Algebraic Function Fields

A Document Prepared for Daniel Daigle

Kevin Johnson

November 8, 2014

Contents

1 Places

For the purpose of these notes, we will let k be any arbitrary field.

Definition 1.1 An algebraic function field F/k of one variable over k is a field extension $k \subseteq F$ such that F is a finite field extension of $k(x)$ for some $x \in F$ which is transcendental over k. For simplicity, we refer to F/k as a function field.

Example 1.2 Let $F = k(x)$ for some transcendental element x over k. Then F is an function field over k and is called the *rational* function field over k.

Example 1.3 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is not a function field because $\sqrt{2}$ is algebraic over $\mathbb{Q}$.

Example 1.4 Let $p = y^2 + x^3 - x \in \mathbb{C}[x, y]$. Since p is irreducible over $\mathbb{C}$ (exercise 6.1), the ring $A = \mathbb{C}[x, y]/(p)$ is an integral domain. Therefore we may consider the field of fractions F of A. Then $F/\mathbb{C}$ is a function field in one variable over $\mathbb{C}$ (exercise 6.1).

Example 1.5 The field of fractions $k(x, y)$ of a polynomial ring $k[x, y]$ in two variables over k is not a function field in one variable: If it were, then $k(x, y)/k(x)$ would have to be a finite extension. This contradicts the algebraic independence of x, y in $k[x, y]$.

Proposition 1.6 Let F/k be an algebraic function field. Then $z \in F$ is transcendental over k if and only if the extension $F/k(z)$ is of finite degree.

Proof. By definiton F is a finite extension of $k(x)$ for some transcendental element $x \in F$. Let $z \in F$, then we have the following chain of inclusions; $k \subseteq k(z) \subseteq F$. Suppose $z \in F$ is transcendental over k. Since F is a finite extension of $k(x)$, z is algebraic over $k(x)$, so there exists $f(T) = a_0(x) + a_1(x)T + ... + a_n(x)T^n \in k(x)[T]\backslash\{0\}$ such that $f(z) = 0$, that is $0 = a_0(x) + a_1(x)z + ... + a_n(x)z^n$. Notice that if all coefficients $a_0(x), a_1(x), ..., a_n(x)$ were only in k, then z would not be transcendental over k. So there must be at least one coefficient in $k(x)$ which is not in k. We may re-write f as a polynomial in one variable with coefficients in $k(z)$ with $f(x) = 0$. Hence x is algebraic over $k(z)$ and $[k(x, z) : k(z)] < \infty$. By definition $[F : k(x, z)] < \infty$, so $[F : k(z)] = [F : k(x, z)][k(x, z) : k(z)] < \infty$. Conversely, assume $z \in F$ is algebraic over k and suppose that $F/k(z)$ is an extension of finite degree, then $[F : k(z)] < \infty$ and thus $[F : k] = [F : k(z)][k(z) : k] < \infty$, which would also imply $[k(x) : k] < \infty$, which is impossible since x is transcendental over k. ■

Definition 1.7 A valuation ring of a function field F/k is a ring $\mathcal{O} \subseteq F$ with the following properties:

(i) $k \subsetneqq \mathcal{O} \subsetneqq F$

(ii) For every $z \in F$, we have that $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$

Example 1.8 Consider the rational function field $k(x)/k$. Let p be an irreducible polynomial in $k[x]$. Then the ideal (p) is prime in $k[x]$ and thus we may consider the localiztion of $k[x]$ at (p), denoted $\mathcal{O}_p$. That is, $\mathcal{O}_p = \{f/g \mid f, g \in k[x], g \notin (p)\}$ $\mathcal{O}_p$ is a valution ring of the function field $k(x)/k$: Clearly $k \subsetneqq \mathcal{O}_p$. Since $1/p \notin \mathcal{O}_p$ but $1/p \in k(x)$, $\mathcal{O}_p \subsetneqq k(x)$. So $\mathcal{O}_p$ satisfies condition (i) of definition 1.7. To verify condition (ii), let $z = f/g \in k(x)$. If $g \notin (p)$, then $z \in \mathcal{O}_p$ by definition. If $g \in (p)$ and $f \notin (p)$, then $z^{-1} \in \mathcal{O}_p$. If Both $f, g \in (p)$. Then $f = p^n u$ and $g = p^m v$ for some $u, v \in k[x]$ such that $u, v \notin (p)$. Suppose $n \geq m$, then $z = f/g = p^{n-m}u/v \in \mathcal{O}_p$, since $v \notin (p)$. If $n < m$, then $z = f/g = u/p^{m-n}v$, hence $z^{-1} \in \mathcal{O}_p$, since $u \notin (p)$. Hence for every $z \in k(x)$, $z \in \mathcal{O}_p$ or $z^{-1} \in \mathcal{O}_p$.

Example 1.9 Let F be the field of fractions of the integral domain A as in example 1.4. Consider the prime ideal $(x, y) \in \mathbb{C}[x, y]$. Since (x, y) contains the kernel of the projection $\mathbb{C}[x, y] \xrightarrow{\pi} A$, the ideal $\mathfrak{m} = \pi((x, y))$ is prime in A (exercise 6.2). Hence we may consider the localization of A at $\mathfrak{m}$, denoted $A_{\mathfrak{m}}$. Then $A_{\mathfrak{m}}$ is a valution ring of the function field $F/\mathbb{C}$ (exercise 6.1).

Proposition 1.10 Let $\mathcal{O}$ be a valuation ring of a function field F/k. Then the following hold;

(a) $\mathcal{O}$ is a local ring where $P = \mathcal{O} \backslash \mathcal{O}^*$ denotes the maximal ideal of $\mathcal{O}$.

(b) Let $0 \neq x \in F$. Then $x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$

(c) Let $\tilde{k}$ denote the algebraic closure of k in F. Then $\tilde{k} \subseteq \mathcal{O}$ and $\tilde{k} \cap P = \{0\}$.

Proof. (a) It suffices to show that P is an ideal of $\mathcal{O}$, as any ideal that properly contains P would also contain a unit: Let $x \in P, z \in \mathcal{O}$, then $x \notin \mathcal{O}^*$ by definition. Hence $xz \notin \mathcal{O}^*$, thus $xz \in P$. Let $x, y \in P$. Then either $xy^{-1} \in \mathcal{O}$ or $x^{-1}y \in \mathcal{O}$. Assume $xy^{-1} \in \mathcal{O}$. Then $1 + xy^{-1} \in \mathcal{O}$, since $1 \in \mathcal{O}$. Hence $x + y = y(1 + xy^{-1}) \in P$.

(b) Notice that $x \in P \Leftrightarrow x \in \mathcal{O} \backslash \mathcal{O}^* \Leftrightarrow x \notin \mathcal{O}^* \Leftrightarrow x^{-1} \notin \mathcal{O}$.

(c) Let $z \in \tilde{k} \backslash \{0\}$ and suppose that $z \notin \mathcal{O}$, then by the definition of a valuation ring, $z^{-1} \in \mathcal{O}$. Since z^{-1} is algebraic over k, there exists a $f(X) = a_0 + a_1 X + ... + a_n X^n \in k[X] \backslash \{0\}$ such that $f(z^{-1}) = 0$. Then, $a_0 + a_1(z^{-1}) + ... + a_n(z^{-1})^n = 0$. Assume f is one of the non-zero polynomials of minimal degree satisfying $f(z^{-1}) = 0$. We may also assume that $a_0 = 1$; To see this, suppose $a_0 = 0$, then $0 = a_1(z^{-1}) + ... + a_n(z^{-1})^n = z^{-1}(a_1 + a_2(z^{-1}) + ... + a_n(z^{-1})^{n-1}$. Since $z^{-1} \neq 0$, we have found another polynomial $g(X) = a_1 + a_2 X + ... + a_n x^{n-1} \in k[X] \backslash \{0\}$ such that $g(z^{-1}) = 0$ and $deg(g) < deg(f)$. This contradicts the minimality of f. If $a_0 \neq 1$ and $a_0 \neq 0$, then since $a_0 \in k$, there exists $a_0^{-1} \in k$ such that $a_0 a_0^{-1} = 1$. Then $a_0^{-1} f = 1 + a_0^{-1} a_1 X + ... + a_0^{-1} a_n X^n$ is a new polynomial that is still zero on z^{-1} and has the same degree as f. Thus we may write $f(X) = 1 + a_1 X + ... + a_n X^n$ and therefore $-1 = z^{-1}(a_1 + ... + a_n (z^{-1})^{n-1}) \implies z = -(a_1 + ... + a_n (z^{-1})^{n-1}) \in \mathcal{O}$. This is a contradiction to the assumption $z \notin \mathcal{O}$. Hence $\tilde{k} \subseteq \mathcal{O}$. Lastly, the inverse of an algebraic element is algebraic and $\tilde{k} \subseteq \mathcal{O}^*$, hence $\tilde{k} \cap P = \{0\}$. ■

Example 1.11 As in example 1.8, consider the rational function field $k(x)/k$. Let p be an irreducible poylnomial in $k[x]$. Then $p\mathcal{O}_p$ is the unique maximal ideal of the valuation ring $\mathcal{O}_p$. To verify this, let $z = f/g \in p\mathcal{O}_p$, then $g \notin (p)$ but $f \in (p)$. Hence $z^{-1} \notin \mathcal{O}_p$. Therefore $z \in \mathcal{O}_p \backslash \mathcal{O}_p^*$. Let $z = f/g \in \mathcal{O}_p \backslash \mathcal{O}_p^*$, then $z^{-1} \notin \mathcal{O}_p$, hence $f \in (p)$ and $g \notin (p)$. Thus $z \in p\mathcal{O}_p$. So $p\mathcal{O}_p = \mathcal{O}_p \backslash \mathcal{O}_p^*$.

Definition 1.12 Let $\mathcal{O}$ be a valution ring of a function field F/k and $P = \mathcal{O} \backslash \mathcal{O}^*$ be its maximal ideal. We call P a *place* of the function field F/k. Since $\mathcal{O}$ is uniquely determined by P, that is, $\mathcal{O} = \{z \in F \mid z^{-1} \notin P\}$, we often denote it $\mathcal{O}_p$, refered to as the valuation ring at place P. We use $\mathbb{P}_F$ to denote the set of all places of F/k and $\mathbb{V}_F$ to denote the set of all valuation rings of F/k.

Example 1.13 Let $F = k(x)$ be the rational function field over k as in example 1.2. Example 1.8 shows $\{k[x]_{(p)} \mid \text{p is irreducible in } k[x]\} \subseteq \mathbb{V}_F$. Theorem 2.2 shows this set is all valuation rings of $k(x)/k$ except one. Furthermore $\{pk[x]_{(p)} \mid \text{p is a irreducible polynomial in } k[x]\} \subseteq \mathbb{P}_F$, where $pk[x]_{(p)}$ denotes the maximal ideal of the local ring $k[x]_{(p)}$

Definition 1.14 Let P be a place of a function field F/k and $\mathcal{O}_P$ the valuation ring at place P. Since P is a maximal ideal, the quotient ring $\mathcal{O}_P/P$ is a field. We call this the residue class field of P, denoted by F_P. The degree of a place P is defined as $\deg P = [F_P : k]$ and we call a place of degree one a *rational* place of F/k.

Example 1.15 For the rational function field $F = \mathbb{C}(x)$ over the complex numbers $\mathbb{C}$, all places of the form $P := p\mathbb{C}[x]_{(p)}$ for some irreducible $p \in \mathbb{C}[x]$, have degree 1: Since $\mathbb{C}$ is algebraically closed, every irreducible polynomial p is linear. Thus the degree of P is equal to the degree of the field extension $[F_P : \mathbb{C}]$. Theorem 2.1 shows that $F_P \cong \mathbb{C}[x]/(p)$. Thus $\deg P = [\mathbb{C}[x]/(p) : \mathbb{C}] = 1$. More generally, all places of this form, over an algebraically closed field are degree 1. This is not true in any arbitrary field: Consider the polynomial $f = x^2 + 1 \in \mathbb{R}[x]$. The place $f\mathbb{R}[x]_{(f)}$ of the function field $\mathbb{R}(x)/\mathbb{R}$ has degree 2.

Definition 1.16 Let k be a field. Let ∞ denote any element that is not in $\mathbb{Z}$ satisfying; $\infty + \infty = \infty + n = n + \infty = \infty$ and $\infty > m$ For all $n, m \in \mathbb{Z}$. A discrete valuation of F/k is a function $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ with the following properties:

i) $v(x) = \infty \Leftrightarrow x = 0$.

ii) $v(xy) = v(x) + v(y)$ for all $x, y \in F$.

iii) $v(x + y) \geq min\{v(x), v(y)\}$ for all $x, y \in F$.

iv) There exists an element $z \in F$ with $v(z) = 1$.

v) $v(a) = 0$ for all $0 \neq a \in k$

Lemma 1.17 Let v discrete valuation on a function field F/k. Then;

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

for all $x, y \in F$ such that $v(x) \neq v(y)$.

Proof. Asssume $v(x) < v(y)$ and suppose $v(x + y) \neq min\{v(x), v(y)\}$. Then $v(x+y) > v(x)$ by (iii). Therefore $v(x) = v((x+y)-y) \geq \min\{v_(x+y), v(y)\} > v(x)$, which is impossible. ■

Example 1.18 Consider the rational function field $k(x)/k$. We define the map $k(x) \xrightarrow{v_\infty} \mathbb{Z} \cup \{\infty\}$ by: for all $z = f/g \in k(x)\backslash\{0\}$, $v_\infty(z) = \deg(g) - \deg(f)$ and $v_\infty(0) = \infty$. Then v_∞ is a discrete valution of the $k(x)/k$.

