, \ldots, u_n$ are linearly independent over $K(x)$). This follows from

$$\begin{aligned} (x^i u_j) + lB + C &= i(x) + lB + (u_j) + C \\ &= i(x)_0 - i(x)_\infty + l(x)_\infty + (u_j) + C \\ &= \underbrace{i(x)_0}_{\geq 0} + \underbrace{(l - i)(x)_\infty}_{\geq 0} + \underbrace{(u_j) + C}_{\geq 0} \geq 0 \end{aligned}$$

By Theorem 59 we obtain

$$n(l+1) \leq \dim(lB+C) \leq l \deg B + c + 1, \qquad c := \deg C.$$

Thus

$$l(\deg B - n) \geq n - c - 1, \qquad \forall l \in \mathbb{N}. \tag{2.11}$$

The RHS is independent of l, i.e. Equation (2.11) is possible only when $\deg B \geq n$, i.e. we have just proved $\deg(x)_\infty = [F : K(x)]$. Since $(x_0) = (x^{-1})_\infty$, we conclude that $\deg(x)_0 = \deg(x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)]$. ■

Example 63 *For $F = K(x)$. For $0 \neq z \in K(x)$ we have $z = a\frac{f(x)}{g(x)}$ with $a \in K \setminus \{0\}$, $f(x), g(x) \in K[x]$ monic and relatively prime. Let*

$$f(x) = \prod_{i=1}^{r} p_i^{n_i}(x), \ \ g(x) = \prod_{j=1}^{s} g_j^{mj}(x)$$

with pairwise distinct irreducible monic polynomials $p_i(x)$, $g_j(x) \in K[x]$. Then the principal divisor $(z) \in D_{K(x)}$ of $z \in K(x)$ is

$$(z) = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j + (\deg(g) - \deg(f))P_\infty,$$

where P_i resp. Q_j are tle places corresponding to $p_i(x)$ resp. $q_i(x)$. By Theorem 59 we have $\dim A \leq 1 + \deg A$ for any $A \geq 0$. We shall show that this relation holds for arbitrary divisor of degree ≥ 0. In order to verify this, let us assume that $\dim A > 0$. Then $A \sim A'$ for some $A' \geq 0$ by Remark 55, so

$$\dim A = \dim A' \leq 1 + \deg A' = 1 + \deg A \tag{2.12}$$

by Lemma 61.

We shall prove a lower bound for $\dim A$, similar to the upper bound Equation (2.12) for divisors of positive degree.

Proposition 64 *There is a constant $\gamma \in \mathbb{Z}$ such that, for all divisors $A \in D_F$, the following holds*

$$\deg A - \dim A \leq \gamma.$$

The constant $\gamma \in \mathbb{Z}$ is independent of A; it depends only on the couple $\{F, K\}$.

Proof: Observe that, by Lemma 58,

$$A_1 \leq A_2 \Longrightarrow \deg A_1 - \dim A_1 \leq \deg A_2 - \dim A_2.$$

Fix an element $x \in F \setminus K$ and consider the specific divisor $B := (x)_\infty$. As in the prove of Theorem 62, there exists a divisor $C \geq 0$ (depending on x) such that $\dim(lB + C) \geq (l+1) \deg B \ \forall l \in \mathbb{N}_0$, see Equation (?). On the other hand by Lemma 58, $\dim(lB + C) \leq \dim(lB) + \deg C$. Combining together, we find

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

Therefore

$$\deg(lB) - \dim(lB) \leq \gamma \qquad \forall\, l \in \mathbb{N}, \tag{2.13}$$

with some $\gamma \in \mathbb{Z}$. We shall show that Equation (2.13) holds for any $A \in D_F$ and not only for $lB \in D_F$. ■

Claim 65 *Given a divisor A, there exist divisors A_1, D and $l \in \mathbb{N}$ such that $A \leq A_1$, $A_1 \sim D$ and $D \leq lB$.*

Proof: Choose $A_1 \geq A$, $A_1 \geq 0$. Then

$$\dim(lB - A_1) \underset{\text{Lemma 58}}{\geq} \dim(lB) - \deg A_1 \underset{(2.13)}{\geq} \deg(lB) - \gamma - \deg A_1 > 0$$

for sufficiently large $l \in \mathbb{N}$. Thus there is $0 \neq z \in \mathcal{L}(lB - A_1)$.
Setting $D := A_1 - (z)$ we obtain $A_1 \sim D$ and $D \leq A_1 - (A_1 - lB) = lB$. This proves the claim.
Using this Claim, we have

$$\begin{aligned} \deg A - \dim A &\underset{\text{Lemma 58}}{\leq} \deg A_1 - \dim A_1 \underset{\text{Lemma 61}}{=} \\ \deg D - \dim D &\underset{\text{Lemma 58}}{\leq} \deg(lB) - \dim(lB) \leq \gamma. \end{aligned}$$

■

Definition 66 *The genus g of F/K is defined by*

$$g := \max\{\deg A - \dim A + 1,\ A \in D_F\}.$$

This definition makes sense in the light of Proposition 64.

Lemma 67 *The genus of F/K is a non-negative integer.*

Proof: Let us choose $0 = A \in D_F$. Then $\deg(0) - \dim(0) + 1 = 0$, i.e. $g \geq 0$. ■

Theorem 68 *(Riemann's Theorem) Let F/K be a function field of genus g.*

1. *For any divisor $A \in D_F$,*

   $$\dim A \geq \deg A + 1 - g.$$

2. *There is $c \in \mathbb{Z}$, $c \equiv c(F, K)$, such that*

   $$\dim A = \deg A + 1 - g$$

   whenever $\deg A \geq c$.

Proof:

1. Just the definition of the genus.
2. Choose a divisor A_0 with $g = \deg A_0 - \dim A_0 + 1$ and set $c := \deg A_0 + g$. If $\deg A \geq c$ then

   $$\dim(A - A_0) \geq \deg(A - A_0) + 1 - g \geq \deg A - c + 1 \geq 1.$$

   So there is an element $0 \neq z \in \mathcal{L}(A - A_0)$. Consider the divisor $A' := A + (z)$, $A' \geq A_0$ (because $0 \neq \mathcal{L}(A - A_0) = \mathcal{L}(A' - A_0)$). Then

   $$\deg A - \dim A \underset{\text{Lemma 61}}{=} \deg A' - \dim A' \underset{\text{Lemma 58}}{\geq} \deg A_0 - \dim A_0 = g - 1.$$

   Hence $\dim A \leq \deg A + 1 - g$. ■

Example 69 *We want to show that the rational field $K(x)/K$ has genus $g = 0$. Let us denote by P_∞ the pole divisor of $x \in K(x)$. For $l \in \mathbb{N}_0$ let us consider $\mathcal{L}(lP_\infty)$. The elements $1, x, \ldots, x^l$ are in $\mathcal{L}(lP_\infty)$, hence*

$$l + 1 \leq \dim(lP_\infty) = \deg(lP_\infty) + 1 - g = l \deg P_\infty + 1 - g = l + 1 - g$$

for $r \gg 0$, $r \in \mathbb{N}$. Thus $g \leq 0$. Since $g \geq 0$ for any function field, the result follows.

5. The Riemann-Roch Theorem

Let F/K be an algebraic function field of genus g.

Definition 70 *For $A \in D_F$,*

$$i(A) := \dim A - \deg A + g - 1$$

is called the index of speciality of A.

Riemann's Theorem (68) states that $i(A) \in N_0$, and $i(A) = 0$ if $\deg A \gg 0$. We are going to prove that $i(A)$ is the dimension of certain vector space.

Definition 71 *An adele of F/K is a map*

$$\alpha : \left\{ \begin{array}{ccc} \mathbb{P}_F & \longrightarrow & F, \\ P & \longrightarrow & \alpha_P. \end{array} \right.$$

such that $\alpha_p \in \mathcal{O}_P$ for almost all $P \in \mathbb{P}_F$. We regard an a adele space as an element of the direct product $\prod_{P \in \mathbb{P}_F} F$ and therefore use the notation $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ (or $\alpha = (\alpha_P)$)*.*
The set $\mathcal{A}_F := \{\alpha | \alpha$ is an adele of $F/K\}$ is called adele space of F/K. It is regarded as a K-vector space given by abelian structure on values. The ring structure will never be used. We use the terminology "almost all"≡"all but finitely many".

The principal adele of an element $x \in F$ is the adele

$$\alpha_P : P \longrightarrow x \in F \qquad \forall P \in \mathbb{P}_F.$$

This gives an a embedding $F \hookrightarrow \mathcal{A}_F$. The valuations v_P of F/K extend naturally to $\mathcal{A}_F$ by setting $v_P(\alpha) := v_P(\alpha_P)$ $(\alpha \equiv (\alpha_P)_P, P \in \mathbb{P}_F)$. By definition, $v_P(\alpha) \geq 0$ for almost all $P \in \mathbb{P}_F$.

Definition 72 *For $A \in D_F$ we define*

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F \mid v_P(\alpha) \geq -v_P(A) \ \forall P \in \mathbb{P}_F\}.$$

This is (infinite dimensional) K-linear subspace of $\mathcal{A}_F$.

Theorem 73 *For any $A \in D_F$, the index of speciality is*

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

Note that although $\mathcal{A}_F$, $\mathcal{A}_F(A)$, F are ∞-dimensional K-vector spaces, the quotient f space $\mathcal{A}_F/(\mathcal{A}_F + F)$ is finite dimensional K-vector space.

Corollary 74

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

Proof (Theorem 73):

1. Let $A_1, A_2 \in D_F,\ A_1 \le A_2$. Then $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ and
$$\dim_K(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) = \deg A_2 - \deg A_1. \tag{2.14}$$
Proof: $A_1 \le A_2 \Rightarrow -A_2 \le -A_1 \Rightarrow \mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$. Using induction argument, it is sufficient to prove (2.14) in the case $A_2 = A_1 + P,\ P \in \mathbb{P}_F$. Choose $t \in F$ with $v_P(t) = v_P(A_1) + 1$ and consider K-linear maps
$$\varphi : \begin{cases} \mathcal{A}_F(A_2) & \longrightarrow & F_P, \\ \alpha & \longmapsto & (t\alpha_P)(P). \end{cases}$$
It is easy to see that φ is surjective and $\operatorname{Ker}(\varphi) = \mathcal{A}_F(A_1)$. Consequently
$$\deg A_2 - \deg A_1 = \deg P - [F_P : K] = \dim_K(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)).$$

2. Let $A_1, A_2 \in D_F$ and $A_1 \le A_2$. Then
$$\dim_K((\mathcal{A}_F(A_2)+F)/(\mathcal{A}_F(A_1)+F)) = (\deg A_2 - \dim A_2) - (\deg A_1 - \dim A_1). \tag{2.15}$$
Proof: We have an exact sequence of linear maps:
$$0 \to \mathcal{L}(A_2)/\mathcal{L}(A_1) \xrightarrow{f_1} \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \xrightarrow{f_2} (\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F) \to 0. \tag{2.16}$$
where f_1, f_2 are natural (K-linear) maps. The only non-trivial assertion is that $\operatorname{Ker} f_2 \subset \operatorname{Im} f_1$. In order to prove this, let $\alpha \in \mathcal{A}_F(A_2)$ with $f_2(\alpha + \mathcal{A}_F(A_1)) = 0$. Then $\alpha \in \mathcal{A}_F(A_1) + F$, so there is some $x \in F$ with $\alpha - x \in \mathcal{A}_F(A_1)$. As $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ we conclude that $x \in \mathcal{A}_F(A_2) \cap F = \mathcal{L}(A_2)$. Therefore $\alpha + \mathcal{A}_F(A_1) = x + \mathcal{A}_F(A_1) = f_1(x + \mathcal{L}(A_1))$ lies in the image of f_1.
The exactness of Equation (2.16) implies
$$\dim_K((\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F)) = \dim_K(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) - \dim_K(\mathcal{L}(A_2)/\mathcal{L}(A_1)) = (\deg A_2 - \deg A_1) - (\dim A_2 - \dim A_1),$$
using the result Equation (2.14) of 1.

