1 Finite Fields and Function Fields

In the first part of this chapter, we describe the basic results on finite fields, which are our ground fields in the later chapters on applications. The second part is devoted to the study of function fields.

Section 1.1 presents some fundamental results on finite fields, such as the existence and uniqueness of finite fields and the fact that the multiplicative group of a finite field is cyclic. The algebraic closure of a finite field and its Galois group are discussed in Section 1.2. In Section 1.3, we study conjugates of an element and roots of irreducible polynomials and determine the number of monic irreducible polynomials of given degree over a finite field. In Section 1.4, we consider traces and norms relative to finite extensions of finite fields.

A function field governs the abstract algebraic aspects of an algebraic curve. Before proceeding to the geometric aspects of algebraic curves in the next chapters, we present the basic facts on function fields. In particular, we concentrate on algebraic function fields of one variable and their extensions including constant field extensions. This material is covered in Sections 1.5, 1.6, and 1.7.

One of the features in this chapter is that we treat finite fields using the Galois action. This is essential because the Galois action plays a key role in the study of algebraic curves over finite fields. For comprehensive treatments of finite fields, we refer to the books by Lidl and Niederreiter [71, 72].

1.1 Structure of Finite Fields

For a prime number p, the residue class ring $\mathbb{Z}/p\mathbb{Z}$ of the ring $\mathbb{Z}$ of integers forms a field. We also denote $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$. It is a prime field in the sense that there are no proper subfields of $\mathbb{F}_p$. There are exactly p elements in $\mathbb{F}_p$. In general, a field is called a *finite field* if it contains only a finite number of elements.

Proposition 1.1.1. Let k be a finite field with q elements. Then:

(i) there exists a prime p such that $\mathbb{F}_p \subseteq k$;
(ii) $q = p^n$ for some integer $n \geq 1$;
(iii) $\alpha^q = \alpha$ for all $\alpha \in k$.

Proof.

(i) Since k has only $q < \infty$ elements, the characteristic of k must be a prime p. Thus, $\mathbb{F}_p$ is the prime subfield of k.

(ii) We consider k as a vector space over $\mathbb{F}_p$. Since k is finite, the dimension $n := \dim_{\mathbb{F}_p}(k)$ is also finite. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of k over $\mathbb{F}_p$. Then each element of k can be uniquely represented in the form $a_1\alpha_1 + \cdots + a_n\alpha_n$ with $a_1, \ldots, a_n \in \mathbb{F}_p$. Thus, $q = p^n$.

(iii) It is trivial that $\alpha^q = \alpha$ if $\alpha = 0$. Assume that α is a nonzero element of k. Since all nonzero elements of k form a multiplicative group k^* of order $q - 1$, we have $\alpha^{q-1} = 1$, and so $\alpha^q = \alpha$.

Using the above proposition, we can show the most fundamental result concerning the existence and uniqueness of finite fields.

Theorem 1.1.2. For every prime p and every integer $n \geq 1$, there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of the polynomial $x^q - x$ over $\mathbb{F}_p$.

Proof. (Existence) Let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p$ and let $k \subseteq \overline{\mathbb{F}_p}$ be the splitting field of the polynomial $x^{p^n} - x$ over $\mathbb{F}_p$. Let R be the set of all roots of $x^{p^n} - x$ in k. Then R has exactly p^n elements since the derivative of the polynomial $x^{p^n} - x$ is $p^n x^{p^n-1} - 1 = -1$. It is easy to verify that R contains $\mathbb{F}_p$ and R forms a subfield of $\overline{\mathbb{F}_p}$ (note that $(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$ for any $\alpha, \beta \in \overline{\mathbb{F}_p}$ and any integer $m \geq 1$). Thus, R is exactly the splitting field k, that is, k is a finite field with p^n elements.

(Uniqueness) Let $k \subseteq \overline{\mathbb{F}_p}$ be a finite field with q elements. By Proposition 1.1.1(iii), all elements of k are roots of the polynomial $x^q - x$. Thus, k is the splitting field of the polynomial of $x^q - x$ over $\mathbb{F}_p$. This proves the uniqueness.

The above theorem shows that for given $q = p^n$, the finite field with q elements is unique in a fixed algebraic closure $\overline{\mathbb{F}_p}$. We denote this finite field by $\mathbb{F}_q$ and call it *the* finite field of order q (or with q elements). It follows from the proof of the above theorem that $\mathbb{F}_q$ is the splitting field of the polynomial $x^q - x$ over $\mathbb{F}_p$, and so $\mathbb{F}_q/\mathbb{F}_p$ is a Galois extension of degree n. The following result yields the structure of the Galois group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

Lemma 1.1.3. The Galois group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ with $q = p^n$ is a cyclic group of order n with generator $\sigma : \alpha \mapsto \alpha^p$.

Proof. It is clear that σ is an automorphism in $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Suppose that σ^m is the identity for some $m \geq 1$. Then $\sigma^m(\alpha) = \alpha$, that is, $\alpha^{p^m} - \alpha = 0$, for all $\alpha \in \mathbb{F}_q$. Thus, $x^{p^m} - x$ has at least $q = p^n$ roots. Therefore, $p^m \geq p^n$, that is, $m \geq n$. Hence, the order of σ is equal to n since $|\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)| = n$.

Lemma 1.1.4. The field $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ if and only if m divides n.

Proof. If m divides n, then there exists a subgroup H of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ with $|H| = n/m$ since $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is a cyclic group of order n by Lemma 1.1.3. Let k be the subfield of $\mathbb{F}_{p^n}/\mathbb{F}_p$ fixed by H. Then $[k : \mathbb{F}_p] = m$. Thus, $k = \mathbb{F}_{p^m}$ by the uniqueness of finite fields.

Conversely, let $\mathbb{F}_{p^m}$ be a subfield of $\mathbb{F}_{p^n}$. Then the degree $m = [\mathbb{F}_{p^m} : \mathbb{F}_p]$ divides the degree $n = [\mathbb{F}_{p^n} : \mathbb{F}_p]$.

Theorem 1.1.5. Let q be a prime power. Then:

(i) $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^n}$ for every integer $n \geq 1$.
(ii) $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is a cyclic group of order n with generator $\sigma : \alpha \mapsto \alpha^q$.
(iii) $\mathbb{F}_{q^m}$ is a subfield of $\mathbb{F}_{q^n}$ if and only if m divides n.

Proof.

(i) Let $q = p^s$ for some prime p and integer $s \geq 1$. Then by Lemma 1.1.4, $\mathbb{F}_q = \mathbb{F}_{p^s} \subseteq \mathbb{F}_{p^{ns}} = \mathbb{F}_{q^n}$.
(ii) Using exactly the same arguments as in the proof of Lemma 1.1.3 but replacing p by q, we obtain the proof of (ii).
(iii) By Lemma 1.1.4, $\mathbb{F}_{q^m} = \mathbb{F}_{p^{ms}}$ is a subfield of $\mathbb{F}_{q^n} = \mathbb{F}_{p^{ns}}$ if and only if ms divides ns. This is equivalent to m dividing n.

We end this section by determining the structure of the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of a finite field $\mathbb{F}_q$.

Proposition 1.1.6. The multiplicative group $\mathbb{F}_q^*$ is cyclic.

Proof. Let $t \leq q-1$ be the largest order of an element of the group $\mathbb{F}_q^*$. By the structure theorem for finite abelian groups, the order of any element of $\mathbb{F}_q^*$ divides t. It follows that every element of $\mathbb{F}_q^*$ is a root of the polynomial $x^t - 1$, hence, $t \geq q-1$, and so $t = q-1$.

Definition 1.1.7. A generator of the cyclic group $\mathbb{F}_q^*$ is called a *primitive element* of $\mathbb{F}_q$.

Let γ be a generator of $\mathbb{F}_q^*$. Then γ^n is also a generator of $\mathbb{F}_q^*$ if and only if $\gcd(n, q-1) = 1$. Thus, we have the following result.

Corollary 1.1.8. There are exactly $\phi(q-1)$ primitive elements of $\mathbb{F}_q$, where ϕ is the Euler totient function.

1.2 Algebraic Closure of Finite Fields

Let p be the characteristic of $\mathbb{F}_q$. It is clear that the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$ is the same as $\overline{\mathbb{F}_p}$.

Theorem 1.2.1. The algebraic closure of $\mathbb{F}_q$ is the union $\cup_{n=1}^{\infty}\mathbb{F}_{q^n}$.

