Exercises and Examples from

The Arithmetic of Elliptic Curves by Silverman

Jack Westbrook

July 31, 2025

Contents

Preface

This document contains worked examples, detailed solutions to selected exercises, and justifications of omitted claims from Joseph Silverman's *The Arithmetic of Elliptic Curves* (2nd ed.). The goal is both to deepen my own understanding and to provide a useful reference for others studying the text.

Chapter I: Algebraic Varieties

Exercises

Chapter II: Algebraic Curves

Section 1

Proposition 1.4

Statement. *Let C/K be a curve, and let $t \in K(C)$ be a uniformizer at some nonsingular point $P \in C(K)$. Then $K(C)$ is a finite separable extension of $K(t)$.*

Here, I just want to prove that t is transcendental over K, so that the claim in the proof given in the book that $K(C)/K(t)$ is finite is immediate from the fact that $\operatorname{trdeg}_K(K(C)) = 1, t \notin K$, and $K(C)$ is finitely generated over K.

Proof. If instead $t \in \bar{K}$, then $\dim_{\bar{K}} M_P/M_P^2 = \dim_{\bar{K}} t\bar{K}[C]_P/t^2\bar{K}[C]_P = \dim_{\bar{K}} \bar{K}[C]_P/\bar{K}[C]_P = 0$, which contradicts that C is smooth at P. because M_P/M_P^2 should be dimension 1. ∎

Section 2

Example 2.9

Statement. Consider the map $\phi : \mathbb{P}^1 \to \mathbb{P}^1, \quad [X, Y] \mapsto [X^3(X-Y)^2, Y^5]$. We will verify all of the claims made in the example, filling in proofs of claims.

Proof. First, let's show that ϕ is a morphism. We see immediately that, letting $f_0 = X^3(X-Y)^2$ and $f_1 = Y^5$, $f_0/f_1 \in \bar{K}(\mathbb{P}^1) = \bar{K}(X,Y)_0$ (the subscript refers to the degree 0 part of $K(X,Y)$), so the the rational map from $\mathbb{P}^1 \to \mathbb{P}^1$ is actually $[X, Y] \mapsto [f_0/f_1, 1]$. But as $f_1 \in \bar{K}(\mathbb{P}^1)$ and multiplying each coordinate function through by f_1 makes the rational map defined at every point since f_0 and f_1 are polynomials in the coordinate functions, the rational map is actually just identically ϕ.

First, we will compute $e_\phi(P) = \operatorname{ord}_P(\phi^* t_{\phi P})$ where $P = [0, 1]$. Letting $\infty = [1, 0]$ be the point at infinity, we will translate to $\mathbb{A}^1$ with coordinate ring $\bar{K}[x]$ where here $x = X$ and $Y = 1$. This is allowed because ramification index is a local property, which is seen because the quantity only depends on the uniformizer at the point P, which is a local definition. In this coordinate system, we have $\phi(x) = x^3(x-1)^2$. Now $\phi P = [0, 1] = 0$, so we have $t_{\phi P} = x$. Then $\phi^* t_{\phi P} = x^3(x-1)^2$. As $(x-1) \notin M_0$ and is regular at 0,

$$e_\phi(P) = \operatorname{ord}_P(\phi^* t_{\phi P}) = \operatorname{ord}_0(x^3(x-1)^2) = 3\operatorname{ord}_0(x) + 2\operatorname{ord}_0(x-1) = 3.$$

Next we let $P = [1, 1]$. We use the same affine coordinates, so $P = 1$ here, and $t_{\phi P} = x$ again. Then

$$e_\phi(P) = \operatorname{ord}_P(\phi^* t_{\phi P}) = \operatorname{ord}_1(x^3(x-1)^2) = 3\operatorname{ord}_1(x) + 2\operatorname{ord}_1(x-1) = 2$$

because $x \notin M_1$ and is regular at 1. Now, all that remains to show

$$\sum_{P \in \phi^{-1}([0,1])} e_\phi(P) = \deg \phi$$

is to show $\phi^{-1}([0, 1]) = \{[0, 1], [1, 1]\}$ and that $\deg \phi = 5$. We have already seen that $\supset$ holds, so now suppose $\phi([X, Y]) = [0, 1]$. Then $X^3(X-Y)^2 = 0$, so either $X = 0$ or $X = Y$. $X = 0$ yields $[0, 1]$ and $X = Y$ yields $[1, 1]$. Lastly, we must show $\deg \phi \coloneqq [K(\mathbb{P}^1) : \phi^* K(\mathbb{P}^1)] = 5$. Let's explicitly prove that $K(X,Y)_0 = K(t)$ without using the fact that $K(t) = K(\mathbb{A}^1) = K(\mathbb{A}^1 \cap \mathbb{P}^1) = K(X,Y)_0$

as stated in I.2.9. It's easy to see that for any $n \in \mathbb{Z}$, $\lambda t^n \in K(X,Y)_0$. By linearity, we can see that $\deg(\sum \alpha_i t^i) = 0$, so clearly quotients of polynomials of that form also have degree 0. Thus $K(t) \subset K(X,Y)_0$. For the reverse inclusion, fix polynomials $F(X,Y), G(X,Y)$, both of degree d. Notice that $X = tY$, so $\frac{F(X,Y)}{G(X,Y)} = \frac{F(tY,Y)}{G(tY,Y)} = \frac{Y^d F(t,1)}{Y^d G(t,1)} = \frac{F(t,1)}{G(t,1)} \in K(t)$ where we can see that $F(tY,Y) = Y^d F(t,1)$ because each term of $F(tY,Y)$ is of the form $\lambda(tY)^a Y^b = \lambda t^a Y^a Y^b = \lambda Y^d t^a$ with $0 \leqslant a, b$ and $a + b = d$.

Since $K(\mathbb{P}^1) = K(X,Y)_0 = K(t)$, $\phi^* K(\mathbb{P}^1) = K(\phi^* t) = K(t^3(t-1)^2)$. Notice that t is a root of the degree five polynomial $T^3(T-1)^2 - t^3(t-1)^2 \in \phi^* K(\mathbb{P}^1)[T]$.

Let's show this polynomial is irreducible (hence the minimal polynomial of t over $\phi^*(K(\mathbb{P}^1))$. Let $s = t^3(t-1)^2$, so s is transcendental over K, and let $k = \phi^* K(\mathbb{P}^1) = K(s)$. Our goal is to show that the polynomial $f(T) = T^3(T-1)^2 - s = T^5 - 2T^4 + T^3 - s \in k[T]$ is irreducible. Because $\deg f = 5$, if f has a nontrivial factorization over k, then either f has a linear factor or $f = gh$ where $\deg g = 3$ and $\deg h = 2$ for $g, h \in k[T]$. First let's show that f has no linear factor, i.e. f has no roots in k. Suppose $\frac{p(s)}{q(s)}$ was such a root with $\gcd(p,q) = 1$. Then $s = \frac{p^3(p-q)^2}{q^5}$. However, $(p-q)^2 \equiv p^2 \mod q$, and as p is invertible modulo q, the same is true for $(p-q)^2$ modulo q, so $\gcd((p-q)^2, q) = 1$ as well. Then s cannot divide q, because if $s \mid q$, we would get that $s \nmid p^3(p-q)^2$ because s is irreducible and $p^3(p-q)^2$ shares no common factors with q. But then $sq^5 = p^3(p-q)^2$ is clearly impossible, since the right hand side has no factors of s. From $sq^5 = p^3(p-q)^2$, we then see that the right hand side contains exactly one factor of s. This is impossible though, as each irreducible factor of the right hand side appears with multiplicity at least 2.