3. If A is a divisor with $\dim A = \deg A + 1 - g$, then
$$\mathcal{A}_F = \mathcal{A}_F(A) + F. \tag{2.17}$$
Proof: We have, for $A_1 \ge A$,
$$\dim A_1 \le \deg A_1 + \dim A - \deg A = \deg A_1 + 1 - g \tag{2.18}$$
by Lemma 58. On the other hand $\dim A_1 \ge \deg A_1 + 1 - g$ by Riemann's Theorem. Therefore
$$\dim A_1 = \deg A_1 + 1 - g \qquad \forall A_1 \ge A. \tag{2.19}$$
Let us prove Equation (2.17). Let $\alpha \in \mathcal{A}_F$. Clearly we can find a divisor $A_1 \ge A$ such that $\alpha \in \mathcal{A}_F(A_1)$ it follows. By Equations (2.15), (2.19),
$$\dim_K((\mathcal{A}_F(A_1) + F)/(\mathcal{A}_F(A) + F)) = (\deg A_1 - \dim A_1) - (\deg A - \dim A) = (g-1) - (g-1) = 0.$$
This implies $\mathcal{A}_F(A) + F = \mathcal{A}_F(A_1) + F$. Since $\alpha \in \mathcal{A}_F(A_1)$ it follows $\alpha \in \mathcal{A}_F(A) + F$ and Equation (2.17) is proved.

Let us consider an arbitrary divisor A. By Riemann's Theorem, Theorem 68, 2., there exists some divisor $A_1 \geq A$ such that $\dim A_1 = \deg A_1 + 1 - g$. By Equation (2.17), $\mathcal{A}_F = \mathcal{A}_F(A_1) + F$ and Equation (2.15) implies

$$\dim_K(\mathcal{A}_F/(\mathcal{A}_F(A) + F)) = \dim_K((\mathcal{A}_F(A_1) + F)/(\mathcal{A}_F(A) + F)) =$$
$$(\deg A_1 - \dim A_1) - (\deg A - \dim A) = (g - 1) + \dim A - \deg A = i(A).$$

■

Theorem 73 can be restated in the following way: $\forall A \in D_F$ it holds

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

which is a version of Riemann-Roch Theorem.

The following concept of Weil differentials leads to an interpretation of the index of speciality of a divisor.

Definition 75 *A Weil differential of F/K is a K-linear map $\omega : \mathcal{A}_F \to K$ vanishing on $\mathcal{A}_F(A) + F$ for some divisor $A \in D_F$. We call*

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

the module of Weil differentials of F/K. For $A \in D_F$ let

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

We regard Ω_F as a K-vector space: if ω_1 vanishes on $\mathcal{A}_F(A_1) + F$ (i.e. $\omega_1 \in \Omega_F(A_1)$) and ω_2 vanishes on $\mathcal{A}_F(A_2) + F$ (i.e. $\omega_2 \in \Omega_F(A_2)$) then $\omega_1 + \omega_2$ vanishes on $\mathcal{A}_F(A_3) + F$ $\forall A_3 \in D_F$ with $A_3 \leq A_1$ and $A_3 \leq A_2$, and $\alpha\omega_1$ vanishes on $\mathcal{A}_F(A_1) + F$ $\forall \alpha \in K$. Clearly $\Omega_F(A)$ is a subspace of Ω_F.

Lemma 76 *For $A \in D_F$ we have* $\dim \Omega_F(A) = i(A)$.

Proof: $\Omega_F(A)$ is in a natural way isomorphic to the space of linear forms on $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$. Since $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$ is finite dimensional of dimension $i(A)$ by Theorem 73, the Lemma follows. ■

A consequence of Lemma 76 is that $\Omega_F \neq 0$. To see this, choose a divisor $A \in D_F$, $\deg A \leq -2$. Then

$$\dim \Omega_F(A) = i(A) = \dim A - \deg A + g - 1 \geq 1,$$
$$\text{hence } \Omega_F(A) \neq 0, \text{ and so } \Omega_F \neq 0.$$

Definition 77 *For $x \in F$, $\omega \in \Omega_F$ define $x\omega : \mathcal{A}_F \to K$ by*

$$(x\omega)(\alpha) := \omega(x\alpha), \qquad \alpha \in \mathcal{A}_F.$$

We see that $x\omega$ is again Weil differential of F/K. If ω vanishes on $\mathcal{A}_F(A) + F$ then $x\omega$ vanishes on $\mathcal{A}_F(A + (x)) + F$. The Definition 77 gives Ω_F the structure of a vector space over F.

Proposition 78 *Ω_F is a one dimensional vector space over F,* $\dim_F(\Omega_F) = 1$.

Proof: We know that $\Omega_F \neq 0$, and so choose $0 \neq \omega_1 \in \Omega_F$. We shall show that for any $\omega_2 \in \Omega_F$ there is some $z \in F : \omega_2 = z\omega_1$. We can assume $\omega_2 \neq 0, \omega_2 \in \Omega_F$. Choose $A_1, A_2 \in D_F$ such that $\omega_1 \in \Omega_F(A_1), \omega_2 \in \Omega_F(A_2)$. For a divisor $B \in D_F$ consider K-linear injective maps ($i = 1, 2$)

$$\varphi_i : \begin{cases} \mathcal{L}(A_i + B) & \longrightarrow & \Omega_F(-B), \\ x & \longmapsto & x\omega_i. \end{cases}$$

We claim that for appropriate choice of $B \in D_F$ it holds

$$\varphi_1(\mathcal{L}(A_1 + B)) \cap \varphi_2(\mathcal{L}(A_2 + B)) \neq \{0\}.$$

If the claim is true, the proof can be finished quickly: 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 $\omega_2 = (x_1x_2^{-1})\omega_1$ for $(x_1x_2^{-1}) \in F$ as desired.
Let us prove the claim. We start with a simple and well-known fact from linear algebra: for $U_1, U_2 \subset V$ vector subspaces of a vector space V holds

$$\dim(U_1 \cap U_2) \geq \dim U_1 + \dim U_2 - \dim V. \tag{2.20}$$

Let $B > 0$ be a divisor of sufficiently high degree, i.e.

$$\dim(A_i + B) = \deg(A_i + B) + 1 - g, \qquad i = 1, 2$$

by Riemann's Theorem. Set $U_i := \varphi_i(\mathcal{L}(A_i + B)) \subseteq \Omega_F(-B)$. Since

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

we obtain

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

If $\deg B$ is sufficiently large, we get

$$\dim U_1 + \dim U_2 - \dim \Omega_F(-B) > 0.$$

By Equation (2.20) $\dim(U_1 \cap U_2) > 0$, i.e. $U_1 \cap U_2 \neq \{0\}$ as desired. ■

Now we are going to attach a divisor to any Weil differential in a canonical way. Let us consider, for $0 \neq \omega \in \Omega_F$, the set of divisors

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

Lemma 79 *Let $0 \neq \omega \in \Omega_F$. Then there is a uniquely determined divisor $W \in M(\omega)$ such that $A \leq W$ $\forall A \in M(\omega)$.*

Proof: By Riemann's Theorem there exists a constant $c \in \mathbb{Z}$, $c = c(F, K)$, such that $i(A) = 0\, \forall A \in D_F$ of degree $\geq c$. By Theorem 73 $\dim(\mathcal{A}_F/(\mathcal{A}_F(A)+F)) = i(A)$, we have $\deg A < c$ for all $A \in M(\omega)$. In other words, we can choose a divisor $W \in M(\omega)$ of maximal degree. Suppose W does not have the property of the Lemma. Then there exists a divisor $A_0 \in M(\omega)$ with $A_0 \not\leq W$, i.e.

$$v_Q(A_0) > v_Q(W) \qquad \text{for some } Q \in \mathbb{P}_F.$$

We claim that than

$$W + Q \in M(\omega) \tag{2.21}$$

which is a contradiction with the maximality of W. In fact, consider an adele $\alpha = (\alpha_P)_P \in \mathcal{A}_F(W + Q)$. We can write $\alpha = \alpha' + \alpha''$ with

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

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 $\mathcal{A}_F(W + Q) + F$ and Equation (2.21) follows. The uniqueness of W is now clear. ■

Definition 80

1. *The divisor ω of a Weil differential $\omega \neq 0$ is the uniquely determined divisor of F/K satisfying*
   (a) *ω vanishes on $\mathcal{A}_F((\omega)) + F$.*
   (b) *If ω vanishes on $\mathcal{A}_F(A) + F$ then $A \leq (\omega)$.*
2. *For $0 \neq \omega \in \Omega_F$ and $P \in \mathbb{P}_F$ we define $v_P(\omega) := v_P((\omega))$.*
3. *A place P is said to be zero (resp. pole) of ω of $v_P(\omega) > 0$ (resp. $v_P(\omega) < 0$). The Weil differential ω is called regular at P if $v_P(\omega) \geq 0$, and ω is said to be regular (or holomorphic in the case $K = \mathbb{C}$) if it is regular at any $P \in \mathbb{P}_F$.*
4. *A divisor W is called a canonical divisor of F/K if $W = (\omega)$ for some $\omega \in \Omega_F$.*

Note that, by Lemma 79, Definition 80 makes sense.

Remark 81 *It follows from Definition 80 that*

$$\Omega_F(A) = \{\omega \in \Omega_F \mid \omega = 0 \text{ or } (\omega) \geq A\}$$

and

$$\Omega_F(0) = \{\omega \in \Omega_F \mid \omega \text{ is regular}\}.$$

It follows from Deffinition 70 and Lemma 76 that

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

Proposition 82

1. *For $0 \neq x \in F$ and $0 \neq \omega \in \Omega_F$ we have $(x\omega) = (x) + (\omega)$.*
2. *Any two canonical divisors of F/K are equivalent.*

Proof: If ω vanishes on $\mathcal{A}_F(A)+F$ then $x\omega$ vanishes on $\mathcal{A}_F(A+(x))+F$, consequently

$$(\omega)+(x)\leq(x\omega).$$

Like wise $(x\omega)+(x^{-1})\leq(x^{-1}x\omega)=(\omega)$. Combinning both inequalities we find

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

This proves 1., part 2. follows from Proposition 78 and 1. ■

Theorem 83 *Let A be an arbitrary divisor, $W=(\omega)$ a canonical divisor of F/K. Then the map*

$$\varphi:\begin{cases}\mathcal{L}(W-A) & \longrightarrow & \Omega_F(A),\\ x & \longmapsto & x\omega,\end{cases}$$

is an isomorphism of K-vector spaces. In particular,

$$i(A)=\dim(W-A).$$

Proof: For $x\in\mathcal{L}(W-A)$ we have

$$(x\omega)=(x)+(\omega)\geq-(W-A)+W=A,$$

hence $x\omega\in\Omega_F(A)$ by Remark 81. Therefore φ maps $\mathcal{L}(W-A)$ into $\Omega_F(A)$, i.e. φ is K-linear and injective. In order to show surjectiviy of φ, consider a Weil differential $\omega_1\in\Omega_F(A)$. By Proposition 78, $\omega_1=x\omega$ for some $x\in F$. Since

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

we obtain $(x)\geq-(W-A)$, so $x\in\mathcal{L}(W-A)$ and $\omega_1=\varphi(x)$. We have proved that $\dim_K\Omega_F(A)=\dim(W-A)$. Since $\dim_K\Omega_F(A)=i(A)$ by Lemma 76, this implies $i(A)=\dim(W-A)$. ■

These results can be summarized in the most important Theorem describing linear systems of algebraic function fields.