Proof. Put $U := \cup_{n=1}^{\infty}\mathbb{F}_{q^n}$. It is clear that U is a subset of $\overline{\mathbb{F}_q}$ since $\mathbb{F}_{q^n}$ is a subset of $\overline{\mathbb{F}_p}$. It is also easy to verify that U forms a field.

Let $f(x) = \sum_{i=0}^{s}\lambda_i x^i$ be a nonconstant polynomial over U. Then for $0 \leq i \leq s$ we have $\lambda_i \in \mathbb{F}_{q^{m_i}}$ for some $m_i \geq 1$. Hence, by Theorem 1.1.5(iii), $f(x)$ is a polynomial over $\mathbb{F}_{q^m}$, where $m = \prod_{i=0}^{s} m_i$. Let α be a root of $f(x)$. Then $\mathbb{F}_{q^m}(\alpha)$ is an algebraic extension of $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^m}(\alpha)$ is a finite-dimensional vector space over $\mathbb{F}_{q^m}$. Hence, $\mathbb{F}_{q^m}(\alpha)$ is also a finite field containing $\mathbb{F}_q$. Let r be the degree of $\mathbb{F}_{q^m}(\alpha)$ over $\mathbb{F}_{q^m}$. Then $\mathbb{F}_{q^m}(\alpha)$ contains exactly q^{rm} elements, that is, $\mathbb{F}_{q^m}(\alpha) = \mathbb{F}_{q^{rm}}$. So α is an element of U. This shows that U is the algebraic closure $\overline{\mathbb{F}_q}$.

We are going to devote the rest of this section to the study of the Galois group $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. We start from the definition of the inverse limit for finite groups. For a detailed discussion of inverse limits of groups, we refer to the book by Wilson [130].

A *directed set* is a nonempty partially ordered set I such that for all $i_1, i_2 \in I$, there is an element $j \in I$ for which $i_1 \leq j$ and $i_2 \leq j$.

Definition 1.2.2. An *inverse system* $\{G_i, \varphi_{ij}\}$ of finite groups indexed by a directed set I consists of a family $\{G_i : i \in I\}$ of finite groups and a family $\{\varphi_{ij} \in \mathrm{Hom}(G_j, G_i) : i, j \in I,\ i \leq j\}$ of maps such that φ_{ii} is the identity on G_i for each i and $\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik}$ whenever $i \leq j \leq k$. Here, $\mathrm{Hom}(G_j, G_i)$ denotes the set of group homomorphisms from G_j to G_i.

For an inverse system $\{G_i, \varphi_{ij}\}$ of finite groups indexed by a directed set I, we form the Cartesian product $\prod_{i\in I} G_i$, viewed as a product group. We consider the subset of $\prod_{i\in I} G_i$ given by

$$D := \left\{ (x_i) \in \prod_{i\in I} G_i : \varphi_{ij}(x_j) = x_i \quad \text{for all } i, j \in I \quad \text{with } i \leq j \right\}.$$

It is easy to check that D forms a subgroup of $\prod_{i\in I} G_i$. We call D the *inverse limit* of $\{G_i, \varphi_{ij}\}$, denoted by $\lim_{\leftarrow} G_i$.

Example 1.2.3. Define a partial order in the set $\mathbb{N}$ of positive integers as follows: for $m, n \in \mathbb{N}$, let $m \leq n$ if and only if m divides n. For each positive integer i, let G_i be the cyclic group $\mathbb{Z}/i\mathbb{Z}$, and for each pair $(i, j) \in \mathbb{N}^2$ with $i|j$, define $\varphi_{ij} : \overline{n} \in G_j \mapsto \overline{n} \in G_i$, with the bar indicating the formation of a residue class. Then it is easy to verify that the family $\{\mathbb{Z}/i\mathbb{Z}, \varphi_{ij}\}$ forms an inverse system of finite groups indexed by $\mathbb{N}$. The inverse limit $\lim_{\leftarrow} \mathbb{Z}/i\mathbb{Z}$ is denoted by $\hat{\mathbb{Z}}$.

Example 1.2.4. Now let $\mathbb{F}_q$ be the finite field with q elements. We consider the family of Galois groups $G_i := \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$ of $\mathbb{F}_{q^i}$ over $\mathbb{F}_q$ for each $i \in \mathbb{N}$. We define a partial order in $\mathbb{N}$ as in Example 1.2.3. For each pair $(i, j) \in \mathbb{N}^2$ with $i|j$, define the homomorphism φ_{ij}: $\sigma_j \in \mathrm{Gal}(\mathbb{F}_{q^j}/\mathbb{F}_q) \mapsto \sigma_j|_{\mathbb{F}_{q^i}} \in \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$, where $\sigma_j|_{\mathbb{F}_{q^i}}$ stands for the restriction of σ_j to $\mathbb{F}_{q^i}$. Then $\{\mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q), \varphi_{ij}\}$ forms an inverse system of finite groups indexed by $\mathbb{N}$.

Theorem 1.2.5. We have

$$\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \simeq \lim_{\leftarrow} \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q).$$

Proof. For each $i \in \mathbb{N}$, we have a homomorphism $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$ obtained by restriction. These together yield a homomorphism

$$\theta : \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to \prod_{i\in\mathbb{N}} \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q).$$

It is clear that the image of θ is contained in $\lim_{\leftarrow} \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$. We show in the following that θ is an isomorphism onto $\lim_{\leftarrow} \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$.

If $\sigma \neq 1$ is in $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, then there exists an element $x \in \overline{\mathbb{F}_q}$ such that $\sigma(x) \neq x$. By Theorem 1.2.1, x belongs to $\mathbb{F}_{q^n}$ for some $n \in \mathbb{N}$. Now the image of σ in $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ maps x to $\sigma(x)$, and thus $\theta(\sigma)$ is not the identity. Hence, θ is injective.

Take (σ_i) in $\lim_{\leftarrow} \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$. If $x \in \overline{\mathbb{F}_q}$ and we set $\sigma(x) = \sigma_i(x)$, where $x \in \mathbb{F}_{q^i}$, then this is an unambiguous definition of a map $\sigma : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$. It is easy to check that σ is an element of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. Since $\theta(\sigma) = (\sigma_i)$, $\lim_{\leftarrow} \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$ is the image of θ.

Corollary 1.2.6. We have

$$\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \simeq \hat{\mathbb{Z}}.$$

Proof. For each $i \in \mathbb{N}$, we can identify the group $\mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$ with $\mathbb{Z}/i\mathbb{Z}$ by Theorem 1.1.5(ii). Under this identification, the family of homomorphisms in Example 1.2.4 coincides with that in Example 1.2.3. Thus, the desired result follows from Theorem 1.2.5.

It is another direct consequence of Theorem 1.2.5 that the restrictions of all automorphisms in $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ to $\mathbb{F}_{q^m}$ give all automorphisms in $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, that is, we obtain the following result.

Corollary 1.2.7. For every integer $m \geq 1$, we have

$$\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \{\sigma|_{\mathbb{F}_{q^m}} : \sigma \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)\}.$$

For each $i \in \mathbb{N}$, let $\pi_i \in \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$ be the automorphism $\pi_i : x \mapsto x^q$. Then the element (π_i) is in $\lim_{\leftarrow} \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$. This yields an automorphism in $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. We call it the *Frobenius (automorphism)* of $\overline{\mathbb{F}_q}/\mathbb{F}_q$, denoted by π. It is clear that $\pi(x) = x^q$ for all $x \in \overline{\mathbb{F}_q}$ and that the restriction of π to $\mathbb{F}_{q^i}$ is π_i, the *Frobenius (automorphism)* of $\mathbb{F}_{q^i}/\mathbb{F}_q$.

1.3 Irreducible Polynomials

Let $\alpha \in \overline{\mathbb{F}_q}$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. The element $\sigma(\alpha)$ is called a *conjugate* of α with respect to $\mathbb{F}_q$.

Lemma 1.3.1. The set of conjugates of an element $\alpha \in \overline{\mathbb{F}_q}$ with respect to $\mathbb{F}_q$ is equal to $\{\pi^i(\alpha) : i = 0, 1, 2, \ldots\}$, where $\pi \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ is the Frobenius automorphism.

