Algebraic Function Fields over Finite Fields

Tutorial Lecture Notes
Institute for Mathematical Sciences
National University of Singapore
July 2001

Harald Niederreiter

National University of Singapore

1. Introduction

The following is a rough definition (in the language of field theory): an *algebraic function field* (in one variable) is a finite extension of a rational function field (in one variable). If the rational function field is over a field k, then we speak of an algebraic function field over k. A rigorous definition will be given in Chapter 6.

Many fundamental aspects of the theory of algebraic function fields are analogous to the theory of algebraic number fields, i.e., of the finite extensions of the field $\mathbf{Q}$ of rational numbers. Historically, the theory of algebraic function fields is a creation of the 19th century and the early 20th century. Fundamental contributions to this theory were made by B. Riemann, G. Roch, D. Hilbert, A. Hurwitz, E. Artin, F.K. Schmidt, H. Hasse, A. Weil, and C. Chevalley.

Algebraic function fields over finite fields allow important applications to coding theory, cryptography, and the construction of low-discrepancy sequences (see [2] for these applications). An algebraic function field over a finite field is also called a *global function field.*

A field is called a *global field* if it is either a global function field or an algebraic number field. A classical monograph on global fields is [5].

2. Finite Fields

A *finite field* is a field with finitely many elements. The cardinality of a finite field is called its *order*. For a general treatment of finite fields we refer to [1] where also the proofs of all theorems in this chapter can be found.

2.1. Example. For every positive integer m we can consider the residue class ring $\mathbf{Z}_m := \mathbf{Z}/m\mathbf{Z}$ of the integers modulo m. The ring $\mathbf{Z}_m$ is a field if and only if m is a prime number. Thus, for every prime number p we have a finite field $\mathbf{Z}_p$ of order p. Note that $\mathbf{Z}_p$ is a finite prime field, i.e., it has no proper subfields. As a set, we can identify $\mathbf{Z}_p$ with $\{0, 1, \ldots, p-1\}$.

Any finite field $\mathbf{F}$ has a uniquely determined prime characteristic p (thus $p \cdot 1 = 0$ in $\mathbf{F}$) and the order of $\mathbf{F}$ is p^n, where n is the dimension of $\mathbf{F}$ as a vector space over its finite prime field (which is isomorphic to $\mathbf{Z}_p$).

Conversely, for every prime power $q = p^n$ there does indeed exist a finite field of order q. Such a finite field can be explicitly constructed as follows. Take the prime number p and an irreducible polynomial $f \in \mathbf{Z}_p[x]$ of degree n (it can be shown that such an f exists). Then the residue class ring $\mathbf{Z}_p[x]/(f)$ is a finite field of order $p^n = q$.

2.2. Theorem. *Any two finite fields of the same order are isomorphic as fields.*

In this sense, it is meaningful to speak of *the* finite field $\mathbf{F}_q$ of prime-power order q. Some authors use the term *Galois field* $\mathrm{GF}(q)$, in recognition of the pioneering work of Galois in this area.

The finite field $\mathbf{F}_q$ of characteristic p may be viewed as the splitting field of the polynomial $x^q - x$ over $\mathbf{Z}_p$. In fact, $\mathbf{F}_q$ consists exactly of all roots of this polynomial.

2.3. Theorem. *Every subfield of $\mathbf{F}_q$, $q = p^n$, has order p^d with a positive divisor d of n. Conversely, if d is a positive divisor of n, then there is a unique subfield of $\mathbf{F}_q$ of order p^d.*

2.4. Example. Let $q = 2^{12}$. Then the subfields of $\mathbf{F}_q$ have the orders $2^1, 2^2, 2^3, 2^4, 2^6, 2^{12}$.

The roots of irreducible polynomials over a finite field are simple and enjoy a special relationship among themselves.

2.5. Theorem. *The roots of an irreducible polynomial over $\mathbf{F}_q$ of degree m are given by the m distinct elements*

$$\alpha^{q^j} \in \mathbf{F}_{q^m}, \quad j = 0, 1, \ldots, m-1,$$

where α is a fixed root.

It follows that any finite extension $\mathbf{F}_{q^m}/\mathbf{F}_q$ is a Galois extension with a cyclic Galois group generated by the *Frobenius automorphism*

$$\sigma(\beta) = \beta^q \quad \text{for all } \beta \in \mathbf{F}_{q^m}.$$

A famous classical theorem describes the multiplicative structure of $\mathbf{F}_q$.

2.6. Theorem. *The multiplicative group $\mathbf{F}_q^*$ of nonzero elements of $\mathbf{F}_q$ is cyclic.*

2.7. Definition. A generator of the cyclic group $\mathbf{F}_q^*$ is called a *primitive element* of $\mathbf{F}_q$.

2.8. Example. 2 is a primitive element of $\mathbf{F}_{11} = \mathbf{Z}_{11}$ since $2^{10} = 1$ in $\mathbf{F}_{11}$ by Fermat's theorem, but $2^1 = 2 \neq 1$, $2^2 = 4 \neq 1$, $2^5 = 32 = 10 \neq 1$ in $\mathbf{F}_{11}$.

3. Valued Fields

3.1. Example. Let $\mathbf{Q}$ be the field of rational numbers and take a prime number p. Using unique factorization in $\mathbf{Z}$, we can write every nonzero $r \in \mathbf{Q}$ in the form

$$r = p^m \frac{a}{b}$$

with a unique $m \in \mathbf{Z}$, where p does not divide the nonzero integers a and b. Then we define

$$|r|_p = p^{-m}.$$

We also set $|0|_p = 0$. The map $|\cdot|_p : \mathbf{Q} \to \mathbf{R}_{\geq 0}$ has the following properties:

(i) $|r|_p = 0$ if and only if $r = 0$;
(ii) $|rs|_p = |r|_p\,|s|_p$ for all $r, s \in \mathbf{Q}$;
(iii) $|r + s|_p \leq \max(|r|_p, |s|_p) \leq |r|_p + |s|_p$ for all $r, s \in \mathbf{Q}$.

The properties (i) and (ii) are trivial. To prove (iii), let $r, s \in \mathbf{Q}^*$ and write as above

$$r = p^m\,\frac{a}{b}, \quad s = p^n\,\frac{c}{d},$$

where w.l.o.g. $m \leq n$. Then

$$r + s = p^m\,\frac{a}{b} + p^n\,\frac{c}{d} = p^m\,\frac{ad + p^{n-m}bc}{bd},$$

and so

$$|r + s|_p \leq p^{-m} = \max(|r|_p, |s|_p).$$

The map $|\cdot|_p$ is called the (normalized) *p-adic absolute value* on $\mathbf{Q}$. There is another obvious map on $\mathbf{Q}$ satisfying (i), (ii), and the inequality (iii) in the wider sense, namely the ordinary absolute value $|\cdot|$. Any map on $\mathbf{Q}$ satisfying (i), (ii), (iii) (again in the wider sense), and having at least one value $\neq 1$ on $\mathbf{Q}^*$ is called an *absolute value* on $\mathbf{Q}$.