Theorem 84 *(Riemann-Roch) Let W be a canonical divisor of F/K. Then, for any $A\in D_F$,*

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

Proof: This is an immediate consequence of Theorem 83 and the definition of $i(A)$. ■

6. The Concequences of the Riemann-Roch Theorem

Lemma 85 *For a canonical divisor W, we have*

$$\deg W = 2g - 2,\ \dim W = g.$$

Proof: For A=0, the Riemann-Roch Theorem 84 and Lemma 57 imply

$$1 = \dim 0 = \deg 0 + 1 - g + \dim(W - 0),$$

i.e. $\dim W = g$. For $A = W$ we obtain

$$g = \dim W = \deg W + 1 - g + \dim(W - W) = \deg W + 2 - g,$$

therefore $\deg W = 2g - 2$. ■

Lemma 86 *If $A \in D_F$ is a divisor of F/K, $\deg A \geq 2g - 1$ then*

$$\dim A = \deg A + 1 - g.$$

Proof: We have $\dim A = \deg A + 1 - g + \dim(W - A)$, where W is canonical divisor. Since $\deg A \geq 2g - 1$ and $\deg W = 2g - 2$, $\deg(W - A) < 0$ and so $\dim(W - A) = 0$ by Lemma 61 $\dim(W - A) = 0$ and the result follows. ■

Note that this bound is the best possible, because for a canonical divisor W,

$$\dim W > \deg W + 1 - g$$

by Lemma 85.

The next results characterize the genus as well as the canonical class of F/K.

Lemma 87 *Suppose that $g_0 \in \mathbb{Z}$ and $W_0 \in D_F$ satisfy*

$$\dim A = \deg A + 1 - g_0 + \dim(W_0 - A) \tag{2.22}$$

for any $A \in D_F$. Then $g_0 = g$, and W_0 is canonical divisor.

Proof: Setting $A = 0$ resp. $A = W_0$ in Equation (2.22) we obtain $\dim W_0 = g_0$ and $\deg W_0 = 2g_0 - 2$ (see Lemma 85). Let W be a canonical divisor of F/K. We choose a divisor A with $\deg A > \max\{2g-2, 2g_0-2\}$. Then $\dim A = \deg A + 1 - g$ by Lemma 86 and $\dim A = \deg A + 1 - g_0$ by Equation (2.22). Therefore $g = g_0$. Now we substitute $A = W$ in Equation (2.22). This yields

$$g = (2g - 2) + 1 - g + \dim(W_0 - W),$$

hence $\dim(W_0 - W) = 1$. Since $\deg(W_0 - W) = 0$ this implies that $W_0 - W$ is principal by Lemma 61, 3., so $W \sim W_0$. ■

Lemma 88 *A divisor B is canonical iff $\deg B = 2g - 2$ and $\dim B \geq g$.*

Proof: Suppose that $\deg B = 2g-2$ and $\dim B \geq g$. Choose a canonical divisor W. Then

$$g \leq \dim B = \deg B + 1 - g + \dim(W - B) = g - 1 + \dim(W - B).$$

Therefore $\dim(W - B) \geq 1$. Since $\deg(W - B) = 0$ it follows from Lemma 61, 3., that $W \sim B$ ■

The rational function fields can be characterized explicitly.

Proposition 89 *For a function field F/K the following conditions are equivalent:*

1. *F/K is rational, i.e. $F = K(x)$ for some $x \in F$ transcendental over K.*
2. *F/K has genus 0, and there is some divisor $A \in D_F$ with $\deg A = 1$.*

Proof:

1. $\Rightarrow$ 2. see Example 69
2. $\Rightarrow$ 1.
   Let $g = 0$ and $\deg A = 1$. Because $\deg A \geq 2g - 1$ we have $\dim A = \deg A + 1 - g = 2$ by Lemma 86. Thus $A \sim A'$ for some positive $A' \in D_F$ (see Remark 55, 2.). Since $\dim A' = 2$ there exists $x \in \mathcal{L}(A') \setminus K$, so $(x) \neq 0$ and $(x) + A' \geq 0$. As $A' \geq 0$ and $\deg A' = 1$, this is possible if $A' = (x)_\infty$, the pole divisor of x. Now

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

   by Theorem 62, so $F = K(x)$. ■

Remark 90 *Note that there exist non-rational function field of genus 0; these cannot have a divisor of degree 1 by Proposition 89. However, if K is an algebraically closed field of a finite field (generally a perfect field), there exists always a divisor of degree 1, hence $g = 0$ iff F/K is rational.*

Chapter 3

Examples of Algebraic Function Fields

We shall restrict to the perfect field K. In particular, the results hold if K is an algebraically closed field, a field of characteristic zero of a finite field.

1. Elliptic Function Fields

Definition 91 *An algebraic function field F/K is said to be an elliptic function field if the following conditions hodl:*

1. *the genus of F/K is 1,*
2. *there exists adivisor $A \in D_F$ with $\deg A = 1$.*

Lemma 92 *Let F/K be an elliptic function field.*

1. *If $\operatorname{char}[K] \neq 2$, there exists $x, y \in F$ such that $F = K(x, y)$ and*
$$y^2 = f(x) \in K[x] \text{ with a square-free polynomial } f(x) \in K[x], \tag{3.1}$$
$\deg(f) = 3$.
2. *If char $(K) = 2$, there exist $x, y \in F$ such that $F = K(x, y)$ and*
$$y^2 + y = f(x) \in K[x], \qquad \deg(f) = 3 \tag{3.2}$$
or
$$y^2 + y = x + \frac{1}{ax + b}, \qquad 0 \neq a, b \in K. \tag{3.3}$$

Proof: Choose $A \in D_F$, $\deg(A) = 1$. By the Riemann-Roch Theorem 84, $\dim A = \deg A - g + 1 = 1$ (vote $\deg A > 2g - 2$). Hence A is equivalent to a positive divisor A_1, $A_1 \sim A$. $A_s \deg A_1 = 1$ we conclude that A_1 a prime divisor $A_1 = P \in \mathbb{P}_F$.
Let us consider the spaces $K = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \ldots \subseteq \mathcal{L}(nP) \subseteq \ldots$ Because $2g - 2 = 0$, the Riemann-Roch Theorem 84 gives $\dim \mathcal{L}(iP) = i \; \forall\, i > 0$, hence $\mathcal{L}(P) = K$ and $\mathcal{L}((i+1)P) \supsetneq \mathcal{L}(iP)$ for $i > 0$. We choose $x_1 \in \mathcal{L}(2P) \setminus K$, $y_1 \in \mathcal{L}(3P) \setminus \mathcal{L}(2P)$.
Then $[F : K(x_1)] = (x_1)_\infty = 2$, $[F : K(y_1)] = (y_1)_\infty = 3$, and so due to the $K-$independents of x_1 and y_1 we have $F = K(x_1, y_1)$.
The seven elements $\{1, x_1, y_1, {x_1}^2, x_1y_1, {x_1}^3, {y_1}^2\} \in \mathcal{L}(6P)$. Since $\mathcal{L}(6P) = 6$ there is a non-trivial relation

$$\alpha_1 {y_1}^2 + \beta_1 x_1 y_1 + \gamma_1 y_1 = \delta_1 {x_1}^3 + \epsilon_1 {x_1}^2 + \lambda_1 x_1 + \mu_1 \tag{3.4}$$

with $\alpha_1,\ \beta_1, \ldots \in K$. The coefficient $\alpha_1 \neq 0$; otherwise Equation (3.4) would reduce to an equation for y_1 over $K(x_1)$ of degree one, which is impossible as $F = K(x_1, y_1)$ and $[F : K(x_1)] = 2$. In the same manner, we see that $\delta_1 \neq 0$. Multiply Equation (3.4) by $\alpha_1^3\delta_1^2$; then

$$\alpha_1^4\delta_1^2 y_1^2 + \cdots = \alpha_1^3\delta_1^3 x_1^3 + \cdots$$

Setting $y_2 := \alpha_1^2\delta_1 y_1,\ x_2 := \alpha_1\delta_1 x_1$, we obtain $F = K(x_2, y_2)$ and

$$y_2^2 + (\beta_2 x_2 + \gamma_2)y_2 = x_2^3 + \epsilon_2 x_2^2 + \lambda_2 x_2 + \mu_2$$

with $\beta_2,\ \gamma_2, \ldots \in K$. We must distinguish two cases:

1. $\mathrm{char}\,(K) \neq 2$
   We set $y := y_2 + \frac{1}{2}(\beta_2 x_2 + \gamma_2)$, $x := x_2$; then $F = K(x, y)$ and

   $$y^2 = x^3 + \epsilon x^2 + \lambda x + \mu = f(x) \in K[x], \qquad \epsilon,\ \lambda,\ \mu \in K.$$

   It remains to show that $f(x)$ is square-free. Suppose the contrary, i.e. $f(x) = (x - \xi)^2(x - \eta)$ for $\xi,\ \eta \in K$. Consider the element $z := \frac{y}{(x-\xi)}$. Then $z^2 = x - \eta$ and so $F = K(x, y) = K(x, z) = K(z)$. This implies that F is rational, a contradiction.

2. $\mathrm{char}\,(K) = 2$ We have already shown that $F = K(x_2, y_2)$ with

   $$y_2^2 + (\beta_2 x_2 + \gamma_2)y_2 = x_2^3 + \epsilon_2 x_2^2 + \lambda_2 x_2 + \mu_2.$$

   We claim $\beta_2 x_2 + \gamma_2 \neq 0$. If $\beta_2 x_2 + \gamma_2 = 0$ then $y_2^2 \in K(x_2)$, i.e. the extension $F/K(x_2)$ is purely inseparable of degree $p = 2$. It is well-known that the only intermediate field $K \subseteq F_0 \subseteq F$ such that F/F_0 is purely inseparable of degree p is the field $F_0 = F^P$, so $K(x_2) = F^P$. However, the genus of $K(x_2)/K$ is zero and the genus of F^P/K is one. This proves the claim.
   We set $y_3 := (\beta_2 x_2 + \gamma_2)^{-1} y_2$, then $F = K(x_2, y_3)$ and

   $$y_3^2 + y_3 = (\beta_2 x_2 + \gamma_2)^{-2}(x_2^3 + \epsilon_2 x_2^2 + \lambda_2 x_2 + \mu_2). \tag{3.5}$$

If $\beta_2 = 0$, the RHS of Equation (3.5) is a polynomial $f(x_2) \in K[x_2]$ of degree 3, which is the promised result. If $\beta_2 \neq 0$ the RHS of Equation (3.5) can be rewritten in the form

$$\nu x_2 + \varrho + \frac{\sigma}{(\beta_2 x_2 + \gamma_2)^2} + \frac{\tau}{\beta_2 x_2 + \gamma_2}, \qquad 0 \neq \nu,\ \varrho,\ \sigma,\ \tau \in K.$$

As K is a perfect field, $\sigma = \sigma_1^2$ for some $\sigma_1 \in K$, and the element $y_4 := y_3 + \sigma_1(\beta_2 x_2 + \gamma_2)$ satisfies an equation

$$y_4^2 + y_4 = \nu_2 x_2 + \varrho_2 + \frac{\tau_2}{\beta_2 x_2 + \gamma_2}, \qquad 0 \neq \nu_2,\ \varrho_2,\ \tau_2 \in K.$$

We have $\tau_2 \neq 0$; otherwise $F = K(x_2, y_4)$ would be rational, $F = K(x_2, y_4) = K(y_4)$. Set $y := y_4$ and $x := \nu_2 x_2 + \varrho_2$ and obtain $F = K(x, y)$ with

$$y^2 + y = x + \frac{1}{ax + b}, \qquad 0 \neq a,\ b \in K.$$

■

We shall list, without proof, a few basic results related to elliptic function fields given by Equation (3.1), (3.2), (3.3).