Proof. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. There exists an integer $m \geq 1$ such that α is an element of $\mathbb{F}_{q^m}$. Then the restrictions $\sigma|_{\mathbb{F}_{q^m}}$ and $\pi|_{\mathbb{F}_{q^m}}$ are both elements of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Moreover, $\pi|_{\mathbb{F}_{q^m}}$ is a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Thus, $\sigma|_{\mathbb{F}_{q^m}} = (\pi|_{\mathbb{F}_{q^m}})^i$ for some $i \geq 0$. Hence, $\sigma(\alpha) = \sigma|_{\mathbb{F}_{q^m}}(\alpha) = (\pi|_{\mathbb{F}_{q^m}})^i(\alpha) = \pi^i(\alpha)$.

Proposition 1.3.2. All distinct conjugates of an element $\alpha \in \overline{\mathbb{F}_q}$ with respect to $\mathbb{F}_q$ are $\alpha, \pi(\alpha), \ldots, \pi^{m-1}(\alpha)$, where m is the least positive integer such that $\mathbb{F}_{q^m}$ contains α, that is, m is such that $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$.

Proof. The restriction $\pi|_{\mathbb{F}_{q^m}}$ of π to $\mathbb{F}_{q^m}$ has order m since it is a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Hence, $\pi^m(\alpha) = (\pi|_{\mathbb{F}_{q^m}})^m(\alpha) = \alpha$. This implies that $\alpha, \pi(\alpha), \ldots, \pi^{m-1}(\alpha)$ yield all conjugates of α. It remains to show that they are pairwise distinct. Suppose that $\pi^n(\alpha) = \alpha$ for some $n \geq 1$. Then it is clear that $\pi^n(\beta) = \beta$ for all $\beta \in \mathbb{F}_q(\alpha)$, that is, $\beta^{q^n} - \beta = 0$ for all elements $\beta \in \mathbb{F}_{q^m}$. Thus, the polynomial $x^{q^n} - x$ has at least q^m roots. Hence, $n \geq m$. This implies that $\alpha, \pi(\alpha), \ldots, \pi^{m-1}(\alpha)$ are pairwise distinct.

Corollary 1.3.3. All distinct conjugates of an element $\alpha \in \overline{\mathbb{F}_q}$ with respect to $\mathbb{F}_q$ are $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$, where m is the least positive integer such that $\mathbb{F}_{q^m}$ contains α, that is, m is such that $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$.

Proof. This follows from Proposition 1.3.2 and the fact that $\pi(\alpha) = \alpha^q$.

By field theory, all conjugates of α with respect to $\mathbb{F}_q$ form the set of all roots of the minimal polynomial of α over $\mathbb{F}_q$. Hence, we get the following result.

Corollary 1.3.4. Let f be an irreducible polynomial over $\mathbb{F}_q$ of degree m and let $\alpha \in \overline{\mathbb{F}_q}$ be a root of f. Then $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ are all distinct roots of f, and moreover $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$.

From the above result we obtain that all roots of an irreducible polynomial f over $\mathbb{F}_q$ are simple and that $\mathbb{F}_{q^m}$ is the splitting field of f over $\mathbb{F}_q$, where $m = \deg(f)$.

Lemma 1.3.5. A monic irreducible polynomial $f(x)$ of degree m over $\mathbb{F}_q$ divides $x^{q^n} - x$ if and only if m divides n.

Proof. Let $\alpha \in \overline{\mathbb{F}_q}$ be a root of $f(x)$. Then we have $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$ by Corollary 1.3.4. If m divides n, then $\mathbb{F}_{q^m}$ is a subfield of $\mathbb{F}_{q^n}$ by Theorem 1.1.5(iii). From Proposition 1.1.1(iii) we get $\beta^{q^n} - \beta = 0$ for all $\beta \in \mathbb{F}_{q^n}$. In particular, $\alpha^{q^n} - \alpha = 0$. Hence, the minimal polynomial $f(x)$ of α over $\mathbb{F}_q$ divides $x^{q^n} - x$.

If $f(x)$ divides $x^{q^n} - x$, then $\alpha^{q^n} - \alpha = 0$. Hence, $\alpha \in \mathbb{F}_{q^n}$ by the existence part of the proof of Theorem 1.1.2. Now $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^n}$ and our desired result follows from Theorem 1.1.5(iii).

Since $x^{q^n} - x$ has no multiple roots, we know from Lemma 1.3.5 that the product of all monic irreducible polynomials over $\mathbb{F}_q$ whose degrees divide n is equal to $x^{q^n} - x$. From this we obtain the number of monic irreducible polynomials over $\mathbb{F}_q$ of given degree, as stated in the following theorem.

Theorem 1.3.6. Let $I_q(n)$ be the number of monic irreducible polynomials over $\mathbb{F}_q$ of fixed degree $n \geq 1$. Then

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d},$$

where the sum is over all positive integers d dividing n and μ is the Möbius function on $\mathbb{N}$ defined by

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1, \\ (-1)^r & \text{if } d \text{ is the product of } r \text{ distinct primes}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Since the product of all monic irreducible polynomials over $\mathbb{F}_q$ whose degrees divide n is equal to $x^{q^n} - x$, we obtain the identity

$$q^n = \sum_{d|n} d\, I_q(d)$$

by comparing degrees. Applying the Möbius inversion formula (e.g., see [72, p. 92]), we get the desired result.

1.4 Trace and Norm

In this section, we discuss two maps from the field $\mathbb{F}_{q^m}$ to the field $\mathbb{F}_q$: trace and norm.

Definition 1.4.1. The *trace* map $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ is defined to be

$$\sum_{\sigma \in G} \sigma,$$

where $G := \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, that is, for any $\alpha \in \mathbb{F}_{q^m}$, we put

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha).$$

If there is no confusion, we simply denote the map by Tr.

For any $\tau \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and $\alpha \in \mathbb{F}_{q^m}$, we have

$$\tau(\mathrm{Tr}(\alpha)) = \tau\left(\sum_{\sigma \in G} \sigma(\alpha)\right) = \sum_{\sigma \in G} (\tau\sigma)(\alpha) = \sum_{\sigma \in G} \sigma(\alpha) = \mathrm{Tr}(\alpha).$$

Thus indeed, Tr is a map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Furthermore, the trace map has the following properties.

Proposition 1.4.2.

(i) $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$ for all $\alpha, \beta \in \mathbb{F}_{q^m}$.
(ii) $\mathrm{Tr}(a\alpha) = a\mathrm{Tr}(\alpha)$ for all $\alpha \in \mathbb{F}_{q^m}$ and $a \in \mathbb{F}_q$.

(iii) $\mathrm{Tr}(\sigma(\alpha)) = \mathrm{Tr}(\alpha)$ for all $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and $\alpha \in \mathbb{F}_{q^m}$. In particular, $\mathrm{Tr}(\pi(\alpha)) = \mathrm{Tr}(\alpha^q) = \mathrm{Tr}(\alpha)$, where $\pi \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is the Frobenius.

The proof of the above proposition easily follows from the definition of the trace map. We glean from (i) and (ii) of the above proposition that Tr is a linear transformation when we view $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$ as vector spaces over $\mathbb{F}_q$.

Since π is a generator of the cyclic group $G = \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ of order m, we have $\mathrm{Tr} = \sum_{\sigma \in G} \sigma = \sum_{i=0}^{m-1} \pi^i$. Hence, for any $\alpha \in \mathbb{F}_{q^m}$, we have

$$\mathrm{Tr}(\alpha) = \sum_{i=0}^{m-1} \pi^i(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}.$$

Theorem 1.4.3.

(i) The trace map is surjective. Thus, the kernel of Tr is a vector space of dimension $m - 1$ over $\mathbb{F}_q$.
(ii) An element α of $\mathbb{F}_{q^m}$ satisfies $\mathrm{Tr}(\alpha) = 0$ if and only if $\alpha = \pi(\beta) - \beta = \beta^q - \beta$ for some $\beta \in \mathbb{F}_{q^m}$.

Proof.