It is a well-known theorem that any absolute value on $\mathbf{Q}$ is equivalent (in the sense of one being a power of the other) to either $|\cdot|$ or $|\cdot|_p$ for some prime number p (see [3, Section 1.3] and [5, Section 1-4]). For any $r \in \mathbf{Q}^*$ we have

$$|r| \cdot \prod_p |r|_p = 1,$$

where the product is over all prime numbers p. This product formula is typical for global fields. To verify this product formula, note that everything on the left-hand side is multiplicative, and so it suffices to consider a nonzero integer r with canonical factorization

$$r = \pm p_1^{m_1} \cdots p_k^{m_k},$$

say. Then $|r|_{p_i} = p_i^{-m_i}$ for $1 \leq i \leq k$ and $|r|_p = 1$ for all other primes p. Therefore

$$|r| \cdot \prod_p |r|_p = p_1^{m_1} \cdots p_k^{m_k} \cdot p_1^{-m_1} \cdots p_k^{-m_k} = 1.$$

Let us now concentrate on $|\cdot|_p$. For all $r \in \mathbf{Q}^*$ we set

$$\nu_p(r) = -\log_p |r|_p = m$$

in the earlier notation. We also put $\nu_p(0) = \infty$. The map $\nu_p : \mathbf{Q} \to \mathbf{Z} \cup \{\infty\}$ has the following properties:

(i) $\nu_p(r) = \infty$ if and only if $r = 0$;
(ii) $\nu_p(rs) = \nu_p(r) + \nu_p(s)$ for all $r, s \in \mathbf{Q}$;
(iii) $\nu_p(r + s) \geq \min(\nu_p(r), \nu_p(s))$ for all $r, s \in \mathbf{Q}$;
(iv) $\nu_p(\mathbf{Q}^*) \neq \{0\}$.

This example gives rise to the following general concept.

3.2. Definition. Let K be an arbitrary field. A (nonarchimedean) *valuation* of K is a map $\nu : K \to \mathbf{R} \cup \{\infty\}$ which satisfies:

(i) $\nu(x) = \infty$ if and only if $x = 0$;
(ii) $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in K$;
(iii) $\nu(x + y) \geq \min(\nu(x), \nu(y))$ for all $x, y \in K$;
(iv) $\nu(K^*) \neq \{0\}$.

If the image $\nu(K^*)$ is a discrete set in $\mathbf{R}$, then ν is called *discrete*. If $\nu(K^*) = \mathbf{Z}$, then ν is called *normalized*. The ordered pair (K, ν) is called a *valued field*. Property (iv) excludes what is sometimes called the trivial valuation of K, which is ∞ at $0 \in K$ and 0 on K^*.

Obviously, ν_p is a (discrete) normalized valuation of $\mathbf{Q}$ for every prime number p. We call ν_p the *p-adic valuation* of $\mathbf{Q}$.

We will be interested only in discrete valuations. In the following, let (K, ν) be a valued field.

3.3. Lemma. (i) $\nu(1) = \nu(-1) = 0$;
(ii) $\nu(-x) = \nu(x)$ *for all* $x \in K$;
(iii) $\nu(xy^{-1}) = \nu(x) - \nu(y)$ *for all* $x \in K, y \in K^*$.

Proof. (i) $1^2 = 1 \Rightarrow 2\nu(1) = \nu(1) \Rightarrow \nu(1) = 0$; and $(-1)^2 = 1 \Rightarrow 2\nu(-1) = \nu(1) = 0 \Rightarrow \nu(-1) = 0$. In both cases, property (ii) in Definition 3.2 was used.
(ii) $\nu(-x) = \nu((-1) \cdot x) = \nu(-1) + \nu(x) = \nu(x)$.
(iii) $0 = \nu(1) = \nu(yy^{-1}) = \nu(y) + \nu(y^{-1}) \Rightarrow \nu(y^{-1}) = -\nu(y)$. The result follows again from property (ii) in Definition 3.2. □

3.4. Proposition. *If $x, y \in K$ with $\nu(x) \neq \nu(y)$, then*

$$\nu(x + y) = \min(\nu(x), \nu(y)).$$

Proof. Suppose w.l.o.g. $\nu(x) < \nu(y)$. Then $\nu(x+y) \geq \nu(x)$ by property (iii) in Definition 3.2. If we had $\nu(x+y) > \nu(x)$, then by the same property and Lemma 3.3(ii),

$$\begin{aligned} \nu(x) &= \nu((x+y)-y) \geq \min(\nu(x+y), \nu(-y)) \\ &= \min(\nu(x+y), \nu(y)) > \nu(x), \end{aligned}$$

a contradiction. □

3.5. Example. Here is a simple illustration of Proposition 3.4. Let $K = \mathbf{Q}$ and ν the p-adic valuation of $\mathbf{Q}$. Take nonzero $x, y \in \mathbf{Z}$. Then we can write $x = p^m a$ and $y = p^n c$ with a and c not divisible by p. Suppose $\nu(x) = m < \nu(y) = n$. Then

$$x + y = p^m a + p^n c = p^m(a + p^{n-m}c)$$

with $a + p^{n-m}c \equiv a \not\equiv 0 \pmod{p}$. Therefore

$$\nu(x+y) = m = \min(\nu(x), \nu(y)).$$

General references for valued fields are [3] and [5].

4. Places and Valuation Rings

All valuations in this chapter are discrete.

Two valuations ν and μ of the field K are called *equivalent* if there exists a constant $c > 0$ such that

$$\nu(x) = c\mu(x) \quad \text{for all } x \in K.$$

Obviously, this yields an equivalence relation between valuations of K. An equivalence class of valuations of K is called a *place* of K.

Since $\nu(K^*)$ is a nonzero discrete subgroup of $(\mathbf{R}, +)$, we have $\nu(K^*) = \alpha\mathbf{Z}$ for some positive $\alpha \in \mathbf{R}$. Thus, there exists a uniquely determined normalized valuation of K that is equivalent to ν. In other words, every place P of K contains a uniquely determined normalized valuation of K, which is denoted by ν_P. Thus, we can identify places of K and (discrete) normalized valuations of K.