Proof. Property (i) follows by definition of v_∞. Let $x = f/g, y = f'/g' \in k(x)$. Then

$$\begin{aligned} v_\infty(xy) &= v_\infty(\frac{f}{g}\frac{f'}{g'}) \\ &= \deg(gg') - \deg(ff') \\ &= \deg(g) + \deg(g') - \deg(f) - \deg(f') \\ &= v_\infty(x) + v_\infty(y) \end{aligned}$$

This shows property (ii). Assume $v_\infty(x) \geq v_\infty(y)$. Then $\deg(g) - \deg(f) \geq \deg(g') - \deg(f') \implies \deg(g) + \deg(f') \geq \deg(g') + \deg(f) \implies \deg(gf') \geq \deg(g'f)$. So

$$\begin{aligned} v_\infty(x + y) &= v_\infty(\frac{f}{g} + \frac{f'}{g'}) \\ &= v_\infty(\frac{fg' + f'g}{gg'}) \\ &= \deg(gg') - \deg(fg' + f'g) \\ &= \deg(gg') - \max\{\deg(fg'), \deg(f'g)\} \\ &= \deg(gg') - \deg(f'g) \\ &= \deg(g) + \deg(g') - \deg(g) - \deg(f') \\ &= \deg(g') - \deg(f') \\ &= v_\infty(y) \\ &= \min\{v_\infty(x), v_\infty(y)\} \end{aligned}$$

So v_∞ satisfies (iii). Lastly $v_\infty(1/x) = 1$ and clearly $v_\infty(a) = 0$ for all $a \in k^*\backslash\{0\}$. So v_∞ satisfies conditions (iv) and (v). Thus v_∞ is a discrete valuation on the function field $k(x)/k$. ■

Theorem 1.19 Let $\mathcal{O}_P$ be a valution ring of a function field F/k with maximal ideal P.

(a) P is a principal ideal.

(b) If $P = t\mathcal{O}$, then each $0 \neq z \in F$ has a unique representation of the form $z = t^n u$ for some $n \in \mathbb{Z}$ and $u \in \mathcal{O}^*$.

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

(d) To a place $P \in \mathbb{P}_F$ we associate a function $F \xrightarrow{v} \mathbb{Z}\cup\{\infty\}$ as follows; Choose a prime element t for P. Then every $0 \neq z \in F$ has a unique representation $z = t^n u$ with $u \in \mathcal{O}_P^*$ and $n \in \mathbb{Z} \cup \{\infty\}$. Define $v_P(z) = v_P(t^n u) := n$ and $v_P(0) := \infty$. The function v_P is a dicrete valuation of F/k. Moreover we have,

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

$$\mathcal{O}_P^* = \{z \in F \mid v_P(z) = 0\}$$

$$P = \{z \in F \mid v_P(z) > 0\}$$

(e) An element $x \in F$ is a prime element for P if and only if $v_P(x) = 1$

(f) Conversly, suppose that v is a discrete valuation of F/k. Then the set $P = \{z \in F \mid v_P(z) > 0\}$ is a place of F/k, and $\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\}$ is the corresponding valuation ring.

(g) Every valuation ring $\mathcal{O}$ of F/k is a maximal proper subring of F.

Proof. See Stichtenoth, theorem 1.1.6 for parts a, b and c. (d): First, we verify the conditions of a discrete valaution. (i) By definiton of v_P we have $v_P(x) = \infty \Leftrightarrow x = 0$. (ii) Let $x, y \in F$ and write $x = t^n u, y = t^m v$ for $n, m \in \mathbb{Z}$ and $u, v \in \mathcal{O}_P^*$. Then $v_P(xy) = v_P(t^n u t^m v) = v_P(t^{n+m} uv) = n + m = v_P(x) = v_P(y)$. (iii) We have $v_P(x+y) = v_P(t^n u + t^m v)$. If $n \geq m$, then $v_P(t^n u + t^m v) = v_P(t^m(t^{n-m}u + v)) = m + (n-m) = n \geq m = min\{v_P(x), v_P(y)\}$. Simularly, if $m \geq n$, then $v_P(t^n u + t^m v) \geq n = min\{v_P(x), v_P(y)\}$. (iv) $v_P(t) = v_P(t^1) = 1$. (v) Suppose $0 \neq a \in k$, then $a \in \mathcal{O}_P^*$, hence $a = t^0 a$, thus $v_P(a) = v_P(p^0 a) = 0$. The remaining assertions in part a) follow directly from the fact that every $0 \neq z \in F$ can be written uniquely as $z = t^n u$ for some $n \in \mathbb{Z}$, $u \in \mathcal{O}^*$ and condition (v), which asserts that every $0 \neq z \in \mathcal{O}_P$ such that $z \notin P$ has discrete valuation 0. (e): If x is a prime element of P, then $x = x^1$, so by definition $v_P(x) = 1$. Let $x \in F$ such that $v_p(x) = 1$. Then $x = t^1 u$ for some $u \in \mathcal{O}^*$, thus $t = xu^{-1}$. Given any $y \in P$, $y = t^m v$ for some $v \in \mathcal{O}^*$ and $m \in \mathbb{Z}$. Hence $y = (xu^{-1})^m v = x^m w$ for $w = u^{-m} v \in \mathcal{O}^*$. So x is a prime element of P. (f): Let $z \in F$, write $z = t^n u$ for some $n \in Z$ and $u \in \mathcal{O}_P^*$. Suppose $n \geq 0$, then clearly $z \in \mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\}$. If $n < 0$, then $z^{-1} = (t^{-n}u)^{-1} = t^n u^{-1}$, hence $z^{-1} \in \mathcal{O}_P$. So $\mathcal{O}_P$ is a valuation ring of F. The units of $\mathcal{O}_P$ are precisely the elements with $v_P(x) \geq 0$ and $v_P(x^{-1}) \geq 0$. Hence $x = t^n u$ and $x = t^{-n} u$ with $n \in \mathbb{Z}$, $u \in \mathcal{O}^*$ and $n \geq 0$ and $-n \geq 0$. Hence $n = 0$. So $P = \{z \in F \mid v_P(z) > 0\} = \{z \in F \mid v_P(z) \geq 0\} \backslash \{z \in F \mid v_P(z) = 0\} = \mathcal{O} \backslash \mathcal{O}^*$. (g): Let $z \in F \backslash \mathcal{O}$. Claim: $F = \mathcal{O}[z]$: Let $y \in F$, then $v_P(yz^{-k}) \geq 0$ for sufficiently large $k \geq 0$. So $w = yz^{-k} \in \mathcal{O}$ and $y = wz^k \in \mathcal{O}[z]$. ■

Proposition 1.20 If P is a place of a function field F/k and $0 \neq x \in P$, then $\deg P \leq [F : k(x)] < \infty$.

Proof. Let $P \in \mathbb{P}_F$ and $0 \neq x \in P$. There are two inequalities to show;

(i) $[F : k(x)] < \infty$

(ii) $\deg P \leq [F : k(x)]$

(i) Since $0 \neq x \in P$ is transcendental, by proposition 1.6, $[F : k(x)]$ is finite. (ii) Suppose $a_1(x)x_1 + a_2(x)x_2 + ... + a_n(x)x_n = 0$ is some non-trivial linear combination of elements in F where $a_1(x), ..., a_n(x) \in k(x)$. Assume that x does not divide each $a_i(x)$, hence each $a_i(x)$ may be expressed as $a_i(x) = a_i + g_i(x)x$ for some $g_i(x) \in k[x]$ and $a_i(x) \in k$, with not all $a_i = 0$. Since $x \in P$ and $g_i(x) \in \mathcal{O}$, we have $a_i(x) \equiv a_i \mod P$. If we apply the residue class map to $a_1(x)x_1 + a_2(x)x_2 + ... + a_n(x)x_n = 0$ we get $0 + P = a_1(x_1 + P) + a_2(x_2 + P)^2 + ... + a_n(x_n + P)^n$ where not all $a_i = 0$. Hence $x_1 + P, x_2 + P, ..., x_n + P$ are linearly dependent over k. Thus, any elements $x_1, ..., x_n \in \mathcal{O}$, who's residue classes $x_1 + P, ..., x_n + P$ are linearly independent over k, are linearly independent over $k(x)$. ■

Definition 1.21 Let F/k be an function field. Let $z \in F$ and $P \in \mathbb{P}_F$. We say that P is a zero of z if $v_P(z) > 0$; P is a pole of z if $v_P(z) < 0$. If $v_P(z) = m > 0$, P is a zero of z of order m; if $v_P(z) = -m < 0$, P is a pole of z of order m.

Example 1.22 Let $F = \mathbb{C}(x)/\mathbb{C}$ be the rational function field and consider the polynomial $f = x^3(x+1) \in F$. Let P_x denote the maximal ideal of $\mathcal{O}_x = \{f/g \mid f, g \in \mathbb{C}[x] \text{ and } g \notin (x)\}$ The prime element for P_x is the polynomial x. Let v_x be the discrete valution corresponding to the polynomial x, as in theorem 1.19. Then $f = x^3(x+1)$. To assert that $v_x(f) = 3$, we need to show that $x + 1$ is a unit in $\mathcal{O}_x$. Notice that $x + 1 \in \mathcal{O}_P$ since $x \nmid 1$. Similarly $(x+1)^{-1} \in \mathcal{O}_P$ since $x \nmid x + 1$. Hence $x + 1 \in \mathcal{O}_P^*$. Therefore the valuation of f at place P_x is $v_x(f) = 3$. Let P_{x+1} denote the maximal ideal of the valuation ring $\mathcal{O}_{x+1} = \{f/g \mid f, g \in \mathbb{C}[x] \text{ and } g \notin (x+1)\}$ The prime element for P_{x+1} is the polynomial $x + 1$. Let v_{x+1} be the discrete valution corresponding to the polynomial $x+1$. A similar argument shows that $v_{x+1}(f) = 1$. So f has zeros at P_x and P_{x+1}. Let v_∞be the discrete valution defined as in example 1.18. Part (f) of theorem 1.19 shows that we may obtain a valution ring $\mathcal{O}_\infty := \{f/g \in \mathbb{C}(x) \mid \deg(g) - \deg(f) \geq 0\}$ with corresponding place $P_\infty := \{f/g \in \mathbb{C}(x) \mid \deg(g) - \deg(f) > 0\}$. Let $z = x^{-1}$. Then part (e) asserts that since $v_\infty(z) = 1$, the element z is a prime element of P_∞. So v_∞ may be redefined the same way as in theorem 1.19, where z is the prime element of the place P_∞. Notice that $f = z^{-4}(x+1)x^{-1}$. To conclude that $v_\infty(f) = -4$, it suffices to show that $(x+1)x^{-1}$ is a unit in $\mathcal{O}_\infty$. We know that the units in $\mathcal{O}$ are exactly those which have valuation 0, by part (d) of theorem 1.19. So we compute $v_\infty((x+1)x^{-1}) = \deg(x) - \deg(x+1) = 1 - 1 = 0$. Hence $v_\infty(f) = -4$. This means the place P_∞ is a pole of f in $\mathbb{C}(x)/\mathbb{C}$.

Theorem 1.23 Let F/k be a function field and let R be a subring of F with $k \subseteq R \subseteq F$. Suppose that $\{0\} \neq I \subsetneq R$ is a proper ideal of R. Then there is a place $P \in \mathbb{P}_F$ such that $I \subseteq P$ and $R \subseteq \mathcal{O}_P$.

Proof. See proof of theorem 1.1.13 in Stinchtenoth. ■

Corollary 1.24 Let F/k be a function field, $z \in F$ transcendental over k. Then z has at least one zero and one pole. In particular $\mathbb{P}_F \neq \varnothing$.

Proof. Let $R = k[x]$ and consider the ideals $I = zR$ and $J = z^{-1}R$. By theorem 1.23 there exists a places $P, Q \in \mathbb{P}_F$ with $z \in P$ and $z^{-1} \in Q$, so both z and z^{-1} have zeros in F. Thus both z and z^{-1} both have poles in Q and P respectively. ■

2 The Rational Function Field

Proposition 2.1 Let $F = k(x)$ be a ration function field, where k is any field. Then the following hold;

(a) Let $p(x)$ be an irreducible polynomial in $k[x]$ and $P = P_{p(x)}$ a place of F, then $F_P \cong k[x]/(p(x))$.

(b) The infinity place defined in example 1.22 is rational.

Proof. (a): The map $f(x) \mapsto f(x) + P$ is homomorphism from $k[x]$ onto F_P with kernel $(p(x))$. (b): Consider the place P_x, corresponding to the polynomial $p = x$. From (a), we know that $F_P \cong k[x]/(x)$. Hence $\deg P_x = [F_p : k] = [k[x]/(x) : k] = 1$. Make the change of coordinate $t = x^{-1}$, then $P_\infty = P_t$. Hence $\deg P_\infty = 1$. ■

Theorem 2.2 There are no places of the rational function field $k(x)/k$ other than the places $P_{p(x)}$ and P_∞ where $p(x)$ is a monic irreducible polynomial in $k[x]$.

