Chapter 1

Background on Function Fields

Some basic definitions and fundamental properties of algebraic function fields are introduced in this chapter. In particular, we focus on those concepts and results that are needed in the subsequent chapters, such as the Riemann-Roch theorem, divisor class groups, Galois extensions of algebraic function fields, ramification theory, constant field extensions, zeta functions, and the Hasse-Weil bound.

In later chapters, we will be interested only in algebraic function fields over finite fields, but a lot of the background material can be developed for arbitrary constant fields. In this chapter, we will not always state results in their most general form, but only in the form in which we need them. Most results will be presented here without proof since they are standard results from textbooks. The reader will find the books of Stichtenoth [152] and Weiss [173] particularly useful. We refer also to the books of Cassels and Fröhlich [13], Deuring [18], Koch [60], Moreno [82], Neukirch [85], and Stepanov [150], [151] for further background.

1.1 Riemann-Roch Theorem

In this section, we always assume that k is an arbitrary field. The field k will serve as the constant field of algebraic function fields.

An extension field F of k is called an **algebraic function field (of one variable) over** k if there exists an element z of F that is transcendental over k and such that F is a finite extension of the rational function field $k(z)$ over k. Furthermore, k is called the **full constant field** of F if k is algebraically closed in F, that is, if each element of F that is algebraic over k belongs to k. For brevity, we simply denote by F/k an algebraic function field (of one variable) with full constant field k. If the full constant field is clear from the context, we often write just F instead of F/k.

A **place** P of F is, by definition, the maximal ideal of some valuation ring of F. We denote by O_P the valuation ring corresponding to P. Later on we will also use the symbol M_P to stand for the ideal P.

A **normalized discrete valuation** of an algebraic function field F over k is a surjective

map $\nu : F \longrightarrow \mathbf{Z} \cup \{\infty\}$ which satisfies:

(i) $\nu(x) = \infty$ if and only if $x = 0$;

(ii) $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in F$;

(iii) $\nu(x + y) \geq \min(\nu(x), \nu(y))$ for all $x, y \in F$;

(iv) $\nu(a) = 0$ for any $a \in k^*$.

As a consequence of these axioms we get the following useful strengthening of (iii):

(iii') $\nu(x + y) = \min(\nu(x), \nu(y))$ for $x, y \in F$ with $\nu(x) \neq \nu(y)$.

There is a bijective correspondence between the places of F and the normalized discrete valuations of F.

For a place P of F, we write ν_P for the normalized discrete valuation of F corresponding to P. We denote by $\mathbf{P}_F$ the set of places of F. For a place P of F/k, its valuation ring

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

is a local ring. Its maximal ideal is

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

The residue class field O_P/M_P, denoted by $\tilde{F}_P$, can be identified with a finite extension of k. The degree $[\tilde{F}_P : k]$ of this extension is called the **degree** of the place P. It is denoted by $\deg(P)$. A place of degree 1 is called **rational**.

Example 1.1.1 Consider the rational function field $F = k(x)$ over k, where x is transcendental over k. For a fixed monic irreducible polynomial $p(x)$ of $k[x]$, a normalized discrete valuation ν_P of F is uniquely determined by putting

$$\nu_P(f(x)) = r \quad \text{if } f(x) \in k[x] \setminus \{0\} \text{ and } p(x)^r \| f(x).$$

It is easy to verify that

$$O_P = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in k[x],\ p(x) \not| \ g(x) \right\}$$

is a valuation ring with maximal ideal

$$\mathrm{M}_P = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in k[x],\ p(x) | f(x),\ p(x) \not| \ g(x) \right\}.$$

Hence $p(x)$ yields a place P. Later on we will also use $p(x)$ to denote the place P. The residue class field corresponding to $p(x)$ is isomorphic to $k[x]/(p(x))$. Thus, the place P is rational if and only if $p(x)$ is a linear polynomial.