(i) An element α of $\mathbb{F}_{q^m}$ is in the kernel of Tr if and only if α is a root of the polynomial $x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}$. Thus, the kernel of Tr contains at most q^{m-1} elements. Therefore, there are at least $q^m/q^{m-1} = q$ elements in the image of Tr. Since the image of Tr is a subset of $\mathbb{F}_q$, we conclude that the image is the same as $\mathbb{F}_q$. As the dimension of the $\mathbb{F}_q$-linear space $\mathbb{F}_{q^m}$ is m, the dimension of the kernel is equal to $m - 1$.
(ii) Consider the $\mathbb{F}_q$-linear map $\phi : \gamma \in \mathbb{F}_{q^m} \mapsto \pi(\gamma) - \gamma$. By Proposition 1.4.2(iii), the image $\mathrm{Im}(\phi)$ is contained in the kernel of Tr. Now $\phi(\gamma) = 0$ if and only if $\pi(\gamma) = \gamma$. This is equivalent to γ being an element of $\mathbb{F}_q$. Hence, the kernel of ϕ is $\mathbb{F}_q$. So $\mathrm{Im}(\phi)$ contains $q^m/q = q^{m-1}$ elements. This implies that $\mathrm{Im}(\phi)$ is the same as the kernel of Tr. Therefore, $\mathrm{Tr}(\alpha) = 0$ if and only if $\alpha \in \mathrm{Im}(\phi)$, that is, there exists an element $\beta \in \mathbb{F}_{q^m}$ such that $\alpha = \phi(\beta) = \pi(\beta) - \beta$.

Definition 1.4.4. The *norm* map $\mathrm{Nm}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ is defined to be

$$\prod_{\sigma \in G} \sigma,$$

where $G := \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, that is, for any $\alpha \in \mathbb{F}_{q^m}$, we put

$$\mathrm{Nm}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

If there is no confusion, we simply denote the map by Nm.

For any $\tau \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and $\alpha \in \mathbb{F}_{q^m}$, we have

$$\tau(\mathrm{Nm}(\alpha)) = \tau\left(\prod_{\sigma \in G} \sigma(\alpha)\right) = \prod_{\sigma \in G} (\tau\sigma)(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) = \mathrm{Nm}(\alpha).$$

Thus indeed, Nm is a map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Furthermore, the norm map has the following properties.

Proposition 1.4.5.

(i) $\mathrm{Nm}(\alpha \cdot \beta) = \mathrm{Nm}(\alpha) \cdot \mathrm{Nm}(\beta)$ for all $\alpha, \beta \in \mathbb{F}_{q^m}$.
(ii) $\mathrm{Nm}(a\alpha) = a^m \mathrm{Nm}(\alpha)$ for all $\alpha \in \mathbb{F}_{q^m}$ and $a \in \mathbb{F}_q$.
(iii) $\mathrm{Nm}(\sigma(\alpha)) = \mathrm{Nm}(\alpha)$ for all $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and $\alpha \in \mathbb{F}_{q^m}$. In particular, $\mathrm{Nm}(\pi(\alpha)) = \mathrm{Nm}(\alpha^q) = \mathrm{Nm}(\alpha)$, where $\pi \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is the Frobenius.

The proof of the above proposition easily follows from the definition of the norm map. We obtain from (i) of the above proposition that Nm is a group homomorphism from $\mathbb{F}_{q^m}^*$ to $\mathbb{F}_q^*$.

Since π is a generator of the cyclic group $G = \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ of order m, we have $\mathrm{Nm} = \prod_{\sigma \in G} \sigma = \prod_{i=0}^{m-1} \pi^i$. Hence, for any $\alpha \in \mathbb{F}_{q^m}$, we have

$$\mathrm{Nm}(\alpha) = \prod_{i=0}^{m-1} \pi^i(\alpha) = \alpha \cdot \alpha^q \cdot \alpha^{q^2} \cdot \cdots \cdot \alpha^{q^{m-1}}.$$

Theorem 1.4.6.

(i) The norm map is an epimorphism from $\mathbb{F}_{q^m}^*$ to $\mathbb{F}_q^*$. Thus, the kernel of Nm is a cyclic group of order $(q^m - 1)/(q - 1)$.
(ii) An element α of $\mathbb{F}_{q^m}$ satisfies $\mathrm{Nm}(\alpha) = 1$ if and only if $\alpha = \pi(\beta)/\beta = \beta^{q-1}$ for some $\beta \in \mathbb{F}_{q^m}^*$.

Proof. Using similar arguments as in the proof of Theorem 1.4.3 and replacing Tr by Nm, we obtain the desired results.

1.5 Function Fields of One Variable

For a given field k, a *function field* over k is a field extension F of k such that there is at least one element $x \in F$ that is transcendental over k. The field k is called a *constant field* of F.

For a function field F over k, we consider the set k_1 of elements of F that are algebraic over k. It is clear that k_1 is a field since sums, products, and inverses of algebraic elements over k are again algebraic over k. Hence, we have the chain of fields $k \subseteq k_1 \subseteq F$.

Lemma 1.5.1. Let F be a function field over k and let k_1 be the set of elements of F that are algebraic over k. Then:

(i) F is also a function field over k_1;
(ii) k_1 is algebraically closed in F, that is, all elements in $F \setminus k_1$ are transcendental over k_1.

Proof.

(i) Let $x \in F$ be a transcendental element over k. We will show that x is also transcendental over k_1. Suppose that x were algebraic over k_1. Let $\sum_{i=0}^{n} c_i T^i$ with $c_i \in k_1$ be the minimal polynomial of x over k_1. Then x is algebraic over $k(c_0, c_1, \ldots, c_n)$. Hence, $k(c_0, c_1, \ldots, c_n, x)$ is a finite extension of $k(c_0, c_1, \ldots, c_n)$. Since all c_i are algebraic over k, it follows that $k(c_0, c_1, \ldots, c_n)$ is also a finite extension of k. Therefore, $[k(c_0, c_1, \ldots, c_n, x) : k] = [k(c_0, c_1, \ldots, c_n, x) : k(c_0, c_1, \ldots, c_n)] \cdot [k(c_0, c_1, \ldots, c_n) : k] < \infty$. Thus $[k(x) : k] \leq [k(c_0, c_1, \ldots, c_n, x) : k] < \infty$. This implies that x is algebraic over k, a contradiction.

(ii) It suffices to show that if $\alpha \in F$ is algebraic over k_1, then α is an element of k_1. Let $\alpha \in F$ be an algebraic element over k_1 and let $\sum_{i=0}^{n} c_i T^i$ with $c_i \in k_1$ be its minimal polynomial over k_1. With the same arguments as in the proof of (i), we can show that $[k(\alpha) : k] < \infty$, that is, α is algebraic over k. Hence, α is in k_1.

For a function field F over k, we say that k is algebraically closed in F if k is the same as $k_1 = \{\alpha \in F : \alpha \text{ is algebraic over } k\}$. In this case, we call k the *full constant field* of F. From now on we always mean that F is a function field over k with full constant field k whenever we write F/k. We will now concentrate on algebraic function fields of one variable, which are defined as follows.

Definition 1.5.2. The function field F/k is an *algebraic function field of one variable* over k if there exists a transcendental element $x \in F$ over k such that F is a finite extension of the rational function field $k(x)$. If in addition the full constant field k is finite, then F/k is called a *global function field*.

The study of algebraic function fields of one variable has a long history. Classical books on this topic include those by Chevalley [18] and Deuring [25]. The more recent book by Stichtenoth [117] puts a special emphasis on global function fields.

In the rest of this section, F/k will always denote an algebraic function field of one variable. We develop the theory of algebraic function fields of one variable by starting from the concept of a valuation. We add ∞ to the field $\mathbb{R}$ of real numbers to form the set $\mathbb{R} \cup \{\infty\}$, and we put $\infty + \infty = \infty + c = c + \infty = \infty$ for any $c \in \mathbb{R}$. We agree that $c < \infty$ for any $c \in \mathbb{R}$.

Definition 1.5.3. A *valuation* of F/k is a map $\nu : F \to \mathbb{R} \cup \{\infty\}$ satisfying the following conditions:

1. $\nu(z) = \infty$ if and only if $z = 0$;
2. $\nu(yz) = \nu(y) + \nu(z)$ for all $y, z \in F$;
3. $\nu(y + z) \geq \min(\nu(y), \nu(z))$ for all $y, z \in F$;
4. $\nu(F^*) \neq \{0\}$;
5. $\nu(\alpha) = 0$ for all $\alpha \in k^*$.

Remark 1.5.4.