4.1. Definition. Let P be a place of K. Then

$$O_P := \{x \in K : \nu_P(x) \geq 0\}$$

is called the *valuation ring* of P.

Using the properties of valuations in Chapter 3, we see that O_P is an integral domain with $1 \in O_P$.

4.2. Proposition. *The multiplicative group of units of* O_P *is given by*

$$U_P := \{x \in K : \nu_P(x) = 0\}.$$

Proof. For $x \in O_P$ we have: x is a unit of $O_P \Leftrightarrow x^{-1} \in O_P \Leftrightarrow \nu_P(x^{-1}) \geq 0 \Leftrightarrow \nu_P(x) \leq 0 \Leftrightarrow \nu_P(x) = 0$. □

4.3. Proposition. O_P *has a unique maximal ideal given by*

$$\mathsf{M}_P := \{x \in K : \nu_P(x) > 0\}.$$

Proof. It is trivial that M_P is an ideal of O_P. Let J with $\mathsf{M}_P \subset \mathsf{J} \subseteq O_P$ be an ideal of O_P. Take $x \in \mathsf{J} \setminus \mathsf{M}_P$, then $\nu_P(x) = 0$ and x is a unit of O_P by Proposition 4.2. Thus $1 = xx^{-1} \in \mathsf{J}$, hence $\mathsf{J} = O_P$, and so M_P is maximal. Finally, let $\mathsf{M} \subset O_P$ be an arbitrary maximal ideal of O_P. Since M cannot contain a unit of O_P, we must have $\mathsf{M} \subseteq \mathsf{M}_P$, and so $\mathsf{M} = \mathsf{M}_P$. □

M_P is in fact a principal ideal: take any $t \in O_P$ with $\nu_P(t) = 1$, then it is easy to check that $\mathsf{M}_P = tO_P$. Such a t is called a *local parameter* at P.

4.4. Definition. The field O_P/M_P is called the *residue class field* of P. The ring homomorphism

$$x \in O_P \mapsto x + \mathsf{M}_P \in O_P/\mathsf{M}_P$$

is called the *residue class map* of P.

4.5. Example. Let ν_p be the p-adic valuation of $\mathbf{Q}$ (see Chapter 3), which is a normalized valuation of $\mathbf{Q}$. In the following, we write all rational numbers a/b in reduced form, i.e., $\gcd(a, b) = 1$. It is easy to see that

$$\begin{aligned} O_p &= \{\frac{a}{b} \in \mathbf{Q} : \gcd(b, p) = 1\}, \\ U_p &= \{\frac{a}{b} \in \mathbf{Q} : \gcd(a, p) = \gcd(b, p) = 1\}, \\ \mathsf{M}_p &= \{\frac{a}{b} \in \mathbf{Q} : p|a\}. \end{aligned}$$

For any $b \in \mathbf{Z}$ we write $\overline{b}$ for the residue class of b modulo p. If $\gcd(b, p) = 1$, then $\overline{b} \in \mathbf{Z}_p = \mathbf{Z}/p\mathbf{Z}$ has a multiplicative inverse $\overline{b}^{-1} \in \mathbf{Z}_p$. The map $\psi : O_p \to \mathbf{Z}_p$ given by

$$\psi(\frac{a}{b}) = \overline{a}\overline{b}^{-1} \in \mathbf{Z}_p \quad \text{for all } \frac{a}{b} \in O_p$$

is well defined. Clearly, ψ is a surjective ring homomorphism with kernel M_p, and so the residue class field O_p/M_p is isomorphic to the finite field $\mathbf{Z}_p$.

4.6. Remark. Valuation rings in K can be characterized purely algebraically as the maximal proper Noetherian subrings of K, or also as the maximal proper principal ideal domains contained in K (see [3, Section 2.1]). This provides an alternative approach to the concept of a place.

The proof of the following theorem can be found in [3, Section 2.1] and [5, Section 1-2].

4.7. Theorem (Weak Approximation Theorem). *Let $P_1, \dots, P_n$ be distinct places of K. Then for any given elements $x_1, \dots, x_n \in K$ and integers $m_1, \dots, m_n$, there exists an element $x \in K$ such that*

$$\nu_{P_i}(x - x_i) \geq m_i \quad \textit{for } i = 1, \dots, n.$$

4.8. Example. Let $K = \mathbf{Q}$. Choosing n distinct places of K means choosing distinct primes $p_1, \dots, p_n$. Let $x_1, \dots, x_n \in \mathbf{Z}$ and take positive integers $m_1, \dots, m_n$. Then by the Chinese remainder theorem there exists an $x \in \mathbf{Z}$ with

$$x \equiv x_i \pmod{p_i^{m_i}} \quad \text{for } i = 1, \dots, n.$$

This just means that

$$\nu_{p_i}(x - x_i) \geq m_i \quad \text{for } i = 1, \dots, n.$$

Thus, the weak approximation theorem can be viewed as an analog of the Chinese remainder theorem for K.

5. Rational Function Fields

Let k be an arbitrary field and let $k(x)$ be the rational function field over k in the variable x (in strict algebraic terms, x is transcendental over k). In this context, k is called the *constant field* of $k(x)$. The elements of $k(x)$ can be represented as $f(x)/g(x)$ with $f(x), g(x) \in k[x]$, $g(x) \neq 0$, $\gcd(f(x), g(x)) = 1$.

Valuations of $k(x)$ can be constructed in an analogous way as for $\mathbf{Q}$ (compare with Chapter 3). The role of the prime numbers is now played by irreducible polynomials. Fix a monic irreducible polynomial $p(x) \in k[x]$. Using unique factorization in $k[x]$, we can write every nonzero $r(x) \in k(x)$ in the form

$$r(x) = p(x)^m \frac{f(x)}{g(x)}$$

with a unique $m \in \mathbf{Z}$, where $p(x)$ does not divide the nonzero polynomials $f(x)$ and $g(x)$. Then we put

$$\nu_{p(x)}(r(x)) = m.$$

We also put $\nu_{p(x)}(0) = \infty$. Then it is easily checked that $\nu_{p(x)}$ is a (discrete) normalized valuation of $k(x)$.