Now we will show that we cannot write $f = gh$ where $\deg g = 3$ and $\deg h = 2$, which will prove that f is irreducible over k. Suppose we can write

$$T^5 - 2T^4 + T^3 - s = f = \left(T^3 + aT^2 + bT + c\right)\left(T^2 + \alpha T + \beta\right)$$

for some $a, b, c, \alpha, \beta \in k$. Then, expanding the RHS and equating the coefficients of the powers of T, we get the following system of equations in k:

$$-2 - \alpha = a \tag{1}$$

$$b = 1 - a\alpha - \beta \tag{2}$$

$$c = -(a\beta + b\alpha) \tag{3}$$

$$c\alpha + b\beta = 0 \tag{4}$$

$$c\beta = -s. \tag{5}$$

We will eliminate the variables a, b, c with this system of equations. By plugging (1) into (2), we obtain the following:

$$b = 1 + 2\alpha + \alpha^2 - \beta. \tag{2'}$$

Plugging (1) and (2') into (3), we get

$$c = 2\beta + 2\alpha\beta - \alpha - 2\alpha^2 - \alpha^3. \tag{3'}$$

Plugging (1), (2'), and (3') into (4), we get

$$0 = -\alpha^4 - 2\alpha^3 - \alpha^2 + 3\alpha^2\beta + 4\alpha\beta + \beta - \beta^2. \tag{4'}$$

Plugging (3') into (5) we get

$$2\beta^2 + 2\alpha\beta^2 - \alpha\beta - 2\alpha^2\beta - \alpha^3 = -s. \tag{5'}$$

Now we will do case division on $\operatorname{char} K$. First, we will assume that $\operatorname{char} K = 2$. If $\alpha = 0$, then $a = 0$ from (1), $b = 1 + \beta$ from (2), $c = 0$ from (3), but then $-s = c\beta = 0$, a contradiction. Now we

assume $\alpha \neq 0$. We have that $a = \alpha$ from (1), $b = 1 + \alpha^2 + \beta$ from (2'), and $c = \alpha(1 + \alpha^2)$ from (3'), and $\alpha\beta + \alpha^3 + s = 0$ from (5'). Then $\beta = \alpha^2 + \frac{s}{\alpha}$. In addition,

$$\beta^2 + (\alpha^2 + 1)\beta + \alpha^4 + \alpha^2 = 0$$

from (4'). Plugging $\beta = \alpha^2 + \frac{s}{\alpha}$ in, we get

$$\alpha^4 + s\alpha + \frac{s}{\alpha} + \frac{s^2}{\alpha^2} = \alpha^4 + \frac{s^2}{\alpha^2} + \alpha^4 + s\alpha + \alpha^2 + \frac{s}{\alpha} + \alpha^4 + \alpha^2 = (\alpha^2 + \frac{s}{\alpha})^2 + (\alpha^2 + 1)(\alpha^2 + \frac{s}{\alpha}) + \alpha^4 + \alpha^2 = 0.$$

Multiplying through by α^2, we have

$$\alpha^6 + s\alpha^3 + s\alpha + s^2 = 0$$

Write $\alpha = \frac{x(s)}{y(s)}$ with $x, y \in K[s]$ and $\gcd(x, y) = 1$. Substituting and multiplying through by y^6, we get the equation

$$x^6 + sx^3y^3 + sxy^5 + s^2y^6 = 0.$$

Then $s \mid x^6$ implies that $s \mid x$, so write $x = sz$ for some $z \in K[s]$. Substituting in again, we get

$$s^6z^6 + s^4z^3y^3 + s^2zy^5 + s^2y^6 = 0.$$

Dividing by s^2, we get

$$s^4z^6 + s^2z^3y^3 + zy^5 + y^6 = 0.$$

Thus $z \mid y^6$, but as x and y are coprime, it follows that z and y are also coprime, hence z and y^6 are coprime, but we just contradicted this statement. This shows that $f(T)$ is irreducible if $\operatorname{char} K = 2$.

Now suppose $\operatorname{char} K \neq 2$. Notice that (4') and (5') are quadratic in β, the first saying that β is a root of

$$f_1(T) = T^2 - (1 + 4\alpha + 3\alpha^2)T + (\alpha^2 + 2\alpha^3 + \alpha^4)$$

and (5') saying β is a root of

$$f_2(T) = 2(1 + \alpha)T^2 - \alpha(1 + 2\alpha)T + (s - \alpha^3).$$

Then we see that, letting $D_1 = (1 + 4\alpha + 3\alpha^2)^2 - 4\alpha^2(1 + 2\alpha + \alpha^2) = (\alpha + 1)^2\left(5\alpha^2 + 6\alpha + 1\right)$ be the discriminant of f_1 and $D_2 = \alpha^2(1 + 2\alpha)^2 - 8(1 + \alpha)(s - \alpha^3)$.

$$\frac{1 + 4a + 3\alpha^2 + \sqrt{D_1}}{2} = \beta = \frac{\alpha(1 + 2\alpha) + \sqrt{D_2}}{4(1 + \alpha)}$$

assuming that $\alpha \neq -1$, and for some choices of square roots of D_1 and D_2. If $\alpha = -1$, then $a = -1$ from (1) as well, so $b = -\beta$ from (2), and then $c = \beta + b = 0$ from (3), but then $b\beta = 0$ from (4) which means that $b = 0$ since $\beta \neq 0$. But then by $b = -\beta$ we get $\beta = 0$ anyway, which is impossible. Thus we may proceed.

Note that $\sqrt{D_1}, \sqrt{D_2}$ are both in k since α and β are. Now because $D_2 = Q(\alpha) - 8(1 + \alpha)s$ where $Q(\alpha) = \alpha^2(1 + 2\alpha)^2 + 8\alpha^3(1 + \alpha)$, we get

$$s = \frac{Q(\alpha) - D_2}{8(1 + \alpha)}.$$

Therefore $K(\alpha) = k = K(s)$, so D_1 is a square in $K(\alpha)$. However, because $D_1 = (\alpha+1)^2(5\alpha^2+6\alpha+1)$, to arrive at a contradiction it suffices to show that $5\alpha^2 + 6\alpha + 1$ is not a square in $K(\alpha)$. Suppose it were, and write $5\alpha^2 + 6\alpha + 1 = (\frac{p(\alpha)}{q(\alpha)})^2$ with $\gcd(p, q) = 1$. Notice that $(\alpha + 1)$ divides $5\alpha^2 + 6\alpha + 1$, and let l be the extra factor ($l = 1$ if $\operatorname{char} K = 5$, $l = \alpha + \frac{1}{5}$ otherwise), and notice $l \neq \alpha + 1$ thanks to our assumption that $\operatorname{char} K \neq 2$. Then $(\alpha + 1)q^2l = p^2$, so $\alpha + 1 \mid p^2$ implies $\alpha + 1 \mid p$. But then $(\alpha + 1)^2 \mid (\alpha + 1)q^2l$ implies that $\alpha + 1 \mid q^2$ because $\alpha + 1 \nmid l$, which implies that $\alpha + 1 \mid q$. But then $\alpha + 1 \mid \gcd(p, q)$, contrary to assumption that these two have no common factor in $K[\alpha]$.

Now we have showed that $f(T)$ is irreducible over $k = K(\mathbb{P}^1)$, so so indeed $\deg \phi = [K(t) : k] = \deg f = 5$ as claimed.

■

Section 3

Example 3.3

Statement. Assume that $\operatorname{char} K \neq 2$. Let $e_1, e_2, e_3 \in \bar{K}$ be distinct, and consider the curve

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3).$$

Then C is smooth and has a single point at infinity, which we denote by P_∞. For $i = 1, 2, 3$, let $P_i = (e_i, 0) \in C$. Then

$$\operatorname{div}(x - e_i) = 2(P_i) - 2(P_\infty),$$
$$\operatorname{div}(y) = (P_1) + (P_2) + (P_3) - 3(P_\infty).$$

Proof. First let's show that C has a single point at infinity. The projective closure of the given affine curve is given by the equation $Y^2Z = (X - e_1Z)(X - e_2Z)(X - e_3Z)$. If $P = [X, Y, Z]$ is a point at infinity, i.e. $Z = 0$, then the coordinates satisfy the equation $X^3 = 0$ so $X = 0$ as well. Thus the only point at infinity is $[0, 1, 0]$. Now let's check that C is smooth. Since smoothness is local, we will first show that $C \cap \mathbb{A}^2$ is smooth. Recall that $P \in C$ is singular iff each partial derivative of the defining equation of C vanishes at P. Assume we have a point $P = (p_1, p_2) \in C$ where

$$2y(P) = \frac{\partial(y^2 - \prod_{i=1}^3 (x - e_i))}{\partial y}(P) = 0 = \frac{\partial(y^2 - \prod_{i=1}^3 (x - e_i))}{\partial x}(P) = \sum_{i=1}^3 \prod_{j \neq i} (x - e_j)(P).$$