Lemma 93

1. $\operatorname{char}(K) \neq 2$
   suppose that $F = K(x, y)$ with $y^2 = f(x) \in K[x]$, where $f(x)$ is a square-free polynomial, $\deg f = 3$. Consider the decomposition $f(x) = c\prod_{i=1}^{r} p_i(x)$ into irreducible monic polynomials $p_i(x) \in K[x]\ \forall\, i = 1, \ldots, r$, $0 \neq c \in K$. Denote by $P_i \in \mathbb{P}_{K(x)}$ the place of $K(x)$ corresponding to $p_i(x)$, and by $P_\infty \in \mathbb{P}_{K(x)}$ the pole of x. Then

   (a) *$K \subseteq F$ is the full constant field of F and F/K is an elliptic function field*

   (b) *The extension $F/K(x)$ is cyclic of degree 2. The places $P_1, \ldots, P_r$ are ramified in $F/K(x)$; each of them has exactly one extension in F, say $Q_1, \ldots, Q_r$ and Q_∞, and we have $e(Q_j,\ P_j) = e(Q_\infty,\ P_\infty) = 2(\forall j)$, $\deg Q_j = \deg P_j$ and $\deg Q_\infty = 1$.*

   (c) *$P_1, \ldots, P_r, P_\infty$ are the only places ramified in $F/K(x)$.*

2. $\operatorname{char}(K) = 2$
   Suppose that $F = K(x, y)$ with $y^2 + y = f(x) \in K[x]$, $\deg(f) = 3$ or $y^2 + y = x + \frac{1}{ax+b}$ with $0 \neq a,\ b \in K$. Denote by $P_\infty \in \mathbb{P}_{K(x)}$ the pole of x in $K(x)$ and by $P' \in \mathbb{P}_{K(x)}$ the zero of $(ax + b) \in K(x)$.Then

   (a) *K is the full constant field of F, and F/K is and elliptic function field.*

   (b) *The extension $F/K(x)$ is cyclic of degree 2. The only places of $K(x)$ which ramify in $F/K(x)$ are P_∞ in the case of Equation (3.1) and P', P_∞ in the case of Equation (3.2). Let Q_∞ (resp. Q' in the case of Equation (3.2)) be the place(s) of F/K lying over P_∞ (resp. P'). Then $\deg Q_\infty = \deg Q' = 1$.*

Example 94 *Let us describe the classical example of an elliptic function field. Consider the lattice $\Gamma \subseteq \mathbb{C}$, i.e. $\Gamma = \mathbb{Z}\gamma_1 \oplus \mathbb{Z}\gamma_2$, $\gamma_1, \gamma_2 \in \mathbb{C} \setminus \{0\}$, $\frac{\gamma_1}{\gamma_2} \notin \mathbb{R}$. An elliptic function $f : \mathbb{C} \to \mathbb{C}$ w.r. to lattice Γ is a meromorphic function satisfying $f(z+\gamma) = f(z)\ \forall \gamma \in \Gamma,\ z \in \mathbb{C}$. The elliptic function field $\mathcal{U}(\Gamma)$ forms a subfield $\mathcal{U}(\mathbb{C})$ of the field of meromorphic functions on the complex plane. The set $\mathbb{C} \subset \mathcal{U}(\Gamma) \subset \mathcal{U}(\mathbb{C})$ is the full subfield of constants. Two specific non-constant elliptic functions are Weierstrass $\mathcal{P}$-function*

$$\mathcal{P}(z) := \frac{1}{z^2} + \sum_{0 \neq \gamma \in \Gamma} \left(\frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2} \right)$$

and its derivative $\mathcal{P}'(z)$. These functions fulfill

1. $\mathcal{U}(\Gamma) = \mathbb{C}\left(\mathcal{P}(z), \mathcal{P}'(z)\right)$,
2. $\left(\mathcal{P}'(z)\right)^2 = 4\mathcal{P}^3(z) - g_2\mathcal{P}(z) - g_3$

with constants $g_2, g_3 \in \mathbb{C}$ and square-free polynomial $f(\mathcal{T}) = 4\mathcal{T}^3 - g_2\mathcal{T} - g_3 \in \mathbb{C}[\mathcal{T}]$. Hence $\mathcal{U}(\Gamma)/\mathbb{C}$ is an elliptic function field by Lemma 93.
For $\alpha \in \mathbb{C}$, any function $0 \neq f \in \mathcal{U}(\Gamma)$ has a Laurent series expansion

$$f(z) = \sum_{i=i_0}^{\infty} a_i (z-\alpha)^i, \qquad a_i \in \mathbb{C},\ i_0 \in \mathbb{Z},\ q_{i_0} \neq 0.$$

Let $v_\alpha : f \to v_\alpha(f) := i_0$ be a discrete valuation corresponding to $\alpha \in \mathbb{C}$, i.e. to the place $P_\alpha \in \mathbb{P}_{\mathcal{U}(\Gamma)/\mathbb{C}}$. It is obvious that $P_\alpha = P_\beta$ iff $\alpha \equiv \beta \bmod \Gamma$. All places of the elliptic function field $\mathcal{U}(\Gamma)/\mathbb{C}$ are obtained in this manner.

Lemma 95 *Let F/K be an elliptic function field. Define*

$$\mathbb{P}_F^{(1)} := \{P \in \mathbb{P}_F \mid \deg P = 1\}.$$

Then

1. *For any divisor $A \in D_F$ $\deg A = 1$, there exists a unique place $P \in \mathbb{P}_F^{(1)}$ with $A \sim P$. In particular, $\mathbb{P}_F^{(1)} \neq 0$.*
2. *Fix a place $P_0 \in \mathbb{P}_F^{(1)}$. Then the map*

$$\begin{array}{rccc} \varphi : & \mathbb{P}_F^{(1)} & \longrightarrow & C_F^0, \\ & P & \longrightarrow & [P - P_0] \end{array}$$

   is bijective.

Proof:

1. Let $A \in D_F$, $\deg A = 1$. Since $\dim A = \deg A - g + 1 > 0$, there is a divisor $A_1 \in D_F$, $A_1 \sim A$, $A_1 > 0$ $(\deg A_1 = \deg A = 1,\ \dim A_1 = \dim A > 0)$ and it follows $A_1 \in \mathbb{P}_F^{(1)}$. This proves the existence.
   Suppose that $A \sim P$ and $A \sim Q$ for $P,\ Q \in \mathbb{P}_F^{(1)}$ and $P \neq Q$. Then $P \sim Q$,

i.e. $\exists\ 0 \neq x \in F$ such that $P - Q = (x)$. It follows $(x)_0 = P,\ (x)_\infty = Q$ and so

$$[F : K(x)] = \deg(x)_\infty = \deg(x)_0 = \deg P = \deg Q = 1,$$

hence $F = K(x)$. This is in contradiction with the fact that F is an elliptic function field, i.e. $[F : K(x)] > 0$. This proves the uniqueness.

2. φ is surjective:
Let $[B] \in C_F^0$. The divisor $B + P_0$ has degree one. By 1. there is a place $P \in \mathbb{P}_F^{(1)}$ with $B + P_0 \sim P$. Then $[B] = [P - P_0] = \varphi(P)$, and φ is surjective.
φ is injective:
Suppose $\varphi(P) = \varphi(Q)$ for $P,\ Q \in \mathbb{P}_F^{(1)}$. Then $P - P_0 \sim Q - P_0$, hence $P \sim Q$. By the uniqueness assertion in 1., it follows that $P = Q$. ■

The bijection φ of the foregoing proposition can be used to transport the group structure of C_F^0 to the set $\mathbb{P}_F^{(1)}$. This means that, for $P,\ Q \in \mathbb{P}_F^{(1)}$, we define

$$P \boxplus Q := \varphi^{-1}(\varphi(P) + \varphi(Q)). \tag{3.6}$$

Theorem 96 *Let F/K be an elliptic function field. Then*

1. *$\mathbb{P}_F^{(1)}$ is and abelian group w. r. to the operation $\boxplus$ defined in Equation (3.6).*
2. *The place P_0 is the neutral element of the group $\left(\mathbb{P}_F^{(1)}, \boxplus\right)$.*
3. *For $P,\ Q,\ R \in \mathbb{P}_F^{(1)}$, The following holds:*
$$P \boxplus Q = R \Longleftrightarrow P + Q \sim R + P_0([P + Q] = [R + P_0]).$$
4. *The map $\varphi : \mathbb{P}_F^{(1)} \to C_F^0$ is isomorphism of abelian groups.*

Proof: 1., 2., 4. are trivial.
3. By Equation (3.6):

$$\begin{aligned} P \boxplus Q = R \Longleftrightarrow \varphi(R) = \varphi(P) + \varphi(Q) \quad &\Longleftrightarrow R - P_0 \sim (P - P_0) + (Q - P_0) \\ &\Longleftrightarrow P + Q \sim R + P_0 \end{aligned}$$

■

Remark 97 *The abelian group law on $\mathbb{P}_F^{(1)}$ is not completely canonical. The reason is that the isomorphism φ depends on the choice $P_0 \in \mathbb{P}_F^{(1)}$. If F is represented in the form $F = K(x, y)$, the usual choice is $P_0 := Q_\infty$, the pole of $0 \neq x \in F$.*

2. Hyperelliptic Function Fields

The second simplest non-rational function field over K is hyperelliptic function field.

Definition 98 *A hyperelliptic function field over K is an algebraic function field F/K of genus $g \geq 2$ which contains a rational subfield $K(x) \subseteq F$ with $[F : K(x)] = 2$.*

Lemma 99

1. *A function field F/K of genus $g \geq 2$ is hyperelliptic iff there exists a divisor $A \in D_F$ with $\deg A = 2$ and $\dim A \geq 2$.*
2. *Any function field F/K of genus 2 is hyperelliptic.*

Proof:

1. Suppose that F/K is hyperelliptic. Choose an element $x \in F$ such that $[F : K(x)] = 2$, and consider the divisor $A := (x)_\infty$. Then $\deg A = [F : K(x)] = 2$, and the elements $1,\ x \in \mathcal{L}(A)$ are K-linearly independent, hence $\dim A \geq 2$.
   Conversely, assume that F/K has genus $g \geq 2$ and that $A \in D_F$ has $\deg A = 2$, $\dim A \geq 2$. There is a divisor $A_1 \geq 0$, $A_1 \sim A$, so that $\deg A_1 = 2$ and $\dim A_1 \geq 2$. Let us take an element $x \in \mathcal{L}(A_1) \setminus K$. Then $(x)_\infty \leq A_1$, and therefore $[F : K(x)] = \deg(x)_\infty \leq 2$. Since F/K is not rational, we conclude $[F : K(x)] = 2$.
2. Now a function field F/K of genus 2 is given. For any canonical divisor $W \in D_F$, we have $\deg W = 2g - 2 = 2$ and $\dim W = g = 2$. This implies, by 1., that F/K is hyperelliptic. ■

In the following Theorem it is described, without proof, the structure of hyperelliptic function field in the case of $\operatorname{char} K \neq 2$.

Theorem 100 *Assume* $\operatorname{char} K \neq 2$.