(i) Condition (3) is called the *triangle inequality*. In fact, we have a stronger result called the *strict triangle inquality*, which says that

$$\nu(y+z) = \min(\nu(y), \nu(z)) \tag{1.1}$$

whenever $\nu(y) \neq \nu(z)$. In order to show (1.1), we can assume that $\nu(y) < \nu(z)$. Suppose that $\nu(y+z) \neq \min(\nu(y), \nu(z))$. Then $\nu(y+z) > \min(\nu(y), \nu(z)) = \nu(y)$ by condition (3). Thus $\nu(y) = \nu((y+z)-z) \geq \min(\nu(y+z), \nu((-1)\cdot z)) = \min(\nu(y+z), \nu(z)) > \nu(y)$, a contradiction.

(ii) If k is finite, then condition (5) follows from the other conditions in Definition 1.5.3. Note that if $k = \mathbb{F}_q$, then $\alpha^{q-1} = 1$ for all $\alpha \in k^*$ by Proposition 1.1.1(iii), and so $0 = \nu(1) = \nu(\alpha^{q-1}) = (q-1)\nu(\alpha)$, which yields $\nu(\alpha) = 0$.

If the image $\nu(F^*)$ is a discrete set in $\mathbb{R}$, then ν is called *discrete*. If $\nu(F^*) = \mathbb{Z}$, then ν is called *normalized*.

Example 1.5.5. Consider the rational function field $k(x)$. The full constant field of $k(x)$ is k since it is easily seen that a nonconstant rational function in $k(x)$ cannot be algebraic over k. Let $p(x)$ be a monic irreducible polynomial in $k[x]$. Let the map $\nu_{p(x)} : k(x) \to \mathbb{Z} \cup \{\infty\}$ be defined as follows:

(i) for a nonzero polynomial $f(x) \in k[x]$ with $p^m(x) \| f(x)$, that is, $p^m(x) | f(x)$ and $p^{m+1}(x) \nmid f(x)$, put $\nu_{p(x)}(f(x)) = m$;
(ii) for a nonzero rational function $f(x)/g(x) \in k(x)$, put $\nu_{p(x)}(f(x)/g(x)) = \nu_{p(x)}(f(x)) - \nu_{p(x)}(g(x))$;
(iii) put $\nu_{p(x)}(0) = \infty$.

It is easy to verify that $\nu_{p(x)}$ is a well-defined map and satisfies the conditions in Definition 1.5.3. Hence, $\nu_{p(x)}$ is a (discrete) normalized valuation of $k(x)$.

Besides the valuations $\nu_{p(x)}$ defined above, we have another (discrete) normalized valuation ν_∞ of $k(x)$ defined by

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

for any two nonzero polynomials $f(x), g(x) \in k[x]$ and $\nu_\infty(0) = \infty$. It is easy to show that ν_∞ is a well-defined valuation map.

We will see later in this section (see Theorem 1.5.8) that every normalized valuation of $k(x)$ is of the form $v_{p(x)}$ for some monic irreducible polynomial $p(x) \in k[x]$ or v_∞.

Two discrete valuations v and λ of F/k are called *equivalent* if there exists a constant $c > 0$ such that

$$v(z) = c\lambda(z) \quad \text{for all } z \in F^*.$$

Obviously, this yields an equivalence relation between discrete valuations of F/k. An equivalence class of discrete valuations of F/k is called a *place* of F/k.

If v is a discrete valuation of F/k, then $v(F^*)$ is a nonzero discrete subgroup of $(\mathbb{R}, +)$, and so we have $v(F^*) = b\mathbb{Z}$ for some positive $b \in \mathbb{R}$. Thus, there exists a uniquely determined normalized valuation of F that is equivalent to v. In other words, every place P of F/k contains a uniquely determined normalized valuation of F/k, which is denoted by v_P. Thus, we can identify places of F/k and (discrete) normalized valuations of F/k.

For a place P of F/k and an element $z \in F^*$, we say that P is a *zero* of z if $v_P(z) > 0$ and that P is a *pole* of z if $v_P(z) < 0$.

For the normalized valuation v_P of F/k we have $v_P(F^*) = \mathbb{Z}$. Thus, there exists an element $t \in F$ satisfying $v_P(t) = 1$. Such an element t is called a *local parameter* (or *uniformizing parameter*) of F at the place P.

For a place P of F/k, we set

$$\mathcal{O}_P = \{z \in F : v_P(z) \geq 0\}.$$

Using the properties of valuations, it is easy to show that $\mathcal{O}_P$ forms a subring of F with $k \subseteq \mathcal{O}_P$. We call $\mathcal{O}_P$ the *valuation ring* of the place P.

Proposition 1.5.6. The valuation ring $\mathcal{O}_P$ has a unique maximal ideal given by

$$\mathsf{M}_P := \{z \in F : v_P(z) \geq 1\}.$$

Proof. It is trivial that M_P is an ideal of $\mathcal{O}_P$. Since $1 \in \mathcal{O}_P \setminus \mathsf{M}_P$, we obtain that M_P is a proper ideal. It remains to show that any proper ideal J of $\mathcal{O}_P$ is contained in M_P. Take $z \in \mathsf{J}$ and suppose that $v_P(z) = 0$. Then $v_P(z^{-1}) = -v_P(z) = 0$, and so $z^{-1} \in \mathcal{O}_P$. Thus, $1 = z^{-1}z \in \mathsf{J}$ and, hence, $\mathsf{J} = \mathcal{O}_P$, a contradiction. Therefore, $v_P(z) \geq 1$ and $\mathsf{J} \subseteq \mathsf{M}_P$.

The ideal M_P is called the *maximal ideal* of the place P. It is, in fact, a principal ideal since $\mathsf{M}_P = t\mathcal{O}_P$ for any local parameter t of F at P.

Remark 1.5.7. Valuation rings in F/k can be characterized purely algebraically as the maximal proper Noetherian subrings of F/k, or also as the maximal principal ideal domains properly contained in F/k (see [105, Section 2.1]). A place of F/k can then be defined as the maximal ideal of some valuation ring in F/k. This alternative approach to the concept of a place is presented in the book of Stichtenoth [117].

We now determine all discrete valuations of the rational function field $k(x)$. The valuations $v_{p(x)}$ and v_∞ are defined as in Example 1.5.5.

Theorem 1.5.8. Every discrete valuation of the rational function field $k(x)$ is equivalent to either $v_{p(x)}$ for some monic irreducible polynomial $p(x)$ in $k[x]$ or to v_∞.

Proof. Let v be a discrete valuation of $k(x)$ and let P be its corresponding place. We distinguish two cases according to the value of $v(x)$.

Case 1: $v(x) \geq 0$. Then $k[x] \subseteq \mathcal{O}_P$ and $v(k(x)^*) \neq \{0\}$ by the properties of a valuation, and so $\mathsf{J} := k[x] \cap \mathsf{M}_P$ 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 $\mathcal{O}_P$, it follows that J is a prime ideal of $k[x]$. Consequently, there exists a monic irreducible $p(x) \in k[x]$ such that J is the principal ideal $(p(x))$. In particular, $c := v(p(x)) > 0$. If $h(x) \in k[x]$ is not divisible by $p(x)$, then $h(x) \notin \mathsf{M}_P$, and so $v(h(x)) = 0$. 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 $m \in \mathbb{Z}$ and $f(x), g(x) \in k[x]$ not divisible by $p(x)$, then

$$v(r(x)) = m v(p(x)) = c v_{p(x)}(r(x)),$$

and so v is equivalent to $v_{p(x)}$.

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

$$f(x) = \sum_{i=0}^{d} \alpha_i x^i = x^d \sum_{i=0}^{d} \alpha_i x^{i-d} = x^d \sum_{i=0}^{d} \alpha_{d-i} x^{-i}$$

with all $\alpha_i \in k$. Furthermore,

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

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

$$v\left(\sum_{i=0}^{d} \alpha_{d-i} x^{-i}\right) = 0$$

by the strict triangle inequality (see Remark 1.5.4(i)). It follows that

$$v(f(x)) = v(x^d) = -dv(x^{-1}) = cv_\infty(f(x)),$$

and so v is equivalent to v_∞.

Remark 1.5.9. If we write $\mathcal{O}_v = \{z \in F : v(z) \geq 0\}$ and $\mathsf{M}_v = \{z \in F : v(z) > 0\}$ for an arbitrary valuation v of F/k and let $\mathcal{O}_v$ and M_v play the roles of $\mathcal{O}_P$ and M_P, respectively, in the proof of Theorem 1.5.8, then the argument in the proof goes through. Thus, this proof demonstrates that every valuation of $k(x)$ is automatically discrete.