There is another normalized discrete valuation ν_∞ of F that is uniquely determined by putting

$$\nu_\infty(f(x)) = -\deg(f(x)) \qquad \text{for } f(x) \in k[x] \setminus \{0\}.$$

This yields the place ∞ with the valuation ring

$$O_\infty = \left\{ \frac{f(x)}{g(x)} : f(x) \in k[x],\ g(x) \in k[x] \setminus \{0\},\ \deg(f(x)) \leq \deg(g(x)) \right\}$$

of F and the maximal ideal

$$\mathrm{M}_\infty = \left\{ \frac{f(x)}{g(x)} : f(x) \in k[x],\ g(x) \in k[x] \setminus \{0\},\ \deg(f(x)) < \deg(g(x)) \right\}.$$

We will sometimes call ∞ the infinite place of F. Since $O_\infty/\mathrm{M}_\infty \simeq k$, it is a rational place of F. The places of the form $p(x)$, which are called the finite places of F, plus the infinite place ∞ are exactly all the places of F. In particular, F has altogether $q+1$ rational places if k is the finite field $\mathbf{F}_q$ of order q.

Recall that a **divisor** D of an algebraic function field F is a formal sum

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

with integer coefficients m_P and $m_P \neq 0$ for at most finitely many $P \in \mathbf{P}_F$. We often write $\nu_P(D)$ for the coefficient m_P of P. Then

$$D = \sum_{P \in \mathbf{P}_F} \nu_P(D) P.$$

The **support** $\mathrm{supp}(D)$ of D is the set

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

The **degree** $\deg(D)$ of D is defined by

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

A divisor D of F is called **positive** if $\nu_P(D) \geq 0$ for all $P \in \mathbf{P}_F$. For two divisors D_1 and D_2 of F we write $D_1 \leq D_2$ if $\nu_P(D_1) \leq \nu_P(D_2)$ for all $P \in \mathbf{P}_F$.

Let P be a place of F and x a nonzero element of F. The place P is called a **zero** of x if $\nu_P(x) > 0$ and a **pole** of x if $\nu_P(x) < 0$. It is clear that a constant element in k has neither poles nor zeros. However, for $x \in F \setminus k$, x has at least one zero place and one pole place.

Let $x \in F^*$ and denote by $Z(x)$, respectively $N(x)$, the set of zero places, respectively pole places, of x. We define the **zero divisor** of $x \in F^*$ by

$$(x)_0 = \sum_{P \in Z(x)} \nu_P(x) P$$

and the **pole divisor** of x by

$$(x)_\infty = \sum_{P \in N(x)} (-\nu_P(x)) P.$$

Then the **principal divisor** of x is given by

$$\mathrm{div}(x) = (x)_0 - (x)_\infty.$$

The degree of $\mathrm{div}(x)$ is equal to 0, i.e.,

$$\deg((x)_0) = \sum_{P \in Z(x)} \nu_P(x) \deg(P) = \sum_{P \in N(x)} (-\nu_P(x)) \deg(P) = \deg((x)_\infty).$$

For a divisor D of F we form the **Riemann-Roch space**

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

Then $\mathcal{L}(D)$ is a finite-dimensional vector space over k, and we denote its dimension by $\ell(D)$. Obviously, we have two facts:

(i) $\ell(0) = 1$;

(ii) $\ell(D) = 0$ if $\deg(D) < 0$.

The dimension $\ell(D)$ is the subject of the Riemann-Roch theorem.

Theorem 1.1.2 (Riemann-Roch Theorem) *Let F be an algebraic function field of genus g. Then for any divisor D of F we have*

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

and equality holds whenever $\deg(D) \geq 2g - 1$.

The Riemann-Roch theorem is often used to define the genus of F implicitly. Thus, we may define the **genus** of F as the integer

$$g := g(F) := \max_D (\deg(D) - \ell(D) + 1),$$

where the maximum is extended over all divisors D of F. By putting $D = 0$ in this definition, we see that the genus of F is nonnegative. For a rational function field F we have $g(F) = 0$. A function field of genus 1 is also called **elliptic**.

Definition 1.1.3 A divisor D of the algebraic function field F of genus g is called **nonspecial** if we have equality in the Riemann-Roch theorem, i.e., if

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

If D is an arbitrary divisor of F and A is a positive divisor of F, then

$$\ell(D + A) \leq \ell(D) + \deg(A),$$

where the sum $D_1 + D_2$ of two divisors D_1 and D_2 of F is the divisor of F with

$$\nu_P(D_1 + D_2) = \nu_P(D_1) + \nu_P(D_2) \qquad \text{for all } P \in \mathbf{P}_F.$$

This result and the Riemann-Roch theorem yield the following consequence.

Corollary 1.1.4 *If D is a nonspecial divisor of F and G is a divisor of F with $G \geq D$, then G is nonspecial.*

Let P be a place of F. An integer $n > 0$ is called a **pole number** of P if there exists an element $x \in F^*$ with $(x)_\infty = nP$. Otherwise, n is called a **gap number** of P.