There is another normalized valuation of $k(x)$ which is obtained from the degree map. If $r(x) = f(x)/g(x)$ is nonzero, then we set

$$\nu_\infty(r(x)) = \deg(g(x)) - \deg(f(x)).$$

We also set $\nu_\infty(0) = \infty$. Again, it is easily checked that ν_∞ is a normalized valuation of $k(x)$. Indeed, the properties (i) and (iv) in Definition 3.2 are trivial. Property (ii) follows from $\deg(gh) = \deg(g) + \deg(h)$ for all $g, h \in k[x]$. To prove (iii), we have in an obvious notation,

$$\begin{aligned}
\nu_\infty\left(\frac{f}{g} + \frac{e}{h}\right) &= \nu_\infty\left(\frac{fh + eg}{gh}\right) = \deg(gh) - \deg(fh + eg) \\
&\geq \deg(gh) - \max(\deg(fh), \deg(eg)) \\
&= \min(\deg(gh) - \deg(fh), \deg(gh) - \deg(eg)) \\
&= \min(\deg(g) - \deg(f), \deg(h) - \deg(e)) = \min\left(\nu_\infty\left(\frac{f}{g}\right), \nu_\infty\left(\frac{e}{h}\right)\right).
\end{aligned}$$

The valuations $\nu_{p(x)}$, $p(x) \in k[x]$ monic irreducible, and ν_∞ are pairwise nonequivalent since $\nu_{p(x)}(p(x)) = 1$, whereas $\nu_{q(x)}(p(x)) = 0$ for monic irreducible $q(x) \neq p(x)$ and $\nu_\infty(p(x)) < 0$. Thus, we get a set of places $\{p(x) \in k[x] : p(x) \text{ monic irreducible}\} \cup \{\infty\}$ of $k(x)$.

5.1. Remark. If k is algebraically closed, then the monic irreducible polynomials over k are exactly the linear polynomials $x - a$ with $a \in k$. Thus, the above set of places can be identified with $k \cup \{\infty\}$. If $k = \mathbf{C}$, then this yields the complex plane with the point at ∞, i.e., the Riemann sphere. Thus, the above set of places of $\mathbf{C}(x)$ is in bijective correspondence with the points (or "places") on the Riemann sphere. This explains how the term "place" originated historically.

We assume from now on that the constant field k is finite, although some results hold for arbitrary k.

5.2. Lemma. *If k is finite, then for any valuation ν of $k(x)$ we have $\nu(a) = 0$ for all $a \in k^*$.*

Proof. If $k = \mathbf{F}_q$, then $a^{q-1} = 1$ for all $a \in \mathbf{F}_q^*$, and so by Lemma 3.3(i),

$$0 = \nu(1) = \nu(a^{q-1}) = (q-1)\nu(a),$$

which yields $\nu(a) = 0$. □

5.3. Theorem. *If k is finite, then the set of all places of $k(x)$ is given by $\{p(x) \in k[x] :$ $p(x)$ monic irreducible$\} \cup \{\infty\}$.*

Proof. We have to show that if P is a place of $k(x)$ and $\nu \in P$, then ν is equivalent to either $\nu_{p(x)}$ or ν_∞.

Case 1: $\nu(x) \geq 0$. Then $k[x] \subseteq O_P$ by Lemma 5.2. Since $\nu(k(x)^*) \neq \{0\}$ by definition, there exists a nonzero $h(x) \in k[x]$ with $\nu(h(x)) > 0$. Thus, $\mathsf{J} := k[x] \cap \mathsf{M}_P$ is a nonzero ideal of $k[x]$. Furthermore, $\mathsf{J} \neq k[x]$ since $1 \notin \mathsf{J}$. Since M_P is a prime ideal of O_P, it follows that J is a prime ideal of $k[x]$. Consequently, there exists a monic irreducible $p(x) \in k[x]$ such that $\mathsf{J} = (p(x))$. In particular, $c := \nu(p(x)) > 0$. If $g(x) \in k[x]$ is not divisible by $p(x)$, then $g(x) \notin \mathsf{M}_P$, and so $\nu(g(x)) = 0$. Thus, if we write a nonzero $r(x) \in k(x)$ in the form

$$r(x) = p(x)^m \frac{f(x)}{g(x)}$$

with $f(x)$ and $g(x)$ not divisible by $p(x)$, then

$$\nu(r(x)) = m\nu(p(x)) = c\nu_{p(x)}(r(x)),$$

and so ν is equivalent to $\nu_{p(x)}$.

Case 2: $\nu(x) < 0$. Then $c := \nu(x^{-1}) > 0$ and $x^{-1} \in \mathsf{M}_P$. Take any nonzero $f(x) \in k[x]$ of degree d, say. Then

$$\begin{aligned} f(x) &= \sum_{i=0}^{d} a_i x^i = x^d \sum_{i=0}^{d} a_i x^{i-d} \\ &= x^d \sum_{i=0}^{d} a_{d-i} x^{-i} \end{aligned}$$

with all $a_i \in k$. Furthermore,

$$\sum_{i=0}^{d} a_{d-i} x^{-i} = a_d + \sum_{i=1}^{d} a_{d-i} x^{-i} = a_d + s(x)$$

with $s(x) \in \mathsf{M}_P$. Since $a_d \neq 0$, we have $\nu(a_d) = 0$, and so

$$\nu(\sum_{i=0}^{d} a_{d-i} x^{-i}) = 0$$

by Proposition 3.4. It follows that

$$\nu(f(x)) = \nu(x^d) = -d\nu(x^{-1}) = c\nu_\infty(f(x)),$$

and so ν is equivalent to ν_∞. □

5.4. Remark. Note that in the proof of Theorem 5.3 we have not used that ν is discrete, and so the proof shows that every valuation of $k(x)$ is automatically discrete.

The places $p(x)$ are often called the *finite places* of $k(x)$ and the place ∞ is often called the *infinite place* of $k(x)$.

5.5. Example. As in Example 4.5 one shows that the residue class field of the place $p(x)$ is isomorphic to $k[x]/(p(x))$. For the place ∞ we have

$$\begin{aligned} O_\infty &= \left\{ \frac{f(x)}{g(x)} \in k(x) : \deg(f(x)) \leq \deg(g(x)) \right\}, \\ U_\infty &= \left\{ \frac{f(x)}{g(x)} \in k(x) : \deg(f(x)) = \deg(g(x)) \right\}, \\ \mathsf{M}_\infty &= \left\{ \frac{f(x)}{g(x)} \in k(x) : \deg(f(x)) < \deg(g(x)) \right\}. \end{aligned}$$

Every $r(x) \in O_\infty$ can be written in the form

$$r(x) = \frac{a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0}{x^d + b_{d-1}x^{d-1} + \cdots + b_0}$$

with all $a_i, b_j \in k$. The map $\psi : O_\infty \to k$ given by

$$\psi(r(x)) = a_d \in k \quad \text{for all } r(x) \in O_\infty$$

is well defined. It is easily seen that ψ is a surjective ring homomorphism with kernel M_∞, and so the residue class field of the place ∞ is isomorphic to k.