Theorem 1.5.8 shows that there are exactly two types of places of the rational function field $k(x)$: (i) the *finite places* containing some valuation $v_{p(x)}$; (ii) the *infinite place* containing the valuation v_∞. Note that the valuations $v_{p(x)}$ and v_∞ are nonequivalent since $v_{p(x)}(p(x)) = 1$, whereas $v_\infty(p(x)) < 0$. Furthermore, $v_{p(x)}$ and $v_{q(x)}$ are nonequivalent for distinct monic irreducible $p(x), q(x) \in k[x]$ since $v_{p(x)}(p(x)) = 1$, whereas $v_{q(x)}(p(x)) = 0$. Thus, there is a one-to-one correspondence between the finite places of $k(x)$ and the monic irreducible polynomials in $k[x]$. We may use this correspondence to speak, for instance, of the place $p(x)$ of $k(x)$ when

we mean the place containing the valuation $\nu_{p(x)}$. To summarize, the set of distinct places of $k(x)$ can be identified with the set

$$\{p(x) \in k[x] : p(x) \text{ monic irreducible}\} \cup \{\infty\}.$$

Definition 1.5.10. Let P be a place of the algebraic function field F/k of one variable over k. The field $F_P := \mathcal{O}_P/\mathsf{M}_P$ is called the *residue class field* of P. The canonical ring homomorphism

$$z \in \mathcal{O}_P \mapsto z(P) := z + \mathsf{M}_P \in F_P$$

is called the *residue class map* of P.

Example 1.5.11. Consider again the rational function field $k(x)$. If $p(x) \in k[x]$ is monic irreducible, then for the finite place $p(x)$ of $k(x)$, we have

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in k[x],\ p(x) \nmid g(x) \right\},$$
$$\mathsf{M}_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in k[x],\ p(x) | f(x),\ p(x) \nmid g(x) \right\}.$$

For any $h(x) \in k[x]$, we write $\overline{h(x)}$ for the residue class of $h(x)$ modulo the ideal $(p(x))$ of $k[x]$. If $p(x) \nmid h(x)$, then $\overline{h(x)} \in k[x]/(p(x))$ has a multiplicative inverse $\overline{h(x)}^{-1} \in k[x]/(p(x))$. The map $\psi_{p(x)} : \mathcal{O}_{p(x)} \to k[x]/(p(x))$ given by

$$\psi_{p(x)}\left(\frac{f(x)}{g(x)}\right) = \overline{f(x)}\ \overline{g(x)}^{-1} \quad \text{for all } \frac{f(x)}{g(x)} \in \mathcal{O}_{p(x)}$$

is well defined. Clearly, $\psi_{p(x)}$ is a surjective ring homomorphism with kernel $\mathsf{M}_{p(x)}$, and so the residue class field of the place $p(x)$ is isomorphic to $k[x]/(p(x))$. For the infinite place ∞ of $k(x)$, we have

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in k[x],\ g(x) \neq 0,\ \deg(f(x)) \leq \deg(g(x)) \right\},$$
$$\mathsf{M}_\infty = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in k[x],\ \deg(f(x)) < \deg(g(x)) \right\},$$

where we put as usual $\deg(0) = -\infty$. Every $r(x) \in \mathcal{O}_\infty$ can be written in the form

$$r(x) = \frac{\alpha_d x^d + \alpha_{d-1} x^{d-1} + \cdots + \alpha_0}{x^d + \beta_{d-1} x^{d-1} + \cdots + \beta_0}$$

with all $\alpha_i, \beta_j \in k$ and $d \geq 0$. The map $\psi_\infty : \mathcal{O}_\infty \to k$ given by

$$\psi_\infty(r(x)) = \alpha_d \quad \text{for all } r(x) \in \mathcal{O}_\infty$$

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.

Theorem 1.5.12. Every valuation of an algebraic function field of one variable is discrete.

Proof. Let F/k be an algebraic function field of one variable. By Definition 1.5.2, there exists a transcendental element $x \in F$ over k such that F is a finite extension of $K := k(x)$. Let ν be an arbitrary valuation of F and let ξ be the restriction of ν to K. It suffices to prove that the index $[\nu(F^*) : \xi(K^*)]$ is finite. Since $\nu(F^*)$ is an infinite subgroup of $(\mathbb{R}, +)$, this shows then that $\xi(K^*) = \{0\}$ is not possible. Hence, ξ is a valuation of K, thus discrete by Remark 1.5.9, and so ν is discrete.

Let $z_1, \ldots, z_n \in F^*$ be such that $\nu(z_1), \ldots, \nu(z_n)$ are in distinct cosets modulo $\xi(K^*)$. We claim that $z_1, \ldots, z_n$ are linearly independent over K. This will then show that

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

So, suppose we had

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

where without loss of generality all $b_i \in K^*$. If we had $\nu(b_i z_i) = \nu(b_j z_j)$ for some i and j with $1 \leq i < j \leq n$, then

$$\nu(z_i) - \nu(z_j) = \nu(b_j) - \nu(b_i) = \xi(b_j b_i^{-1}) \in \xi(K^*),$$

a contradiction to the choice of $z_1, \ldots, z_n$. Thus, $\nu(b_1 z_1), \ldots, \nu(b_n z_n)$ are all distinct, and so the strict triangle inequality yields

$$\nu\left(\sum_{i=1}^{n} b_i z_i\right) = \min_{1 \le i \le n} \nu(b_i z_i) < \infty,$$

which is again a contradiction.

In the above proof, we have shown, in particular, that the restriction of a valuation of F/k to $k(x)$ yields a valuation of $k(x)$. 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 $k(x)$. We say that Q *lies over* P or that P *lies under* Q. Therefore, every place of F lies either over a place of $k(x)$ corresponding to a monic irreducible polynomial in $k[x]$ or over the infinite place of $k(x)$.

Theorem 1.5.13. The residue class field of every place of F/k 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 $K := k(x)$ with x as in Definition 1.5.2. Let $R_Q := \mathcal{O}_Q/\mathsf{M}_Q$ and $R_P := \mathcal{O}_P/\mathsf{M}_P$ be the corresponding residue class fields and note that $\mathcal{O}_P \subseteq \mathcal{O}_Q$. The map $\rho : R_P \to R_Q$ given by

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

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 $z_1, \ldots, z_n \in \mathcal{O}_Q$ be such that $z_1 + \mathsf{M}_Q, \ldots, z_n + \mathsf{M}_Q$ are linearly independent over $\rho(R_P)$. We claim that $z_1, \ldots, z_n$ are linearly independent over K. This will then show that

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

Since R_P is a finite extension (of an isomorphic copy) of k (see Example 1.5.11), this proves the theorem. So, suppose we had

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

with $b_1, \ldots, b_n \in K$ not all 0. Without loss of generality

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

Then $b_1 \neq 0$ and

$$z_1 + \sum_{i=2}^{n} b_i b_1^{-1} z_i = 0.$$

By the condition on $v_P(b_1)$, we have $b_i b_1^{-1} \in \mathcal{O}_P$ for $2 \le i \le n$. Passing to the residue classes modulo M_Q, we get

$$(z_1 + \mathsf{M}_Q) + \sum_{i=2}^{n} \rho(b_i b_1^{-1} + \mathsf{M}_P)(z_i + \mathsf{M}_Q) = 0 + \mathsf{M}_Q,$$

a contradiction to the choice of $z_1, \ldots, z_n$.

In view of Theorem 1.5.13, the following definition is meaningful.

Definition 1.5.14. 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.

Example 1.5.15. Let $F = k(x)$ be the rational function field over k. As we noted in Example 1.5.5, the full constant field of F is k. By Example 1.5.11, 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 infinite place of F is equal to 1. If $k = \mathbb{F}_q$, then the rational function field F has thus exactly $q + 1$ rational places.

Next we prove the approximation theorem for valuations of algebraic function fields of one variable. The following two preparatory results are needed for the proof.

Lemma 1.5.16. If P_1 and P_2 are two distinct places of F/k, then there exists an element $z \in F$ such that $v_{P_1}(z) > 0$ and $v_{P_2}(z) \le 0$.

Proof. First consider any $u \in F$ with $v_{P_2}(u) = 0$. If $v_{P_1}(u) \neq 0$, then either $z = u$ or $z = u^{-1}$ works. Thus, we are left with the case where $v_{P_2}(u) = 0$ always implies $v_{P_1}(u) = 0$.

