Exercises and Examples from

The Arithmetic of Elliptic Curves by Silverman

Jack Westbrook

November 17, 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

Exercise 4

Statement. Let $V/\mathbb{Q}$ be the variety

$$V : 5X^2 + 6XY + 2Y^2 = 2YZ + Z^2.$$

Prove that $V(\mathbb{Q}) = \varnothing$.

Proof. First, we do a linear change of variables, $X \mapsto X - \frac{3}{5}Y$, which takes $5X^2 + 6XY + 2Y^2$ to $5X^2 + \frac{1}{5}Y^2$, so in this new coordinate system

$$V : 5X^2 + \frac{1}{5}Y^2 - 2YZ - Z^2 = 0.$$

Now we apply the change of variables $Y \mapsto 5Y$, giving

$$V : 5X^2 + 5Y^2 - 10YZ - Z^2 = 0.$$

Lastly, we do the change of variables $Z \mapsto Z - 5Y$, which takes $5Y^2 - 10YZ - Z^2$ to $30Y^2 - Z^2$, so in this coordinate system

$$V : 5X^2 + 30Y^2 = Z^2.$$

Let $H : Z = 0$ be a hyperplane in $\mathbb{P}^2$. Notice that $H \cap V(\mathbb{Q}) = \varnothing$ because if $Z = 0$, as $5X^2 + 30Y^2 = Z^2$, it would follow that $X = Y = 0$. Thus it suffices to show that $V(\mathbb{Q}) \subseteq H$. By taking any solution to have integral coordinates, our claim will follow if we can show that if a, b, c are integers such that $5a^2 + 30b^2 = c^2$, then $a = b = c = 0$. Now suppose we had such a triple (a, b, c), not all zero. We may assume that $\gcd(a, b, c) = 1$, else we could obtain a contradiction by infinite descent. Considering the equation modulo 5, we get that $5 \mid c$, so relabeling $c \to \frac{c}{5}$ and dividing by 5, we have

$$a^2 + 6b^2 = 5c^2.$$

Taking this equation modulo 3, we get

$$a^2 \equiv 2c^2 \mod 3$$

which implies that $a \equiv c \equiv 0 \mod 3$. With this, we take the equation $a^2 + 6b^2 = 5c^2$ modulo 9 and get

$$6b^2 \equiv 0 \mod 9$$

which implies that $b \equiv 0 \mod 3$ as well. This contradicts the assumption that $\gcd(a, b, c) \neq 1$, showing $V(\mathbb{Q}) \subset H$, hence $V(\mathbb{Q}) = V(\mathbb{Q}) \cap H = \varnothing$. as claimed. ∎

Exercise 10

Statement. For each prime $p \geqslant 3$, let V_p be the variety given by the equation

$$V_p : X^2 + Y^2 = pZ^2.$$

(a) Prove that V_p is isomorphic over $\mathbb{Q}$ to $\mathbb{P}^1$ iff $p \equiv 1 \mod 4$.

(b) Prove that for $p \equiv 3 \mod 4$, no two V_p's are isomorphic over $\mathbb{Q}$.

First we will prove (a). We will also write t for $[t, 1] \in \mathbb{P}^1$ and ∞ for $[1, 0]$. Most of the proof of (a) is devoted to the derivation of isomorphism and its inverse when $p \equiv 1 \mod 4$. Thus the length of the proof can be significantly reduced by simply defining two morphisms and verifying that they are inverses.

Proof. Let $\mathbb{A}^2 : Z = 0$. We observe that $V_p \setminus \mathbb{A}^2 = \{[i, 1, 0], [-i, 1, 0]\}$ because $Z = 0$ implies that $X^2 + Y^2 = 0$, so $X = \pm iY$. We will call the first point P_+ and the second P_-, and let $P_\perp = [a, b, 1]$. Thus we can use affine notation, keeping in mind that we have the two extra points at infinity. We will also take for granted the classical results in number theory that an odd prime can be written as the sum of two squares iff it is congruent to 1 mod 4 and also that the Legendre symbol $\left(\frac{-1}{p}\right) = 1$ iff $p \equiv 1 \mod 4$.