5.6. Remark. For every nonzero $r(x) \in k(x)$ we have

$$\nu_\infty(r(x)) + \sum_{p(x)} \nu_{p(x)}(r(x)) \deg(p(x)) = 0,$$

where the sum is over all monic irreducible $p(x) \in k[x]$. Note that the sum makes sense since $\nu_{p(x)}(r(x)) = 0$ for all but finitely many $p(x)$. Because of the properties of valuations, it suffices to verify the formula for nonzero monic $f(x) \in k[x]$. If

$$f(x) = \prod_{i=1}^{n} p_i(x)^{m_i}$$

is the canonical factorization of $f(x)$ in $k[x]$, then

$$\begin{aligned}\sum_{p(x)} \nu_{p(x)}(f(x)) \deg(p(x)) &= \sum_{i=1}^{n} m_i \deg(p_i(x)) \\ &= \deg(f(x)) \\ &= -\nu_\infty(f(x)).\end{aligned}$$

This formula is an additive analog of the product formula for $\mathbf{Q}$ in Example 3.1.

6. Algebraic Function Fields and Their Valuations

We have already given a rough definition of algebraic function fields in Chapter 1. The rigorous definition is as follows. *We consider only algebraic function fields over a finite field k.*

6.1. Definition. A field F is an *algebraic function field* over the finite field k if there exists a transcendental element $z \in F$ over k such that F is a finite extension of the rational function field $k(z)$.

The simplest example of an algebraic function field is of course a rational function field over a finite field.

6.2. Proposition. *Every valuation of an algebraic function field is discrete.*

Proof. Let F be an algebraic function field. With the notation in Definition 6.1, put $K = k(z)$. Let ν be an arbitrary valuation of F and let μ be the restriction of ν to K. It suffices to prove that the index $[\nu(F^*) : \mu(K^*)]$ is finite. Since $\nu(F^*)$ is an infinite subgroup of $(\mathbf{R}, +)$, this shows then that $\mu(K^*) = \{0\}$ is not possible. Hence μ is a valuation of K, thus discrete by Remark 5.4, and so ν is discrete.

Let $x_1, \ldots, x_n \in F^*$ be such that $\nu(x_1), \ldots, \nu(x_n)$ are in distinct cosets modulo $\mu(K^*)$. We claim that $x_1, \ldots, x_n$ are linearly independent over K. This will then show

$$[\nu(F^*) : \mu(K^*)] \leq [F : K] < \infty.$$

So suppose we have

$$\sum_{i=1}^{n} b_i x_i = 0,$$

where w.l.o.g. all $b_i \in K^*$. If we had $\nu(b_i x_i) = \nu(b_j x_j)$ for some $i \neq j$, then

$$\nu(x_i) - \nu(x_j) = \nu(b_j) - \nu(b_i) = \mu(b_j b_i^{-1}) \in \mu(K^*),$$

a contradiction to the choice of $x_1, \ldots, x_n$. Thus $\nu(b_1x_1), \ldots, \nu(b_nx_n)$ are all distinct, and so Proposition 3.4 yields

$$\infty = \nu\left(\sum_{i=1}^{n} b_i x_i\right) = \min_{1\le i\le n} \nu(b_i x_i).$$

This means $b_ix_i = 0$ for $1 \le i \le n$, again a contradiction. □

In the above proof we have shown, in particular, that the restriction of a valuation of F to $k(z)$ yields a valuation of $k(z)$. Obviously, for equivalent valuations of F the restrictions are again equivalent. Thus, a place Q of F corresponds by restriction to a unique place P of $k(z)$. We say that Q *lies over* P or that P *lies under* Q. Therefore, every place of F lies either over a place of $k(z)$ corresponding to a monic irreducible polynomial in $k[z]$ or over the infinite place of $k(z)$.

6.3. Proposition. *Let F be an algebraic function field over k. Then the residue class field of every place of F is a finite extension of (an isomorphic copy of) k.*

Proof. Let Q be a place of F that lies over the place P of $K := k(z)$ (with z as in Definition 6.1). Let $R_Q := O_Q/\mathsf{M}_Q$ and $R_P := O_P/\mathsf{M}_P$ be the corresponding residue class fields and note that $O_P \subseteq O_Q$. The map $\rho : R_P \to R_Q$ given by

$$\rho(b + \mathsf{M}_P) = b + \mathsf{M}_Q \quad \text{for all } b \in O_P$$

is well defined since $\mathsf{M}_P \subseteq \mathsf{M}_Q$. It is clear that ρ is an injective ring homomorphism, and so R_Q contains the isomorphic copy $\rho(R_P)$ of R_P as a subfield.

Let $x_1, \ldots, x_n \in O_Q$ be such that $x_1 + \mathsf{M}_Q, \ldots, x_n + \mathsf{M}_Q$ are linearly independent over $\rho(R_P)$. We claim that $x_1, \ldots, x_n$ are linearly independent over K. This will then show

$$[R_Q : \rho(R_P)] \le [F : K] < \infty.$$

Since R_P is a finite extension (of an isomorphic copy) of k (see Example 5.5), this proves the proposition. So suppose we have

$$\sum_{i=1}^{n} b_i x_i = 0$$

with $b_1, \ldots, b_n \in K$ not all 0. W.l.o.g.

$$\nu_P(b_1) = \min_{1\le i\le n} \nu_P(b_i).$$

Then $b_1 \ne 0$ and

$$x_1 + \sum_{i=2}^{n} b_i b_1^{-1} x_i = 0.$$

By the definition of b_1 we have $b_i b_1^{-1} \in O_P$ for $2 \leq i \leq n$. Passing to the residue classes modulo M_Q, we get

$$(x_1 + \mathsf{M}_Q) + \sum_{i=2}^{n} \rho(b_i b_1^{-1} + \mathsf{M}_P)(x_i + \mathsf{M}_Q) = 0 + \mathsf{M}_Q,$$

a contradiction to the choice of $x_1, \ldots, x_n$. □

The following result (see [4, Section III.1] and [5, Section 2-4] for its proof) shows, in particular, that every valuation of a rational function field over k can be extended to a valuation of an algebraic function field over k.

6.4. Theorem. *Let F be a finite extension of the rational function field $k(z)$. Then every place of $k(z)$ lies under at least one and at most $[F : k(z)]$ places of F.*

Let F again be an algebraic function field over the finite field k. Let $\tilde{k}$ be the algebraic closure of k in F, i.e.,

$$\tilde{k} = \{x \in F : x \text{ is algebraic over } k\}.$$

Clearly, $\tilde{k}$ is a field with $k \subseteq \tilde{k} \subseteq F$. The field $\tilde{k}$ is called the *full constant field* of F. The following result shows that $\tilde{k}$ is again a finite field.