We see $0 = 2y(P) = 2p_2$ implies $p_2 = 0$ since $\operatorname{char} \bar{K} \neq 2$. Since $P \in C$, we get that

$$0 = p_2^2 = (p_1 - e_1)(p_1 - e_2)(p_1 - e_3)$$

so $p_1 = e_l$ for some $l = 1, 2, 3$. But then

$$0 = \sum_{i=1}^3 \prod_{j \neq i} (x - e_j)(P) = (x - e_j)(x - e_k)(P) = (p_1 - e_j)(p_1 - e_k)$$

where the rightmost two expressions, the j, k are the other values in $1, 2, 3$ not equal to l. But this implies that p_1 is either equal to e_j or e_k, which is impossible since these values are distinct from e_l. Now we just need to show C is smooth at P_∞. We will check this in another affine chart $U : Y \neq 0$. Here we use the coordinates $x' = \frac{X}{Y}$ and $z = \frac{Z}{Y}$, so

$$C \cap U : z = (x' - e_1 z)(x' - e_2 z)(x' - e_3 z)$$

and under these coordinates, $P_\infty = (0, 0) = O$. Thus we just need to show that the partial derivatives do not both vanish at the origin. We compute that

$$1 = 1 + (\sum_{i=1}^3 e_i \prod_{j \neq i} (x' - e_j z)(O) = \frac{\partial(z - (x' - e_1 z)(x' - e_2 z)(x' - e_3 z)}{\partial z}(O)$$

so indeed it's not the case that the partial derivatives vanish at O.

Now let's compute $\operatorname{div}(x - e_i)$. Notice for any $P \in \mathbb{A}^2 \cap C$, $\operatorname{ord}_P(x - e_i) \geqslant 0$ since $x - e_i$ is regular on $\mathbb{A}^2$. If $\operatorname{ord}_P(x - e_i) > 0$, i.e. $x(P) = e_i$, then $P = (e_i, p_2)$. But $P \in C$ means $p_2^2 = \prod_j (e_i - e_j) = 0$ so $p_2 = 0$, and thus $P = P_i$. Thus $\operatorname{div}(x - e_i) = n(P_i) - n(P_\infty)$ for some $n \in \mathbb{N}$, because $\deg \operatorname{div}(x - e_i) = 0$ by Proposition 3.1. Now let's compute $n = \operatorname{ord}_{P_i}(x - e_i)$. First, we claim that $M_{P_i} = (x - e_i, y)$. We observe $x - e_i, y \in M_{P_i}$, so it suffices to show $(x - e_i, y)$ is maximal in $\bar{K}[C]$. But we see that $\bar{K}[C]/(x - e_i, y) = \bar{K}[x, y]/(y^2 - \prod_j (x - e_j), x - e_i, y) = K[x, y]/(x - e_i, y) \cong \bar{K}$ so the claim holds.

Now we will work in $\bar{K}[C]_{P_i}$, where we invert all functions not in $M_{P_i} = (x - e_i, y)$. In this ring, we have $\frac{y^2}{\prod_{j\neq i}(x-e_j)} = x - e_i$. Thus $\operatorname{ord}_{P_i}(x - e_i) = 2\operatorname{ord}_{P_i}(y) \geqslant 2$ so $x - e_i \in M_{P_i}^2$. Therefore

$$M_{P_i}/M_{P_i}^2 = (x - e_i, y)/(x - e_i) = (y)/(x - e_i).$$

Then $M_{P_i}/M_{P_i}^2$ is spanned by y as a $\bar{K}$ vector space, so by Exercise 2.1, we get that $M_{P_i} = (y)$, i.e. y is a uniformizer at P_i, as long as $y \notin M_{P_i}^2$. If this were false, then $M_{P_i}/M_{P_i}^2 = 0$, contradicting that it has dimension 1 by our proof that C is smooth at P_i, so $y \notin M_{P_i}^2$. Note that $K[C]$ is not a field since $y \notin (y^2 - \prod_j(x-e_j))$, so $(y^2 - \prod_j(x-e_j)) \subsetneq (y, y^2 - \prod_j(x-e_j))$ demonstrates that $(y^2 - \prod_j(x-e_j))$ is not maximal. Since we have already shown that $\operatorname{ord}_{P_i}(x - e_i) = 2\operatorname{ord}_{P_i}(y) = 2$. The last thing to verify is that $\bar{K}[C]$ is indeed a domain, i.e. $f(x, y) = y^2 - \prod_j(x - e_j)$ is irreducible. If we could write $f = gh$ where g, h are not units, then necessarily each must have y-degree 1, i.e. we may write $g = y + p(x)$ and $h = y + q(x)$ where $p, q \in \bar{K}[x]$. Then $y^2 - \prod_j(x - e_j) = gh = y^2 + (p + q)y + pq$, which implies that

$$p + q = 0$$

and

$$pq = -\prod_j(x - e_j).$$

The first condition says $p = -q$, so plugging into the second equation, we get

$$p^2 = \prod_j(x - e_j).$$

But $x - e_1$ is an irreducible factor of p^2 means it's a factor of p, but then $(x - e_1)^2 \mid \prod_j(x - e_j)$, which is false as the e_j are distinct.

Now of course we know from the proposition that $\operatorname{div}(x - e_i) = 2(P_i) - 2(P_\infty)$, but let's explicitly compute $\operatorname{ord}_{P_\infty}(x - e_i)$. Using the coordinates x', z for $U : Y \neq 0$, the coordinate ring $\bar{K}[C] = \bar{K}[x', z]/(z - \prod_j(x' - e_j z)$. Since $x = \frac{X}{Z}, y = \frac{Y}{Z}, x' = \frac{X}{Y}$ and $z = \frac{Z}{Y}$, we have $x - e_i = \frac{X - e_i Z}{Z} = \frac{X/Y - e_i Z/Y}{Z/Y} = \frac{x' - e_i z}{z}$. In this chart, $P_\infty = (0, 0) = O$. First, notice that $(x', z) \subset M_O$ because each function is regular and vanishes at O. Also, we have $\bar{K}[C]/(x', z) = \bar{K}[x', z]/(z - \prod_j(x' - e_j z), x', z) \cong \bar{K}$ means (x', z) is maximal, and thus $M_O = (x', z)$. Therefore $x' - e_j z \in M_O$ for every $j = 1, 2, 3$. But in $K[C]$, we have $z = \prod_j(x' - e_j z)$, so $z \in M_O^3$. Therefore

$$M_O/M_O^2 = (x', z)/M_O^2 = (x')/M_O^2$$

so by the same Exercise 2.1 we get that x' is a uniformizer at P_∞ if we can show that $x' \notin M_O^2$. If this were false, then $\dim_{\bar{K}} M_O/M_O^2 = 0$, contradicting that C is smooth at P_∞, so indeed $x' \notin M_O^2$. Then $z \in M_O^3 = ((x')^3)$ means there exists some $q \in \bar{K}[C]$ such that $z = (x')^3 q$. This means that

$$x' - e_i z = x' - e_i(x')^3 q = x'(1 - e_i(x')^2 q).$$

We compute that $1 - e_i(x')^2 q \equiv 1 \mod x'$, so $1 - e_i(x')^2 q \notin M_O$, hence $\operatorname{ord}_O(1 - e_i(x')^2 q) = 0$. This implies that

$$\operatorname{ord}_O(x' - e_i z) = \operatorname{ord}_O(x') + \operatorname{ord}_O(1 - e_i(x')^2 q) = 1.$$

By the exact same proof, we obtain that $\operatorname{ord}_O(x' - e_j z) = 1$ for any j. Then

$$\operatorname{ord}_O(z) = \operatorname{ord}_O(\prod_j(x' - e_j z)) = \sum_j \operatorname{ord}_O(x' - e_j z) = 3.$$

Now we have

$$\operatorname{ord}_{P_\infty}(x - e_i) = \operatorname{ord}_O(\frac{x' - e_i z}{z}) = \operatorname{ord}_O(x' - e_i z) - \operatorname{ord}_O(z) = 1 - 3 = -2.$$

Also, we remark that we did not have to prove that this $\bar{K}[C]$ is a domain because it is isomorphic to the other $\bar{K}[C]$ used for the other affine chart, which we did prove is a domain.