Proof. Let P be a place of $k(x)/k$. There are two cases; $x \in \mathcal{O}_P$ or $x \notin \mathcal{O}_P$. Suppose the former. Then $k[x] \subset \mathcal{O}_P$. Let $I = k[x] \cap P$. I is a prime ideal of $k[x]$. Thus $k[x]/I$ embeds into the field $k(x)_P$ through the residue class map. Hence $I \neq 0$ by proposition 1.10. So there exists a *uniquely determined* irreducible monic polynomial $p(x) \in k[x]$ such that $I = p(x)k[x]$. Every $g(x) \in k[x]$ with $p(x) \nmid g(x)$ is not in I, so $g(x) \notin P$ and $1/g(x) \in \mathcal{O}_P$ by proposition 1.10. Therefore $\mathcal{O}_P = \{\frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x] \text{ and } p(x) \nmid g(x)\} \subseteq \mathcal{O}_P$. By theorem 1.19, all valuation rings are maximal proper subrings, thus $\mathcal{O}_P = \mathcal{O}_{p(x)}$. For the second case; $x \notin \mathcal{O}_P$, we must have $k[x^{-1}] \in \mathcal{O}_P$ because $\mathcal{O}_P$ is a valuation ring. So, as in case 1, $x^{-1} \in P \cap k[x^{-1}]$ and $P \cap k[x^{-1}] = x^{-1}k[x^1]$. So

$$
\begin{aligned}
\mathcal{O}_P &\subseteq \{\frac{f(x^{-1})}{g(x^{-1})} \mid f(x^{-1}), g(x^{-1}) \in k[x^{-1}] \text{ and } x^{-1} \nmid g(x^{-1})\} \\
&= \{\frac{a_0 + a_1x^{-1} + ... + a_nx^{-n}}{b_0 + b_1x^{-1} + ... + b_mx^{-m}} \mid b_0 \neq 0\} \\
&= \{\frac{a_0x^{n+m} + ... + a_nx^m}{b_0x^{n+m} + ... + b_mx^n} \mid b_0 \neq 0\} \\
&= \{\frac{u(x)}{v(x)} \mid u(x)v(x) \in k[x] \text{ and } \deg u(x) \leq \deg v(x)\} \\
&= \mathcal{O}_\infty
\end{aligned}
$$

■

3 Divisors

Definition 3.1 Let F/k be a function field over a field k. The divisor group of F/k is defined as the free abelian group which is generated by the places of F/k, denoted $\mathrm{Div}(F)$. The elements of $\mathrm{Div}(F)$ are called divisors of F/k. In other words; a divisor is a formal sum;

$$D = \sum_{P \in \mathbb{P}_F} n_P P$$

with $n_P \in \mathbb{Z}$, almost all $n_P = 0$. Two divisors $D = \sum n_P P$ and $D' = \sum n'_P P$ are added coefficientwise;

$$D + D' = \sum_{p \in \mathbb{P}_F} (n_p + n'_p)P$$

The zero element of the divisor group $\mathrm{Div}(F)$ is the divisor;

$$0 := \sum_{p \in \mathbb{P}_F} r_P P$$

where all $r_P = 0$. For all $Q \in \mathbb{P}_F$ and $D \in \mathrm{Div}(F)$ we define $v_Q(D) := n_Q$.

Example 3.2 Consider the rational function field $\mathbb{C}(x)/\mathbb{C}$. Since $\mathbb{C}$ is algebraically closed, we may identify the places of $\mathbb{C}(x)/\mathbb{C}$ with $\mathbb{C} \cup \{\infty\}$ as follows: Let P be a place of $\mathbb{C}(x)/\mathbb{C}$. By theorem 2.2, if P is not the infinity place, then it can be indentified with a irreducible polynomial p in $\mathbb{C}[x]$. Since $\mathbb{C}$ is algebraically closed, $p = x - a$ for some $a \in \mathbb{C}$. Through this, all non-infinity places maybe be identified with some $a \in \mathbb{C}$. We identify P_∞ with ∞. In this view, $3(i) + \sqrt{3}i(\infty) \in \mathrm{Div}(\mathbb{C}(x))$

Example 3.3 Let F/k be a function field and $D = \sum_P n_P P$ where $n_P = 1$ for all $P \in \mathbb{P}_F$. Then $D \notin \mathrm{Div}(F)$ since it has infinitely many nonzero coefficients.

Lemma 3.4 Let F/k be a function field. Every $z \in F$ has finitely many zeros and finitely many poles.

Proof. See Stichtenoth corollary 1.3.4. for proof. ∎

Definition 3.5 Let F/k be a function field. A partial ordering on $\mathrm{Div}(F)$ is defined by;

$$D_1 \leq D_2 \Leftrightarrow v_P(D_1) \leq v_P(D_2) \text{ for all } P \in \mathbb{P}_F$$

A divisor $D \geq 0$ is called possitive (or effective). The degree of a divisor is defined as;

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

which is a homomorphism $\mathrm{Div}(F) \xrightarrow{\deg} \mathbb{Z}$. By Lemma 3.4 any nonezero element $x \in F$ has finitely many zeros and poles in $\mathbb{P}_F$. Thus this definition makes sense.

Definition 3.6 Let F/k be a function field. Let $0 \neq x \in F$ and denote by Z (respectively N) the set of all zeros (repectively poles) of x in $\mathbb{P}_F$. Then we define

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

$$(x)_\infty := \sum_{P \in N} (-v_P(x)) P$$

$$(x) := (x)_0 - (x)_\infty$$

where $(x)_0, (x)_\infty$, and (x) are called the zero divisor of x, the pole divisor of x and the principal divisor of x respectively.

Example 3.7 Let $F = \mathbb{C}(x)/\mathbb{C}$ be the rational function field and consider the polynomial $f = x^3(x+1) \in F$. Recall from example 1.22 that the valutions of f at places P_x,P_{x+1} and P_∞ were $3, 1$ and -4 respectively. Let p be a monic irreducible polynomial in $\mathbb{C}[x]$ other than x and $x+1$. Consider the place $P = P_p$. Suppose $p \mid f$, then $f = ph$ for some monic $h \in \mathbb{C}[x]$. So $p = x^n(x+1)^m$ and $h = x^r(x+1)^s$ for some $n, m, r, s \in \mathbb{Z}^+$ such that $n + r = 3$ and $m + s = 1$.

Since $p \neq x$, $p \neq x+1$ and p is irreducible, it follows that $n = m = 0$ and $h = f$. Therefore $f = p^0 x^3(x+1)$ and $p \nmid f$, so $(x^3(x+1))^{-1} \in \mathcal{O}_P$. Furthermore $x^3(x+1) \in \mathcal{O}_P$, since $p \nmid 1$. Which implies $x^3(x+1) \in \mathcal{O}_P^*$ and $v_P(f) = 0$. This imples, by theorem 2.2, that the only zeros of f in $\mathbb{C}(x)/\mathbb{C}$ are the places P_x and P_{x+1}, while the only pole of f in $\mathbb{C}(x)/\mathbb{C}$ is P_∞. Hence for the element $f \in \mathbb{C}(x)/\mathbb{C}$ we obtain divisors;

$$(f)_0 = 3P_x + P_{x+1}$$

$$(f)_\infty = 4P_{1/x}$$

$$(f) = 3P_x + P_{x+1} - 4P_{1/x}$$

Definition 3.8 Let F/k be a function field. The set of divisors;

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

is called the group of principal divisors of F/k.

Example 3.9 Again, consider the rational function field $F = \mathbb{C}(x)/\mathbb{C}$. Let $f \in \mathbb{C}[x] \backslash \{0\}$ and suppose we know the prime factorization of $f = ap_1^{e_1}p_2^{e_2}...p_n^{e_n}$ for $e_1, e_2, ..., e_n \in \mathbb{N}$, $a \in \mathbb{C}$ and $p_1, p_2, ..., p_n$ distinct monic irreducible polynomials in $\mathbb{C}[x]$. Denote the place of $\mathbb{C}(x)$ at prime p_i by $P_i = P_{p_i}$ for $i = 1, 2, ...n$. Then at places $P_1, P_2, ..., P_n \in \mathbb{P}_F$, f has valuation $v_{P_i}(f) = e_i$ for $i = 1, 2, ..., n$. To verify this claim it suffices to show that $fp_i^{-e_i} \in \mathcal{O}_{P_i}^*$ for all $i = 1, 2, ...n$. Since $p_1, p_2, ..., p_n$ are distinct irreducible polynomials in $\mathbb{C}[x]$, it follows that $p_i \nmid p_j$ for all $j \neq i$, thus $v_{p_i}(fp_i^{-e_i}) \leq 0$ for all $i = 1, 2, ..., n$. Since $e_1, e_2, ..., e_n \geq 0$, it follows that $v_{p_i}(fp_i^{-e_i}) \geq 0$, and thus $v_{p_i}(fp_i^{-e_i}) = 0$ for all $i = 1, 2, ..., n$. By Theorem 1.19 part d, $fp_i^{-e_i} \in \mathcal{O}_{P_i}^*$ for all $i = 1, 2, ..., n$. From theorem 2.2, we get that besides the infinity place, these are the only zeros of f: for any other zero would have to be at a place corresponding to a irreducible polynomial not in the representation of f and thus would have valuation 0. Hence the f has zero divisor

$$(f)_0 = \sum_{i=1}^{n} e_i P_i$$

We calculate the valutation at the infinity place P_∞;

$$v_\infty(f) = \deg(1) - \deg(ap_1^{e_1}p_2^{e_2}...p_n^{e_n}) = 0 - \sum_{i=1}^{n} e_i \cdot \deg(p_i)$$

Since $p_1, p_2, ..., p_n \in \mathbb{C}[x]$, they all have degree 1, $v_\infty(f) = \sum_{i=1}^{n} e_i$. So

$$(f)_\infty = (\sum_{i=1}^{n} e_i)P_\infty$$

$$(f) = \sum_{i=1}^{n} e_i P_i - (\sum_{i=1}^{n} e_i) P_\infty$$

To calculate the degree of $(f)_0, (f)_\infty, (f)$, we need to find the degrees of the places $P_1, P_2, ..., P_n$ and P_∞. That is, calculate $\deg P_i = [F_{P_i} : \mathbb{C}] = [\mathcal{O}_{P_i}/P_i] : \mathbb{C}]$ for $i = 1, 2, ..., n$ and $\deg P_\infty$. By proposition 2.1 part (a), $F_{P_i} = \mathcal{O}_{P_i}/P_i \cong \mathbb{C}[x]/(p_i)$ for all $i = 1, 2, ..., n$. Since each p_i is linear, $[\mathbb{C}[x]/(p_i) : \mathbb{C}] = 1$ for all $i = 1, 2, ...n$. Part (b) of proposition 2.1 states that $degP_\infty = 1$, hence;

$$\deg(f)_0 = \sum_{i=1}^{n} e_i \cdot \deg P_i = \sum_{i=1}^{n} e_i = \deg_{\mathbb{C}[x]}(f)$$

$$\deg(f)_\infty = (\sum_{i=1}^{n} e_i) \cdot P_\infty = \sum_{i=1}^{n} e_i = \deg_{\mathbb{C}[x]}(f)$$

$$\deg(f) = \sum_{i=1}^{n} e_i - \sum_{i=1}^{n} e_i = 0$$

So the degree of every principal divisor of a polynomial in $\mathbb{C}[x]$ has degree 0. Theorem 3.17 will generalize this result.

Definition 3.10 Let F/k be a function field. For a divisor $A \in Div(F)$ we define the Riemann-Roch space associated to A by

$$\mathscr{L}(A) := \{x \in F \mid (x) \geq -A\}$$

Lemma 3.11 Let F/k be a function field. Let $A \in Div(F)$. Then $\mathscr{L}(A)$ is a vector space over k.

Proof. Let $x, y \in \mathscr{L}(A)$. Then $v_P(x) \geq -v_P(A)$ and $v_P(y) \geq -v_P(y)$ for all $P \in \mathbb{P}_F$. Suppse $v_P(x) < v_P(y)$ for all $P \in \mathbb{P}_F$. Then $v_P(x + y) = min\{v_P(x), v_P(y)\} = v_P(x) \geq v_P(A)$. So $x + y \in \mathscr{L}(A)$. Let $a \in k$. Then $v_P(ax) = v_P(a) + v_P(x) = 0 + v_P(x) = v_P(x) \geq -v_P(A)$ for all $P \in \mathbb{P}_F$. ■

Definition 3.12 Let F/k be a function field. For a divisor $A \in Div(F)$ the integer $\ell(A) := dim\mathscr{L}(A)$ is called the dimension of the divisor A.

Example 3.13 Let $p = y^2 + x^3 - x$ and consider the integral domain A as in example 1.4. Let $\pi : \mathbb{C}[x, y] \to A$ be the canonical homomorphism of the quotient ring. For simplicity, define $x := \pi(x)$ and $y := \pi(y)$. Then $A = \mathbb{C}[x, y]$ where $x, y \in A$ satisfy $y^2 + x^3 - x = 0$. Exercise 6.1 shows that A is a free $\mathbb{C}[x]$-module, with basis $\{1, y\}$. So each element of A has a unique expression of the form $p(x)y + q(x)$ where $p(x), q(x)$ are polynomials in x. From exercise 6.1 we also know that $F/\mathbb{C}$ is a function field over $\mathbb{C}$. Let $\mathbb{V} = \mathbb{V}(F/\mathbb{C})$ be the set of valuation rings of $F/\mathbb{C}$ and $\mathbb{P} = \mathbb{P}(F/\mathbb{C})$ the set of places. If we make the following assumptions;

- There is exactly one element $\mathcal{O} \in \mathbb{V}$ such that $A \nsubseteq \mathcal{O}$. Denote it by $\mathcal{O}_\infty$, let P_∞ be its maximal ideal, and let $v_\infty : F^* \to \mathbb{Z}$ be its valuation.
- $v_\infty(x) = -2$
- A is equal to the intersection of all rings $\mathcal{O} \in \mathbb{V} \setminus \{\mathcal{O}_\infty\}$.

Then we have the following;

(a) If $f \in F^*$ then $v_P(f) \geq 0$ for all $P \in \mathbb{P} \setminus \{P_\infty\} \iff f \in A$.

(b) $v_\infty(y) = -3$

(c) For any $f = p(x)y + q(x) \in A$, let $m = \deg_x(p(x))$ and $n = \deg_x(q(x))$.

  (i) $v_\infty(p(x)y) = -2n - 3$

  (ii) $v_\infty(q(x)) = -2m$

  (iii) $v_\infty(p(x)y) \neq v_\infty(q(x))$

  (iv) $v_\infty(f) = -\max\{2n + 3, 2m\}$

(d) Let $N \geq 2$. Then $\mathscr{L}(2NP_\infty)$ has basis $\{y, xy, x^2y, ..., x^{N-2}y, 1, x, x^2, ..., x^N\}$ and dimension $\ell(2NP_\infty) = 2N$.

Proof. (a) Let $f \in F^*$. $v_P(f) \geq 0$ for all $P \in \mathbb{P}_F \backslash \{P_\infty\}$ if and only if $f \in O_P$ for all $P \in \mathbb{P}_F \backslash \{P_\infty\}$ if and only if $f \in A$ by assumption 3.13.