Corollary 1.1.5 (Weierstrass Gap Theorem) *Let F have genus $g \geq 1$ and let P be a rational place of F. Then there are exactly g gap numbers $i_1, \ldots, i_g$ of P and they satisfy*

$$1 = i_1 < \cdots < i_g \leq 2g - 1.$$

Proof. This is an immediate consequence of the following three facts:

(i) For any $i \geq 1$ we have $\mathcal{L}((i-1)P) \subseteq \mathcal{L}(iP)$, and $\mathcal{L}((i-1)P) = \mathcal{L}(iP)$ if and only if i is a gap number of P.

(ii) $\ell(iP) \leq \ell((i-1)P) + 1$.

(iii) $\ell(0 \cdot P) = 1$ and $\ell((2g-1)P) = g$. □

For a place P of F, an element $t \in F$ with $\nu_P(t) = 1$ is called a **local parameter** at (or a **prime element** for) P.

For a place $P \in \mathbf{P}_F$ and a function $f \in F$ with $\nu_P(f) \geq 0$, we denote by $f(P)$ the residue class $f + \mathsf{M}_P$ of f in $\tilde{F}_P$. Thus, $f(P) \in \tilde{F}_P$ can be viewed as an element of a finite extension of k.

Now we choose a sequence $\{t_r\}_{r=-\infty}^{\infty}$ of elements in F such that

$$\nu_P(t_r) = r$$

for all integers r. For a given function $f \in F$, we can find an integer v such that $\nu_P(f) \geq v$. Hence

$$\nu_P\left(\frac{f}{t_v}\right) \geq 0.$$

Put

$$a_v = \left(\frac{f}{t_v}\right)(P),$$

i.e., a_v is the value of the function f/t_v at P. Then a_v is an element of $\tilde{F}_P$. Note that the function $f/t_v - a_v$ satisfies

$$\nu_P\left(\frac{f}{t_v} - a_v\right) \geq 1,$$

hence we know that

$$\nu_P\left(\frac{f - a_v t_v}{t_{v+1}}\right) \geq 0.$$

Put

$$a_{v+1} = \left(\frac{f - a_v t_v}{t_{v+1}}\right)(P).$$

Then a_{v+1} belongs to $\tilde{F}_P$ and $\nu_P(f - a_v t_v - a_{v+1} t_{v+1}) \geq v + 2$.

Assume that we have obtained a sequence $\{a_r\}_{r=v}^{m}$ $(m > v)$ of elements of $\tilde{F}_P$ such that

$$\nu_P(f - \sum_{r=v}^{k} a_r t_r) \geq k + 1$$

for all $v \le k \le m$. Put

$$a_{m+1} = \left(\frac{f - \sum_{r=v}^{m} a_r t_r}{t_{m+1}} \right)(P).$$

Then $a_{m+1} \in \tilde{F}_P$ and $\nu_P(f - \sum_{r=v}^{m+1} a_r t_r) \ge m+2$. In this way we continue our construction of the a_r. Then we obtain an infinite sequence $\{a_r\}_{r=v}^{\infty}$ of elements of $\tilde{F}_P$ such that

$$\nu_P(f - \sum_{r=v}^{m} a_r t_r) \ge m+1$$

for all $m \ge v$. We summarize the above construction in the formal expansion

$$f = \sum_{r=v}^{\infty} a_r t_r, \tag{1.1}$$

which is called the **local expansion** of f at P. A typical choice for the t_r is $t_r = t^r$ with t being a local parameter at P.

The above local expansion shows that for a given element $f \in F$ and a place P of F, there exists a sequence $\{f_n = \sum_{i=v}^{n} a_i t_i\}_{n=v}^{\infty}$ of special elements of F such that f_n tends to f at P, i.e., $\nu_P(f_n - f) \to \infty$ as $n \to \infty$. The following result shows approximation at several places.

Theorem 1.1.6 (Approximation Theorem) *Let $\mathcal{S}$ be a proper nonempty subset of $\mathbf{P}_F$ and $P_1, \ldots, P_r \in \mathcal{S}$. Then for any given elements $x_1, \ldots, x_r \in F$ and integers $n_1, \ldots, n_r \in \mathbf{Z}$, there exists an element $x \in F$ such that $\nu_{P_i}(x - x_i) = n_i$ for all $i = 1, \ldots, r$ and $\nu_P(x) \ge 0$ for all $P \in \mathcal{S} \setminus \{P_1, \ldots, P_r\}$.*

1.2 Divisor Class Groups and Ideal Class Groups

Throughout this section, the constant field k is finite. Thus, an algebraic function field F over k is now a **global function field**.