6.5. Proposition. *The field $\tilde{k}$ is a finite extension of k.*

Proof. By Theorem 6.4 there exists a place Q of F. Take any $x \in \tilde{k}^*$. By means of its minimal polynomial over k we get

$$x^d + c_{d-1}x^{d-1} + \cdots + c_0 = 0$$

with $c_0, \ldots, c_{d-1} \in k$ and $c_0 \neq 0$. If we had $\nu_Q(x) < 0$, then

$$\nu_Q(x^d + c_{d-1}x^{d-1} + \cdots + c_0) = \nu_Q(x^d) < 0$$

by Proposition 3.4, a contradiction. If we had $\nu_Q(x) > 0$, then

$$\nu_Q(x^d + c_{d-1}x^{d-1} + \cdots + c_0) = \nu_Q(c_0) = 0$$

by Proposition 3.4, again a contradiction. Thus we must have $\nu_Q(x) = 0$. Now consider the map $\psi : \tilde{k} \to R_Q := O_Q/\mathsf{M}_Q$ given by

$$\psi(x) = x + \mathsf{M}_Q \quad \text{for all } x \in \tilde{k}.$$

The above considerations show that ψ is injective, hence $|\tilde{k}| \leq |R_Q| < \infty$, the latter by Proposition 6.3. □

Note that $k(z) \subseteq \tilde{k}(z) \subseteq F$, and so F is a finite extension of $\tilde{k}(z)$. Furthermore, z is transcendental over $\tilde{k}$ by Proposition 6.5, and so F is also an algebraic function field over $\tilde{k}$. In the following, we will usually assume that k is already the full constant field of F. If we want to stress this, then we use the notation F/k for an algebraic function field with full constant field k.

In view of Proposition 6.3, the following definition makes sense.

6.6. Definition. The *degree* $\deg(P)$ of a place P of F/k is defined to be the degree of the residue class field of P over k. A place of F/k of degree 1 is also called a *rational place* of F/k.

6.7. Example. Let $F = k(x)$ be the rational function field over k. It is obvious that for any nonconstant rational function $r(x) \in F$ there exists a finite place P of F such that $\nu_P(r(x)) \neq 0$. Thus, the full constant field of F is k. By Example 5.5, the degree of a finite place $p(x)$ of F is equal to the degree of the polynomial $p(x)$ and the degree of the place ∞ of F is equal to 1. If $k = \mathbf{F}_q$, then F has thus exactly $q+1$ rational places.

For an algebraic function field F/k, we denote by $\mathcal{P}_F$ the set of all places of F. Note that $\mathcal{P}_F$ is a denumerable set. The following result (see [4, Section I.6]) is a strengthening of Theorem 4.7 in the case under consideration.

6.8. Theorem (Strong Approximation Theorem). *Let $\mathcal{S}$ be a proper nonempty subset of $\mathcal{P}_F$ and let $P_1, \ldots, P_n \in \mathcal{S}$ be distinct. Then for any given elements $x_1, \ldots, x_n \in F$ and integers $m_1, \ldots, m_n$, there exists an element $x \in F$ such that*

$$\begin{aligned} \nu_{P_i}(x - x_i) &= m_i \quad \text{for } i = 1, \ldots, n, \\ \nu_P(x) &\geq 0 \quad \text{for all } P \in \mathcal{S} \setminus \{P_1, \ldots, P_n\}. \end{aligned}$$

7. Divisors

Let F/k be an algebraic function field with full constant field k (k finite).

7.1. Definition. A *divisor* D of F is a formal sum

$$D = \sum_{P \in \mathcal{P}_F} m_P P$$

with all $m_P \in \mathbf{Z}$ and $m_P \neq 0$ for at most finitely many $P \in \mathcal{P}_F$.

A place $P \in \mathcal{P}_F$ is also a divisor (put $m_P = 1$, $m_Q = 0$ for all $Q \in \mathcal{P}_F$ with $Q \neq P$). In this context, a place is called a *prime divisor*.

The divisors of F form a group under the obvious addition law

$$\begin{aligned} D+E &= \sum_{P\in\mathcal{P}_F} m_P P + \sum_{P\in\mathcal{P}_F} n_P P \\ &= \sum_{P\in\mathcal{P}_F} (m_P+n_P)P. \end{aligned}$$

The zero element is the zero divisor

$$0 := \sum_{P\in\mathcal{P}_F} m_P P \quad \text{with all } m_P = 0.$$

The additive inverse of $D = \sum_{P\in\mathcal{P}_F} m_P P$ is

$$-D = \sum_{P\in\mathcal{P}_F} (-m_P)P.$$

The abelian group of all divisors of F is called the *divisor group* $\mathrm{Div}(F)$ of F. It can also be described as the free abelian group generated by the places (prime divisors) of F.

7.2. Remark. Note the following simple analogy between polynomials and divisors. A polynomial is an assignment which associates with each monomial x^i, $i = 0, 1, \ldots$, a coefficient a_i such that all but finitely many $a_i = 0$. A divisor is an assignment which associates with each place $P \in \mathcal{P}_F$ an integer coefficient m_P such that all but finitely many $m_P = 0$. Addition of divisors operates in the same way as addition of polynomials.

7.3. Definition. The *support* $\mathrm{supp}(D)$ of the divisor $D = \sum_{P\in\mathcal{P}_F} m_P P$ is given by

$$\mathrm{supp}(D) = \{P \in \mathcal{P}_F : m_P \neq 0\}.$$

By the definition of a divisor, $\mathrm{supp}(D)$ is a finite subset of $\mathcal{P}_F$. If $D = \sum_{P\in\mathcal{P}_F} m_P P$, it is often convenient to write $m_P = \nu_P(D)$. Thus, a divisor D can also be represented in the form

$$D = \sum_{P\in\mathrm{supp}(D)} \nu_P(D)P.$$

7.4. Definition. If $D \in \mathrm{Div}(F)$ is as above, then the *degree* $\deg(D)$ of D is defined by

$$\deg(D) = \sum_{P\in\mathrm{supp}(D)} \nu_P(D)\deg(P).$$

7.5. Proposition. *The degree map* $\deg : \mathrm{Div}(F) \to \mathbf{Z}$ *is a group homomorphism.*

Proof. This is a straightforward verification. □

Consequently, the divisors of F of degree 0 form a subgroup $\mathrm{Div}^0(F)$ of $\mathrm{Div}(F)$. We can introduce a partial order on $\mathrm{Div}(F)$ by saying that $D_1 \leq D_2$ if

$$\nu_P(D_1) \leq \nu_P(D_2) \quad \text{for all } P \in \mathcal{P}_F.$$

A divisor $D \geq 0$ is called *positive* (or *effective*).