1. *Let F/K be a hyperelliptic function field of genus g. Then there exist $x, y \in F$ such that $F = K(x, y)$ and*
$$y^2 = f(x) \in K[x] \tag{3.7}$$
with a square-free polynomial $f(x)$ of degree $2g + 1$ or $2g + 2$.
2. *Conversely, if $F = K(x, y)$ and $y^2 = f(x) \in K[x]$ with a square-free polynomial $f(x)$ of degree $m > 4$, then F/K is hyperelliptic of genus*
$$g = \begin{cases} \frac{m-1}{2} & \text{if } m \equiv 1 \bmod 2, \\ \frac{m-2}{2} & \text{if } m \equiv 0 \bmod 2. \end{cases}$$
3. *Let $F = K(x, y)$ with $y^2 = f(x)$ as in Equation (3.7). Then the places $P \in \mathbb{P}_{K(x)}$ which ramify in $F/K(x)$ are the following:*

(a) all zeros of $f(x)$ *if* $\deg f \equiv 0 \bmod 2$*,*

(b) all zeros of $f(x)$ *and the pole of* x *if* $\deg f \equiv 1 \bmod 2$*.*

Hence if $f(x)$ *decomposes into linear factors, exactly* $2g+2$ *places of* $K(x)$ *are ramified in* $F/K(x)$*.*

3. Tame Cyclic Extensions of the Rational Function Fields

Let us characterize algebraic function fields $F = K(x, y)$ which are defined by an equation

$$y^n = a \prod_{i=1}^{s} (p_i(x))^{n_i} \tag{3.8}$$

with $s \in \mathbb{N}$ pairwise distinct irreducible monic polynomials $p_i(x) \in K[x]$, $0 \neq a \in K$ and $0 \neq n_i \in \mathbb{Z}$. We shall assume for brevity that

$$\operatorname{char} K \not| \, n \text{ and } \gcd(n, n_i) = 1 \text{ for } 1 \leq i \leq s. \tag{3.9}$$

Let us describe, without proof, the structure of this field extension.

Lemma 101 *Suppose that $F = K(x, y)$ is defined by Equations (3.8), (3.9). Then*

1. *K is the full constant field of F, and $[F : K(x)] = n$. If K contains a primitive n-th root of unity, $F/K(x)$ is cyclic.*
2. *Let P_i (resp. P_∞) denote the zero of $p_i(x)$ (resp. the pole of $0 \neq x \in F$) in $K(x)$. The places $P_1, \ldots, P_s$ are totally ramified in $F/K(x)$. All places $Q_\infty \in \mathbb{P}_F$ with $Q_\infty | P_\infty$ have ramification index $e(Q_\infty | P_\infty) = \frac{n}{d}$ where*

$$d := \gcd\left(n, \sum_{i=i}^{s} n_i \deg p_i(x)\right). \tag{3.10}$$

   No places $P \in \mathbb{P}_{K(x)}$ other than $P_1, \ldots, P_s, P_\infty$ ramify in $F/K(x)$.

3. *The genus of F/K is*

$$g = \frac{n-1}{2}\left(-1 + \sum_{i=1}^{s} \deg p_i(x)\right) - \frac{d-1}{2},$$

   with d as in Equation (3.10).

Example 102 *Let $F = K(x, y)$ with $y^2 = \frac{x^m - b}{x^m - c}$, $b, c \in K \setminus \{0\}$, $b \neq c$, $\operatorname{char} K \not| \min$. Then the Equations (3.8), (3.9) hold and the Lemma 101 implies*

$$g = (n-1)(m-1).$$

Example 103 *The function field $F = K(x, y)$ with defining equation*

$$ax^m + by^n = c, \qquad a, b, c \in K \setminus \{0\}, \ \operatorname{char} K \not| \min$$

has genus

$$g = \frac{1}{2}((n-1)(m-1) + 1 - \gcd(m, n)).$$

Chapter 4

Algebraic Function Fields over Finite Constant Fields

Throughout this chapter, F denotes an algebraic function field of genus g whose full field of constants is the finite field $\mathbb{F}_q$.

1. The Zeta Function of a Function Field

Let us recall a divisor $A = \sum_{P \in \mathbb{P}_F} a_P P,\ a_P \in \mathbb{Z}$, is positive if all $a_P \geq 0$; we write $A \geq 0$.

Lemma 104 *For any $n \geq 0$, there exist only finitely many positive divisors of degree n.*

Proof: A positive divisor is a sum of prime divisors. Hence it is sufficient to prove that the set $S := \{P \in \mathbb{P}_F : \deg P \leq n\}$ is finite. We choose an element of $x \in F/\mathbb{F}_q$ and consider the set $S_0 := \{P_0 \in \mathbb{P}_{\mathbb{F}_q(x)} | \deg P_0 \leq n\}$. Obviously $P \cap \mathbb{F}_q(x) \in S_0$ for any $P \in S$, and any $P_0 \in S_0$ has only finitely many extensions in F. Therefore we have only to show that S_0 is finite. Since the places of $\mathbb{F}_q(x)$ (except the pole of x) correspond to irreducible monic polynomials $p(x) \in \mathbb{F}_q[x]$ of the same degree and the finiteness of S_0 follows (?) ∎

Let us recall some notation: P_F denotes the subgroup of D_F of principal divisors $(x) = \sum_{P \in \mathbb{P}_F} v_P(x) P$ $(0 \neq x \in F,\ v_P(x) \in \mathbb{Z})$. The factor group $C_F := D_F/P_F$ is called divisor class group of $F/\mathbb{F}_q$. Two divisors $A, B \in D_F$ are equivalent, $A \sim B$, if $B = A + (x)$ for some principal divisor $(x) \in P_F$. The class of A in the divisor class group C_F is denoted $[A]$, i.e. $A \sim B \Leftrightarrow A \in [B] \Leftrightarrow B \in [A] \Leftrightarrow [A] = [B]$. Moreover, equivalent divisors have the same degree and dimension, so

$$\deg[A] := \deg A,\ \dim[A] := \dim A$$

are well defined for a divisor class $[A] \in C_F$.

Definition 105 *The set*

$$D_F^0 := \{A \in D_F \mid \deg A = 0\},$$

which is obviously a subgroup of D_F, is called the group of divisors of degree zero, and

$$C_F^0 := \{[A] \in C_F \mid \deg[A] = 0\}$$

is the group of divisor classes of degree zero (C_F^0 is the group of $\mathbb{F}_q$-rational points of the Jacobian).

Lemma 106 *C_F^0 is a finite group. Its order $h = h_F$ is called the class number of $F/\mathbb{F}_q$, i.e. $h := h_F := \operatorname{ord} C_F^0$.*

Proof: Choose a divisor $B \in D_F$ of degree $\geq g$, say $n := \deg B$, and consider the set of divisor classes

$$C_F^n := \{[C] \in C_F \mid \deg[C] = n\}.$$

The map

$$\begin{cases} C_F^0 & \longrightarrow & C_F^n \\ [A] & \longrightarrow & [A+B] \end{cases}$$

is bijective (this is trivial), so we only have to verify that C_F^n is finite. We claim that for any divisor class $[C] \in C_F^n$, there exists a divisor $A \in [C]$ with $A \geq 0$. In fact, since $\deg C = n \geq g$, we have

$$\dim[C] \geq n + 1 - g \geq 1$$

by the Riemann-Roch Theorem 84, and the assertion follows from the fact that if $A \in D_F$, $\deg A \geq 0$, $\dim A \geq 1$, then there is $A_1 \sim A$, $A_1 \geq 0$. By the Lemma 104 there are only finitely many divisors $A \geq 0$ of degree n, so the claim implies (?) of C_F. ■

We define the integer $\partial > 0$ by

$$\partial := \min\{\deg A \mid A \in D_F \text{ and } \deg A > 0\}.$$

The image of the degree map $\deg : D_F \to \mathbb{Z}$ is the subgroup of $\mathbb{Z}$ generated by ∂, and the degree of any divisor of $F/\mathbb{F}_q$ is a multiple of ∂. Later on we shall prove $\partial = 1$. In what follows, we shall study the numbers

$$A_n := \#\{A \in D_F \mid A \geq 0 \text{ and } \deg A = n\}. \tag{4.1}$$

For instance, $A_0 = 1$ and A_1 is the number of places $P \in \mathbb{P}_F$ of degree one.

Lemma 107

1. *$A_n = 0$ if $\partial \not| \, n$.*
2. *For a fixed divisor class $[C] \in C_F$, we have*

$$\#\{A \in [C] \mid A \geq 0\} = \frac{1}{q-1}\left(q^{\dim[C]} - 1\right).$$

3. $\forall n \in \mathbb{N}$, $n \geq 2g-1$ *with* $\partial | n$*:*

$$A_n = \frac{h}{q-1}\left(q^{n+1-g}-1\right).$$

Proof:

1. Is trivial (by definition of ∂).
2. The conditions $A \in [C]$, $A \geq 0$ are equivalent to $A = (x) + C$ for some $x \in F$ with $(x) \geq -C$, i.e. $x \in \mathcal{L}(C) \setminus \{0\}$. There are exactly $q^{\dim[C]} - 1$ elements $x \in \mathcal{L}(C) \setminus \{0\}$, and two of them yield the same divisor iff they differ by an element of the full constant field $0 \neq \alpha \in \mathbb{F}_q$.
3. There are $h = h_F$ divisor classes of degree n, say $[C_1], \ldots, [C_h]$. By 2. and the Riemann-Roch Theorem 84,

$$\#\{A \in [C_j] \mid A \geq 0\} = \frac{1}{q-1}\left(q^{\dim[C_j]}-1\right) = \frac{1}{q-1}\left(q^{n+1-g}-1\right).$$

Any divisor of degree n lies in exactly one of the divisor classes $[C_1], \ldots, [C_h]$, hence

$$A_n = \sum_{j=1}^{h} \#\{A \in [C_j] \mid A \geq 0\} = \frac{h}{q-1}\left(q^{n+1-g}-1\right).$$

■

Definition 108 *The power series*

$$Z(t) := Z_F(t) := \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}[[t]],$$

where A_n is defined by Equation (4.1), is called the Zeta function of $F/\mathbb{F}_q$.

We shall show that this element of the ring of formal power series is convergent in the neighbourhood of $0 \in \mathbb{C}$.

Theorem 109 *The power series $Z(t) := \sum_{n=0}^{\infty} A_n t^n$ is convergent for $|t| < q^{-1}$. In this region, we have*

1. If $F/\mathbb{F}_q$ has genus $g = 0$, then

$$Z(t) = \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right) \tag{4.2}$$

2. If $g \geq 1$, then $Z(t) = G(t) + F(t)$ with

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg C \leq 2g-2} q^{\dim C} t^{\deg C}, \tag{4.3}$$

$$G(t) = \frac{h}{q-1}\left(q^{1-g}(qt)^{2g-2+\partial}\frac{1}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right). \tag{4.4}$$

Proof:

1. $g = 0$ Let us first prove that a function field of genus zero has class number $h = 1$, i.e. every divisor $A \in D_F$, $\deg A = 0$, is principal. This fact follows from the Riemann-Roch Theorem 84: as $0 > 2g - 2$, $\dim A = \deg A + 1 - g = 1$, and so we can find an element $0 \neq x \in F : (x) \geq -A$. Both divisors are of degree 0, hence $A + (x) = 0$ is a divisor of an element of constants of F, i.e. $A = -(x) = (x^{-1})$ is principal. Now Lemma 107 implies

$$\begin{aligned}\sum_{n=0}^{\infty} A_n t^n &= \sum_{n=0}^{\infty} A_{\partial n} t^{\partial n} = \sum_{n=0}^{\infty} \frac{1}{q-1}(q^{\partial n+1} - 1)t^{\partial n} \\ &= \frac{1}{q-1}\left(q\sum_{n=0}^{\infty}(qt)^{\partial n} - \sum_{n=0}^{\infty} t^{\partial n}\right) \\ &= \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right). \qquad (4.5)\end{aligned}$$

for $|qt| < 1$ (note that for $q > 1$ we have implication $|qt| < 1 \Rightarrow |t| < 1$).