Denote the **divisor group** of F by $\mathrm{Div}(F)$, i.e., $\mathrm{Div}(F)$ is the free abelian group generated by all places of F:

$$\mathrm{Div}(F) = \left\{ \sum_{P \in \mathcal{S}} m_P P : \mathcal{S} \text{ is a finite subset of } \mathbf{P}_F \text{ and } m_P \in \mathbf{Z} \text{ for all } P \in \mathcal{S} \right\}.$$

Let $\mathrm{Div}^0(F)$ be the subset of $\mathrm{Div}(F)$ consisting of all divisors of F of degree 0. Then $\mathrm{Div}^0(F)$ is a subgroup of $\mathrm{Div}(F)$. The group $\mathrm{Div}^0(F)$ is called the **divisor group of degree zero** of F.

Since $\deg(\mathrm{div}(x)) = 0$ for any $x \in F^*$, we have

$$\mathrm{Princ}(F) := \{\mathrm{div}(x) : x \in F^*\} \subseteq \mathrm{Div}^0(F).$$

Moreover, $\mathrm{Princ}(F)$ forms a subgroup of $\mathrm{Div}(F)$ which is called the **principal divisor group** of F. The factor group $\mathrm{Div}(F)/\mathrm{Princ}(F)$ is called the **divisor class group** of F.

The divisor class $[D] := D + \mathrm{Princ}(F)$ of $D \in \mathrm{Div}(F)$ consists of all divisors G of F that are **equivalent** to D, in the sense that $G = D + \mathrm{div}(x)$ for some $x \in F^*$. Now we consider the factor group

$$\mathrm{Div}^0(F)/\mathrm{Princ}(F).$$

It is a finite group and it is called the **divisor class group** (or the **group of divisor classes**) **of degree zero** of F, denoted by $\mathrm{Cl}(F)$. The cardinality of $\mathrm{Cl}(F)$ is called the **divisor class number** of F, denoted by $h(F)$.

Now choose a nonempty subset $\mathcal{S}$ of $\mathbf{P}_F$ with $\mathcal{S} \neq \mathbf{P}_F$ and define the **$\mathcal{S}$-integral ring** of F by

$$O_{\mathcal{S}} = \{z \in F : \nu_P(z) \geq 0 \text{ for all } P \in \mathcal{S}\}.$$

Then $O_{\mathcal{S}}$ is a Dedekind ring. In particular, we have $O_{\{P\}} = O_P$. Thus,

$$O_{\mathcal{S}} = \bigcap_{P \in \mathcal{S}} O_P.$$

A nonempty subset U of F is said to be a **fractional $\mathcal{S}$-ideal** (or an **$\mathcal{S}$-ideal**) of F if:

(i) $\mathsf{U} \neq \{0\}$, and

(ii) U is an $O_{\mathcal{S}}$-module, and

(iii) there exists an element $a \in F^*$ such that $a\mathsf{U} \subseteq O_{\mathcal{S}}$.

An $\mathcal{S}$-ideal U is called **integral** if $\mathsf{U} \subseteq O_{\mathcal{S}}$. Thus, an integral $\mathcal{S}$-ideal is an ordinary nonzero ideal of the ring $O_{\mathcal{S}}$. It is trivial that F is not an $\mathcal{S}$-ideal since $zF = F \neq O_{\mathcal{S}}$ for any $z \in F^*$. We denote the set of all fractional $\mathcal{S}$-ideals of F by $\mathrm{Fr}_{\mathcal{S}}(F)$ or $\mathrm{Fr}_{\mathcal{S}}$.

For any $\mathcal{S}$-ideals U and V of F, it is easy to check that

$$\mathsf{U} + \mathsf{V} = \{x + y : x \in \mathsf{U},\ y \in \mathsf{V}\},$$

$$\mathsf{U} \cdot \mathsf{V} = \{\sum_{i=1}^{n} x_i y_i : x_i \in \mathsf{U},\ y_i \in \mathsf{V},\ n \in \mathbf{N}\},$$

and $\mathsf{U} \cap \mathsf{V}$ are $\mathcal{S}$-ideals of F. Note that $\mathrm{Fr}_{\mathcal{S}}$ forms an abelian group under the multiplication operation "$\cdot$". It is called the **fractional ideal group** of $O_{\mathcal{S}}$ or the **fractional $\mathcal{S}$-ideal group** of F.