(b) Recall lemma 1.17. Then

$$\begin{aligned}
2v_\infty(y) &= v_\infty(y^2) \\
&= v_\infty(x - x^3) \\
&= v_\infty(x) + v_\infty(1 + x) + v_\infty(1 - x) \\
&= v_\infty(x) + \min\{v_\infty(1), v_\infty(-x)\} + \min\{v_\infty(1), v_\infty(x)\} \\
&= (-2) + (-2) + (-2) \\
&= -6
\end{aligned}$$

Hence $v_\infty(y) = -3$

(c) Since p, q are polynomials in $\mathbb{C}[x]$, we may write them as $p_1^{e_1} p_2^{e_2} ... p_s^{e_s}$ and $q_1^{f_1} q_2^{f_2} ... q_t^{f_t}$ respectively, where $p_1, ..., p_s, q_1, ... q_t$ are linear polynomials in $\mathbb{C}[x]$ and $e_1, ..., e_s, f_1, ..., f_t \in \mathbb{Z}$. Hence

$$\begin{aligned}
v_\infty(py) &= v_\infty(p_1^{e_1} p_2^{e_2} ... p_s^{e_s} y) \\
&= e_1 v_\infty(p_1) + ... + e_s v_\infty(p_s) + v_\infty(y) \\
&= e_1(-2) + ... + e_s(-2) - 3 \\
&= -2n - 3
\end{aligned}$$

$$\begin{aligned} v_\infty(q) &= v_\infty(q_1^{f_1} q_2^{f_2} ... q_t^{f_t}) \\ &= f_1 v_\infty(q_1) + ... + f_t v_\infty(p_t) \\ &= f_1(-2) + ... + f_t(-2) \\ &= -2m \end{aligned}$$

Notice that

$$\begin{aligned} v_\infty(py) = v_\infty(q) &\implies -2n - 3 = -2m \\ &\implies m = n + 3/2 \end{aligned}$$

Which is impossible since $q \in \mathbb{C}[x]$. Hence $v_\infty(py) \neq v_\infty(q)$. Therefore

$$\begin{aligned} v_\infty(f) &= v_\infty(p(x)y + q(x)) \\ &= \min\{v_\infty(p(x)y), v_\infty(q(x))\} \\ &= \min\{-2n - 3, -2m\} \\ &= -\max\{2n + 3, 2m\} \end{aligned}$$

(d) Let $N \geq 2$ and write $f = py + q$. $f \in \mathscr{L}(2NP_\infty)$ if and only if $v_P(f) + v_P(2NP_\infty) \geq 0$ for all $P \in \mathbb{P}_F$ by definition. By part (a), we know that $v_P(f) \geq 0$ for all $P \in \mathbb{P}_F \backslash P_\infty$ if and only if $f \in A$. Since $v_P(2NP_\infty) = 0$ for all $P \in \mathbb{P}_F \backslash P_\infty$, we require $v_P(f) \geq 0$ for all $P \in \mathbb{P}_F \backslash P_\infty$. Thus $f \in A$. Hence

$$\begin{aligned} \mathscr{L}(2NP_\infty) &= \{f \in A \mid \max\{2\deg(q), 3 + 2\deg(p)\} \leq 2N\} \\ &= \{py + q \in A \mid \deg(p) \leq N - 3/2, \deg(q) \leq N\} \\ &= \{py + q \in A \mid \deg(p) \leq N - 2, \deg(q) \leq N\} \end{aligned}$$

Hence $\{y, xy, x^2y, ..., x^{N-2}y, 1, x, x^2, ..., x^N\}$ is a basis for $\mathscr{L}(2NP_\infty)$ over $\mathbb{C}$ and $\ell(2NP_\infty) = (N - 1) + N + 1 = 2N$.

■

Example 3.14 Let F/k be a function field over k and $A \in \mathrm{Div}(F)$. We have $\mathscr{L}(0) = k$ and if $A < 0$ then $\mathscr{L}(A) = \{0\}$.

Proof. To show the first assertion, let $0 \neq x \in k$, then $(x) = 0$. So $x \in \mathscr{L}(0)$. Let $0 \neq x \in \mathscr{L}(0)$. Then $(x) \geq 0$, but then x has no pole, so by corollary 1.24, so $x \in k$. Suppose $A < 0$ and let $0 \neq x \in \mathscr{L}(A)$. Then $(x) \geq -A > 0$, but then x has at least one zero and no pole. This is impossible. Hence $x = 0$. ■

Proposition 3.15 Let A, B be two divisors of F/k with $A \leq B$. Then we have $\mathscr{L}(A) \subseteq \mathscr{L}(B)$ and $\dim(\mathscr{L}(B)/\mathscr{L}(B)) \leq \deg B - \deg A$.

Proof. Assume that A, B be two divisors of F/k with $A \leq B$. We show $\mathscr{L}(A) \subseteq \mathscr{L}(B)$. Let $x \in \mathscr{L}(A)$, then $v_P(x) + v_P(x) \geq v_P(x) + v_P(B) \geq 0$, so $x \in \mathscr{L}(B)$. Hence $\mathscr{L}(A) \subseteq \mathscr{L}(B)$. To vertify the second claim, assume that $B = A + P$ for some $P \in \mathbb{P}_F$. This is possible since the general case follows by induction. Let $t \in F$ such that $v_P(t) = v_P(B) = v_P(A) + 1$. For $x \in \mathscr{L}(B)$ we have $v_P(x) \geq -v_P(B) = -v_P(t)$, so $xt \in \mathcal{O}_P$. So we obtain a $k - linear$ map $\varphi : \mathscr{L}(B) \Longrightarrow F_P$, $x \mapsto xt + P$. An element x is in the the kernel of φ if and only if $v_P(xt) > 0$, that is $v_P(x) \geq -v_P(A)$. So $\ker\varphi = \mathscr{L}(A)$. Thus φ induces an *injective* k-linear map from $\mathscr{L}(B)/\mathscr{L}(A)$ to F_P. Therefore $\dim\mathscr{L}(B)/\mathscr{L}(A) \leq \dim F_P = \deg B - \deg A$. ∎

Lemma 3.16 Let F/k be a function field and let $P_1, ..., P_r$ be zeros of the element $x \in F$. Then $\sum_{i=1}^{r} v_{P_i}(x) \leq [F : k(x)]$.

Proof. See Stichtenoth Proposition 1.3.3. ∎

Theorem 3.17 All principal divisors have degree zero. More precisely, let $x \in F\backslash k$ and $(a)_0$ resp. $(a)_\infty$ denote the zero resp. pole divisor of x. Then

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

.

Proof. Let $n := [F : k(x)]$. Then $\deg(x)_\infty \leq n$ by 3.16, we have $\sum_{i=1}^{r} v_{P_i}(x) \leq [F : k(x)]$. Thus it remains to show that $n \geq \deg(x)_\infty$. Let $v_1, ...v_n$ as a basis for $F/k(x)$. Let $A \geq 0$ be a divisor such that $(v_i) \geq A$ for $i = 1, .., n$. Then we have $\mathscr{L}(r(x)_\infty + A) \geq n(r+1)$ for all $r \geq 0$, since $x^i v_j \in \mathscr{L}(r(x)_\infty + 1)$ for $0 \leq i \leq r$, $1 \leq j \leq n$. Letting $c := \deg A$ we get $n(r+1) \leq \mathscr{L}(r(x)_\infty + A) \leq r \cdot (x)_\infty + c + 1$. Thus $r(\deg(x)_\infty - n) \geq n - c - 1$ for all $r \in \mathbb{N}$. Hence $\deg(x)_\infty \geq n$. ∎

Proposition 3.18 There is a constant $\gamma \in \mathbb{Z}$ such that for all divisors $A \in Div(F)$ the following holds:

$$degA - l(A) \leq \gamma$$

Proof. First observe that by proposition 3.15, $A_1 \leq A_2 \Rightarrow \deg A_1 - \mathscr{L}(A_1) \leq \deg A_2 - \mathscr{L}(A_2)$. Let $x \in F\backslash k$ and consider the divisor $(x)_\infty$. There exists a divisor $C \geq 0$ such that $\mathscr{L}(r(x)_\infty + C) \geq (r+1) \cdot \deg(x)_\infty$ for all $r \geq 0$. We also have $\mathscr{L}(r(x)_\infty + C) \leq \mathscr{L}(r(x)_\infty) + \deg C$ from proposition 3.15. Hence $\mathscr{L}(r(x)_\infty) \geq (r+1) \cdot \deg(x)_\infty - \deg C = \deg(r(x)_\infty) + ([F : k(x)] - \deg C)$. Hence $\deg(r(x)_\infty) - \mathscr{L}(r(x)_\infty) \leq \gamma$ for all $r > 0$ with some $\gamma \in \mathbb{Z}$. *Claim*: For all $A \in \mathrm{Div}(F)$, there exists divisors A_1, D and a integer $r \geq 0$ such that $A \leq A_1$, $A = D + P$ for some $P \in \mathbb{P}_F$ and $D \leq r(x)_\infty$. *Proof of claim:* Let $A_1 \geq A$

such that $A_1 > 0$. Then $\mathscr{L}(r(x)_\infty - A_1) \geq \mathscr{L}(r(x)_\infty) - \deg A_1 \geq \deg(r(x)_\infty) - \gamma - \deg A_1 > 0$ for sufficiently large r. Thus there exists some nonzero element $z \in \mathscr{L}(r(x)_\infty - A_1)$. Letting $D := A_1 - (z)$, we obtain $A = D + P$ where $P + -(z)$ and $D \leq A_1 - (A_1 - r(x)_\infty) = r(x)_\infty$ as desired. Thus the claim is verified. From this, observe that $\deg A - \mathscr{L}(A) \leq \deg A_1 - \mathscr{L}(A_1) = \deg D - \mathscr{L}(D) \leq \deg(r(x)_\infty) - \mathscr{L}(r(x)_\infty) \leq \gamma$. ■

Definition 3.19 Let F/k be a function field. The genus of g of F/k is defined by

$$g := max\{degA - l(A) + 1 \mid A \in Div(F)\}$$

Theorem 3.20 (Riemann's Theorem) Let F/k be a function field of genus g. Then there exists an integer c, depending only on the function field F/k, such that $l(A) = degA + 1 - g$ whenever $degA \geq c$.

Proof. Let A_0 such that $g = \deg A_0 \mathscr{L}(A_0) + 1$ and set $c = \deg A_0 + g$. If $\deg A \geq c$ then $\mathscr{L}(A - A_0) \geq \deg(A - A_0) + 1 - g \geq c - \deg A_0 + 1 - g = 1$. So there is an element $0 \neq z \in \mathscr{L}(A - A_0)$. Consider the divisor $A' = A + (z) \geq A_0$. We have $\deg A' - \mathscr{L}(A') \geq \deg A_0 - \mathscr{L}(A_0) = g - 1$. Hence $\mathscr{L}(A) \leq \deg A + 1 - g$. ■

Example 3.21 Recall the setup of example 3.13. Let $N > 0$ be arbitrarly large. We know that $\mathscr{L}(2NP_\infty) = 2N$. Assume $\deg P_\infty = 1$. Then by Riemann's Theorem, $g = \deg(2NP_\infty) - \mathscr{L}(2NP_\infty) + 1 = 1$. Then we may conclude that $F/\mathbb{C}$ has genus 1, that is the curve $p = y^2 + x^3 - x$ has genus 1. Similary, from exercise i, we know that $\mathscr{L}(NP_\infty) = N + 1$, where P_∞ denotest the infinity place of the function field $k(x)/k$. From proposition 2.1, $\deg P)\infty = 1$. Thus by Riemann's theorem $g = \deg(NP_\infty) - \mathscr{L}(NP_\infty) + 1 = N - N - 1 + 1 = 0$ Hence the rational function field has genus 0.

4 Dicriticals

Lemma 4.1 Let E/k be a field extension and $u, v \in E$. Then we have field extensions:

$$@R = 0pt@C = 6ptEk(u,v)@-[dl]@-[dr]@-[uu]k(u)k(v)k@-[ul]@-[ur]$$

Assume that each of u, v is transcendental over k. Then the following are equivalent:

- (u, v) is algebraically dependent over k;
- v is algebraic over $k(u)$;
- u is algebraic over $k(v)$.