2. $g \geq 1$. The calculation is quite analogous:

$$\begin{aligned}\sum_{n=0}^{\infty} A_n t^n &= \sum_{\deg C \geq 0} \#\{A \in [C] \mid A \geq 0\} t^{\deg C} \\ &= \sum_{\deg C \geq 0} \frac{q^{\dim C} - 1}{q-1} t^{\deg C} \\ &= \frac{1}{q-1} \sum_{0 \leq \deg C \leq 2g-2} q^{\dim C} t^{\deg C} \\ &\quad + \frac{1}{q-1} \sum_{\deg C > 2g-2} q^{\deg C - g + 1} t^{\deg C} \\ &\quad - \frac{1}{q-1} \sum_{\deg C \geq 0} t^{\deg C} \\ &= F(t) + G(t),\end{aligned}$$

with a polynomial

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg C \leq 2g-2} q^{\dim C} t^{\deg C} \qquad (4.6)$$

and a rational function

$$\begin{aligned}(q-1)G(t) &= \sum_{n=\frac{(2g-2)}{\partial}+1}^{\infty} h q^{n\partial + 1 - g} t^{n\partial} - \sum_{n=0}^{\infty} h t^{n\partial} \qquad (4.7) \\ &= h q^{1-g} (qt)^{2g-2+\partial} \frac{1}{1-(qt)^{\partial}} - h \frac{1}{1-t^{\partial}}.\end{aligned}$$

■

Corollary 110 *$Z(t)$ can be extended to a rational function on $\mathbb{C}$; it has a simple pole at $t = 1$.*

Proof: Obvious, since $\frac{1}{1-t^{\delta}}$ has a simple pole at $t = 1$. ■

Aim: We would like to study the behavior of the Zeta function of $F/\mathbb{F}_q$ under finite constant field extension.

Recall that an infinite product $\prod_{i=1}^{\infty}(1 + a_i)$ $(-1 \neq a_i \in \mathbb{C})$ is said to be convergent with limit $(0 \neq a_i \in \mathbb{C})$, if $\lim_{n\to\infty} \prod_{i=1}^{n}(1 + a_i) = a \neq 0$. The product is called absolutely convergent if $\sum_{i=1}^{\infty} |a_i| < \infty$. It is well-known, [RU], that the absolute convergence implies convergence of the product, and the limit of an absolutely convergent product is independent of the order of the factors. Moreover, if the product $\prod_{i=1}^{\infty}(1+a_i) = a$ is absolutely convergent, then $\prod_{i=1}^{\infty}(1 + a_i)^{-1}$ converge absolutely too, and $\lim_{n\to\infty} \prod_{i=1}^{n}(1 + a_i)^{-1} = a^{-1}$.

Lemma 111 *(Euler product) For $|t| < q^{-1}$, the Zeta function can be represented as an absolutely convergent product*

$$Z(t) = \prod_{p\in\mathbb{P}_F} \left(1 - t^{\deg P}\right)^{-1}. \tag{4.8}$$

In particular, $Z(t) \neq 0$ for $|t| < q^{-1}$.

Proof: The RHS of Equation (4.8) converges absolutely for $|t| < q^{-1}$, since

$$\sum_{p\in\mathbb{P}_F} |t|^{\deg P} \leq \sum_{n=0}^{\infty} A_n|t|^n < \infty$$

By Lemma 111. Each factor of Equation (4.8) can be expanded as geometric series:

$$\prod_{p\in\mathbb{P}_F} \left(1 - t^{\deg P}\right)^{-1} = \prod_{p\in\mathbb{P}_F} \sum_{n=0}^{\infty} t^{\deg(nP)} = \sum_{\substack{A\in D_F \\ A\geq 0}} t^{\deg A} = \sum_{n=0}^{\infty} A_n t^n = Z(t)$$

■

Let us fix an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ and consider the constant field extension $\overline{F} = F\overline{\mathbb{F}}_q$ of $F/\mathbb{F}_q$. For any $r \geq 1$ there is exactly one extension $\mathbb{F}_{q^r}/\mathbb{F}_q$, $[\mathbb{F}_{q^r} : \mathbb{F}_q] = r$, $\mathbb{F}_{q^r} \subseteq \overline{\mathbb{F}}_q$, and we set $F_r := F\mathbb{F}_{q^r} \subseteq \overline{F}$.

Lemma 112

1. *F_r/F is cyclic extension, $[F_r : F] = r$, i.e. F_r/F is Galois extension with a cyclic Galois group of order r. The Galois group Gal(F_r/F) is generated by Frobenius automorphism $\sigma : \alpha \mapsto \alpha^q$ $\forall\alpha \in \mathbb{F}_{q^r}$.*
2. *$\mathbb{F}_{q^r}$ is the full constant field of F_r.*
3. *$F_r/\mathbb{F}_{q^r}$ has the same genus as $F/\mathbb{F}_q$.*

Proof:

1. It is well known that $\mathbb{F}_{q^r}/\mathbb{F}_q$ is cyclic of degree r, and its Galois group is generated by the Frobenius map $\alpha \mapsto \alpha^q \ \forall \alpha \in \mathbb{F}_{q^r}$. Since $[F_r : F] = [\mathbb{F}_{q^r} : \mathbb{F}_q]$ by Theorem 113 , the assertion follows.

2., 3. follows from Theorem 113. ■

The following results are standard and can be found in [(?)]. Let $K' \supseteq K$ be an algebraic extension. The composition $F' := FK'$ is a function field over K'. It is not clear a priory, whether K' is the full constant field of FK'.

Theorem 113 *Let $F' = FK'$ be an algebraic constant field extension of F/K (finite or infinite). Then*

1. *K' is the full constant field of F'.*
2. *Any subset of F, linearly independent over K, remains so over K'.*
3. *$[F : K(x)] = [F' : K'(x)] \forall\ x \in F \setminus K$.*
4. *Let α be algebraic over K. Then $[K(\alpha) : K] = [F(\alpha) : F]$.*
5. *F'/F is unramified, and so* genus $(F'/K') =$ genus (F/K).

There is a simple polynomial identity. If $m \geq 1,\ r \geq 1\ (m, r \in \mathbb{N}),\ d = \gcd(m, r)$ then

$$\left(X^{\frac{r}{d}} - 1\right)^d = \prod_{\mu^r=1} (X - \mu^m)$$

where $\{\mu\}_r$ runs over all r-th roots of unity in $\mathbb{C}$. In fact, both sides of equation are monic polynomials of the same degree $(= r)$, and each $\frac{r}{d}$-th root of unity is a d-fold root of them. Hence the polynomials are equal and the substitution $X = t^{-m}$ yields

$$\left(1 - t^{\frac{mr}{d}}\right)^d = \prod_{\mu^r=1} (1 - (\mu t)^m).$$

Lemma 114 *Let $Z(t)$ (resp. $Z_r(t)$) denote the Zeta function of F (resp. $F_r = F\mathbb{F}_{q^r}$). Then $Z_r(t^r) = \prod_{\mu^r=1} Z(\mu t)\ \forall t \in \mathbb{C}$.*

Proof: It is sufficient to prove the result for $|t| < q^{-1}$. In this region the Euler product gives

$$Z_r(t^r) = \prod_{P \in \mathbb{P}_F} \prod_{P'|P} \left(1 - t^{r \deg P'}\right)^{-1}.$$

For a fixed place $P \in \mathbb{P}_F$, we denote $m := \deg P$ and $d = \gcd(r, m)$; then

$$\prod_{P'|P} \left(1 - t^{r \deg P'}\right) = \left(1 - t^{\frac{mr}{d}}\right)^d = \prod_{\mu^r=1} (1 - (\mu t)^m) = \prod_{\mu^r=1} \left(1 - (\mu t)^{\deg P}\right)$$

and finally

$$Z_r(t^r) = \prod_{\mu^r=1} \prod_{P \in \mathbb{P}_F} \left(1 - (\mu t)^{\deg P}\right)^{-1} = \prod_{\mu^r=1} Z(\mu t)$$

■

Corollary 115 $\partial = 1$.

Proof: For $\mu^\partial = 1$, we get ($\partial | \deg P \ \forall P \in \mathbb{P}_F$)

$$\begin{aligned} Z(\mu t) &= \prod_{P\in\mathbb{P}_F} \left(1-(\mu t)^{\deg P}\right)^{-1} = \prod_{P\in\mathbb{P}_F} \left(1-\mu^{\deg P} t^{\deg P}\right)^{-1} \\ &= \prod_{P\in\mathbb{P}_F} \left(1-t^{\deg P}\right)^{-1} = Z(t), \end{aligned}$$

therefore $Z_\partial(t^\partial) = \prod_{\mu^\partial=1} Z(\mu t) = Z^\partial(\mu t)$ by Lemma 114. The rational function $Z_\partial(t^\partial)$ has a simple pole at $t = 1$ by Lemma (?) and $Z^\partial(t)$ has a pole of order ∂ (by the same Lemma (?)). Hence $\partial = 1$. ∎

Lemma 116

1. *Any function field $F/\mathbb{F}_q$ of genus 0 is rational, and its Zeta function is*

$$Z(t) = \frac{1}{(1-t)(1-qt)}.$$

2. *If $F/\mathbb{F}_q$ has genus $g \geq 1$, its Zeta function can be written in the form*

$$Z(t) = F(t) + G(t)$$

with

$$F(t) = \frac{1}{q-1} \sum_{0\leq \deg[C]\leq 2g-2} q^{\dim[C]} t^{\deg[C]}$$

and

$$G(t) = \frac{h}{q-1}\left(q^g t^{2g-1}\frac{1}{1-qt} - \frac{1}{1-t}\right).$$

Proof: The proof is trivial and is an immediate consequence of the previous results. ∎

Theorem 117 *(Functional Equation of the Zeta Function). The Zeta function of $F/\mathbb{F}_q$ satisfies the functional equation.*

$$Z(t) = q^{g-1} t^{2g-2} Z\left(\frac{1}{qt}\right).$$

Proof:

1. For $g = 0$ it is trivial.

2. For $g \geq 1$, we write $Z(t) = F(t) + G(t)$. For W a canonical divisor of F, we get

$$(q-1)F(t) = \sum_{0\leq \deg[C]\leq 2g-2} q^{\dim[C]} t^{\deg[C]}$$

$$\begin{aligned}
&= \sum_{0\le \deg[C]\le 2g-2} q^{\deg[C]+1-g+\dim[W-C]} t^{\deg[C]} \\
&= q^{g-1}t^{2g-2} \sum_{0\le \deg[C]\le 2g-2} q^{\deg[C]-(2g-2)+\dim[W-C]} t^{\deg[C]-(2g-2)} \\
&= q^{g-1}t^{2g-2} \sum_{0\le \deg[C]\le 2g-2} q^{\dim[W-C]} \left(\frac{1}{qt}\right)^{\deg[W-C]} \\
&= q^{g-1}t^{2g-2}(q-1)F\left(\frac{1}{qt}\right),
\end{aligned}$$

where we used $\deg(W) = 2g-2$ and, if $[C]$ runs over all divisor classes $0 \le \deg[C] \le 2g-2$, so does $[W-C]$.
For the function $G(t)$ we obtain

$$\begin{aligned}
q^{g-1}t^{2g-2}G\left(\frac{1}{qt}\right) &= \frac{h}{q-1}q^{g-1}t^{2g-2}\left(q^g\left(\frac{1}{qt}\right)^{2g-1}\frac{1}{1-q\frac{1}{qt}} - \frac{1}{1-\frac{1}{qt}}\right) \\
&= \frac{h}{q-1}\left(\frac{1}{t}\frac{1}{1-\frac{1}{t}} - \frac{q^g t^{2g-1}}{qt\left(1-\frac{1}{qt}\right)}\right) \\
&= G(t).
\end{aligned}$$