For any $z \in F^*$, the $\mathcal{S}$-ideal $zO_{\mathcal{S}}$ is called a **principal $\mathcal{S}$-ideal**. It is obvious that all principal $\mathcal{S}$-ideals of F form a subgroup of $\mathrm{Fr}_{\mathcal{S}}$, denoted by $\mathrm{Princ}_{\mathcal{S}}(F)$ or $\mathrm{Princ}_{\mathcal{S}}$. The factor group

$$\mathrm{Fr}_{\mathcal{S}}/\mathrm{Princ}_{\mathcal{S}}$$

is called the **fractional ideal class group** of $O_{\mathcal{S}}$ or the **fractional $\mathcal{S}$-ideal class group** of F, and is denoted by $\mathrm{Cl}(O_{\mathcal{S}})$.

Proposition 1.2.1 *If $\mathbf{P}_F \setminus \mathcal{S}$ is a finite nonempty set, then the fractional ideal class group $\mathrm{Cl}(O_{\mathcal{S}})$ is a finite abelian group.*

If $\mathbf{P}_F \setminus \mathcal{S}$ is a finite nonempty set, we call the cardinality of $\mathrm{Cl}(O_{\mathcal{S}})$ the **fractional ideal class number** of $O_{\mathcal{S}}$, denoted by $h(O_{\mathcal{S}})$.

Lemma 1.2.2 *For $P \in \mathcal{S}$ and $\mathsf{U} \in \mathrm{Fr}_{\mathcal{S}}$, put*

$$\nu_P(\mathsf{U}) = \min_{z \in \mathsf{U}} \nu_P(z).$$

Then:

(i) $\nu_P(zO_{\mathcal{S}}) = \nu_P(z)$ *for any* $z \in F^*$;

(ii) $\nu_P(\mathsf{U}+\mathsf{V}) = \min(\nu_P(\mathsf{U}), \nu_P(\mathsf{V}))$ *and* $\nu_P(\mathsf{UV}) = \nu_P(\mathsf{U}) + \nu_P(\mathsf{V})$ *for any two $\mathcal{S}$-ideals* U *and* V;

(iii) U *is integral if and only if* $\nu_P(\mathsf{U}) \geq 0$ *for all* $P \in \mathcal{S}$.

Proof. (i) Since $1 \in O_{\mathcal{S}}$, we have $\nu_P(zO_{\mathcal{S}}) \leq \nu_P(z)$ by the definition. For any $zx \in zO_{\mathcal{S}}$ with $x \in O_{\mathcal{S}}$, we have $\nu_P(zx) = \nu_P(z) + \nu_P(x) \geq \nu_P(z)$, and so $\nu_P(zO_{\mathcal{S}}) \geq \nu_P(z)$.

(ii) Note that

$$\begin{aligned} \nu_P(\mathsf{U}+\mathsf{V}) &= \min_{x \in \mathsf{U},\, y \in \mathsf{V}} \nu_P(x+y) \\ &= \min_{x \in \mathsf{U},\, y \in \mathsf{V}} \min(\nu_P(x+0), \nu_P(y+0), \nu_P(x+y)) \\ &= \min_{x \in \mathsf{U},\, y \in \mathsf{V}} \min(\nu_P(x), \nu_P(y)) \\ &= \min(\nu_P(\mathsf{U}), \nu_P(\mathsf{V})) \end{aligned}$$

and

$$\begin{aligned} \nu_P(\mathsf{UV}) &= \min_{x_i \in \mathsf{U},\, y_i \in \mathsf{V}} \nu_P\left(\sum x_i y_i\right) \\ &= \min_{x \in \mathsf{U},\, y \in \mathsf{V}} \nu_P(xy) \\ &= \min_{x \in \mathsf{U}} \nu_P(x) + \min_{y \in \mathsf{V}} \nu_P(y) \\ &= \nu_P(\mathsf{U}) + \nu_P(\mathsf{V}). \end{aligned}$$

(iii) This follows immediately from the definitions. □

For each $P \in \mathcal{S}$, let us put

$$\mathsf{M}_P(\mathcal{S}) = \{z \in F : \nu_P(z) \geq 1, \nu_Q(z) \geq 0 \text{ for all } Q \in \mathcal{S} \text{ with } Q \neq P\}.$$