Proof. (4.1) $\implies$ (4.1) Assume (u, v) are algebraically dependent over k. Then there exists

$$f(X, Y) = \sum_{i,j\in\mathbb{N}} a_{ij} X^i Y^j \in k[X, Y]\backslash\{0\}$$

such that $f(u, v) = \sum_{i,j\in\mathbb{N}} a_{ij} u^i v^j = 0$. Consider

$$g(Y) = \sum_{i,j\in\mathbb{N}} a_{ij} u^i Y^j \in k[u][Y]\backslash\{0\}$$

We still have $g(v) = \sum_{i,j} a_{ij} u^i v^j = 0$. Hence v is algebraic over $k[u] \subset k(u)$.
(4.1) $\implies$ (4.1); Assume v is algebraic over $k(u)$. Then there exists

$$f(Y) = \sum_{i\in\mathbb{N}} a_i(u) Y^i \in k(u)[Y]\backslash\{0\}$$

such that $f(v) = 0$. Since $a_i(u) \in k(u)$ for all i, $a_i(u) = \frac{f_i(u)}{g_i(u)}$ where $f_i(u), g_i(u) \in k[u]$ and $g_i(u) \neq 0$. Let

$$a(u) := \prod_i g_i(u) \in k[u]\backslash\{0\}$$

Then consider

$$g(Y) := a(u)f(Y) = a(u)\sum_{i\in\mathbb{N}} a_i(u)Y^i = \sum_{i\in\mathbb{N}} a(u)a_i(u)Y^i$$

Note that $h_i(u) := a(u)a_i(u) \in k[u]$ for all i and we still have $g(v) = 0$. We can rewrite $g(Y)$ as

$$g(X) = \sum_{i\in\mathbb{N}} h_i(X)v^i \in k[v][X]\backslash\{0\}$$

and we still have $g(u) = \sum_{i\in\mathbb{N}} h_i(u)v^i = 0$. Hence u is algebraic over $k[v] \subset k(v)$
(4.1) $\implies$ (4.1); Assume u is algebraic over $k(v)$. Then there exists

$$f(X) = \sum_{i\in\mathbb{N}} a_i(v) X^i \in k(v)[X]\backslash\{0\}$$

such that $f(u) = 0$. Since $a_i(v) \in k(v)$ for all i, $a_i(v) = \frac{f_i(v)}{g_i(v)}$ where $f_i(v), g_i(v) \in k[Y]$ and $g_i(v) \neq 0$. Let

$$a(v) := \prod_i g_i(v) \in k[v]\backslash\{0\}$$

Then consider

$$g(X) = a(v)f(X) = a(v)\sum_{i\in\mathbb{N}} a_i(v)X^i = \sum_{i\in\mathbb{N}} a(v)a_i(v)X^i$$

Note that $h_i(v) := a(v)a_i(v) \in k[v]$ for all i and we still have $g(u) = 0$. We can rewrite $g(Y)$ as

$$g(X, Y) = \sum_{i \in \mathbb{N}} h_i(Y)X^i \in k[X, Y]\backslash\{0\}$$

We still have $g(X, Y) = \sum_{i \in \mathbb{N}} h_i(v)u^i = 0$. Hence (u, v) is algebraically independent over k. ■

Lemma 4.2 Let k be a field and let $k(x_1, \ldots, x_n)$ be the field of fractions of the polynomial ring $k[x_1, \ldots, x_n]$ in n variables over k (where $n \geq 1$). Then k is algebraically closed in $k(x_1, \ldots, x_n)$.

Proof. Induction on n. When $n = 1$, then we are considering the rational function field in one variable over k. Let P be a place of $k(x)/k$ of degree 1. That is $P := P_{x-a}$ for $a \in k$. The algebraic closure of k, denoted $\tilde{k}$, embeds into $k(x)_P$, since $P \cap \tilde{k} = \{0\}$. Then we have $k \subseteq \tilde{k} \subseteq k(x)_P = k$. Hence k is algebraically closed in $k(x)$. Assume that $n > 1$. Inductive hypothesis: k is algebraically closed in $k(x_1, \ldots, x_{n-1})$. To prove that k is algebraically closed in $k(x_1, \ldots, x_n)$, we consider an element w of $k(x_1, \ldots, x_n)$ that is algebraic over k. We have to show that $w \in k$. Observe that w is algebraic over $k(x_1, \ldots, x_{n-1})$. Write $F = k(x_1, \ldots, x_n)$ and $K = k(x_1, \ldots, x_{n-1})$. Then F/K is the rational function field of one variable, so K is algebraically closed in F, so $w \in K$. As $w \in k(x_1, \ldots, x_{n-1})$ is algebraic over k, the inductive hypothesis implies that $w \in k$. ■

For this section, let k be a field, $A = k[x, y]$ the polynomial ring in two variables over k, and $L = \operatorname{Frac} A = k(x, y)$, the field of rational functions in two variables. The objects k, A and L are fixed throughout. For each choice of $F \in A \setminus k$, we may consider the subfield $K = k(F)$ of L (since F is an element of the field $L = k(x, y)$, it follows that $k(F)$ is a subfield of L). We have $k \subset K \subset L$ where k and L are always the same but K depends on the choice of F. We are particularly interested in the field extension L/K. Our first objective is to show that L/K is a function field of one variable. There are several steps in the proof of this.

Remark By lemma 4.2, k is algebraically closed in L. However, whether or not K is algebraically closed in L depends on the choice of F. For instance, if $F = x$ then L/K is the rational function field of one variable, so K is algebraically closed in L in this case. But if $F = x^2$ then x is an element of L that is algebraic over K but that does not belong to K, so K is not algebraically closed in L in this case.

Proposition 4.3 Show that the following are equivalent:

(i) (F, x) is algebraically dependent over k;

(ii) x is algebraic over K;

(iii) F is algebraic over $k(x)$;

(iv) $F \in k(x)$;

(v) $F \in k[x]$.

Proof. Since A is a polynomial ring in two variables x, y, by definition (x, y) is algebraically independent over k, so we have that x is transcendental over k. Suppose F is algebraic over k, then $F \in k$ by 4.2, and this contradicts the hypothesis $F \in A \setminus k$. Therefore we may use lemma 4.1 to show that i, ii and iii are all equivalent. ((iii) $\Rightarrow$ (iv)): Since $L/k(x)$ is the rational function field in one variable, it follows that $k(x)$ is algebraically closed in L. ((iv) $\Rightarrow$ (v)): $F \in k[x, y] \backslash k$ by definition. Hence if $F \in k(x)$. We want to show that $k(x) \cap k[x, y] = k[x]$. It is clear that $k[x] \subseteq k(x) \cap k[x, y]$. Consider an element $\xi \in k(x) \cap k[x, y]$. Since $\xi \in k(x)$, we may write $\xi = fg^{-1}$ for $f, g \in k[x]$ and $g \neq 0$. Thus $g \in k[x, y]$. So g must belong to $\mathbb{C}$. Hence $k(x) \cap k[x, y] = k[x]$. ((v) $\Rightarrow$ (iii)): If $F \in k[x]$, then F is algebraic over $k[x] \subset k(x)$. ■

Remark The result of proposition 4.3 remains valid if one replaces all 'x' by 'y' in the statement. In particular, if y is algebraic over K then $F \in k[y]$.

Corollary 4.4 At least one of x, y is transcendental over K.

Proof. Let $F \in A \backslash k$. Then if $F \notin k(x)$, then x is transcendental over K by proposition 4.3. Similarly, if $F \notin k(y)$, then y is transcendental over K. ■

Proposition 4.5 For some $t \in \{x, y\}$, $L/K(t)$ is a finite extension and therefore L/K is a function field of one variable. Furthermore, $F \in k[x]$.

Proof. Suppose that both $L/K(x)$ and $L/K(y)$ are not finite. Then we get the following chain of inclusions $k(x) \subseteq K(x) \subset L$ and $k(y) \subseteq K(y) \subset L$. Observe that both $L/k(x)$ and $L/k(y)$ are function fields in one variable. So the fact that both $L/K(x)$ and $l/K(y)$ are not finite implies that $K(x)/k(x)$ and $K(y)/k(y)$ are both algebraic. In particular, F is algebraic over $k(x)$ and $k(y)$. Hence by proposition 4.3 $F \in k[x]$ and $F \in k[y]$, which is impossible. So for some $t \in \{x, y\}$, $L/K(t)$ is a finite extension. ■

Remark So, for any choice of $F \in A \setminus k$, L/K is a function field of one variable (it is important that $F \notin k$ here; if $F \in k$, then $k(F) = k$ and the field extension L/k has transcendental degree 2). The properties of the function field L/K depend on the choice of F: whether or not K is algebraically closed in L depends on the choice of F; whether or not L/K is the rational function field depends on the choice of F.

Example 4.6 Let $k = \mathbb{C}$. Then for each of the following values of F, the function field L/K is the rational function field.

1. $F = xy^2$
2. $F = x^2y^3$
3. $F = x(y + x^3)$
4. $F = y^2 + x^2 - 1$

To prove this, it suffices to find $G \in L$ such that $L = K(G)$.

1. $K(y) = \mathbb{C}(xy^2, y) = \mathbb{C}(xy^2y^{-2}, y) = \mathbb{C}(x, y) = L$
2. $K(xy) = \mathbb{C}(x^2y^3, xy) = \mathbb{C}(x^2y^3x^{-2}y^{-2}, xy) = \mathbb{C}(y, xy) = \mathbb{C}(x, y) = L$
3. $K(x) = \mathbb{C}(x(y + x^3), x) = \mathbb{C}(y + x^3, x) = \mathbb{C}(y + x^3 - x^3, x) = \mathbb{C}(x, y) = L$
4. Let $u = x + iy$ and $v = x - iy$ of $L = \mathbb{C}(x, y)$. Notice that $uv = x^2 + y^2 = F + 1$. So $K = \mathbb{C}(x^2 + y^2 - 1) = \mathbb{C}(x^2 + y^2) = \mathbb{C}(uv)$ and consequently $K(v) = \mathbb{C}(uv, v) = \mathbb{C}(u, v) = L$.

Notation 4.7 Let $F \in A \setminus k$.

(a) Let $\mathbb{V}(F)$ be the set of all valuation rings of the function field L/K. The notation '$\mathbb{V}(F)$' reminds us that this set of rings depends on the choice of F.

(b) Let $\mathbb{P}(F)$ be the set of places of L/K.

(c) Let $\mathbb{V}^\infty(F) = \{ R \in \mathbb{V}(F) \mid A \nsubseteq R \}$.

Note that $\mathbb{V}^\infty(F) = \{ R \in \mathbb{V}(F) \mid \{x, y\} \nsubseteq R \}$.

Proposition 4.8 Let $F \in A \setminus k$.

(a) $\mathbb{V}^\infty(F)$ is a nonempty set.

(b) $\mathbb{V}^\infty(F)$ is a finite set.

Proof. (a): By 4.4, we know that at least one of x, y is transcendental over K. Assume x is transcendental over K, then by corollary 1.24, x has at least one pole. That is, there exists a place P such that $v_P(x) < 0$. Let $\mathcal{O}_P$ be the valuation ring of L corresponding to P. Hence $V^\infty(F) \neq \varnothing$. (b): ∎

Definition 4.9 Let $F \in A \setminus k$. The elements of the nonempty finite set $\mathbb{V}^\infty(F)$ are called the *dicriticals* of F. We define the *degree* of a dicritical R of F to be $\deg P$, where P is the place of R.

Example 4.10 Let $F = x$. In this case, we have $K = k(x)$; so $L = K(y)$ is the rational function field. The place at infinity of $K(y)$ is $R = K[z]_{(z)}$ where $z = y^{-1}$; since $y \notin R$, we have $R \in \mathbb{V}^{\infty}(F)$. The degree of this dicritical is 1, because we know that the place at infinity of $K(y)$ has degree 1. If R' is any valuation ring of L/K other than R then $R' = K[y]_{(p)}$ for some irreducible polynomial $p \in K[y]$; then $x \in K \subseteq K[y]_{(p)}$ and $y \in K[y]_{(p)}$, so $\{x, y\} \subseteq R'$ and $R' \notin \mathbb{V}^{\infty}(F)$. Hence $\mathbb{V}^{\infty}(x) = \{K[z]_{(z)}\}$. Since $\deg K[z]_{(z)} = 1$. We say that F has only 1 rational dicritical.

Example 4.11 The polynomial $F = xy$ has two dicriticals, $k[z_1]_{(z_1)}$ and $K[z_2]_{(z_2)}$, where $z_1 = x^{-1}$ and $z_2 = y^{-1}$.

Definition 4.12 Use square brackets to represent unordered lists of positive integers. For instance, $[1, 1, 2] = [1, 2, 1] = [2, 1, 1] \neq [1, 2, 2]$. Let $F \in A \setminus k$. Let $R_1, \dots, R_s$ be the distinct dicriticals of F, where R_i is a dicritical of degree d_i. Then we write $\Delta(F) = [d_1, \dots, d_s]$.

Examples 4.13 From 4.10, $\Delta(x) = \Delta(y) = [1]$. By 4.11, $\Delta(xy) = [1, 1]$.

5 Field Generators

Definition 5.1 An integral domain is said to be *normal* if it is integrally closed in its field of fractions.

Proposition 5.2 Every UFD is normal.

Proof. Let A be a UFD and let F be the field of fractions of A. Let $z \in F$, writen $z = a/b$ such that $0 \neq b, a \in A$ and a, b share no commmon primes in their factorizations. If z is integral over A. Then $z^n + a_{n-1}z^{n-1} + ... + a_1 z + a_0 = 0$ for some $a_0, a_1, ..., a_{n-1} \in A$. That is, $(a/b)^n + a_{n-1}(a/b)^{n-1} + ... + a_1(a/b) + a_0 = 0$. We may clear denominators to obtain $a^n + a_{n-1}a^{n-1}b + ... + a_1 ab^{n-1} + a_0 b^n = 0$. Then $a^n = -b(a_{n-1}a^{n-1} + ... + a_1 ab^{n-2} + a_0 b^{n-1})$. This means b divides a. If b is not a unit, then this imples that any prime elements in the factorization of b appear in the factorization of a^n, and thus also in a. This is a contradiction to the supposition that a, b share no common primes in their factorization. So b must be a unit. Thus $z \in A$. ∎

Example 5.3 The ring $A = \mathbb{C}[x, y]/(y - x^2)$ is normal: Let $\varphi : \mathbb{C}[x, y] \longrightarrow \mathbb{C}[t]$ be given by $f(x, y) \mapsto f(t, t^2)$. Then φ is an onto homomorphism with kernel $(y - x^2)$. Thus $\mathbb{C}[x, y]/(y - x^2) \cong \mathbb{C}[t]$, which is a UFD.

Example 5.4 The converse is not true in general. If we let $A = \mathbb{C}[x, y, z]/(xy - z^2)$. Then A is normal but not a UFD. To prove this, let $\varphi : \mathbb{C}[z, y, z] \longrightarrow \mathbb{C}[s, t]$ given as $f(x, y, z) \mapsto f(s^2, t^2, st)$. Then φ is homomorphism an onto the ring $B = \mathbb{C}[s^2, t^2, st]$ with kernel $(xy - z^2)$. Hence $A \cong B$. We prove that B is normal by showing that the integral closure of $\mathbb{C}[s,t]$ in $\mathbb{C}(s,t,\sqrt{st})$ is $\mathbb{C}[s,t,\sqrt{st}]$. Let $u+v\sqrt{st} \in \mathbb{C}(s,t,\sqrt{st})$ be integral over $\mathbb{C}[s,t]$ for some $u,v \in \mathbb{C}(s,t)$. Then since the integral closure of a integral domain is an integral domain, $u - v\sqrt{st}$ is in the integral closure of $\mathbb{C}[s,t]$ in $\mathbb{C}(s,t,\sqrt{st})$ as well. Thus their sum, $2u$ belongs to this closure. Since $\mathbb{C}[s,t]$ is normal, $u \in \mathbb{C}[s,t]$. Similarily, $v\sqrt{st} \in \mathbb{C}[s,t]$. Hence $v^2st \in \mathbb{C}[s,t], v \in \mathbb{C}(s,t)$. Clearly, then v can have no denominator, thus $v \in \mathbb{C}[s,t]$. Hence $u + v\sqrt{st} \in \mathbb{C}[s,t]$. To see that A is not a UFD, notice that $z^2 = xy$.