Let $y \in F^*$ be arbitrary and let $t \in F$ be a local parameter at P_2. Then we can write $y = t^n u$ with $n \in \mathbb{Z}$ and $v_{P_2}(u) = 0$. It follows that $v_{P_1}(u) = 0$, and so $v_{P_1}(y) = n v_{P_1}(t)$. Since v_{P_1} is normalized, we must have $v_{P_1}(t) = \pm 1$. If $v_{P_1}(t) = 1$, then $v_{P_1}(y) = n = v_{P_2}(y)$ for all $y \in F^*$, a contradiction to $P_1 \neq P_2$. Thus, $v_{P_1}(t) = -1$, and then we take $z = t^{-1}$.

Lemma 1.5.17. If $P_1, \ldots, P_n$ are distinct places of F/k, then there exists an element $z \in F$ such that $v_{P_1}(z) > 0$ and $v_{P_i}(z) < 0$ for $2 \leq i \leq n$.

Proof. We proceed by induction on n. For $n = 2$, we apply Lemma 1.5.16 and we get $w \in F$ with $v_{P_1}(w) > 0$ and $v_{P_2}(w) \leq 0$ as well as $y \in F$ with $v_{P_2}(y) > 0$ and $v_{P_1}(y) \leq 0$. Then we take $z = wy^{-1}$.

Assume that the lemma is true for $n - 1$ distinct places for some $n \geq 3$. By this hypothesis, there exists $w \in F$ such that $v_{P_1}(w) > 0$ and $v_{P_i}(w) < 0$ for $2 \leq i \leq n - 1$. There also exists $y \in F$ with $v_{P_1}(y) > 0$ and $v_{P_n}(y) < 0$. If $v_{P_n}(w) < 0$, we take $z = w$. If $v_{P_n}(w) \geq 0$, we put $z = w + y^r$ with an integer $r \geq 1$. Then $v_{P_1}(z) > 0$, and for $2 \leq i \leq n$ we obtain

$$v_{P_i}(z) = \min\left(v_{P_i}(w), r v_{P_i}(y)\right) < 0$$

by choosing r in such a way that the strict triangle inequality applies.

Theorem 1.5.18 (Approximation Theorem). Let $P_1, \ldots, P_n$ be distinct places of F/k. Then for any given elements $w_1, \ldots, w_n \in F$ and integers $m_1, \ldots, m_n$, there exists an element $z \in F$ such that

$$v_{P_i}(z - w_i) = m_i \quad \text{for } 1 \leq i \leq n.$$

Proof. We first treat the special case $w_1 = 1$, $w_2 = \cdots = w_n = 0$, and we show the weaker result that there exists $y \in F$ with

$$v_{P_1}(y - 1) > m_1, \qquad v_{P_i}(y) > m_i \quad \text{for } 2 \leq i \leq n. \tag{1.2}$$

By Lemma 1.5.17 we get $w \in F$ with $v_{P_1}(w) > 0$ and $v_{P_i}(w) < 0$ for $2 \le i \le n$. Now put $y = (1 + w^s)^{-1}$ with an integer $s \ge 1$. Then for sufficiently large s we have $v_{P_1}(y-1) = v_{P_1}(-w^s(1+w^s)^{-1}) = sv_{P_1}(w) > m_1$ and $v_{P_i}(y) = -v_{P_i}(1 + w^s) = -sv_{P_i}(w) > m_i$ for $2 \le i \le n$.

Now let $w_1, \ldots, w_n \in F$ be arbitrary. Choose $b \in \mathbb{Z}$ such that $v_{P_i}(w_j) \ge b$ for all $1 \le i, j \le n$ and put $d_i = m_i - b$ for $1 \le i \le n$. By (1.2) we obtain $y_1, \ldots, y_n \in F$ such that for $1 \le i, j \le n$ we have

$$v_{P_i}(y_i - 1) > d_i, \qquad v_{P_i}(y_j) > d_i \quad \text{for } j \ne i.$$

Let $y = \sum_{j=1}^{n} w_j y_j$. Then we can write

$$y - w_i = w_i(y_i - 1) + \sum_{\substack{j=1 \\ j \ne i}}^{n} w_j y_j,$$

and so

$$v_{P_i}(y - w_i) > b + d_i = m_i \quad \text{for } 1 \le i \le n \tag{1.3}$$

by the triangle inequality.

Finally, for each $i = 1, \ldots, n$, choose $u_i \in F$ such that $v_{P_i}(u_i) = m_i$. By (1.3) there exists $z \in F$ with

$$v_{P_i}(z - (u_i + w_i)) > m_i \quad \text{for } 1 \le i \le n.$$

Then

$$v_{P_i}(z - w_i) = \min\left(v_{P_i}(z - u_i - w_i), v_{P_i}(u_i)\right) = m_i$$

for $1 \le i \le n$ by the strict triangle inequality.

Let P be a place of F/k and let $t \in F$ be a local parameter of F at P. Given an element $z \in F$, we choose an integer r such that $v_P(z) \ge r$. Then $zt^{-r} \in \mathcal{O}_P$, and so we can put

$$a_r = (zt^{-r})(P).$$

Note that a_r is an element of the residue class field F_P of P. Next we observe that

$$v_P(z - a_r t^r) \geq r + 1,$$

and so

$$v_P(zt^{-r-1} - a_r t^{-1}) \geq 0.$$

Thus, we can put

$$a_{r+1} = (zt^{-r-1} - a_r t^{-1})(P).$$

Then $a_{r+1} \in F_P$ and

$$v_P(z - a_r t^r - a_{r+1} t^{r+1}) \geq r + 2.$$

Now we construct further elements $a_j \in F_P$ inductively. Assume that for an integer $m > r$ we have already obtained elements $a_r, a_{r+1}, \ldots, a_m \in F_P$ such that

$$v_P\left(z - \sum_{j=r}^{m} a_j t^j\right) \geq m + 1.$$

Then we put

$$a_{m+1} = \left(zt^{-m-1} - \sum_{j=r}^{m} a_j t^{j-m-1}\right)(P) \in F_P,$$

and this yields

$$v_P\left(z - \sum_{j=r}^{m+1} a_j t^j\right) \geq m + 2.$$

We summarize this construction in the formal expansion

$$z = \sum_{j=r}^{\infty} a_j t^j \tag{1.4}$$

which is called the *local expansion* of z at P. Note that if $a_r \neq 0$ in (1.4), then $v_P(z) = r$.

1.6 Extensions of Valuations

Let F/k and E/k' be algebraic function fields of one variable such that $F \subseteq E$, $[E : F] < \infty$, and their full constant fields k and k' satisfy $k \subseteq k'$. Note that then $[k' : k] < \infty$. In this section we discuss the relationships between valuations, or equivalently places, of F and E. More general situations in which a valuation is extended from a given field to an extension field are treated in the books of Ribenboim [105] and Weiss [129].

Lemma 1.6.1. For any valuation v of E/k', we have

$$[v(E^*) : v(F^*)] \leq [E : F] < \infty.$$

Proof. This is shown in the same way as in the special case considered in the proof of Theorem 1.5.12.

If v is a valuation of E/k', then it is trivial that its restriction to F/k satisfies the conditions (1), (2), (3), and (5) in Definition 1.5.3. Moreover, Lemma 1.6.1 implies that the restriction also has the property (4). Thus, the restriction of v to F/k yields a valuation of F/k. Clearly, for equivalent valuations of E the restrictions are again equivalent. Hence, a place Q of E corresponds by restriction to a unique place P of F. We extend a terminology introduced in Section 1.5 and say that Q *lies over* P or that P *lies under* Q. Recall that v_Q denotes the normalized valuation belonging to the place Q.

Definition 1.6.2. If the place Q of E lies over the place P of F, then the *ramification index* $e(Q|P)$ of Q over P is the positive integer

$$e(Q|P) := [v_Q(E^*) : v_Q(F^*)] = [\mathbb{Z} : v_Q(F^*)].$$

We say that Q is *unramified* in the extension E/F if $e(Q|P) = 1$, that Q is *ramified* in the extension E/F if $e(Q|P) > 1$, and that Q is *totally ramified* in the extension E/F if $e(Q|P) = [E : F]$.