Then $\mathsf{M}_P(\mathcal{S})$ is called a **prime ideal** of $O_{\mathcal{S}}$. It is clear that

$$\mathsf{M}_P(\mathcal{S}) = O_{\mathcal{S}} \cap \mathsf{M}_P \quad \text{and} \quad O_{\mathcal{S}}/\mathsf{M}_P(\mathcal{S}) \simeq \tilde{F}_P.$$

Proposition 1.2.3 *Every $\mathcal{S}$-ideal* U *has a unique decomposition into prime ideals*

$$\mathsf{U} = \prod_{P \in \mathcal{S}} \mathsf{M}_P(\mathcal{S})^{\nu_P(\mathsf{U})}.$$

Its inverse is

$$\mathsf{U}^{-1} = \prod_{P \in \mathcal{S}} \mathsf{M}_P(\mathcal{S})^{-\nu_P(\mathsf{U})}.$$

Corollary 1.2.4 (i) $zO_{\mathcal{S}} = \prod_{P \in \mathcal{S}} \mathsf{M}_P(\mathcal{S})^{\nu_P(z)}$ *for any* $z \in F^*$.
(ii) $\mathsf{U} + \mathsf{V} = \prod_{P \in \mathcal{S}} \mathsf{M}_P(\mathcal{S})^{\min(\nu_P(\mathsf{U}), \nu_P(\mathsf{V}))}$ *for any two* $\mathcal{S}$*-ideals* U *and* V.
(iii) $\mathsf{UV} = \prod_{P \in \mathcal{S}} \mathsf{M}_P(\mathcal{S})^{\nu_P(\mathsf{U}) + \nu_P(\mathsf{V})}$ *for any two* $\mathcal{S}$*-ideals* U *and* V.

Proof. This follows directly from Lemma 1.2.2 and Proposition 1.2.3. □

There is a close relationship between the divisor class group $\mathrm{Cl}(F)$ of degree zero of F and the fractional ideal class group $\mathrm{Cl}(O_{\mathcal{S}})$ of $O_{\mathcal{S}}$. We present the result only for the case where $\mathbf{P}_F \setminus \mathcal{S}$ consists of a single place (see Rosen [130] for a more general result).

Proposition 1.2.5 *If* $\mathcal{S} = \mathbf{P}_F \setminus \{P\}$ *for some place* P*, then there exists an exact sequence*

$$0 \longrightarrow \mathrm{Cl}(F) \longrightarrow \mathrm{Cl}(O_{\mathcal{S}}) \longrightarrow \mathbf{Z}/d\mathbf{Z} \longrightarrow 0,$$

where d *is the degree* $\deg(P)$ *of* P*. In particular,*

$$h(O_{\mathcal{S}}) = dh(F).$$

Furthermore, $\mathrm{Cl}(F)$ *is isomorphic to* $\mathrm{Cl}(O_{\mathcal{S}})$ *if* P *is a rational place.*

Proof. Consider the homomorphism

$$\theta_1 : \mathrm{Div}^0(F) \longrightarrow \mathrm{Cl}(O_{\mathcal{S}}), \quad \sum_Q m_Q Q \mapsto \left(\prod_{Q \neq P} \mathsf{M}_Q(\mathcal{S})^{m_Q} \right) \mathrm{Princ}_{\mathcal{S}}.$$

Then it is easy to check that $\ker(\theta_1) = \mathrm{Princ}(F)$, and so θ_1 induces an injective homomorphism

$$\theta : \mathrm{Cl}(F) \longrightarrow \mathrm{Cl}(O_{\mathcal{S}}).$$

Define another homomorphism

$$\phi_1 : \mathrm{Fr}_{\mathcal{S}} \longrightarrow \mathbf{Z}/d\mathbf{Z}, \quad \prod_{Q \neq P} \mathsf{M}_Q(\mathcal{S})^{m_Q} \mapsto \sum_{Q \neq P} m_Q \deg(Q) + d\mathbf{Z}.$$

Note that ϕ_1 is surjective since the degree map $\mathrm{Div}(F) \longrightarrow \mathbf{Z}$ is surjective by [152, Corollary V.1.11]. Furthermore, it is easily seen that $\mathrm{Princ}_{\mathcal{S}} \subseteq \ker(\phi_1)$, and so ϕ_1 induces a surjective homomorphism

$$\phi : \mathrm{Cl}(O_{\mathcal{S}}) \longrightarrow \mathbf{Z}/d\mathbf{Z}.$$

It is straightforward to show that $\ker(\phi) = \mathrm{im}(\theta)$. □

Let $D = \sum_P \nu_P(D) P$ be a positive divisor of F. If $x \in F^*$, we define

$$x \equiv 1 \pmod{D}$$

to mean that x satisfies the following condition:

if $P \in \mathrm{supp}(D)$, then x lies in the valuation ring O_P and $\nu_P(x - 1) \geq \nu_P(D)$.