Remark Recall that if R is an integral domain and $S \subseteq R \setminus \{0\}$ is a multiplicative set then $S^{-1}R$ is an integral domain and $R \subseteq S^{-1}R \subseteq \mathrm{Frac}(R)$, so R and $S^{-1}R$ have the same field of fractions.

Lemma 5.5 Let R be an integral domain and $S \subseteq R \setminus \{0\}$ a multiplicative set. If R is normal then so is $S^{-1}R$.

Proof. Let R be an integral domain (not necessarily normal), $S \subseteq R \setminus \{0\}$ a multiplicative set, $K = \mathrm{Frac}\, R$, and consider $R \subseteq \tilde{R} \subseteq K$ where $\tilde{R}$ is the integral closure of R in K. Then Prop. 5.12 of Atiyah-McDonald implies that $S^{-1}\tilde{R}$ is the integral closure of $S^{-1}R$ in $S^{-1}K = K$. If we now assume that R is normal then $\tilde{R} = R$, so $S^{-1}R$ is the integral closure of $S^{-1}R$ in K, i.e., $S^{-1}R$ is normal. ■

Proposition 5.6 Let F/K be a rational function field of one variable, let P be a place of F/K of degree 1, and let $\mathcal{O}_P$ be the corresponding valuation ring of F/K. Then there exists $t \in F$ satisfying $F = K(t)$ and $\mathcal{O}_P = k[t^{-1}]_{(t^{-1})}$. Moreover, for any such t, $K[t]$ is the intersection of all valuation rings that belong to the set $\mathbb{V}(F/K) \setminus \{\mathcal{O}_P\}$.

Proof. Omitted ■

let k be a field, $A = k[x,y]$ the polynomial ring in two variables over k, $L = \mathrm{Frac}\, A = k(x,y)$ the field of rational functions in two variables, and $K = k(F)$. Let $\mathbb{V}(F)$ be the set of all valuation rings of the function field L/K. Let $\mathbb{V}^\infty(F) = \left\{ R \in \mathbb{V}(F) \mid A \nsubseteq R \right\}$ be the set of dicriticals of F.

Definition 5.7 Let $A = k[x,y]$ be a polynomial ring in two variables over a field k. A *field generator* of $A = k[x,y]$ is an element $F \in A$ that satisfies: $k(x,y) = k(F,G)$ for some $G \in k(x,y)$. If $F \in A$ satisfies the stronger condition $k(x,y) = k(F,G)$ for some $G \in k[x,y]$ we call F a *good* field generator of A. A field generator that is not good is said to be bad.

Remark Given any $F \in k[x,y] \setminus k$, we know that $k(x,y)/k(F)$ is a function field of one variable. Observe that F is a field generator of $k[x,y]$ if and only if $k(x,y)/k(F)$ is the rational function field.

Proposition 5.8 Suppose that F is a field generator of $A = k[x, y]$ such that 1 occurs in the list $\Delta(F)$, then F is a good field generator.

Proof by Daniel Daigle: Let $F \in A$ be a field generator of A such that '1' occurs in $\Delta(F)$. Write $L = k(x, y)$ and $K = k(F)$, then L/K is the rational function field of one variable. Let $\mathbb{V}(F)$ be the set of all valuation rings of the function field L/K. Let

$$\mathbb{V}^{\infty}(F) = \left\{ R \in \mathbb{V}(F) \mid A \nsubseteq R \right\} = \{R_1, \dots, R_s\}$$

be the set of dicriticals of F. Since '1' occurs in $\Delta(F)$, one of $R_1, \dots, R_s$ is a dicritical of degree 1; relabelling $R_1, \dots, R_s$ if necessary, we may arrange that R_1 is a dicritical of degree 1. Let P be the maximal ideal of R_1; then

P is a place of degree 1 of the rational function field L/K.

Moreover, R_1 is the valuation ring of P, i.e., $R_1 = \mathcal{O}_P$. By 5.6, there exists $t \in L$ satisfying $L = K(t)$, $\mathcal{O}_P = k[t^{-1}]_{(t^{-1})}$, and

$$K[t] = \bigcap_{\mathcal{O} \in E} \mathcal{O} \tag{5.8.1}$$

where $E = \mathbb{V}(F) \setminus \{\mathcal{O}_P\}$.
Consider the ring $\mathcal{A} = S^{-1}A$ where $S = k[F] \setminus \{0\} \subset A \setminus \{0\}$. Then

$$A \text{ is a UFD} \overset{5.2}{\Longrightarrow} A \text{ is a normal} \overset{5.5}{\Longrightarrow} \mathcal{A} \text{ is a normal.}$$

Since $\mathrm{Frac}(\mathcal{A}) = L$, it follows that $\mathcal{A}$ is integrally closed in L. Thus, by Cor. 5.22 of Atiyah-McDonald, $\mathcal{A}$ is equal to the intersection of all valuation rings $\mathcal{O}$ of L that satisfy $\mathcal{A} \subseteq \mathcal{O}$.

$$\mathcal{A} = \bigcap_{\mathcal{O} \in E'} \mathcal{O} \tag{5.8.2}$$

where E' = set of all valuation rings $\mathcal{O}$ of L that satisfy $\mathcal{A} \subseteq \mathcal{O}$. Note that $L \in E'$; let us prove that

$$E' \subseteq E \cup \{L\}. \tag{5.8.3}$$

Indeed, consider $\mathcal{O} \in E'$ such that $\mathcal{O} \neq L$, and let us prove that $\mathcal{O} \in E$. Since $\mathcal{O}$ is a valuation ring of L such that $\mathcal{O} \neq L$ and

$$k(F) = S^{-1}k[F] \subseteq S^{-1}A = \mathcal{A} \subseteq \mathcal{O},$$

it follows that $\mathcal{O}$ is a valuation ring of L/K, i.e., $\mathcal{O} \in \mathbb{V}(F)$. Since $A \subseteq \mathcal{A} \subseteq \mathcal{O}$, we have $\mathcal{O} \notin \{R_1, \dots, R_s\}$, so $\mathcal{O} \in \mathbb{V}(F) \setminus \{R_1\} = E$. This proves (5.8.3).
It follows that

$$\text{for each } \mathcal{O} \in E', \quad K[t] \subseteq \mathcal{O}. \tag{5.8.4}$$

Indeed, if $\mathcal{O} \in E'$ then (5.8.3) implies that $\mathcal{O} \in E$ or $\mathcal{O} = L$; in the first case we have $K[t] \subseteq \mathcal{O}$ by (5.8.1), and in the second case we have $K[t] \subseteq L = \mathcal{O}$. So (5.8.4) is true. It follows from (5.8.4) that

$$K[t] \subseteq \bigcap_{\mathcal{O} \in E'} \mathcal{O} \ = \ \mathcal{A},$$

so in particular $t \in \mathcal{A} = S^{-1}A$; then $t = G/s$ for some $G \in A$ and $s \in S = k[F] \setminus \{0\}$. Since $s \in K^*$, we have $K[t] = K[st] = K[G]$, so

$$k(F,G) = K(G) = K(t) = L,$$

showing that F is a good field generator of A. ■

6 Exercises

Exercise 6.1 Consider the poylnomial ring $\mathbb{C}[x,y]$. Let $p = y^2 + x^3 - x \in \mathbb{C}[x,y]$ and $\pi : \mathbb{C}[x,y] \longrightarrow A = \mathbb{C}[x,y]/(p)$ by defined by $\pi(f) = f + (p)$ for all $f \in \mathbb{C}[x,y]$. Let F be the field of fractions of A and $\mathfrak{m} \subset A$ be image of the prime ideal (x,y) under π. Show

(a) p is irreducible in $\mathbb{C}[x,y]$

(b) A is a free $\mathbb{C}[x]$-module, with basis $\{1, y\}$.

(c) $F/\mathbb{C}$ is a function field in one variable.

(d) $A_{\mathfrak{m}}$ is a valution ring of the function field $F/\mathbb{C}$.

Solution (a): Suppose $p = gh$ for $g, h \in \mathbb{C}[x,y] \backslash \{0\}$. We may view p as a polynomial in one variable y over $\mathbb{C}[x]$. Hence $deg_y(p) = deg_y(gh) = deg(g) + deg(h)$. Since $deg_y(p) = 2$, there are three cases for the y-degrees of g and h:

(i) $\deg_y(g) = 1$ and $\deg_y(h) = 1$

(ii) $\deg_y(g) = 2$ and $\deg_y(h) = 0$

(iii) $\deg_y(h) = 2$ and $\deg_y(g) = 0$

Suppose $deg_y(g) = deg_y(h) = 1$. Write $g = a_1 y + a_2$ and $h = b_1 y + b_2$ where $a_1, a_2, b_1, b_2 \in \mathbb{C}[x]$. Then $p = gh = (a_1 y + a_2)(b_1 y + b_2) = a_1 b_1 y^2 + (a_1 b_2 + a_2 b_1)y + a_2 b_2$. Thus we have the equations;

$$\begin{aligned} &a_1 b_1 = 1 \\ &a_1 b_2 + a_2 b_1 = 0 \\ &a_2 b_2 = x^3 - x \end{aligned}$$

$a_1b_1 = 1 \Longrightarrow a_1 = b_1^{-1}$. Then $a_1b_2 + a_2b_1 = 0$ becomes $b_2 = -b_1^2a_2$. Then in $a_2b_2 = x^3 - x$ we have $a_2b_2 = -a_2^2b_1^2 = -(a_2b_1)^2 = x^3 - x$ which is impossible since $x^3 - x = x(x-1)(x+1)$ is not a square. So either f or g is a unit. If $\deg_y(g) = 2$ and $\deg_y(h) = 0$, then we may write $g = a_1y^2 + a_2y + a_3$ and $h = b$ for some $a_1, a_2, a_3, b \in \mathbb{C}[x]$. Then

$$y^2 + x^3 - x = g = a_1by^2 + a_2by + a_3b$$

This would mean that $a_1b = 1$. Hence $b \in \mathbb{C}[x]^*$. So b must be a unit of $\mathbb{C}[x, y]$ as well. For the last case (where $\deg_y(h) = 2$ and $\deg_y(g) = 0$), the same argument will show that $g \in \mathbb{C}[x, y]^*$. Thus p is irreducibe in $\mathbb{C}[x, y]$.

(b): Suppose $a + by = 0$ for nonzero $a, b \in \mathbb{C}[x]$. Recall the "re-definition" $x = \pi(x)$ and $y = \pi(y)$. To avoid confusion, let X, Y be used to represent variables in $\mathbb{C}[X, Y]$ and x, y be used to represent variables in A. Then $a+bY \in \ker(\pi) = (p)$ - but this is impossible since $\deg_Y(p) = 2 \geq deg_Y(a + bY) = 1$. This means that $\{1, y\}$ is an independent set in A. Clearly $\text{span}\{1, y\} \subseteq A$. Let $f \in A$. Then

$$f = a_0 + a_1x + a_2y + a_3xy + a_4x^2 + a_5y^2 + a_6x^2y + a_7xy^2 + a_8x^2y^2 + ... + a_nx^ny^m$$

for some $a_0, a_1, ..., a_n \in \mathbb{C}$ where $y^2 + x^3 - x = 0$. In each term of f divisible by y^2, substitute y^2 with $x - x^3$. Then

$$f = ...+a_3xy+a_4x^2+a_5(x-x^3)+a_6x^2y+a_7x(x-x^3)+a_8x^2(x-x^3)+...+a_nx^n(x-x^3)^ky^l$$

where $k = m/2, l = 0$ if m is even and $k = (m-1)/2, l = 1$ if m is odd. Factoring out the y in some of terms, we may rearrange f as;

$$f = a_0+a_1x+a_4x^2+a_5(x-x^3)+a_7x(x-x^3)+...+(a_2+a_3x+a_6x^2+...+a_nx^n(x-x^3)^k)y$$

Hence $f \in \text{span}_{\mathbb{C}[x]}\{1, y\}$. So A is a free $\mathbb{C}[x]$-module, with basis $\{1, y\}$.

(c): Since $\mathbb{C} \cap (p) = \{0\}$, the composition of the cannonical projection map of the quotient ring A with the inclusion homomorphism $f \mapsto f/1$ of A to F embeds $\mathbb{C}$ in F. So we may view $\mathbb{C}$ as a subfield of F. To show that $F/\mathbb{C}$ is a transcendental extension of fields, condsider $y \in F$. Suppose y is algebraic over $\mathbb{C}$, then $a_0 + a_1y + ... + a_ny^n \in (p)$ for some $a_0, ..., a_n \in \mathbb{C}$. That would mean that $a_0 + a_1y + ... + a_ny^n = g(x, y)(p) = g(x, y)(y^2 + x - x)$ for some nonzero $g(x, y) \in \mathbb{C}[x, y]$. But $\deg_x(a_0 + a_1y + ... + a_ny^n) = 0$ and $\deg_x(y^2 + x^3 - x) = 3$. So there does not exists such a g. Hence y is transcendental over $\mathbb{C}$. We want to show that $F/\mathbb{C}(x)$ is finite. Let $0 \neq z \in F$. Write $z = f/g$ for $f, g \in A$ with $g \neq 0$. By (b), we may write $f = a + by$ for $a, b \in \mathbb{C}[x]$. Since $0 \neq z$, we may assume $a \neq 0$ or $b \neq 0$. *Claim*: If $m(T) \in \mathbb{C}(x)[T]\backslash\{0\}$ is some polynomial satisfying $m(f) = 0$. Then we may find another nonzero polynomail $m'(T)$, that depends on g, such that $m(z) = 0$.