For one direction, suppose $p \equiv 1 \mod 4$ Then we may write $p = a^2 + b^2$ for some integers a, b, where clearly $ab \neq 0$. For $p \equiv 1 \mod 4$, we define a map

$$\psi : V_p \to \mathbb{P}^1, \quad P \mapsto \begin{cases} [y - b, x - a], & \text{if } P = [x, y, 1] \text{ and } P \neq P_\perp \\ [a, -b], & \text{if } P = P_\perp \\ [\mp i, 1], & \text{if } P = P_\pm. \end{cases}.$$

This map takes a point P and associates it with the slope of the line passing through $P_\perp$ and P, but where we define the line to be the tangent line if $P = P_\perp$ and make our own definition for the slope of the line to the points at infinity to make it an inverse to the function ϕ defined later. We let $u = x - a$ and $v = y - b$, so under these new coordinates, $V_p : u^2 + v^2 + 2au + 2bv = 0$ and $P_\perp = (0, 0)$. We notice that $v(v + 2b) + u(u + 2a) = 0$, and as $v + 2b$ and $u + 2a$ do not vanish at $P_\perp$ and are regular, both u and v are uniformizers for $M_{P_\perp}$ (clearly $(u, v) = M_{P_\perp}$). Also, we have

$$v = -\frac{a}{b}u - \frac{a}{2b}(u^2 + v^2).$$

In particular, $\frac{v}{u}(0, 0) = -\frac{a}{b}$. Now we consider the points at infinity, so we have $uZ = U$ and $vZ = V$. Then our candidate rational function is $[V, U]$ since this rational function agrees with ψ except possibly at the points at infinity. However, we also see that since $U = X - aZ$ and $Y - bZ$, it follows that $[V, U](P_\pm) = [Y, X](P_\pm) = [1, \pm i] = [\mp i, 1]$. Therefore

$$\psi([X, Y, Z]) = [Y - bZ, X - aZ]$$

is a morphism.

Next, we need to define a map in the opposite direction. For $t = [u, v]$, we define $L_t : v(Y - bZ) = u(X - aZ)$. Because L_t and V_p are clearly not contained in one another for any $t \in \mathbb{P}^1$, Bezout's theorem tells us that in $\mathbb{P}^2$, $L_t \cap V_p$ contains two points (possibly non-distinct). We can now define P_t to be the point other than (a, b) in $L_t \cap V_p$. We will now show that $P_t = (a, b)$ iff L_t is tangent to V_p at (a, b), and $P_t = P_\pm$ iff $t = \mp i$.

First, let's show that if L_t is tangent to V_p at (a, b), i.e., $L_t : a(x - a) + b(y - b) = 0$ or equivalently $L_t : ax + by = p$, then $L_t \cap V_p = \{(a, b)\}$. We check that $[\pm i, 1, 0]$ is not in the line $L_t : aX + bY = pZ$, so we may now take the point of intersection to lie in $\mathbb{A}^2$.

Suppose (x, y) is in the intersection, so $ax + by = p$ and also $x^2 + y^2 = p$. Then $y = \frac{p-ax}{b}$, so

$$p = x^2 + y^2 = x^2 + \frac{p^2 - 2apx + a^2x^2}{b^2}.$$

Equivalently,

$$b^2p = (a^2 + b^2)x^2 - 2apx + p^2$$

and since $a^2 + b^2 = p$, we divide through by p and get

$$x^2 - 2ax + p - b^2 = 0.$$

Since $p - b^2 = a^2$, we have $(x - a)^2 = x^2 - 2ax + a^2 = 0$, giving $x = a$. Then $(a, y) \in L_t$ gives that $y = b$ as well.

For the reverse direction, suppose $L_t \cap V_p = \{(a, b)\}$. If $t = \infty$, then $L_t : x = a$. Notice that $(x, y) \in L_t \cap V_p$ then iff $x = a$ and $y^2 = b^2$, i.e. $y = \pm b$. In particular, $(a, -b) \in L_t \cap V_p$, so by assumption $b = -b$, i.e., $b = 0$, which is a contradiction. If $t = \pm i$, we easily observe that $P_\pm \in L_t \cap V_p$, so $P_t = P_\pm$. Thus we may take $t \neq \infty \pm i$, so $L_t : y - b = t(x - a)$.

We see that $(x, y) \in L_t \cap V_p$ iff $y = t(x - a) + b$ and $x^2 + y^2 = p$. The first equation substituted into the second gives

$$a^2 + b^2 = x^2 + t^2(x - a)^2 + 2bt(x - a) + b^2.$$

Expanding, we have the quadratic equation

$$(1 + t^2)x^2 + 2t(b - at)x + a((t^2 - 1)a - 2bt) = 0.$$

Because (a, b) is the only point of intersection, it follows that a is the only solution in $\bar{\mathbb{Q}}$ to the above equation, since if a' were a distinct equation, then we just set $b' = t(a' - a) + b$ to get a distinct point $(a', b') \in L_t \cap V_p$.