Now, let's compute $\operatorname{div}(y)$. On $\mathbb{A}^2$, y is regular so for every $P \in \mathbb{A}^2$, $\operatorname{ord}_P(y) \geqslant 0$. If $\operatorname{ord}_P(y) > 0$, i.e. $y(P) = 0$, then $P = (p_1, 0)$. But since $P \in C$, we have $0 = \prod_j (p_1 - e_j)$ so $p_1 = e_i$ for some i, and thus $P = P_i$. Let's now compute $\operatorname{ord}_{P_i}(y)$. From the computation for $\operatorname{div}(x - e_i)$, we know that y is a uniformizer at each P_i. Thus $\operatorname{ord}_{P_i}(y) = 1$, so again using the fact that $\deg \operatorname{div}(y) = 0$, $\operatorname{div}(y) = (P_1) + (P_2) + (P_3) - 3(P_\infty)$. But this is no fun, so we're going to explicitly verify that $\operatorname{ord}_{P_\infty}(y) = -3$. We observe

$$\operatorname{ord}_{P_\infty}(y) = \operatorname{ord}_{P_\infty}(\frac{Y}{Z}) = \operatorname{ord}_O(\frac{1}{z}) = -\operatorname{ord}_O(z) = -3$$

by our previous computations.

Since we're already going above and beyond and since the computation for $\operatorname{div}(y)$ was so short, we will compute $\operatorname{div}(x)$ for fun. Let $\lambda \in \bar{K}$ be such that $\lambda^2 = -\prod_j e_j$. Since x is regular on $\mathbb{A}^2$, for any $P = (p_1, p_2) \in C$, $\operatorname{ord}_P(x) \geqslant 0$. Moreover, if $\operatorname{ord}_P(x) > 0$, then $p_1 = 0$, and from $p_2^2 = \prod_j (p_1 - e_j) = -\prod_j e_j$, it follows that either $P = P_+ \coloneqq (0, \lambda)$ or $P = P_- \coloneqq (0, -\lambda)$. Then $\operatorname{div}(x) = c_+(P_+) + c_-(P_-) + n(P_\infty)$. Let $P = P_+$. Then $M_P = (x, y - \lambda)$ because indeed these two generators are in M_P, and $\bar{K}[C]/(x, y-\lambda) = \bar{K}[x, y]/(y^2 - \prod_j (x - e_j), x, y - \lambda) \cong \bar{K}$. First, let's consider the case where $e_i = 0$ for some i, or equivalently $\lambda = 0$. Then $\operatorname{div}(x) = \operatorname{div}(x - e_i) = 2(P_i) - 2(P_\infty)$ as was already proven. Now we assume $\lambda \neq 0$. First, we compute

$$(y - \lambda)^2 = y^2 - 2y\lambda + \lambda^2 = \prod_j (x - e_j) - 2y\lambda + \lambda^2 = x^3 - (\sum_j e_j)x^2 + (\sum_j \prod_{i \neq j} e_i)x - 2\lambda(y - \lambda).$$

As an immediate application,

$$(y - \lambda)^2 \equiv (\sum_j \prod_{i \neq j} e_i)x - 2\lambda(y - \lambda) \mod x^2$$

Letting $\alpha = \sum_j \prod_{i \neq j} e_i$,

$$M_P/M_P^2 = (x, y - \lambda)/(x^2, x(y - \lambda), \alpha x - 2\lambda(y - \lambda)).$$

If $\alpha = 0$ then we obtain that $y - \lambda = 0$ in M_P/M_P^2, and if $\alpha \neq 0$, we have $y - \lambda = \frac{\alpha}{2\lambda} x$ in M_P/M_P^2, so regardless M_P/M_P^2 is spanned by x as a $\bar{K}$ vector space. Thus x is a uniformizer at P. As an alternative proof, we compute that

$$\bar{K}[x, y]/(y^2 - \prod (x - e_j), x) \cong \bar{K}[y]/(y^2 - \lambda^2) \cong \bar{K}$$

implies (x) is maximal in $K[C]$. Thus $M_{P_+} = (x) = M_{P_-}$ because $x \in M_{P_+} \cap M_{P_-}$. Thus $\operatorname{ord}_{P_+}(x) = 1 = \operatorname{ord}_{P_-}(x)$, so we could deduce that $\operatorname{div}(x) = (P_+) + (P_-) - 2(P_\infty)$. However, let's compute $\operatorname{ord}_{P_\infty}(x)$ explicitly. We have

$$\operatorname{ord}_{P_\infty}(x) = \operatorname{ord}_{P_\infty}(\frac{X}{Z}) = \operatorname{ord}_O(\frac{x'}{z}) = \operatorname{ord}_O(x') - \operatorname{ord}_O(z) = -2.$$

■

Example 3.5

Statement. Let C be a smooth curve, let $f \in \bar{K}(C)$ be a nonconstant function, and let $f : C \to \mathbb{P}^1$ be the corresponding map (II.2.2). Then

$$\operatorname{div}(f) = f^*((0) - (\infty))$$

Proof. By definition, we have

$$\begin{aligned} f^*((0)-(\infty)) &= \sum_{P\in f^{-1}(0)} e_f(P)(P) - \sum_{Q\in f^{-1}(\infty)} e_f(Q)(Q) \\ &= \sum_{P\in f^{-1}(0)} \operatorname{ord}_P(t_0\circ f)(P) - \sum_{Q\in f^{-1}(\infty)} \operatorname{ord}_Q(t_\infty\circ f)(Q) \\ &= \sum_{P\in f^{-1}(0)} \operatorname{ord}_P(f)(P) - \sum_{Q\in f^{-1}(\infty)} \operatorname{ord}_Q(\frac{1}{f})(Q) \end{aligned}$$

where

$$t_0\circ f = x\circ f = \begin{cases} f(P), & \text{if } \operatorname{ord}_P(f)\geqslant 0 \\ \infty, & \text{if } \operatorname{ord}_P(f)<0 \end{cases}$$

corresponds to f, and where

$$t_\infty\circ f = \frac{1}{x}\circ f = \begin{cases} \frac{1}{f(P)}, & \text{if } \operatorname{ord}_P(f)=0 \\ \infty, & \text{if } \operatorname{ord}_P(f)>0 \\ 0, & \text{if } \operatorname{ord}_P(f)<0 \end{cases}$$

which corresponds to $\frac{1}{f}$. But as $\operatorname{ord}_Q(\frac{1}{f} = -\operatorname{ord}_Q(f)$, we get

$$\begin{aligned} &\sum_{P\in f^{-1}(0)} \operatorname{ord}_P(f)(P) - \sum_{Q\in f^{-1}(\infty)} \operatorname{ord}_Q(\frac{1}{f})(Q) \\ &= \sum_{P\in f^{-1}(0)} \operatorname{ord}_P(f)(P) + \sum_{Q\in f^{-1}(\infty)} \operatorname{ord}_Q(f)(Q) = \operatorname{div}(f) \end{aligned}$$

where the last equality is because if $P\notin f^{-1}(0)\cup f^{-1}(\infty)$, then $\operatorname{ord}_P(f)=0$. ■

Proposition 3.6

Statement. *Let $\phi: C_1\to C_2$ be a nonconstant map of smooth curves. Then*

(a) $\deg(\phi^*D) = (\deg\phi)(\deg D)$ *for all* $D\in\operatorname{Div}(C_2)$.

(b) $\phi^*(\operatorname{div} f) = \operatorname{div}(\phi^* f)$ *for all* $f\in\bar{K}(C_2)^*$.

(c) $\deg(\phi_*D) = \deg D$ *for all* $D\in\operatorname{Div}(C_1)$.

(d) $\phi_*(\operatorname{div} f) = \operatorname{div}(\phi_* f)$ *for all* $f\in\bar{K}(C_1)^*$.

(e) $\phi_*\circ\phi^*$ *acts as multiplication by* $\deg\phi$ *on* $\operatorname{Div}(C_2)$.

(f) If $\psi: C_2\to C_3$ *is another such map, then*

$$(\psi\circ\phi)^* = \phi^*\circ\psi^* \text{ and } (\psi\circ\phi)_* = \psi_*\circ\phi_*.$$

We will prove all of the above except (d), which was proven in another textbook. We'll start with (a).