■

Definition 118 *The polynomial $L(t) \equiv L_F(t) := (1-t)(1-qt)Z(t)$ is called the L-polynomial of $F/\mathbb{F}_q$.*

It is clear from the Lemma 116 that $L(t)$ is a polynomial, $\deg L(t) \le 2g$, and it contains all information about the numbers $A_n (n \ge 0)$ since

$$L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n.$$

Theorem 119

1. *$L(t) \in \mathbb{Z}[t]$, $\deg(L(t)) = 2g$.*
2. *(Functional Equation)*
$$L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right).$$
3. *$L(1) = h$, the class number of $F/\mathbb{F}_q$.*
4. *Following 1., write $L(t) = a_0 + a_1 t + \ldots + a_{2g}t^{2g}$. Then*
   - *(a) $a_0 = 1,\ a_{2g} = q^g$.*
   - *(b) $a_{2g-i} = q^{g-i}a_i$ for $0 \le i \le g$*
   - *(c) $a_1 = N - (q+1)$, where N is the number of places $P \in \mathbb{P}_F$ of degree one.*

5. *$L(t)$ factors in the ring $\mathbb{C}[t]$ as*

$$L(t) = \prod_{i=1}^{2g}(1-\alpha_i t).$$

The complex numbers $\alpha_1, \ldots, \alpha_{2g}$ are algebraic integers, and they can be arranged in such a way that $\alpha_i \alpha_{i+g} = q$ holds for $i = 1, \ldots, g$.

6. *If $L_r(t) = (1-t)(1-q^r t)Z_r(t)$ denotes the L-polynomial of the constant field extension $F_r = F\mathbb{F}_{q^r}$, then*

$$L_r(t) = \prod_{i=1}^{2g}(1-\alpha_i^r t),$$

where α_i are given by

$$L(t) = \prod_{i=1}^{2g}(1-\alpha_i t).$$

Proof: We shall assume $g \geq 1$ because all assertions are trivial for $g = 0$.

1. We have already remarked $\deg(L(t)) \leq 2g$. In 4. we shall prove $a_{2g} = q^g$, i.e. $\deg(L(t)) = 2g$. The assertion $L(t) \in \mathbb{Z}[t]$ follows from

$$L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n$$

by comparing coefficients.

2. It follows immediately from the functional equation for Zeta function (Theorem 117).

3. We have

$$\begin{aligned} L(t) &= (1-t)(1-qt)F(t) + (1-t)(1-qt)G(t) \\ &= (1-t)(1-qt)F(t) + \frac{h}{q-1}\left(q^g t^{2g-1}(1-t) - (1-qt)\right). \end{aligned}$$

Because $F(t)$ is polynomial, we get $L(1) = h$.

4. Write $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g}$. The functional equation 2 yields

$$L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right) = \frac{a_{2g}}{q^g} + \frac{a_{2g-1}}{q^{g-1}} + \cdots + q^g a_0 t^{2g}.$$

Therefore $a_{2g-i} = q^{g-i} a_i$ for $i = 0, \ldots, g$ and 4b is proved. Comparing the coefficients of t^0 and t^1 in the equation $L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n$, we get $a_0 = A_0$, $a_1 = A_1 - (q+1)A_0$. Since, by definition, $A_0 = 1$ and $A_1 = N$, we obtain $a_0 = 1$ and $a_1 = N - (q+1)$. Finally, $a_{2g} = q^g a_0 = q^g$, which proves 4a.

5. Let us consider reciprocal polynomial

$$L^*(t) := t^{2g}L\left(\frac{1}{t}\right) = a_0t^{2g} + a_1t^{2g-1} + \cdots + a_{2g} = t^{2g} + a_1t^{2g-1} + \cdots + q^g. \tag{4.9}$$

$L^*(t)$ is a monic polynomial with coefficients in $\mathbb{Z}$, so its roots $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ are algebraic integers, and $L^*(t) = \prod_{i=1}^{2g}(t - \alpha_i)$. Hence

$$L(t) = t^{2g}L^*\left(\frac{1}{t}\right) = \prod_{i=1}^{2g}(1 - \alpha_i t).$$

Observe that the roots α_i of $L^*(t)$ are inverses of the roots of $L(t)$ since $L(\alpha_i^{-1}) = 0$. The functional equation (4.2) implies $L^*(\alpha) = 0 \Leftrightarrow L^*\left(\frac{q}{\alpha}\right) = 0$, and we arrange the roots of $L^*(t)$ as

$$\alpha_1, \frac{q}{\alpha_1}, \ldots, \alpha_k, \frac{q}{\alpha_k}, \underbrace{q^{\frac{1}{2}}, \ldots, q^{\frac{1}{2}}}_{\text{m } times}, \underbrace{-q^{\frac{1}{2}}, \ldots, -q^{\frac{1}{2}}}_{\text{n } times}.$$

By Equation (4.9),

$$\alpha_1 \frac{q}{\alpha_1} \cdots \alpha_k \frac{q}{\alpha_k} \left(q^{\frac{1}{2}}\right)^m \left(-q^{\frac{1}{2}}\right)^n = q^g,$$

and so n is even. Since $n + m + 2k = 2g$, m is also even. This implies that we can rearrange $\alpha_1, \ldots, \alpha_{2g}$ such that $\alpha_i\alpha_{g+i} = q$ holds for $i = 1, \ldots, g$.

6. By Lemma 114

$$\begin{aligned}
L_r(t^r) &= (1 - t^r)(1 - q^rt^r) Z_r(t^r) = (1 - t^r)(1 - q^rt^r) \prod_{\mu^r=1} Z(\mu t) \\
&= (1 - t^r)(1 - q^rt^r) \prod_{\mu^r=1} \frac{L(\mu t)}{(1 - \mu t)(1 - q\mu t)} = \prod_{\mu^r=1} L(\mu t) \\
&= \prod_{i=1}^{2g} \prod_{\mu^r=1} (1 - \alpha_i \mu t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t^r), \qquad (4.10)
\end{aligned}$$

Hence

$$L_r(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t).$$

■

This Theorem implies that the number

$$N(F) := N = \#\{P \in \mathbb{P}_F \mid \deg P = 1\} \tag{4.11}$$

can be calculated if the L-polynomial $L(t)$ of $F/\mathbb{F}_q$ is known. More generally, we consider for $r \geq 1$ the number

$$N_r := N(F_r) = \#\{P \in \mathbb{P}_F \mid \deg P = 1\}, \tag{4.12}$$

where $F_r = F\mathbb{F}_{q^r}$ is the constant field extension of $F/\mathbb{F}_q$ of degree r.

Corollary 120 *For any $r \geq 1$,*

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r, \tag{4.13}$$

where $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ are reciprocal of the roots of $L(t)$.
In particular, since $N_1 = N(F)$, we have

$$N(F) = q + 1 - \sum_{i=1}^{2g} \alpha_i. \tag{4.14}$$

Proof: By Theorem 119, 4., $N_r - (q^r + 1)$ is the coefficient of t in the L-polynomial $L_r(t)$. On the other hand, since $L_r(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t)$, this coefficient is $-\sum_{i=1}^{2g} \alpha_i^r$. ■

In the case the numbers N_r are known for sufficiently many r, one can calculate the coefficients of $L(t)$ as follows.

Corollary 121 *Let $L(t) = \sum_{i=0}^{2g} a_i t^i$ be the L-polynomial of $F/\mathbb{F}_q$, and $S_r := N_r - (q^r + 1)$. Then*

1. $$\frac{L'(t)}{L(t)} = \sum_{r=1}^{\infty} S_r t^{r-1}. \tag{4.15}$$

2. *$a_0 = 1$, and*
$$i a_i = S_i a_0 + S_{i-1} a_1 + \cdots + S_1 a_{i-1} \tag{4.16}$$
for $i = 1, \ldots, g$.

Hence, given $N_1, \ldots, N_g$ we can determine $L(t)$ by Equation (4.16) and the equation $a_{2g-i} = q^{g-i} a_i$ (for $i = 0, \ldots, g$, see Theorem 119).

Proof:

1. Write $L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$ as in Theorem 119. Then
$$\begin{aligned} \frac{L'(t)}{L(t)} &= \sum_{i=1}^{2g} \frac{-\alpha_i}{(1 - \alpha_i t)} = \sum_{i=1}^{2g}(-\alpha_i) \sum_{r=0}^{\infty} (\alpha_i t)^r = \sum_{r=1}^{\infty} \left(\sum_{i=1}^{2g} (-\alpha_i^r) \right) t^{r-1} \\ &= \sum_{r=1}^{\infty} S_r t^{r-1} \end{aligned} \tag{4.17}$$
by the definition of S_r.

2. By Theorem 119, 4a we know $a_0 = 1$. It follows from 1
$$a_1 + 2a_2 t + \cdots + 2g a_{2g} t^{2g-1} = \left(a_0 + a_1 t + \cdots + a_{2g} t^{2g}\right) \sum_{r=1}^{\infty} S_r t^{r-1}.$$
The comparison of coefficients of $t^0, t^1, \ldots, t^{g-1}$ yields Equation (4.16). ■

2. The Hasse-Weil Theorem

We retain the notation of previous section, i.e. $F/\mathbb{F}_q$ is a function field of genus $g(F) = g$ over finite field $\mathbb{F}_q$, $Z_F(t) = \frac{L_F(t)}{(1-t)(1-qt)}$ its Zeta function, $\{\alpha_1, \dots, \alpha_{2g}\}$ the reciprocals of the roots of $L_F(t)$, $N_F = \#\{P \in \mathbb{P}_F | \deg P = 1\}$, $F_r = F\mathbb{F}_{q^r}$ is the constant field extension of degree r, $N_r = N(F_r)$. We are going to prove

Theorem 122 *(Hasse-Weil) The reciprocals of the roots of $L_F(t)$ satisfy*

$$|\alpha_i| = q^{\frac{1}{2}} \qquad \forall\ i = 1, \dots, 2g.$$

Remark 123 *The Hasse-Weil Theorem 122 is often referred to as the Riemann Hypothesis for Algebraic Function Fields. The Zeta Function $Z_F(t)$ is an analogue of the classical Riemann ζ-function*

$$\zeta(s) := \sum_{n=1}^{\infty} n^{-s} \qquad (s \in \mathbb{C},\ \mathrm{Re}(s) > 1) \tag{4.18}$$

in the following manner. Define the (absolute) norm of the divisor $A \in D_F$ by

$$N(A) := q^{\deg A}.$$

For instance, the (absolute) norm $N(P)$, $P \in \mathbb{P}_F$, is the cardinality of its residue class field F_P. Then

$$\zeta_F(s) := Z_F(q^{-s})$$

can be rewritten as

$$\zeta_F(s) = \sum_{n=0}^{\infty} A_n q^{-sn} = \sum_{\substack{A \in D_F, \\ A \geq 0}} N(A)^{-s}, \tag{4.19}$$

which is the appropriate analog of the number field case (4.18). The ζ-function (4.18) has an analytic continuation as a meromorphic function on $\mathbb{C}$. The classical Riemann hypothesis (still unproven!) states that - besides the so-called trivial zeros $s = -2,\ -4,\ -6, \dots$ - all zeros of $\zeta(s)$ lie on the line $\mathrm{Re}(s) = \frac{1}{2}$. In the function field case, the Hasse-Weil Theorem 122 states that

$$\zeta_F(s) = 0 \Longrightarrow Z_F(q^{-s}) = 0 \Longrightarrow |q^{-s}| = q^{-\frac{1}{2}}.$$

Since $|q^{-s}| = q^{-\mathrm{Re}(s)}$, this means $\zeta_F(s) = 0 \Rightarrow \mathrm{Re}(s) = \frac{1}{2}$.