If F is the rational function field and $f \in F^*$, then it is obvious that $\nu_P(f) \neq 0$ for at most finitely many $P \in \mathcal{P}_F$. The same is true for an arbitrary algebraic function field F/k. Thus, the following definition makes sense.

7.6. Definition. Let F be an algebraic function field and $f \in F^*$. Then the *principal divisor* $\mathrm{div}(f)$ of f is defined by

$$\mathrm{div}(f) = \sum_{P \in \mathcal{P}_F} \nu_P(f) P.$$

7.7. Remark. If f is in the full constant field k of F and $f \neq 0$, then it follows as in the proof of Lemma 5.2 that $\nu_P(f) = 0$ for all $P \in \mathcal{P}_F$. Therefore we get $\mathrm{div}(f) = 0$. The converse holds also, since it can be shown that for any $f \in F \backslash k$, i.e., for any transcendental f over k, there exists at least one $P \in \mathcal{P}_F$ with $\nu_P(f) \neq 0$.

If F is the rational function field and $f \in F^*$, then

$$\deg(\mathrm{div}(f)) = \sum_{P \in \mathcal{P}_F} \nu_P(f) \deg(P) = 0$$

by Remark 5.6 and the information about the degree of $P \in \mathcal{P}_F$ in Example 6.7. The same formula holds also for an arbitrary algebraic function field F/k (see [4, Section I.4]).

7.8. Proposition. *The degree of every principal divisor is equal to* 0.

It is easily checked that the set $\mathrm{Princ}(F)$ of principal divisors of F forms a subgroup of $\mathrm{Div}^0(F)$; note e.g. that

$$\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g) \quad \text{for all } f, g \in F^*.$$

The factor group

$$\mathrm{Cl}(F) := \mathrm{Div}^0(F)/\mathrm{Princ}(F)$$

is finite (see [4, Section V.1]) and its cardinality $h(F) := |\mathrm{Cl}(F)|$ is called the *divisor class number* of F.

8. The Riemann-Roch Theorem

F/k is again an algebraic function field with full constant field k (k finite).

For any divisor D of F/k we form the *Riemann-Roch space*

$$\mathcal{L}(D) := \{f \in F^* : \mathrm{div}(f) + D \geq 0\} \cup \{0\}.$$

Explicitly, this means that $\mathcal{L}(D)$ consists of all $f \in F$ with

$$\nu_P(f) \geq -\nu_P(D) \quad \text{for all } P \in \mathcal{P}_F.$$

8.1. Proposition. *$\mathcal{L}(D)$ is a vector space over k.*

Proof. $\mathcal{L}(D)$ is nonempty since $0 \in \mathcal{L}(D)$. Let $f_1, f_2 \in \mathcal{L}(D)$ and $a \in k$. Then for any $P \in \mathcal{P}_F$,

$$\nu_P(f_1 + f_2) \geq \min(\nu_P(f_1), \nu_P(f_2)) \geq -\nu_P(D)$$

and

$$\nu_P(af_1) = \nu_P(a) + \nu_P(f_1) \geq -\nu_P(D).$$

Thus, $f_1 + f_2 \in \mathcal{L}(D)$ and $af_1 \in \mathcal{L}(D)$. □

8.2. Example. For the zero divisor we have $\mathcal{L}(0) = k$. Note that for $f \in F^*$ we have $f \in \mathcal{L}(0) \Leftrightarrow \nu_P(f) \geq 0$ for all $P \in \mathcal{P}_F$. But

$$\deg(\mathrm{div}(f)) = \sum_{P \in \mathcal{P}_F} \nu_P(f) \deg(P) = 0$$

by Proposition 7.8, and so $f \in \mathcal{L}(0) \Leftrightarrow \nu_P(f) = 0$ for all $P \in \mathcal{P}_F \Leftrightarrow f \in k^*$, the latter by Remark 7.7.

8.3. Remark. If $\deg(D) < 0$, then necessarily $\mathcal{L}(D) = \{0\}$. For if we had a nonzero $f \in \mathcal{L}(D)$, then by applying the degree map to

$$\mathrm{div}(f) + D \geq 0$$

we get $0 + \deg(D) \geq 0$, a contradiction.

The vector space $\mathcal{L}(D)$ has, in fact, a finite dimension over k which is denoted by $\ell(D)$. Thus, by the above, we have $\ell(0) = 1$ and $\ell(D) = 0$ if $\deg(D) < 0$. Information on $\ell(D)$ is given in the following fundamental theorem (see [4, Sections I.4 and I.5]).

8.4. Theorem (Riemann-Roch Theorem). *Let F/k be an algebraic function field. Then there exists a constant c such that for any divisor D of F we have*

$$\ell(D) \geq \deg(D) + 1 - c.$$

As a consequence of the Riemann-Roch theorem, we can define the number

$$g = \max_{D \in \mathrm{Div}(F)} (\deg(D) - \ell(D) + 1).$$

The integer $g = g(F)$ is called the *genus* of F and is the most important invariant of an algebraic function field. By putting $D = 0$ in the definition, we see that $g \geq 0$. Note that by definition we have

$$\ell(D) \geq \deg(D) + 1 - g \quad \text{for all } D \in \mathrm{Div}(F).$$

By the following result (see [4, Section I.5]), we have equality if $\deg(D)$ is sufficiently large.

8.5. Theorem (Supplement to the Riemann-Roch Theorem). *If $\deg(D) \geq 2g - 1$, then*

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

8.6. Example. If F is a rational function field, then it is easy to verify that

$$\ell(D) \geq \deg(D) + 1 \quad \text{for all } D \in \mathrm{Div}(F).$$

Therefore $g(F) = 0$. In fact, rational function fields over finite fields can be characterized by the property of having genus 0.

An algebraic function field of genus 1 is also called an *elliptic function field.* Elliptic function fields F/k with $k = \mathbf{F}_q$ can be characterized (see [4, Section VI.1]). In all cases, F is a quadratic extension of $K := k(x)$. If q is odd, then $F = K(y)$ for some $y \in F$ with

$$y^2 = f(x),$$

where $f \in k[x]$ is squarefree of degree 3. If q is even, then $F = K(y)$ for some $y \in F$ with either

$$y^2 + y = f(x)$$

with $f \in k[x]$ of degree 3 or

$$y^2 + y = x + \frac{1}{ax + b}$$

with $a, b \in k$ and $a \neq 0$.