Proof. We know that for any $Q\in C_2$, $\sum_{P\in\phi^{-1}(Q)} e_\phi(P) = \deg\phi$ by Proposition 2.6a. Let $D = \sum_{Q\in C_2} n_Q(Q)$. We compute that

$$\begin{aligned} \deg(\phi^*D) &= \deg(\sum_{Q\in C_2} n_Q \sum_{P\in\phi^{-1}(Q)} e_\phi(P)(P)) = \sum_{Q\in C_2} n_Q \sum_{P\in\phi^{-1}(Q)} e_\phi(P) \\ &= \sum_{Q\in C_2} n_Q \deg\phi = \deg\phi\deg D. \end{aligned}$$

■

For (b), we will use Exercise 2.2.

Proof. We compute that

$$\phi^*(\operatorname{div} f) = \sum_{Q \in C_2} \operatorname{ord}_Q(f) \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P)$$

On the other hand, we have

$$\operatorname{div}(\phi^* f) = \sum_{P \in C_1} \operatorname{ord}_P(\phi^* f)(P) = \sum_{P \in C_1} e_\phi(P) \operatorname{ord}_{\phi P}(f)(P) = \sum_{Q \in C_2} \sum_{P \in \phi^{-1}(Q)} \operatorname{ord}_Q(f) e_\phi(P)(P)$$

where the second equality comes from Exercise 2.2, and clearly the two expressions are equal. ■

Now we move on to prove (c).

Proof. Let $D = \sum_{P \in C_1} n_P(P)$. Then

$$\deg(\phi_* D) = \deg(\sum_{P \in C_1} n_P(\phi P)) = \deg(\sum_{Q \in C_2} (\sum_{P \in \phi^{-1}(Q)} n_P)(Q)) = \sum_{Q \in C_2} (\sum_{P \in \phi^{-1}(Q)} n_P) = \sum_{P \in C_1} n_P$$

as claimed. ■

We do not prove (d), because the textbook references another textbook for the proof. Now for (e),

Proof. Let $D = \sum_{Q \in C_2} n_Q(Q)$. We compute that

$$\begin{aligned} \phi_* \circ \phi^*(\sum_{Q \in C_2} n_Q(Q)) &= \phi_*(\sum_{Q \in C_2} n_Q \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P)) = \sum_{Q \in C_2} n_Q \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(Q) \\ &= \sum_{Q \in C_2} n_Q \deg \phi(Q) = (\deg \phi) D, \end{aligned}$$

again using the fact that $\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi$. ■

Lastly, we prove (f):

Proof. We compute that

$$(\psi \circ \phi)^*(\sum_{Q \in C_3} n_Q(Q)) = \sum_{Q \in C_3} n_Q \sum_{P \in (\psi \circ \phi)^{-1}(Q)} e_{\psi \circ \phi}(P)(P) = \sum_{Q \in C_3} n_Q \sum_{P \in \phi^{-1}(\psi^{-1}(Q))} e_\phi(P) e_\psi(\phi P)$$

with the last equality by Proposition 2.6c. On the other hand,

$$\begin{aligned} \phi^* \circ \psi^*(\sum_{Q \in C_3} n_Q(Q)) &= \phi^*(\sum_{Q \in C_3} n_Q \sum_{R \in \psi^{-1}(Q)} e_\psi(R)(R)) = \sum_{Q \in C_3} n_Q \sum_{R \in \psi^{-1}(Q)} \sum_{P \in \phi^{-1}(R)} e_\psi(R) e_\phi(P)(P) \\ &= \sum_{Q \in C_3} n_Q \sum_{P \in \phi^{-1}(\psi^{-1}(Q))} e_\psi(\phi P) e_\phi(P)(P) \end{aligned}$$

and the two expressions are indeed equal. Now let's show that the pushforwards distribute over composition as well. This is pretty direct, as

$$(\psi \circ \phi)_*(\sum_{P \in C_1} n_P(P)) = \sum_{P \in C_1} n_P(\psi \circ \phi(P)) = \psi_*(\sum_{P \in C_1} n_P(\phi P)) = \psi_* \circ \phi_*(\sum_{P \in C_1} n_P(P)).$$

■

Section 4

Example 4.5

Statement. There are no holomorphic differentials on $\mathbb{P}^1$.

Since the full proof is given in the book, we will just expand a couple of claims made in the proof. First, we will show that $dt = -t^2 d(\frac{1}{t})$.

Proof.

$$0 = d1 = d(t \cdot \frac{1}{t}) = \frac{1}{t}dt + td(\frac{1}{t})$$

so by simple algebra we get the claim. ■

Lastly, we will prove the claim that $\deg \operatorname{div}(\omega) = \deg \operatorname{div}(dt)$.

Proof. By Proposition 4.3a, write $\omega = fdt$. Then

$$\deg \operatorname{div}(\omega) = \deg \operatorname{div}(fdt) = \deg(\operatorname{div}(f) + \operatorname{div}(dt)) = \deg \operatorname{div}(f) + \deg \operatorname{div}(dt)) = \deg \operatorname{div}(dt)$$

because $\deg \operatorname{div}(f) = 0$ by Proposition 3.1b. ■

Exercises

Exercise 2.1

Statement. Let $(R, \mathfrak{m}, k)$ be a Noetherian local domain that is not a field. Then the following are equivalent:

(i) R is a discrete valuation ring (DVR)

(ii) $\mathfrak{m}$ is principal

(iii) $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$

I take the definition of R being a DVR to mean that there exists a function $\nu : K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ where K is the quotient field of R such that $R = \mathcal{O}_K \coloneqq \{x \in K \mid \nu(x) \geqslant 0\}$, and for all $x, y \in K$, $\nu(xy) = \nu(x) + \nu(y)$, $\nu(x + y) \geqslant \min\{\nu(x), \nu(y)\}$, and $\nu(x) = \infty \iff x = 0$ where the ordering and operations and addition with the symbol ∞ are as expected.

Proof. (i) $\Rightarrow$ (ii): Let $t \in R$ be such that $\nu(t) = 1$. We claim that $\mathfrak{m} = (t)$. To prove this, we will first show that for $x \in K$, $\nu(x) = 0 \iff x \in R^*$. For one direction, suppose $x \in R^*$. First, we compute that

$$1 = \nu(t) = \nu(t \cdot 1) = \nu(t) + \nu(1) = 1 + \nu(1)$$

so $\nu(1) = 0$. Now we will quickly show that for any nonzero $y \in K$, $\nu(y^{-1}) = -\nu(y)$. To see this,

$$0 = \nu(1) = \nu(yy^{-1}) = \nu(y) + \nu(y^{-1})$$

Then as $\nu(x), \nu(x^{-1}) \geqslant 0$ and $R = \mathcal{O}_K$, it follows that $\nu(x) = 0$. For the converse, suppose $\nu(x) = 0$ (which implies $x \in R \setminus 0$ by $\mathcal{O}_K = R$ and $\nu(0) = \infty$). Then $\nu(\frac{1}{x}) = -\nu(x) = 0$, and as $R = \mathcal{O}_K$, we get that $\frac{1}{x} \in R$, i.e. $x \in R^*$.

To show $(t) \subset \mathfrak{m}$, if this were false then necessarily $t \in R^*$ because R is local. But by our result above, we would then get that $\nu(t) = 0$, contradicting our assumptions on t. For the reverse inclusion, fix $x \in \mathfrak{m}$. Then $\nu(x) \geqslant 1$ otherwise x would be a unit again by our result. Then

$$\nu(\frac{x}{t}) = \nu(x) + \nu(\frac{1}{t}) = \nu(x) - \nu(t) = \nu(x) - 1 \geqslant 0.$$

Then $\frac{x}{t} \in \mathcal{O}_K = R$, so $x \in (t)$. This shows $\mathfrak{m} = (t)$ as desired.

(ii) $\Rightarrow$ (i): Let $\mathfrak{m} = (t)$. Define for $x \in R$ $\nu(x) = \sup\{n \in \mathbb{N} \mid x \in \mathfrak{m}^n\}$. First of all, notice that if $\nu(x) = \infty$ for some $x \in R$, then $x \in \bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = 0$ by Krull's intersection theorem. Thus $\nu(x) = \infty \iff x = 0$.