Since a is a double root, letting $\Delta(t)$ be equal to $\frac{1}{4}$ the discriminant of the quadratic in x, it must be the case that $\Delta(t) = 0$ i.e.

$$\Delta(t) = t^2(b - at)^2 - a(1 + t^2)((t^2 - 1)a - 2bt) = 0$$

By expanding $\Delta(t)$ as a polynomial in t, we get that

$$\Delta(t) = (a + bt)^2 = 0$$

i.e., $t = -\frac{a}{b}$. Therefore

$$y - b - t(x - a) = y - b + \frac{a}{b}(x - a),$$

so indeed $L_t : a(x - a) + b(y - b) = 0$ as claimed.

Now we will show the second claim. We have already shown in the proof of the first claim that $P_{\pm i} = P_\mp$. For the reverse direction, we will primarily use results in the proof of the first claim, namely that if $t^2 \neq -1$, then there is a quadratic in x whose roots are a and some other number a'. Then $(a', t(a' - a) + b)$ lies in the intersection $L_t \cap V_p \cap \mathbb{A}^2$, so this point is P_t, and is in particular, not $P_\pm$

Now we define $\phi(t) = P_t$. More explicitly, we have from our work before and the quadratic formula

$$\phi(t) = \begin{cases} \left(\frac{a(t^2-1)-2bt}{1+t^2}, \frac{b-bt^2-2at}{1+t^2}\right), & \text{if } t \neq \infty, \pm i \\ P_\mp, & \text{if } t = \pm i \\ (a, -b), & \text{if } t = \infty \end{cases}$$

Then we guess that

$$\phi([U, V]) = [a(U^2 - V^2) - 2bUV, b(V^2 - U^2) - 2aUV, U^2 + V^2].$$

To verify this, it suffices to check that the two functions agree on $[U,V] = [i,1],[1,i],[1,0]$. For $[U,V] = [1,0]$, we compute

$$[a(U^2 - V^2) - 2bUV, b(V^2 - U^2) - 2aUV, U^2 + V^2] = [a, -b, 1] = \phi([U,V])$$

so the morphism agrees with ϕ at ∞. If $[U,V] = [i,1]$, then

$$[a(U^2-V^2)-2bUV, b(V^2-U^2)-2aUV, U^2+V^2] = [-2a-2bi, 2b-2ai, 0] = [a+bi, i(a+bi), 0] = P_-.$$

Finally, we compute that if $[U,V] = [1,i]$, then

$$[a(U^2-V^2)-2bUV, b(V^2-U^2)-2aUV, U^2+V^2] = [2a-2bi, -2b-2ai, 0] = [i(-b-ai), -b-ai, 0] = P_+$$

which shows that the morphism agrees with ϕ everywhere, hence our guess is correct. By the original definition of the maps ψ and ϕ, it is clear the two functions are inverses. To be sure our computations are correct though, we first compute that if $U = Y - bZ$ and $V = X - aZ$, then

$$U^2 + V^2 = X^2 + Y^2 + (a^2 + b^2)Z^2 - 2Z(aX + bY) = 2pZ^2 - 2Z(aX + bY)$$

and

$$U^2 - V^2 = Y^2 + b^2Z^2 - 2bYZ - X^2 - a^2Z^2 + 2aXZ$$

and

$$UV = XY + abZ^2 - aYZ - bXZ.$$

Therefore

$$\begin{aligned}
&a(U^2 - V^2) - 2bUV \\
&= a(Y^2 + b^2Z^2 - 2bYZ - X^2 - a^2Z^2 + 2aXZ) - 2b(XY + abZ^2 - aYZ - bXZ) \\
&= a(Y^2 - X^2) - 2bXY + 2pXZ - apZ^2 \\
&= (2pZ^2 - 2Z(aX + bY))\frac{X}{Z}.
\end{aligned}$$

In addition,

$$\begin{aligned}
&b(V^2 - U^2) - 2aUV \\
&= b(-Y^2 - b^2Z^2 + 2bYZ + X^2 + a^2Z^2 - 2aXZ) - 2a(XY + abZ^2 - aYZ - bXZ) \\
&= 2pYZ - 2bY^2 - 2aXY \\
&= (2pZ^2 - 2Z(aX + bY))\frac{Y}{Z}
\end{aligned}$$

so we can now compute that

$$\begin{aligned}
&\phi \circ \psi([X,Y,Z]) = \phi([Y - bZ, X - aZ]) \\
&= [(2pZ^2 - 2Z(aX + bY))\frac{X}{Z}, (2pZ^2 - 2Z(aX + bY))\frac{Y}{Z}, (2pZ^2 - 2Z(aX + bY))]
\end{aligned}$$

so $\phi \circ \psi = \mathrm{id}_{\mathbb{P}^1}$.