Proof of claim: Assume there exists a nonzero polynomial $m(T) \in \mathbb{C}(x)[T]$ such that $m(f) = 0$. Write $m(T) = a_0 + a_1T + ... + a_nT^n$ for $a_1, ..., a_n \in \mathbb{C}(x)$. Consider the terms in the polynomial g. Write $g(x, y) = \sum_{i,j\in\mathbb{N}} b_{ij}x^iy^j$. If each term of g is either in $\mathbb{C}(x)$ or divisible by y^2, then we may multiply $m(T)$ by $h(x) = (\sum_{i,j\in\mathbb{N}} b_{ij}x^i(x - x^3)^j)^n$ Then all the denominators of $m(z)$ will be cleared by $h(x)$, which belongs to $\mathbb{C}(x)$. So if we define $m'(T) = h(x)m(T)$, then $m'(z) = 0$. Alternatively, suppose any of the terms of g are of the form uy^n for $u \in \mathbb{C}(x)$ and n odd. We may assume that only one of the terms of g is of this form and that $n = 1$: If more of the terms are of this form then repeat the following process again. The case $n > 1$, follows by induction. So we may write $g = a + by$ for some $a, b \in \mathbb{C}(x)$. let $h(x) = (a^2 - b^2(x - x^3)^2)^n$ and let $m'(T) = h(x)m(T)$. Thus

$$
\begin{aligned}
m'(z) &= (a^2 - b^2(x - x^3)^2)^n(a_0 + a_1(\frac{f}{a + by}) + ... + a_n(\frac{f}{a + by})^n) \\
&= (a + by)^n(a - by)^n(a_0 + a_1(\frac{f}{a + by}) + ... + a_n(\frac{f^n}{(a + by)^n})) \\
&= (a + by)^n(a - by)^n a_0 + a_1(a + by)^{n-1}(a - by)^n f + ... + a_n f^n(a - by)^n \\
&= 0
\end{aligned}
$$

So it suffices to find a nonzero polynomial $m(T) \in \mathbb{C}(x)[T]$ such that $m(f) = 0$. Let $m(T) = (T-a)^2-b^2(x-x^3)$. Then clearly $m(a+by) = (a+by-a)^2-b^2y^2 = 0$. Since $a \neq 0$ or $b \neq 0$, it follows that $m(T)$ is nonzero. Hence $F/\mathbb{C}(x)$ is finite. Thus $F/\mathbb{C}$ is a function field

(d): By definition, $A_\mathfrak{m} = \{f/g \mid f, g \in A, g \neq 0 \text{ and } g \notin \mathfrak{m}\}$. So $\mathbb{C} \subsetneqq A_\mathfrak{m} \subsetneqq F$ is clear. Let $z \in F$. Write $z = f/g$ for $f, g \in A$ and $g \neq 0$. Suppose $f, g \in \mathfrak{m}$.

Then we may write $f = ax + by, g = cx + dy$ for $a, b, c, d \in \mathbb{C}[x, y]$. Thus

$$\begin{aligned}
z &= f/g \\
&= \frac{ax + by}{cx + dy} \\
&= \frac{(ax + by)(cx - dy)}{(cx + dy)(cx - dy)} \\
&= \frac{acx^2 + (cb - ad)xy - bdy^2}{c^2x^2 - d^2y^2} \\
&= \frac{acx^2 + (cb - ad)xy - bd(x - x^3)}{c^2x^2 - d^2(x - x^3)} \\
&= \frac{acx + (cb - ad)y - bd(1 - x^2)}{c^2x - d^2(1 - x^2)} \\
&= \frac{acx + (cb - ad)y - bd + bdx^2}{c^2x - d^2 + d^2x^2}
\end{aligned}$$

Notice, if $b \neq 0, d \neq 0$, then both the numerator and denominator do not belong to $\mathfrak{m}$ since $\mathfrak{m} \cap \mathbb{C} = \{0\}$. So $z \in A^*_{\mathfrak{m}}$. If $d = 0$ then $z = a/c$. If both $a, c \in \mathfrak{m}$, then we may repeat the same process again. If both $b = 0$ and $d \neq 0$. Then only $z \in A^*_{\mathfrak{m}}$. Thus $A_{\mathfrak{m}}$ is a valuation ring of F.

Exercise 6.2 Let $A \xrightarrow{\varphi} B$ be a surjective homomorphism of rings. Let $\mathfrak{p}$ be a prime ideal in R containing the kernel of φ. Then $\varphi(\mathfrak{p})$ is prime in S.

Solution Let $x, y \in B$ and suppose $xy \in \varphi(\mathfrak{p})$. Since φ is surjectivity, there exists $a, b \in A$ such that $\varphi(a) = x$, $\varphi(b) = y$. Choose $c \in \mathfrak{p}$ such that $\varphi(c) = xy$. Then $ab - c \in ker(\varphi)$, so $ab \in \mathfrak{p}$. Thus, either a or b is in $\mathfrak{p}$, which means either x or y is in $\varphi(\mathfrak{p})$.

Exercise 6.3 (Stichtenoth, Exercise 1.1) Consider the rational function field $K(x)/K$ and a non-constant element $z = f(x)/g(x) \in K(x)\backslash K$, where $f(x), g(x) \in K[x]$ are relatively prime. We call $deg(z) = max\{deg(f), deg(g)\}$ the degree of z.

(i) Show that $[K(x) : K(z)] = deg(z)$, and write down the minimal polynomial of x over $K(z)$

(ii) Show that $K(x) = K(z)$ if and only if $z = (ax+b)/(cx+d)$ with $a, b, c, d \in K$ and $ad - bc \neq 0$.

Solution We find the minimal polynomial of the field extension $K(x)/K(z)$.

(i) Consider the polynomial $m(t) = zg(t) - f(t) \in K(z)[t]$. Notice that $0 \neq z = f(x)/g(x) \implies f(x) \neq 0 \implies m(t) \neq 0$ and that $m(x) = 0$. Also, if $deg(g(x)) \geq deg(f(x))$, then $deg(m(t)) = deg(g(t)) = deg(g(x))$. Otherwise $deg(m(t)) = deg(f(t)) = deg(f(x))$. So $deg(m(t)) = deg(z)$, as required. Lastly we need to show that $m(t)$ is irreducible over $K(z)$. By Gauss's lemma, it is sufficient to check that $m(t)$ is irreducible over $K[z]$ but $K[z][t] = K[t][z]$, in which $m(t)$ is linear. Hence m is the minimal polynomial of the field extension $K(x)/K(z)$ and $[K(x) : K(z)] = deg(m(t)) = deg(z)$ as required.

(ii) Assume $z = (ax + b)/(cx + d)$ with $a, b, c, d \in K$ and $ad - cd \neq 0$. The condition $ad - bc \neq 0$ implies that $z \notin K$. By part i), $[K(x) : K(z)] = deg(z) = 1$, Hence $K(x) = K(z)$. Assume $K(x) = K(z)$ and suppose $z \neq (ax + b)/(cx + d)$ for any $a, b, c, d \in K$ satisfying $ad - bc \neq 0$. Then either $z \in K$ or $deg(z) \geq 2$. If $z \in K$, then $K(z) = K$, which would imply $K(x) = K$, a contradiction to the fact that x is transcendental over K. If $deg(z) \geq 2$, then by part i), $[K(x) : K(z)] \geq 2$. This contradicts the fact that every field is a one dimensional vector space over itself. So our supposition must be false, thus $z = (ax + b)/(cx + d)$ with $a, b, c, d \in K$ and $ad - bc \neq 0$.

Exercise 6.4 (Stichtenoth, Exercise 1.2) For a field extension L/M we denote by $Aut(K(x)/K)$ the group of automorphisms of L/M (i.e., automorphisms of L which are the identity on M). Let $K(x)/K$ be the rational function field over K. Show:

(i) For every $\sigma \in Aut(K(x)/K)$ there exists $a, b, c, d \in K$ such that $ad - bc \neq 0$ and $\sigma(x) = (ax + b)/(cx + d)$.

(ii) Given $a, b, c, d \in K$ with $ad - bc \neq 0$, there is a unique automorphism $\sigma \in Aut(K(x)/K)$ with $\sigma(x) = (ax + b)/(cx + d)$.

(iii) Denote by $GL_2(K)$ the group of invertible 2×2 - matrices over K. For $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in GL_2(K)$ denote by σ_A the automophism of $K(x)/K$ with $\sigma_A(x) = (ax + b)/(cx + d)$. Show that the map that sends A to σ_A, is a homomorphism of $GL_2(K)$ onto $Aut(K(x)/K)$. Its kernel is the set of diagonal matrices of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ with $a \in K^\times$, hence

$$Aut(K(x)/K) \cong GL_2(K)/K^\times$$

(The group $GL_2(K)/K^\times$ is called the projective linear group and is denoted by $PGL_2(K)$.)

Solution Any given tuple $(a, b, c, d) \in K^4$ will satisfy $ad - bc = 0$ unless otherwise specified.

(i) Let $\sigma \in Aut(K(x)/K)$. We show that $K(x) = K(\sigma(x))$. Let $f \in K(\sigma(x))$, then

$$f(\sigma(x)) = \frac{a_n\sigma(x)^n + a_{n-1}\sigma(x)^{n-1} + ... + a_0}{b_m\sigma(x)^m + b_{m-1}\sigma(x)^{m-1} + ... + b_0}$$

for $a_0, ..., a_n, b_0, ..., b_m \in K$. Since $\sigma(a) = a$ for all $a \in K$ and σ is a homomorphism, we may rewrite f as

$$\sigma(\frac{a_n x^n + a_{n-1}x^n + ... + a_0}{b_m x^m + b_{m-1}x^{m-1} + ... + b_0}) \in im(\sigma)$$

Since σ is surjective, $f \in im(\sigma) = K(x)$.

Let $f \in K(x)$, then $f \in im(\sigma)$ by surjectivity of σ. Hence there exists some $g \in K(x)$ such that $\sigma(g(x)) = f(x)$. Write

$$g(x) = \frac{a_n x^n + a_{n-1}x^n + ... + a_0}{b_m x^m + b_{m-1}x^{m-1} + ... + b_0}$$

then

$$f(x) = \sigma(\frac{a_n x^n + a_{n-1}x^n + ... + a_0}{b_m x^m + b_{m-1}x^{m-1} + ... + b_0}) = \frac{a_n \sigma(x)^n + a_{n-1}\sigma(x)^{n-1} + ... + a_0}{b_m \sigma(x)^m + b_{m-1}\sigma(x)^{m-1} + ... + b_0}$$

Hence $f \in K(\sigma(x))$. That is, $K(x) = K(\sigma(x))$ as required. By part (ii) of exercise 1, $\sigma(x) = (ax + b)/(cx + d)$.

(ii) Let $a, b, c, d \in K$, define $\sigma : K(x) \longrightarrow K(x)$ by $\sigma(f(x)/g(x))$

(iii) Let $\Phi : GL_2(K) \longrightarrow Aut(K(x)/K)$ be defined as $\Phi(A) = \sigma_A$ for all $A \in GL_2(K)$.

Remark To verify that two automorphisms $\sigma_2, \sigma_1 \in Aut(K(x)/K)$ are equivalent, it suffices so show that $\sigma_1(x) = \sigma_2(x)$. This is because every automorphism of $Aut(K(x)/K)$ is uniquely determined by x.

First, Φ preserves identity: $\Phi(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})(x) = (1x + 0)/(0x + 1) = x = i(x)$ where i is the indentiy automorphism of $Aut(K(x)/K)$. Let $A, B \in GL_2(K)$. Then $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}, B = \begin{pmatrix} e & g \\ f & h \end{pmatrix}$ for $a, b, c, d, e, f, g, h \in K$.

Then

$$
\begin{aligned}
\Phi(\begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} e & g \\ f & h \end{pmatrix})(x) &= \Phi(\begin{pmatrix} ae+cf & ag+ch \\ be+df & bg+dh \end{pmatrix})(x) \\
&= \frac{(ae+cf)x+be+df}{(ag+ch)x+bg+dh}(x) \\
&= \frac{e(ax+b)+(cx+d)f}{g(ax+b)+(cx+d)h} \\
&= \frac{[e(ax+b)+(cx+d)f](cx+d)}{[g(ax+b)+(cx+d)h](cx+d)} \\
&= \frac{\frac{e(ax+b)+(cx+d)f}{(cx+d)}}{\frac{g(ax+b)+(cx+d)h}{(cx+d)}} \\
&= \frac{\frac{e(ax+b)}{(cx+d)}+f}{\frac{g(ax+b)}{(cx+d)}+h} \\
&= \frac{e\sigma_A(x)+f}{g\sigma_A(x)+h} \\
&= \sigma_A(\frac{ex+f}{gx+h})(x) \\
&= \sigma_A \circ \sigma_B(x) \\
&= \Phi(\begin{pmatrix} a & c \\ b & d \end{pmatrix})\Phi(\begin{pmatrix} e & g \\ f & h \end{pmatrix})(x)
\end{aligned}
$$

Hence Φ is a group homomorphism. Clearly $\Phi(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix})(x) = \frac{ax+0}{0x+a} = x = i(x)$. So $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in ker(\Phi)$. Let $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in ker(\Phi)$, then $\frac{ax+b}{cx+d} = x \Rightarrow 0 = cx^2 + (d-a)x - b \Rightarrow a = d, b = c = 0$. Notice that $a = d = 0$ implies $ad - bc = 0$, which is not allowed here. Hence $ker(\Phi) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ where $a \in K^\times$. Let $\sigma \in Aut(K(x)/K)$, then by part (i), there exists $a, b, c, d \in K$ such that $\sigma(x) = \frac{ax+b}{cx+d}$, that is there exists $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in GL_2(K)$ such that $\Phi(A) = \sigma$. Hence Φ is surjective and $Aut(K(x)/K) \cong GL_2(K)/\mathfrak{K}$, where $\mathfrak{K} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ for $a \in K^\times$.