We verify that for any nonzero $x, y \in R$ where $\nu(x) = a$ and $\nu(y) = b$, clearly $xy \in \mathfrak{m}^{a+b}$ so $\nu(xy) \geqslant a + b$. If $xy \in \mathfrak{m}^m$ for any $m \geqslant a + b + 1$, then also $xy \in \mathfrak{m}^{a+b+1}$, so it suffices to show that $xy \notin \mathfrak{m}^{a+b+1}$. We know that $x = t^a\alpha$ and $y = t^b\beta$ for $\alpha, \beta \notin \mathfrak{m}$, i.e. $\alpha, \beta \in R^*$ because R is local. Combining, we get $t^{a+b}\alpha\beta = xy$, hence $t^{a+b+1} \nmid xy$, otherwise we would get an inverse for t in R, contradicting that t generates the maximal ideal $\mathfrak{m}$. This shows $\nu(xy) = \nu(x) + \nu(y)$. If either x or y were 0, the result is immediate. We will now show $\nu(x+y) \geqslant \min\{\nu(x), \nu(y)\}$. The result is obvious if $x = 0 = y$, so we may assume without loss of generality that $x \neq 0$ and $\nu(x) \leqslant \nu(y)$. Then $x \equiv y \equiv 0 \mod \mathfrak{m}^n$ where $n \coloneqq \nu(x)$, so $x + y \equiv 0 \mod \mathfrak{m}^n$, showing $x + y \in \mathfrak{m}^n$ as well, implying $\nu(x + y) \geqslant n$ as desired.

Now extend ν to K by setting $\nu(\frac{x}{y}) = \nu(x) - \nu(y)$. This is well defined because for any nonzero $z \in R$, $\nu(\frac{xz}{yz}) = \nu(xz) - \nu(yz) = (\nu(x) + \nu(z)) - (\nu(y) + \nu(z)) = \nu(x) - \nu(y) = \nu(\frac{x}{y})$. One also verifies

$$\begin{aligned}\nu(\frac{x_1}{x_2} \cdot \frac{y_1}{y_2}) = \nu(\frac{x_1y_1}{x_2y_2}) = \nu(x_1y_1) - \nu(x_2y_2) = (\nu(x_1) + \nu(y_1)) - (\nu(x_2) + \nu(y_2))\\ = (\nu(x_1) - \nu(x_2)) + (\nu(y_1) - \nu(y_2)) = \nu(\frac{x_1}{x_2}) + \nu(\frac{y_1}{y_2}).\end{aligned}$$

In addition, for any $n \in \mathbb{Z}$, we have $\nu(t^n) = n$ from the fact that $\nu(1) = 0$ ($t \neq 0$ because R is not a field, so t^n is well defined in K), so ν is surjective.

Now fix any nonzero $x = \frac{x_1}{x_2}, y = \frac{y_1}{y_2} \in K$, where we may assume by possibly relabeling that $\nu(x) \leqslant \nu(y)$. Then

$$\nu(x + y) = \nu(\frac{x_1y_2 + y_1x_2}{x_2y_2}) = \nu(x_1y_2 + y_1x_2) - \nu(x_2y_2) \geqslant \min\{\nu(x_1y_2), \nu(y_1x_2)\} - \nu(x_2y_2).$$

Since $\nu(x_1y_2) \leqslant \nu(y_1x_2)$ is equivalent to $\nu(x) \leqslant \nu(y)$ by additivity of ν,

$$\nu(x + y) \geqslant \nu(x_1y_2) - \nu(x_2y_2) = \nu(\frac{x_1y_2}{x_2y_2}) = \nu(x)$$

as desired. All that remains is to show that $R = \mathcal{O}_K$. For one inclusion, it's clear that for any $x \in R$, $\nu(x) \geqslant 0$, so $R \subset \mathcal{O}_K$. For the reverse inclusion, fix $\frac{x}{y} \in \mathcal{O}_K$. Then $\nu(x) \geqslant \nu(y)$. Letting $n = \nu(y)$, we have $y = t^nu$ where $u \in R^*$, and write $x = t^nz$ for some $z \in R$. Now we see $\frac{x}{y} = \frac{t^nz}{t^nu} = \frac{z}{u} \in R$ because $\frac{1}{u} \in R$.

(ii) $\Rightarrow$ (iii): Let $\mathfrak{m} = (t)$. We claim that $\bar{t}$ is a basis for $\mathfrak{m}/\mathfrak{m}^2$ as a k-vector space. We may take an arbitrary element of $\mathfrak{m}$ to be of the form tx for some $x \in R$. Then by definition, $\bar{x} \cdot \bar{t} = \bar{x}\bar{t}$ in $\mathfrak{m}/\mathfrak{m}^2$, showing $\bar{t}$ spans. All that remains is to show that $\bar{t} \neq 0$. Suppose for a contradiction that $\bar{t} = 0$, i.e. $t \in \mathfrak{m}^2 = (t^2)$. Then there exists some $x \in R$ such that $t = xt^2$. Since R is a domain and $t \neq 0$ (otherwise $\mathfrak{m} = 0$ implies R is a field), it follows that $1 = xt$, so $t \in R^*$, contradicting that $\mathfrak{m}$ is a maximal ideal.

(iii) $\Rightarrow$ (ii): Let $\mathfrak{m}/\mathfrak{m}^2 = k\bar{t}$. Since R is a local ring, $J(R) = \mathfrak{m}$. By assumption, for any $x \in \mathfrak{m}$, there exists some $y \in R$ such that $x \equiv yt \mod \mathfrak{m}^2$, i.e. $\mathfrak{m} \subset tR + \mathfrak{m}^2$. As $t \in \mathfrak{m}$ and $\mathfrak{m}^2 \subset \mathfrak{m}$, it follows that $\mathfrak{m} = tR + \mathfrak{m}^2 = tR + J(R)\mathfrak{m}$. Applying Nakayama's Lemma, it follows that $tR = \mathfrak{m}$. ■

Exercise 2.2

Statement. Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves, let $f \in \bar{K}(C_2)^*$, and let $P \in C_1$. Then

$$\operatorname{ord}_P(\phi^* f) = e_\phi(P) \operatorname{ord}_{\phi P}(f).$$

This result was used in the proof of Proposition 3.6b.

Proof. Let t_P be a uniformizer for $\bar{K}[C_1]_P$, and define $t_{\phi P}$ similarly. Let $n = \operatorname{ord}_P(\phi^* f)$, so $\alpha t_P^n = f \circ \phi$ for some $\alpha \in \bar{K}[C_1]_P^*$. Also let $m = \operatorname{ord}_{\phi P}(f)$ and $k = e_\phi(P) = \operatorname{ord}_P(\phi^* t_{\phi P})$. Then $\beta t_P^k = t_{\phi P} \circ \phi$ and $\gamma t_{\phi P}^m = f$, with β, γ units in their respective local rings. Then we observe

$$\alpha t_P^n = f \circ \phi = (\gamma t_{\phi P}^m) \circ \phi = (\phi^* \gamma)\,(t_{\phi P} \circ \phi)^m = (\phi^* \gamma)(\beta t_P^k)^m = (\phi^* \gamma)\beta^m t_P^{km}.$$

This implies that $n = km$ (the desired result) because $\phi^* \gamma$ must be a unit in $K[C_1]_P$ as ϕ^* is a ring homomorphism and γ is a unit in the source of ϕ^*. ∎

Exercise 2.4

Statement. Let C be a smooth curve and let $D \in \operatorname{Div}(C)$. Independent of the Riemann-Roch theorem, the below results hold:

(a) $\mathcal{L}(D)$ is a $\bar{K}$ vector space.

(b) If $\deg D \geqslant 0$, then

$$\ell(D) \leqslant \deg D + 1.$$

This result is used as the proof of Proposition 5.2b. First we will prove (a), and we will write $D = \sum_{P \in C} n_P(P)$.