There is no general explicit formula for the genus of an algebraic function field. However, for certain special families of algebraic function fields, such as in the example below, there is such a formula. In general, the computation of the genus of an algebraic function field is a nontrivial problem.

8.7. Example. Let $k = \mathbf{F}_q$ with q odd and let $K := k(x)$ be the rational function field. Let $F = K(y)$ be the quadratic extension defined by

$$y^2 = f(x),$$

where $f \in k[x]$ is squarefree of degree $d \geq 1$. Then

$$g(F) = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

A proof can be found in [4, Section III.7].

9. Zeta Function and Hasse-Weil Bound

As usual, F/k is an algebraic function field with full constant field k (k finite). A general reference for this chapter is [4, Chapter V].

9.1. Proposition. *An algebraic function field F/k has at most finitely many rational places.*

Proof. By Definition 6.1, there exists a $z \in F \setminus k$ such that $[F : k(z)] < \infty$. All rational places of F lie over rational places of $k(z)$ (use the first part of the proof of Proposition 6.3). By Theorem 6.4, for each rational place P of $k(z)$ there are at most $[F : k(z)]$ rational places of F lying over P. Moreover, if $k = \mathbf{F}_q$, then there are only $q + 1$ rational places of $k(z)$ by Example 6.7. Hence the number of rational places of F is at most $(q+1)[F : k(z)]$. □

Now we can define the zeta function of an algebraic function field $F/\mathbf{F}_q$. For each integer $n \geq 1$, consider the composite field

$$F_n := \mathbf{F}_{q^n} \cdot F.$$

This is an algebraic function field over $\mathbf{F}_{q^n}$ (called a *constant field extension* of F). Let N_n denote the number of rational places of $F_n/\mathbf{F}_{q^n}$, which is a finite number by Proposition 9.1.

9.2. Definition. The *zeta function* of $F/\mathbf{F}_q$ is defined to be the formal power series

$$Z(F, t) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n}{n} t^n\right) \in \mathbf{C}[[t]]$$

over the complex numbers.

9.3. Example. We compute the zeta function of the rational function field F over $\mathbf{F}_q$. We have $N_n = q^n + 1$ for all $n \geq 1$ by Example 6.7. Hence we get

$$\begin{aligned}\log Z(F,t) &= \sum_{n=1}^{\infty} \frac{q^n+1}{n} t^n = \sum_{n=1}^{\infty} \frac{(qt)^n}{n} + \sum_{n=1}^{\infty} \frac{t^n}{n} \\ &= -\log(1-qt) - \log(1-t) \\ &= \log \frac{1}{(1-t)(1-qt)},\end{aligned}$$

that is,

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

9.4. Theorem (Weil Theorem). *Let $F/\mathbf{F}_q$ be an algebraic function field of genus g. Then:*
(i) *$Z(F,t)$ is a rational function of the form*

$$Z(F,t) = \frac{L(F,t)}{(1-t)(1-qt)},$$

where $L(F,t) \in \mathbf{Z}[t]$ is a polynomial of degree $2g$ with $L(F,0) = 1$ and leading coefficient q^g. Moreover, $L(F,1)$ is equal to the divisor class number $h(F)$ of F.
(ii) *Factor $L(F,t)$ into the form*

$$L(F,t) = \prod_{j=1}^{2g} (1 - \omega_j t) \in \mathbf{C}[t].$$

Then $|\omega_j| = q^{1/2}$ for $1 \leq j \leq 2g$.

9.5. Theorem (Hasse-Weil Bound). *Let $F/\mathbf{F}_q$ be an algebraic function field of genus g. Then the number $N(F)$ of rational places of $F/\mathbf{F}_q$ satisfies*

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

Proof. By the definition of $Z(F,t)$ we obtain

$$\begin{aligned}N(F) = N_1 &= \left.\frac{d(\log Z(F,t))}{dt}\right|_{t=0} \\ &= Z'(F,0).\end{aligned}$$

On the other hand, by Theorem 9.4(i) we get

$$\begin{aligned} Z'(F,0) &= \left.\left(\frac{L'(F,t)}{L(F,t)} + \frac{1}{1-t} + \frac{q}{1-qt}\right)\right|_{t=0} \\ &= a_1 + 1 + q, \end{aligned}$$

where a_1 is the coefficient of t in $L(F,t)$. Comparing coefficients in the identity in Theorem 9.4(ii), we obtain

$$a_1 = -\sum_{j=1}^{2g} \omega_j.$$

Combining the three identities above yields

$$N(F) = q + 1 - \sum_{j=1}^{2g} \omega_j.$$

Therefore

$$|N(F) - (q+1)| = |\sum_{j=1}^{2g} \omega_j| \leq \sum_{j=1}^{2g} |\omega_j| = 2gq^{1/2}$$

by Theorem 9.4(ii). □

9.6. Remark. A refined approach yields the *Serre bound*

$$|N(F) - (q+1)| \leq g\lfloor 2q^{1/2} \rfloor.$$

In particular, we get an upper bound on $N(F)$ depending only on g and q. Hence the following definition makes sense.

9.7. Definition. For a fixed prime power q and an integer $g \geq 0$, let

$$N_q(g) := \max N(F),$$

where the maximum is over all algebraic function fields $F/\mathbf{F}_q$ of genus g.

It is trivial that $N_q(0) = q + 1$. From the Serre bound we get

$$N_q(g) \leq q + 1 + g\lfloor 2q^{1/2} \rfloor.$$

If we put

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g},$$

then we conclude that $A(q) \leq \lfloor 2q^{1/2} \rfloor$ for all q. Vlăduţ and Drinfeld have improved this to

$$A(q) \leq q^{1/2} - 1 \quad \text{for all } q,$$

and from a result of Ihara it follows that

$$A(q) = q^{1/2} - 1 \quad \text{for all squares } q.$$

Further information on $A(q)$ can be found in [2, Chapter 5]. The quantity $A(q)$ is very important for applications to algebraic-geometry codes (see [2, Section 6.2] and [4, Section VII.2]).

References

[1] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, rev. ed., Cambridge Univ. Press, Cambridge, 1994.

[2] H. Niederreiter and C.P. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, Cambridge Univ. Press, Cambridge, 2001.

[3] P. Ribenboim, *The Theory of Classical Valuations*, Springer, New York, 1999.

[4] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.

[5] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.