Let $\mathcal{S}$ be a proper subset of $\mathbf{P}_F$ such that $\mathcal{S}$ contains $\mathrm{supp}(D)$ and $\mathbf{P}_F \setminus \mathcal{S}$ is finite. Let $\mathrm{Fr}_{D,\mathcal{S}}$ be the subgroup of $\mathrm{Fr}_{\mathcal{S}}$ consisting of the $\mathcal{S}$-ideals that are relatively prime to D, that is,

$$\mathrm{Fr}_{D,\mathcal{S}} = \{\mathrm{U} \in \mathrm{Fr}_{\mathcal{S}} : \nu_P(\mathrm{U}) = 0 \text{ for all } P \in \mathrm{supp}(\mathrm{D})\}.$$

Define the subgroup $\mathrm{Princ}_{D,\mathcal{S}}$ of $\mathrm{Fr}_{D,\mathcal{S}}$ by

$$\mathrm{Princ}_{D,\mathcal{S}} = \{xO_{\mathcal{S}} : x \in F^*,\ x \equiv 1 \pmod{D}\}.$$

We also use $\mathrm{Princ}_D(O_{\mathcal{S}})$ to denote $\mathrm{Princ}_{D,\mathcal{S}}$. The factor group

$$\mathrm{Fr}_{D,\mathcal{S}}/\mathrm{Princ}_{D,\mathcal{S}}$$

is called the **$\mathcal{S}$-ray class group** modulo D. It is a finite group and denoted by $\mathrm{Cl}_D(O_{\mathcal{S}})$. If $D = 0$, then we obtain the fractional $\mathcal{S}$-ideal class group $\mathrm{Cl}(O_{\mathcal{S}})$.

1.3 Algebraic Extensions and the Hurwitz Formula

Throughout this section, we assume that F'/k' and F/k are two algebraic function fields, that F'/F is a finite separable extension, and that $k' \supseteq k$. The constant field k is assumed to be finite, for simplicity, although the results hold also for more general k, e.g. for perfect fields k.

Let P be a place of F and P' a place of F' lying over P, that is, $P \subseteq P'$. We sometimes express this situation by $P'|P$. Choose a local parameter $t_P \in F$ at P, then the positive integer $\nu_{P'}(t_P)$ is called the **ramification index** of P' over P. It is independent of the choice of the local parameter t_P at P. We denote $\nu_{P'}(t_P)$ by $e_{P'}(F'/F)$ or $e(P'|P)$. We say that F'/F is **ramified** at P' if $e_{P'}(F'/F) > 1$ and **unramified** at P' if $e_{P'}(F'/F) = 1$. Alternatively, P' is called ramified, respectively unramified, in F'/F. Furthermore, we say that P' is **totally ramified** in F'/F if $e_{P'}(F'/F) = [F' : F]$. Let $\tilde{F}'_{P'}$ and $\tilde{F}_P$ be the residue class fields of P' and P, respectively. Then $\tilde{F}'_{P'}/\tilde{F}_P$ is a finite extension and the degree $[\tilde{F}'_{P'} : \tilde{F}_P]$ of this extension is called the **relative degree** of P' over P, denoted by $f_{P'}(F'/F)$ or $f(P'|P)$.

It follows from the definitions of ramification index and relative degree that we have the following tower formulas.

Proposition 1.3.1 *Suppose that $F \subseteq F' \subseteq F''$ is a field tower of finite separable extensions and that P, P', P'' are places of F, F', F'', respectively, with $P''|P'|P$. Then*

$$e_{P''}(F''/F) = e_{P''}(F''/F')e_{P'}(F'/F),$$

$$f_{P''}(F''/F) = f_{P''}(F''/F')f_{P'}(F'/F).$$

The following proposition expresses an important relationship between ramification indices, relative degrees, and the degree of the extension.