Proof. Fix $f, g \in \mathcal{L}(D)$ and $\lambda \bar{K}$. If we can show that $\lambda f \in \mathcal{L}(D)$ and $f + g \in \mathcal{L}(D)$ we are done. If any of f, g, λ are 0, the claims are obvious, so we may suppose they are all nonzero. We see $\lambda f \in \mathcal{L}(D) \iff \operatorname{div}(\lambda f) \geqslant -D$, which is true because $\operatorname{div}(\lambda f) = \operatorname{div}(f)$. To see, $f + g \in \mathcal{L}(D)$, we observe

$$f + g \in \mathcal{L}(D) \iff \operatorname{div}(f+g) \geqslant -D \iff \sum_{P \in C} \operatorname{ord}_P(f+g)(P) \geqslant -D \iff \forall P, \operatorname{ord}_P(f+g) \geqslant -n_P.$$

But we know that, for any $P \in C$, $\operatorname{ord}_P(f+g) \geqslant \min\{\operatorname{ord}_P(f), \operatorname{ord}_P(g)\} \geqslant -n_P$. ∎

Now for the more difficult proof, that of (b). First, I will give the easy proof which has exactly the same idea as the second, it's just that the second proves many more facts about the rings we associate to C, but is also significantly longer because it essentially proves a special case of the Cohen structure theorem.

Proof. We prove the result by induction on $\deg D$, with the base case $\deg D = 0$ proven in the second proof of the result.

Now for the inductive step, let $Q \in C$ be such that $n_Q \geqslant 1$. We define a map $\Phi : \mathcal{L}(D) \to \bar{K}[C]/M_Q$ given by $\Phi(f) = t^{n_Q} f \mod t$, where t is a uniformizer at Q. Again by the proof below, we have that $\bar{K}[C]/M_Q \cong \bar{K}$. Also, since $f \in \mathcal{L}(D)$, we have $\operatorname{ord}_Q(f) \geqslant -n_Q$, hence $\operatorname{ord}_Q(t^{n_Q} f) \geqslant 0$, so we can evaluate $t^{n_Q} f \mod t$. We can easily observe that $\Phi(f) = 0$ iff $t \mid t^{n_Q} f$ iff $\operatorname{ord}_Q(f) \geqslant 1 - n_Q$. In addition, for any $f \in \mathcal{L}(D)$, we have $\operatorname{ord}_Q(f) \geqslant 1 - n_Q$ iff $f \in \mathcal{L}(D - (Q))$, thus proving $\ker \Phi = \mathcal{L}(D - (Q))$. Thus by the rank-nullity theorem,

$$\ell(D) = \ell(D - (Q)) + \operatorname{rank} \Phi \leqslant \deg D + 1$$

by the inductive hypothesis. ∎

Proof. We will prove the result by induction on $\deg D$ with the base case being $\deg D = 0$. For the base case, first suppose $D = 0$. In this case, for nonzero $f \in \bar{K}(C)^*$,

$$f \in \mathcal{L}(D) \iff \operatorname{div}(f) \geqslant 0 \iff \forall P \in C, \operatorname{ord}_P(f) \geqslant 0.$$

But since $\deg \operatorname{div}(f) = 0$, if $\operatorname{div}(f) \neq 0$ then there exists some pole of f, implying that $f \notin \mathcal{L}(D)$. Thus $\operatorname{ord}_P(f) \geqslant 0$ for all P iff $\operatorname{div} f = 0$, which is true iff $f \in \bar{K}^*$ by Proposition 3.1a. Thus $\mathcal{L}(0) = \bar{K}$, which has dimension $1 = \deg D + 1$. Now assume that $D \neq 0$, and let $Q \in C$ be such that $n_Q \geqslant 1$. Also let $\operatorname{div} f = \sum_P m_P(P)$. Then $f \in \mathcal{L}(D)^*$ means that for every P, $m_P \geqslant -n_P$. Therefore $\sum_P m_P \geqslant \sum_P -n_P$, with equality iff $m_P = -n_P$ for every P. But we see that

$$0 = \sum_P m_P \geqslant \sum_P -n_P = -\sum_P n_P = 0$$

which implies that equality holds throughout, hence $m_P = -n_P$ for every P. Then for any $g \in \mathcal{L}(D)^*$, we observe that since $\operatorname{div}(f) = \operatorname{div}(g)$,

$$0 = \operatorname{div}(f) - \operatorname{div}(g) = \operatorname{div}(\frac{f}{g})$$

so $\frac{f}{g} \in \bar{K}^*$. This proves that $\ell(D) = \dim \mathcal{L}(D) \leqslant 1 = \deg(D) + 1$ as claimed.

Now for the inductive step, let $Q \in C$ be such that $n_Q \geqslant 1$. The inductive hypothesis tells us that $\mathcal{L}(D - (Q))$ is dimension at most $\deg D$. Thus it suffices to show that $\dim \mathcal{L}(D)/\mathcal{L}(D - (Q)) \leqslant 1$. Let t be a uniformizer for C at Q, which is transcendental over $\bar{K}$ by the expanded proof of Proposition I.1.4. First we claim that $\bar{K}[C]/(t)$ is isomorphic to $\bar{K}$. For this claim, we will prove that if R is a ring containing a subfield k, and where $t \in R$ is transcendental over k and R is integral over $k[t]$, then

(i) k is a subring of R/t.

(ii) R/t is integral over k.

We have a natural ring homomorphism $K \hookrightarrow R \twoheadrightarrow R/tR$, so we will claim this map is injective, i.e. $k \cap tR = 0$. If this intersection were nonzero, t is a unit in R. Therefore $k(t) \subset R$, and as R is integral over $k[t]$, it follows that $k(t)$ is integral over $k[t]$. Let $\sum_{i=0}^n P_i(t)X^i$ be the minimal polynomial of $\frac{1}{t}$ over $k[t]$, so $P_n(t) = 1$. Then

$$0 = \sum_{i=0}^n P_i(t)t^{n-i} \equiv P_n(0) \mod tk[t].$$

However, since $P_n(0) = 1$, we get that $tk[t] = k[t]$ which is obviously false. This shows that $k \cap tR = 0$, so indeed k is a subfield of R/t. For the second claim, fix $\bar{r} \in R/t$, and let $\sum_{i=0}^n P_i(t)X^i$ be the minimal polynomial of r over $k[t]$. Then

$$0 = \sum_{i=0}^n P_i(t)r^i \equiv \sum_{i=0}^n P_i(0)\bar{r}^i \mod t,$$

and $P_n(0) = 1$ since $P_n = 1$ means that we have found a monic polynomial over k that $\bar{r}$ satisfies, hence the result.

We apply this to our situation, with $R = \bar{K}[C]$ and $k = \bar{K}$. Then $\bar{K}[C]/(t)$ is algebraic over $\bar{K}$, and since $\bar{K}$ is algebraically closed, indeed $\bar{K}[C]/(t) \cong \bar{K}$. Now we claim that the natural inclusion $\bar{K}[t]/(t^n) \hookrightarrow R/(t^n)$ is an isomorphism of $\bar{K}$ vector spaces for every $n \geqslant 1$, where R satisfies the same conditions as it did before, except that now we assume $R/(t) = \bar{K}$ and R is a domain. We will prove this by induction on n, with the base case $n = 1$ already proven above.