Exercise 6.5 (Stichtenoth, Exercise 1.4) Let $K(x)$ be the rational function field over K. Find bases for the following Riemann-Roch spaces:

(i) $\mathscr{L}(rP_\infty)$

(ii) $\mathscr{L}(rP_\alpha)$

(iii) $\mathscr{L}(P_{p(x)})$

where $R \geq 0$, and the places P_∞, P_α and $P_{p(x)}$ are as in section 1.2 of Stichtenoth.

Solution (i): Let $r \geq 0$. $\mathscr{L}(rP_\infty)$: Write $z \in K(x)^*$ as $z = f/g$ where f, g are relatively prime in $K[x]$. Then $z \in \mathscr{L}(rP_\infty)$ if and only if $v_P(z) + v_P(rP_\infty) \geq 0$ for all $P \in \mathbb{P}_{K(x)}$ if and only if $v_P(z) + 0 \geq 0$ for all $P \in \mathbb{P}_{K(x)} \backslash \{P_\infty\}$ and $v_\infty(z) + r \geq 0$ if and only if $z \in K[x]$ and $r \geq \deg(f)$. Hence $\mathscr{L}(rP_\infty)$ is the vector space of all polynomial in $K[x]$ with degree less than or equal to r. Transcedance of x over K implies $1, x, x^2, ..., x^r$ are linearly independent over K and clearly they span $\mathscr{L}(rP_\infty)$. Hence $\ell(rP_\infty) = r + 1$.
(ii): Since P_a corresponds to the linear polynomial $p = x - a$, so $\deg P = 1$. By proposition 5.6, there exists $t \in K(x)$ such that $\mathcal{O}_{P_a} = K[t^{-1}]_{(t^{-1})}$. Then from the solution to (i), $\{1, t, t^2, ..., t^r\}$ is a K-basis for $\mathscr{L}(rP_\alpha)$ with dimension $r+1$.
(iii): Let $n = \deg p(x)$. Then since $p(x)$ is irriducible over K, all other places of the form $P_{q(x)}$ for some irreducible polynomial $q(x) \in K[x]$ will have valuation 0. Thus by theorem 3.17, $v_\infty(p) = -n$. Hence if $z \in \mathscr{L}(P_{p(x)})$, then $v_\infty(z) \geq -n$. Similarly, $v_P(z) \geq 0$ for all $P \in \mathbb{P}_F \backslash \{P_{p(x)}, P_\infty\}$. So $z \in K[x]$. This implies that z is a polynomial in $K[x]$ with degree less than or equal to n. Then clearly $\mathscr{L}(P_{p(x)})$ has K-basis $\{1, x, ..., x^n\}$, which implies $\ell(P_{p(x)}) = n + 1$.

Exercise 6.6 (Stichtenoth, Exercise 1.5)
(*Representation of rational funcitons by partial fractions*)

(i) Show that every $z \in K(x)$ can be written as

$$z = \sum_{i=1}^{r} \sum_{j=1}^{k_i} \frac{c_{ij}(x)}{p_i(x)^j} + h(x)$$

where

(a) $p_1(x), ..., p_r(x)$ are distinc monic irreducible polynomials in $K[x]$,

(b) $k_1, ..., k_r \geq 1$,

(c) $c_{ij}(x) \in K[x]$ and $deg(c_{ij}(x)) < deg(p_i(x))$,

(d) $c_{ik_i}(x) \neq 0$ for $1 \leq i \leq r$,

(e) $h(x) \in K[x]$

(ii) Show that the above representation of z is unique.

Solution (i) Let $z = f(x)/g(x) \in K(x)$. If $\deg(f) \geq \deg(g)$, then we may write $f = q(x)g(x) + r(x)$ with $q(x), r(x) \in K[x]$ and $\deg(r(x)) < \deg(g(x))$. Then $f(x)/g(x) = q(x) + r(x)/g(x)$ and we may use the following argument for $r(x)$ instead of $f(x)$. Hence it suffices to consider the case where $\deg(g(x)) > \deg(f(x))$. Write $g(x) = p_1(x)^{e_1} p_2(x)^{e_2} ... p_s(x)^{e_s}$

where $e_1, e_2, ..., e_s \in \mathbb{Z}^+$ and $p_1, p_2, ..., p_s$ are distinct prime factors of $g(x)$. Suppose $deg(f) < deg(g)$. Then

$$\gcd(p_1(x)^{e_1}, p_2(x)^{e_2}...p_s(x)^{e_s}) = 1$$

hence there exists $h_1(x), h_2(x) \in K[x]$ such that

$$1 = h_1(x)p_1(x)^{e_1} + h_2(x)p_2(x)^{e_2}...p_s(x)^{e_s}$$

Thus

$$f(x) = f(x)h_1(x)p_1(x)^{e_1} + f(x)h_2(x)p_2(x)^{e_2}...p_s(x)^{e_s}$$

We may divide and write $h_1(x)f(x) = p_1(x)^{e_1}q(x)+r_1(x)$ for some $q(x), r_1(x) \in K[x]$ with $deg(r(x)) < deg(q(x))$. Let

$$r_2(x) = h_2(x)p_1(x)^{e_1}p_2(x)^{e_2}...p_s(x)^{e_s} + q(x)p_2(x)^{e_2}...p_s(x)^{e_s}$$

$$\begin{aligned}
f(x) &= p_1(x)^{e_1}r_2(x) - p_1(x)^{e_1}p_2(x)^{e_2}...p_s(x)^{e_s}q(x) \\
&\quad + p_1(x)^{e_1}p_2(x)^{e_2}...p_s(x)^{e_s}f(x) + p_2(x)^{e_2}...p_s(x)^{e_s}r_1(x) \\
&= p_1(x)^{e_1}r_2(x) + p_2(x)^{e_2}...p_s(x)^{e_s}r_1(x)
\end{aligned}$$

Hence $\frac{f(x)}{g(x)} = \frac{r_1(x)}{p_1(x)^{e_1}} + \frac{r_2(x)}{p_2(x)^{e_2}...p_s(x)^{e_s}}$. Claim: $deg(r_2(x)) < deg(p_2(x)^{e_2}...p_s(x)^{e_s})$: Suppose the opposite, then $deg(p_1(x)^{e_1}r_2(x)) \geq deg(p_1(x)^{e_1}p_2(x)^{e_2}...p_s(x)^{e_s})$ but we also have

$$deg(p_1(x)^{e_1}p_2(x)^{e_2}...p_s(x)^{e_s}) > deg(deg(p_1(x)^{e_1}p_2(x)^{e_2}...p_s(x)^{e_s}r_1(x))$$

Then

$$\begin{aligned}
deg(f(x)) &= deg(p_1(x)^{e_1}r_2(x) + p_2(x)^{e_2}...p_s(x)^{e_s}r_1(x)) \\
&= deg(p_1(x)^{e_1}p_2(x)^{e_2}...p_s(x)^{e_s}r_2(x)) \\
&\geq deg(p_1(x)^{e_1}p_2(x)^{e_2}...p_s(x)^{e_s}) \\
&= deg(p_1(x)^{e_1}) + deg(p_2(x)^{e_2}...p_s(x)^{e_s}) \\
&< deg(f(x))
\end{aligned}$$

This is a contradiction, so the claim is verified.

Hence we may repeat this processess $s-1$ times to obtain the expression

$$\frac{f(x)}{g(x)} = \sum_{i=1}^{s} \frac{r_i(x)}{p_i(x)^{e_i}}$$

We now need to expand the powers of $p_i(x)$ for $i = 1, ..., s$. For $i = 1, ..., s$, let $r_{i0}(x) = p_i(x)$ and for $j = 1, ..., e_s$ we can use the division algorithm to find $q_{ij}(x), r_{ij}(x) \in K[x]$ such that

$$q_{i(j-1)}(x) = q_ij(x)p_i(x) + r_{ij}(x)$$

where $\deg(r_{ij}(x)) < \deg(q_{ij}(x))$. Using back substitution, we find

$$\begin{aligned}
r_i(x)_i(x) &= q_{i0}(x) \\
&= q_{i1}(x)p_i(x) + r_{i1}(x) \\
&= (q_{i2}(x)p_i(x) + r_{i2}(x))p_i(x) + r_{i1}(x) \\
&= ... \\
&= q_{ie_s}(x)p_i(x)^{e_s} + r_{ie_s}(x)p_i(x)^{e_s-1} \\
&+ r_{i(e_s-1)}(x)p_i(x)^{e_s-2} + ... + r_{i2}(x)p_i(x) + r_{i1}(x) \\
\implies \frac{r_i(x)}{p_i(x)^{e_s}} &= q_{ie_s}(x) + \frac{r_{ie_s}(x)}{p_i(x)} + \frac{r_{i(e_s-1)}(x)}{p_i(x)^2} + ... + \frac{r_{i2}(x)}{p_i(x)^{e_s-1}} + \frac{r_{i1}(x)}{p_i(x)^{e_s}}
\end{aligned}$$

Hence

$$\frac{f(x)}{g(x)} = \sum_{i=1}^{s}(q_{ie_s}(x) + \sum_{j=1}^{i} \frac{r_{ij}(x)}{p_i(x)^j})$$

Let $h(x) = \sum_{i=1}^{s} q_{ie_s}(x)$, $c_{ij}(x) = r_{if(x)}$, $e = k$ and $r = s$. Then

$$z = \sum_{i=1}^{r}\sum_{j=1}^{k_i} \frac{c_{ij}(x)}{p_i(x)^j} + h(x)$$

as required.

Exercise 6.7 (Stichtenoth, Exercise 1.7) A valuation ring of field L is a subring $\mathcal{O} \subsetneq L$ such that for all $z \in L$ one has $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

(i) Show that every valuation ring is a local ring (i.e., it has a unique maximal ideal)

(ii) Now we consider the field $L = \mathbb{Q}$. Show that for every prime number $p \in \mathbb{Z}$, the set $\mathbb{Z}_{(p)} := \{a/b \in \mathbb{Q} \mid a, b \in \mathbb{Z}, b \notin (p)\}$ is a valuation ring of $\mathbb{Q}$. What is the maximal ideal of $\mathbb{Z}_{(p)}$?

(iii) Let $\mathcal{O}$ be a valuation ring of $\mathbb{Q}$. Show that $\mathcal{O} = \mathbb{Z}_{(p)}$ for some prime number p.

Solution We use the definition of a "valuation ring" as given above.

(i) Let $\mathcal{O}$ be a valuation ring of a field L. We claim that $\mathfrak{m} = \mathcal{O} \backslash \mathcal{O}^*$ is the only maximal ideal of $\mathcal{O}$. Let $x \in \mathfrak{m}$ and $y \in \mathcal{O}$. Notice $xy \in \mathcal{O}^* \implies x \in \mathcal{O}^*$, which is impossible since $x \in \mathfrak{m} = \mathcal{O} \backslash \mathcal{O}^*$. Hence $xy \in \mathfrak{m}$. Let both $x, y \in \mathfrak{m}$. Since $\mathcal{O}$ is a valuation ring, either $xy^{-1} \in \mathcal{O}$ or $x^{-1}y \in \mathcal{O}$. Assume $xy^{-1} \in \mathcal{O}$, then $1 + xy^{-1} \in \mathcal{O}$. Hence $y + x = y(1 + xy^{-1}) \in \mathfrak{m}$, since $y \in \mathfrak{m}$. So $\mathfrak{m}$ is an ideal of $\mathcal{O}$. Suppose I is another ideal of $\mathcal{O}$ with $\mathfrak{m} \subsetneq I \subset \mathcal{O}$. Then I must contain a unit of $\mathcal{O}$, which would imply $I = \mathcal{O}$. lastly any other maximal ideal M of $\mathcal{O}$ would be properly contained in $\mathfrak{m}$. So $\mathfrak{m}$ the only maximal ideal of the local ring $\mathcal{O}$.

(ii) Let p be a prime number and $z = a/b \in$ with $gcd(a, b) = 1$. If $p \nmid b$, then $z \in \mathbb{Z}_{(p)}$. If $p \mid b$ but $p \nmid a$, then $z^{-1} = b/a \in \mathbb{Z}_{(p)}$. If $p \mid a$ and $p \mid b$, then $gcd(a, b) \neq 1$, which contradicts our assumption that $gcd(a, b) = 1$. Hence $\mathbb{Z}_{(p)}$ is a valutation ring of . We claim that the maximal ideal of $\mathbb{Z}_{(p)}$ is $(p)\mathbb{Z}_{(p)} := \{a/b \in \mid a, b \in \mathbb{Z}, b \notin (p), a \in (p)\}$. We want to show that $(p)\mathbb{Z}_{(p)} = \mathbb{Z}_{(p)} \backslash \mathbb{Z}^*_{(p)}$. Let $z = a/b \in \mathcal{O}^*$ such that $gcd(a, b) = 1$, then $z^{-1} = b/a \in \mathcal{O}$. That is $p \nmid a$ and $p \nmid b$.

(iii) Let P be the maximal ideal of $\mathcal{O}$, by theorem 1.19 there exists $t \in P$ such that $(t) = P$. Write $t = p/q$ for $p, q \in \mathbb{Z} \backslash \{0\}$. Suppose $q \neq 1$. Then $(t) \subsetneqq (p) \subsetneqq \mathbb{Q}$. Which would contradict the minimality of P. Hence we may assume that $t = p$. Suppose p is not prime, then there exists $n, m \in \mathbb{Z}$ with $n, m > 1$ such that $p = nm$. But then $(p) \subsetneqq (n) \subsetneqq \mathbb{Q}$, again a contradiction. Thus p must be prime.