Corollary 124 *(Hasse-Weil Bound) The number $N = N(F)$ of places of $F/\mathbb{F}_q$ of degree one can be estimated by*

$$|N - (q+1)| \leq 2gq^{\frac{1}{2}}$$

Proof: The result follows from Corollary (?)

$$N - (q+1) = -\sum_{i=1}^{2g} \alpha_i.$$

■

Note that Corollary 124 applied to the function field $F_r/\mathbb{F}_{q^r}$ gives

$$|N_r - (q^r + 1)| \leq 2gq^{\frac{r}{2}} \qquad \forall r \geq 1.$$

Lemma 125 *Let $m \geq 1$. The Hasse-Weil Theorem 122 holds for $F/\mathbb{F}_q$ iff it holds for (some) the constant field extension $F_m/\mathbb{F}_{q^m}$.*

Proof: The reciprocals of the roots of $L_F(t)$ are $\{\alpha_1, \ldots, \alpha_{2g}\}$. By Theorem (?) the reciprocals of the roots of $L_m(t)$ are $\{\alpha_1^m, \ldots, \alpha_{2g}^m\}$. The Lemma follows immediately from

$$|\alpha_i| = q^{\frac{1}{2}} \Longleftrightarrow |\alpha_i^m| = (q^m)^{\frac{1}{2}}.$$

■

Lemma 126 *Assume there is a $c \in \mathbb{R}$ such that, for any $r \geq 1$,*

$$|N_r - (q^r + 1)| \leq c q^{\frac{r}{2}}. \tag{4.20}$$

Then the Hasse-Weil Theorem 122 holds for $F/\mathbb{F}_q$.

Proof: By Corollary 124

$$N_r - (q^r + 1) = -\sum_{i=1}^{2g} \alpha_i^r,$$

i.e. by Equation (4.20)

$$\left| \sum_{i=1}^{2g} \alpha_i^r \right| \leq c q^{\frac{r}{2}} \qquad \forall r \geq 1. \tag{4.21}$$

consider the meromorphic function

$$H(t) := \sum_{i=1}^{2g} \frac{\alpha_i t}{1 - \alpha_i t}.$$

Let $\varrho := min \left\{ \left|\alpha_i^{-1}\right| |1 \leq i \leq 2g \right\}$, which is the convergence radius of power series expansion of $H(t)$ around t=0 (since $\alpha_1^{-1}, \ldots, \alpha_{2q}^{-1}$ are the only singularities of $H(t)$). On the other hand, we obtain for $|t| < \varrho$

$$H(t) = \sum_{i=1}^{2g} \sum_{r=1}^{\infty} (\alpha_i t)^r = \sum_{r=1}^{\infty} \left(\sum_{i=1}^{2g} \alpha_i^r \right) t^r.$$

By Equation (4.21) this series converges for $|t| < q^{-\frac{1}{2}}$, hence $q^{-\frac{1}{2}} \leq \varrho$. This implies $q^{\frac{1}{2}} \geq |\alpha_i|$ for $i = 1, \ldots, 2g$. Since, by Theorem (?), $\prod_{i=1}^{2g} \alpha_i := q^g$, we conclude that $|\alpha_i| = q^{\frac{1}{2}}$. ■

Observe that the inequalities 4.21 are equivalent to an upper and a lower bound for N_r: there exist constants $c_1 > 0,\ c_2 > 0$ such that

$$N_r \leq q^r + 1 + c_1 q^{\frac{r}{2}} \qquad \forall r \geq 1 \tag{4.22}$$
$$N_r \geq q^r + 1 - c_2 q^{\frac{r}{2}} \qquad \forall r \geq 1. \tag{4.23}$$

Therefore, using the Lemma 125, the Hasse-Weil Theorem 122 is equivalent to the proof of Equations (4.22), (4.23).

Proposition 127 *Suppose that $F/\mathbb{F}_q$ satisfies the following assumptions:*

1. *q is a square,*
2. *$q > (g+1)^4$.*

Then the number N=N(F) of places of $F/\mathbb{F}_q$ of degree one can be estimated by

$$N < (q+1) + (2g+1)q^{\frac{1}{2}}.$$

Proof: We can assume that there exists a place $Q \in \mathbb{P}_F$, $\deg Q = 1$ (otherwise is the assertion trivial (N=0)). Set

$$q_0 := q^{\frac{1}{2}},\ m := q_0 - 1,\ n := 2g + q_0.$$

Then

$$r := q-1+(2g+1)q^{\frac{1}{2}} = q_0^2-1+(n+1-q_0)q_0 = q_0^2-1+q_0-q_0^2+nq_0 = m+nq_0. \tag{4.24}$$

Let $\mathcal{T} := \{i | 0 \leq i \leq m : i \text{ is a pole number of } Q\}$. For every $i \in \mathcal{T}$, choose an element $u_i \in F$ with pole divisor iQ. Then the set $\{u_i | i \in \mathcal{T}\}$ is a basis of $L(mQ)$. We consider the space

$$L := L(mQ)L(nQ)^{q_0} \subseteq L(rQ).$$

Note that, by definition, L consists of all finite sums $\sum_\nu x_\nu y_\nu^{q_0}$ with $x_\nu \in L(mQ)$, $y_\nu \in L(nQ)$; obviously L is $\mathbb{F}_q$-vector space, an $L \subseteq L(rQ)$ by (4.24). Our aim is to construct $0 \neq x \in L$ such that

$$x(P) = 0 \qquad \forall P \in \mathbb{P}_F \text{ with } \deg P = 1,\ P \neq Q. \tag{4.25}$$

Suppose we have such and element x. Then all places, except Q, are the zeros of x, and the zero divisor $(x)_0$ has degree

$$\deg(x)_0 \geq N - 1. \tag{4.26}$$

As $x \in L \subseteq L(rQ)$,

$$\deg(x)_0 = \deg(x)_\infty \leq r = q - 1 + (2g+1)q^{\frac{1}{2}}. \tag{4.27}$$

Combining these inequalities, we get $N \leq q + (2g+1)q^{\frac{1}{2}}$, which proves the assertion of the Lemma. The main assertion (4.25) will be proved in several steps.

Claim 128 *Any $y \in L$ can be written uniquely in the form*

$$y = \sum_{i \in \mathcal{T}} u_i z_i^{q_0} \tag{4.28}$$

with $z_i \in L(nQ)$, $\{u_i | i \in \mathcal{T}\}$ is the above-mentioned basis of $L(mQ)$. The existence of a representation (4.28) follows immediately from the definition of L. In order to prove the uniqueness, we assume there is an equation

$$\sum_{i \in \mathcal{T}} u_i x_i^{q_0} = 0 \tag{4.29}$$

with $x_i \in L(nQ)$, not all $x_i = 0$ $(i \in \mathcal{T})$. For any index $i \in \mathcal{T}$, $x_i \neq 0$, we have $v_Q(u_i x_i^{q_0}) \equiv v_Q(u_i) \equiv -i \bmod q_0$. Since $m = q_0 - 1$, i.e. $q_0 = m+1$, the numbers $i \in \mathcal{T}$ are pair wise distinct modulo q_0. Therefore the Strict Triangle inequality for valuation v_Q yields $(m \geq 1 \Rightarrow q_0 \geq 2)$

$$v_Q\left(\sum_{i\in\mathcal{T}} u_i x_i^{q_0}\right) = \min\left\{v_Q\left(u_i x_i^{q_0}\right) \mid i \in \mathcal{T}\right\} \neq \infty.$$

This contradicts to (4.28), because $v_Q\left(\sum_{i\in\mathcal{T}} u_i x_i^{q_0}\right) = v_Q(0) = \infty$, and the Claim 128 is proved.

Let us consider the map $\lambda : L \to L((q_0 m + n)Q)$ given by $\lambda\left(\sum_{i\in\mathcal{T}} u_i z_i^{q_0}\right) := \sum u_i^{q_0} z_i$, $z_i \in L(nQ)$. By Claim 128, this map is well-defined. Observe that λ is not $\mathbb{F}_q$-linear, but it is a homomorphism of the additive group of L into $L((q_0 m + n)Q)$.

Claim 129 *The kernel of λ is not $\{0\}$.*
As $\lambda : L \to L((q_0 m + n)Q)$ is a homomorphism, it is sufficient to prove

$$\dim_{\mathbb{F}_q} L > \dim_{\mathbb{F}_q} L((q_0 m + n)Q). \tag{4.30}$$

By Claim 128 and the Riemann-Roch Theorem,

$$\dim_{\mathbb{F}_q} L = \dim_{\mathbb{F}_q} L(mQ) \dim_{\mathbb{F}_q} L(nQ) \geq (m+1-g)(n+1-g).$$

On the other hand, since

$$q_0 m + n = q_0(q_0 - 1) + (2g + q_0) = 2g + q > 2g - 2,$$

we obtain

$$\dim_{\mathbb{F}_q} L((q_0 m + n)Q) = (2g + q) - g + 1 = g + q + 1.$$

Hence (4.30) follows from the inequality

$$(m+1-g)(n+1-g) > g + q + 1. \tag{4.31}$$

This inequality is the consequence of the set of equivalences

$$\begin{aligned} & (m+1-g)(n+1-g) > g+q+1 \\ \Leftrightarrow\quad & (q_0 - g)(2g + q_0 + 1 - g) > g + q + 1 \\ \Leftrightarrow\quad & q - g^2 + q_0 - g > g + q + 1 \\ \Leftrightarrow\quad & q_0 > g^2 + 2g + 1 = (g+1)^2 \\ \Leftrightarrow\quad & q > (g+1)^4 \end{aligned}$$

which we assumed in the formulation of the Proposition, i.e. Equation (4.31) is proved and the Claim 129 follows.

Claim 130 *Let $0 \neq x \in L$ be an element in $\mathrm{Ker}(\lambda)$ and $P \neq Q$ be a place of degree one. Then $x(P) = 0$.*
Note that $y(P) \neq \infty$ for any $y \in L$ because Q is the only pole of $y \in F/\mathbb{F}_q$. More over, since $\mathbb{F}_q$ is the residue class field of P, we have $y(P)^q = y(P)$. Now we consider an element $x \in L$ with $\lambda(x) = 0$. We write $x = \sum_{i\in\mathrm{T}} u_i z_i^{q_0}$ and

obtain

$$\begin{aligned} x(P)^{q_0} &= \left(\sum_{i\in \mathrm{T}} u_i(P) z_i(P)^{q_0}\right)^{q_0} = \sum_{i\in \mathrm{T}} u_i^{q_0}(P) z_i(P)^q \\ &= \left(\sum_{i\in \mathrm{T}} u_i^{q_0} z_i\right)(P) = \lambda(x)(P) = 0 \bmod \mathbb{F}_{q_0}, \end{aligned}$$

i.e. $x(P) = x(P)^{q_0} = 0$ *and the Claim 130 is proved.*

This finally proves the Proposition. ■

The second inequality, i.e. the lower Gound of Hasse-Weil Theorem, will not be proved.