Now suppose n holds, and we aim to show that the same is true for $n + 1$. By hypothesis then, the below diagram commutes in the category of $\bar{K}$ vector spaces:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \bar{K} & \xrightarrow{\cdot \bar{t}^n} & \bar{K}[t]/(t^{n+1}) & \longrightarrow & \bar{K}[t]/(t^n) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \cdot \bar{t}^n} & & \downarrow & & \downarrow{\scriptstyle \sim} & & \\ 0 & \longrightarrow & (t^n)/(t^{n+1}) & \longrightarrow & R/(t^{n+1}) & \longrightarrow & R/(t^n) & \longrightarrow & 0. \end{array}$$

Our goal will be to use the five lemma to conclude that the middle arrow is an isomorphism. Thus, we claim that the rows are exact and that the first vertical arrow is an isomorphism. Exactness of the top row is easy using the third isomorphism theorem, since t is transcendental over $\bar{K}$, so we can check

$$\bar{K}[t]/(t^n) \cong \frac{\bar{K}[t]/(t^{n+1})}{(t^n)/(t^{n+1})} = \frac{\bar{K}[t]/(t^{n+1})}{\bar{K}t^n}.$$

Exactness of the bottom row is exactly the third isomorphism theorem, so it remains to show that $\bar{K}t^n = (t^n)/(t^{n+1})$. Define $\pi : R \twoheadrightarrow \bar{K}$ as the composition $R \twoheadrightarrow R/(t) \to \bar{K}$ where $R/(t) \to \bar{K}$ is an isomorphism of rings fixing $\bar{K}$, given to us by our hypotheses on R. Notice now that π is $\bar{K}$-linear since both maps that make up π are $\bar{K}$-linear. Now we define a map

$$\phi : t^n R \to \bar{K}, \quad x \mapsto \pi(\frac{x}{t^n}).$$

We notice that for $x = t^{n+1}r \in t^{n+1}R$,

$$\phi(x) = \pi(\frac{t^{n+1}r}{t^n}) = \pi(tr) = 0.$$

Thus we get a map $\bar{\phi} : (t^n)/(t^{n+1}) \to \bar{K}$. Now we will show $\bar{\phi}$ is an isomorphism. First suppose that $\overline{t^n r} \in \ker \bar{\phi}$. Then

$$0 = \bar{\phi}(\overline{t^n r}) = \phi(t^n r) = \pi(r).$$

Because $\ker \pi = (t)$, it follows that $r \in (t)$, so $\overline{t^n r} = 0$. Now let's show that ϕ is surjective by fixing $\lambda \in \bar{K}$. Then

$$\bar{\phi}(\overline{t^n \lambda}) = \phi(t^n \lambda) = \pi(\lambda) = \lambda.$$

Moreover,

$$\bar{\phi}^{-1}(\lambda) = \overline{t^n \lambda} = \lambda \bar{t}^n$$

so $\bar{\phi}^{-1}$ is first vertical map.

Now we can apply the five lemma to obtain that the middle map is an isomorphism as well, which completes the proof of the inductive step.

Now that $\bar{K}[t]/(t^n) \hookrightarrow R/(t^n)$ is an isomorphism of $\bar{K}$ vector spaces and is a ring homomorphism, it follows that this map is an isomorphism of rings.

Because t is transcendental over $\bar{K}$, we have that the t-adic completion of $\bar{K}[t]$ is just $\bar{K}[\![t]\!]$, but by our proof and the universal property of completions, we get that the t-adic completion of R is canonically isomorphic to $\bar{K}[\![t]\!]$ as well.

Thus by letting $R = \bar{K}[C]$, we get that $\widehat{\bar{K}[C]} \cong \bar{K}[\![t]\!]$ where the completion is the t-adic completion.

We now see that since $\bar{K}[C] \subset \widehat{\bar{K}[C]}$,

$$\bar{K}(C) = \operatorname{Frac} \bar{K}[C] \subset \operatorname{Frac} \widehat{\bar{K}[C]} \cong \operatorname{Frac} \bar{K}[\![t]\!] = \bar{K}(\!(t)\!)$$

Moreover, for $f \in \bar{K}(C)$, if we write $f = \sum_{n \in \mathbb{Z}} a_i t^i$, we define $\operatorname{ord}_t(f) = \min\{n \in \mathbb{Z} \mid a_n \neq 0\}$, which is guaranteed to exist since all but finitely many of the a_n for negative n are zero, and we set $\operatorname{ord}(0) = \infty$. One easily verifies that this is a valuation on $\bar{K}(\!(t)\!)$, and makes $\bar{K}[\![t]\!]$ a DVR. Now we claim that ord_t extends ord_Q on $\bar{K}(C)$. Suppose $f = \sum_{i=n}^{\infty} a_i t^i$ is in $\bar{K}(C)$, where $a_i \neq 0$, or equivalently $\operatorname{ord}_t(f) = n$. Suppose that $n = 0$, which implies $f \in \bar{K}[\![t]\!]$ and $t \nmid f$. Now we claim that $\bar{K}(C) \cap \bar{K}[\![t]\!] = \bar{K}[C]_Q$. We will show that for a Noetherian local domain R with field of fractions K, $K \cap \widehat{R} = R$. Suppose $f = \frac{a}{b}$

with $a, b \in R$, $b \neq 0$, and $f \in \widehat{R}$. Then $fb = a$ in $\widehat{R}$, so $a \in b\widehat{R} \cap R = bR$, with the last equality holding because we can show that for any local Noetherian ring R and any ideal I of R, $I\widehat{R} \cap R = I$. Lemma 7.15 of [1] tells us that the completion functor is exact on finitely generated modules. We have the exact sequence

$$0 \to I \to R \to R/I \to 0$$

of finitely generated R-modules, hence the below sequence is also exact:

$$0 \to \widehat{I} \to \widehat{R} \to \widehat{R/I} \to 0.$$

Then

$$R \cap \widehat{I} = \ker(R \to \widehat{R} \to \widehat{R/I}) = \ker(R \to \widehat{R/I}) = \ker(R \to R/I \to \widehat{R/I}) = I$$

which follows from the fact we will prove below, that all of the completion maps above are injective. To see this, let M be a finitely generated R-module. For any $m \in M$, the image of m under the completion map were trivial iff $m \in \bigcap_{n \geqslant 1} \mathfrak{m}^n M = 0$ by Krull's intersection theorem. where $\mathfrak{m}$ is the maximal ideal of R.

Continuing, we have $a \in bR$, so $b \mid a$ in R, and thus $\frac{a}{b} \in R$ as well. This shows that $K \cap \widehat{R} \subset R$, and the reverse inclusion is obvious. This result gives that indeed $\bar{K}(C) \cap \bar{K}[\![t]\!] = \bar{K}[C]_Q$. By our result, we have $f \in \bar{K}(C) \cap \bar{K}[\![t]\!] = \bar{K}[C]_Q$, so $\operatorname{ord}_Q(f) \geqslant 0$.

Since $t \nmid f$ in $\bar{K}[\![t]\!]$, then $t \nmid f$ in $K[C]_Q$ either, hence $\operatorname{ord}_Q(f) = 0$. Now we proceed to the general case.

Notice that $\operatorname{ord}_t(t^{-n} f) = \operatorname{ord}_t(\sum_{i=0}^{\infty} a_{i+n} t^i) = 0$. By our previous work, we get $\operatorname{ord}_Q(t^{-n} f) = 0$ as well. However,

$$\operatorname{ord}_Q(t^{-n} f) = \operatorname{ord}_Q(f) - n \operatorname{ord}_Q(t) = \operatorname{ord}_Q(f) - n.$$

These two facts show that $\operatorname{ord}_Q(f) = n = \operatorname{ord}_t(f)$ as desired.

Now we know that ord_t extends ord_Q to $\bar{K}(\!(t)\!)$. With this, we define a map $\Phi : \mathcal{L}(D) \to \bar{K}$, given by

$$\Phi(\sum_{n \in \mathbb{Z}} a_n t^n) = a_{-n_Q}.$$

One easily verifies that Φ is $\bar{K}$-linear. We also observe that if $f \in \mathcal{L}(D - (Q))$, then $\operatorname{ord}_Q(f) > -n_Q$, hence $a_{-n_Q} = 0$, and thus $\Phi(f) = 0$. This shows $\mathcal{L}(D - (Q)) \subset \ker \Phi$. For the reverse inclusion, suppose $f = \sum_{n \in \mathbb{Z}} a_n t^n$ and $f \in \ker \Phi$. We know for that all $P \in C$, $\operatorname{ord}_P(f) \geqslant -n_P$ by definition of $f \in \mathcal{L}(D)$. By hypothesis that $0 = \Phi(f) = a_{-n_Q}$ and $\operatorname{ord}_Q(f) \geqslant -n_Q$, it follows that $\operatorname{ord}_Q(f) \geqslant 1 - n_Q$. Therefore $f \in \mathcal{L}(D - (Q))$, completing the proof that $\ker \Phi = \mathcal{L}(D - (Q))$. Therefore

$$\dim \mathcal{L}(D) = \operatorname{nullity} \Phi + \operatorname{rank} \Phi = \ell(D - (Q)) + \operatorname{rank} \Phi \leqslant \deg D + 1.$$

■

References

[1] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Vol. 150. Graduate Texts in Mathematics. New York: Springer-Verlag, 1995. ISBN: 978-0-387-94268-1.