With v_P denoting as usual the normalized valuation belonging to the place P, Definition 1.6.2 shows that

$$v_Q(z) = e(Q|P)v_P(z) \quad \text{for all } z \in F^*.$$

If the places Q and P are as above, then their residue class fields E_Q and F_P satisfy $[E_Q : k'] < \infty$ and $[F_P : k] < \infty$ according to Theorem 1.5.13. Furthermore, the well-defined map $z(P) \mapsto z(Q)$ for $z \in \mathcal{O}_P$ provides an embedding of F_P into E_Q, and so E_Q can be viewed as a finite extension of F_P.

Definition 1.6.3. If the place Q of E lies over the place P of F, then the *relative degree* $f(Q|P)$ of Q over P is the positive integer $f(Q|P) := [E_Q : F_P]$.

According to a general principle concerning extensions of valuations (see for example, [129, Theorem 1.6.5]), if the place P of F is given and $Q_1, \ldots, Q_r$ are distinct places of E lying over P, then

$$\sum_{i=1}^{r} e(Q_i|P) f(Q_i|P) \leq [E : F]. \tag{1.5}$$

This shows, in particular, that there can be at most $[E : F]$ places of E lying over P. Note also that if one of the places of E lying over P is totally ramified in E/F, then there can be no other places of E lying over P.

Definition 1.6.4. A place P of F *splits completely* in the extension E/F if there are exactly $[E : F]$ places of E lying over P.

It follows from (1.5) that if P splits completely in E/F, then $e(Q|P) = f(Q|P) = 1$ for each place Q of E lying over P.

Given a place P of F, does there exist a place of E lying over it? There is an elegant argument in Ribenboim [105, Chapter 4, Theorem 1], which uses Zorn's lemma and shows that any valuation of a field can be extended to any algebraic extension of the field. Explicit constructions of extended valuations can be found in Ribenboim [105, Chapter 4] and Weiss [129, Chapter 2].

It is a well-known fact (see [117, Theorem III.1.11]) that if the full constant field k of F is perfect, that is, if every algebraic extension of k is separable, and if $Q_1, \ldots, Q_r$ are *all* distinct places of E lying over P, then (1.5) can be strengthened to

$$\sum_{i=1}^{r} e(Q_i|P) f(Q_i|P) = [E : F]. \tag{1.6}$$

This provides an important relationship between ramification indices, relative degrees, and the degree of the extension E/F. Since every finite field is perfect (see, e.g., Corollary 1.3.4), (1.6) holds in particular if F (and therefore E) is a global function field.

1.7 Constant Field Extensions

Throughout this section, we are given:

(i) a global function field $F/\mathbb{F}_q$ with full constant field $\mathbb{F}_q$;
(ii) the composite field $F_n := F \cdot \mathbb{F}_{q^n}$, called a *constant field extension* of F and contained in a fixed algebraic closure of F, where n is a positive integer.

If $\mathbb{F}_{q^n} = \mathbb{F}_q(\beta)$, then we have $F_n = F(\beta)$. We recall from Theorem 1.1.5 (ii) that the Galois group $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is a cyclic group.

Lemma 1.7.1. With the notation above, we have:

(i) F_n/F is a cyclic extension with $[F_n : F] = n$ and $\mathrm{Gal}(F_n/F) \simeq \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$;
(ii) the full constant field of F_n is $\mathbb{F}_{q^n}$.

Proof.

(i) Let $\mathbb{F}_{q^n} = \mathbb{F}_q(\beta)$ and let f be the minimal polynomial of β over $\mathbb{F}_q$. We will prove that f is irreducible over F. Suppose that f had a factorization $f = gh$ over F with g and h monic and $\deg(g) \geq 1$, $\deg(h) \geq 1$. It is obvious that all roots of g and h are elements of $\mathbb{F}_{q^n}$. Hence, from the fact that the coefficients of a monic polynomial are polynomial expressions of its roots, it follows that g and h are polynomials over $\mathbb{F}_{q^n}$. Thus, all coefficients

of g and h are algebraic over $\mathbb{F}_q$. Hence, each coefficient of g and h is an element of $\mathbb{F}_q$ since $\mathbb{F}_q$ is algebraically closed in F, and we obtain a contradiction to f being irreducible over $\mathbb{F}_q$. This shows that $[F_n : F] = n$ and $\mathrm{Gal}(F_n/F) \simeq \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$.

(ii) It is trivial that the full constant field of F_n contains $\mathbb{F}_{q^n}$ since $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a finite extension. Let $z \in F_n$ be an algebraic element over $\mathbb{F}_{q^n}$. Then $\mathbb{F}_{q^n}(z)/\mathbb{F}_q$ is a finite extension, and so from (i) we get

$$n = [F_n : F] = [F \cdot \mathbb{F}_{q^n}(z) : F] = [\mathbb{F}_{q^n}(z) : \mathbb{F}_q].$$

Hence, $\mathbb{F}_{q^n}(z) = \mathbb{F}_{q^n}$, that is, $z \in \mathbb{F}_{q^n}$. This means that $\mathbb{F}_{q^n}$ is the full constant field of F_n.

By Lemma 1.7.1 we can identify $\mathrm{Gal}(F_n/F)$ with $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ in the following way. Let $\{\beta_1 = 1, \beta_2, \ldots, \beta_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then for any $\tau \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ and $x = \sum_{i=1}^{n} \beta_i x_i \in F_n$ with all $x_i \in F$, put

$$\tau(x) = \sum_{i=1}^{n} \tau(\beta_i) x_i.$$

Then τ is a Galois automorphism of F_n/F and all elements of $\mathrm{Gal}(F_n/F)$ are obtained in this way.

Theorem 1.7.2. Let $F_n = F \cdot \mathbb{F}_{q^n}$ be a constant field extension of F. Then for any place P of F and any place Q of F_n lying over P, the following holds:

(i) $e(Q|P) = 1$;
(ii) $\deg(Q) = d/\gcd(d, n)$, where $d = \deg(P)$ is the degree of P;
(iii) $f(Q|P) = n/\gcd(d, n)$;
(iv) there are exactly $\gcd(d, n)$ places of F_n lying over P.

Proof.

(i) Let $\{\beta_1, \ldots, \beta_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then its discriminant $\Delta(\beta_1, \ldots, \beta_n)$ is an element of $\mathbb{F}_q^*$, and so

$$v_P(\Delta(\beta_1, \ldots, \beta_n)) = 0.$$

Hence, $\{\beta_1, \ldots, \beta_n\}$ is a P-integral basis of F_n/F, that is, every element in the integral closure of $\mathcal{O}_P$ in F_n can be written as a linear combination of $\beta_1, \ldots, \beta_n$ with coefficients from $\mathcal{O}_P$. The desired conclusion follows now from Dedekind's discriminant theorem (see [129, Theorem 4.8.14]).

(ii) We first prove that the residue class field R_Q of Q is the composite field $F_P \cdot \mathbb{F}_{q^n}$, where F_P is the residue class field of P. It is obvious that $F_P \cdot \mathbb{F}_{q^n}$ can be viewed as a subfield of R_Q (compare with Section 1.6). Since a basis $\{\beta_1, \ldots, \beta_n\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a P-integral basis of F_n/F, we can write any element of R_Q in the form $z(Q)$, where

$$z = \sum_{i=1}^{n} z_i \beta_i$$

with $z_1, \ldots, z_n \in \mathcal{O}_P$. Hence,

$$z(Q) = \sum_{i=1}^{n} z_i(Q)\beta_i = \sum_{i=1}^{n} z_i(P)\beta_i \in F_P \cdot \mathbb{F}_{q^n},$$

showing that $R_Q = F_P \cdot \mathbb{F}_{q^n}$. This yields

$$\begin{aligned} \deg(Q) = [R_Q : \mathbb{F}_{q^n}] &= [F_P \cdot \mathbb{F}_{q^n} : \mathbb{F}_{q^n}] = [\mathbb{F}_{q^d} \cdot \mathbb{F}_{q^n} : \mathbb{F}_{q^n}] \\ &= \frac{d}{\gcd(d, n)}. \end{aligned}$$

(iii) We have

$$\begin{aligned} f(Q|P) = [R_Q : F_P] &= [F_P \cdot \mathbb{F}_{q^n} : F_P] = [\mathbb{F}_{q^d} \cdot \mathbb{F}_{q^n} : \mathbb{F}_{q^d}] \\ &= \frac{n}{\gcd(d, n)}. \end{aligned}$$

(iv) This follows from (i), (iii), and (1.6).