On the other hand,

$$\begin{aligned}
&\psi \circ \phi([U,V]) = \psi([a(U^2 - V^2) - 2bUV, b(V^2 - U^2) - 2aUV, U^2 + V^2]) \\
&= [b(V^2 - U^2) - 2aUV - b(U^2 + V^2), a(U^2 - V^2) - 2bUV - a(U^2 + V^2)] \\
&= [-2(bU + aV)U, -2(bU + aV)V]
\end{aligned}$$

so also $\psi \circ \phi = \mathrm{id}_{V_p}$.

For the other direction, suppose $p \equiv 3 \mod 4$. We will first show that $V_p(\mathbb{Q}) = \varnothing$. For suppose $[x, y, z] \in V_p(\mathbb{Q})$, where we may take $x, y, z \in \mathbb{Z}$ and $\gcd(x, y, z) = 1$. Since $x^2 + y^2 = pz^2$, we have

$$x^2 \equiv -y^2 \mod p.$$

If $p \mid y$, then $p \mid x$, but then $pz^2 \equiv 0 \mod p^2$ which implies $p \mid z$ as well, contradicting $\gcd(x, y, z) = 1$. Thus we may assume $p \nmid y$ so in $\mathbb{Z}/p\mathbb{Z}$, y is invertible. Then in $\mathbb{Z}/p\mathbb{Z}$, we see that

$$(xy^{-1})^2 = x^2y^{-2} = -y^2y^{-2} = -1$$

which would then show that $\left(\frac{-1}{p}\right) = 1$, contradicting the assumption that $p \equiv 3 \mod 4$.

Now that $V_p(\mathbb{Q}) = \varnothing$, we will show that there is no morphism defined over $\mathbb{Q}$ from $\mathbb{P}^1$ to V_p. If $\phi = [\phi_0, \phi_1, \phi_2]$ were such a morphism where we may take each $\phi_i \in \mathbb{Q}(\mathbb{P}^1)$ by assumption that ϕ is defined over $\mathbb{Q}$, then $\phi(0) = [\phi_0(0), \phi_1(0), \phi_2(0)] \in V_p$. But then $\phi(0) \in V_p(\mathbb{Q})$ since each $\phi_i \in \mathbb{Q}(\mathbb{P}^1) = \mathbb{Q}(t)$ implies $\phi_i(0) \in \mathbb{Q}$ for each i. The result is now immediate. ∎

Now we will prove (b), letting p, q be primes congruent to $3 \mod 4$.

Proof. For field extension $K/\mathbb{Q}$ and a variety $V \subset \mathbb{P}^n$ defined over $\mathbb{Q}$, write $V(K)$ for the K-points, i.e. the zero locus of the polynomials defining V, considered as elements of $K[X_0, \ldots, X_n]$. For any variety $V/\mathbb{Q}$, the set

$$S(V) \;:=\; \{\, v \text{ place of } \mathbb{Q} \mid V(\mathbb{Q}_v) = \varnothing \,\}$$

is invariant under isomorphisms defined over $\mathbb{Q}$. This is because for any field extension $K/\mathbb{Q}$ and any varieties $V, V' \subset \mathbb{P}^n$ defined over $\mathbb{Q}$, there is a functor taking V to $V(K)$. If $\phi : V \to V'$ is a morphism of varieties, then we get the map $\phi_K : V(K) \to V'(K)$ where $\phi_K = [\phi_0, \ldots, \phi_n]$ since $\mathbb{Q}(V) \subset K(V_K)$ (if $f = \frac{f_1}{f_2}$ with each $f_i \in \mathbb{Q}[X_0, \ldots, X_n]/(g_1, \ldots, g_r)$, for any $g \in \mathbb{Q}[X_0, \ldots, X_r](g_0, \ldots, g_r)$, $g \equiv 0 \mod K[X_0, \ldots, X_n](g_1, \ldots, g_r)$ so $f_i + g = f_i$ in $K[X_0, \ldots, X_n]/K[X_0, \ldots, X_n](g_1, \ldots, g_r)$, and $f_i \in K[X_0, \ldots, X_n](g_1, \ldots, g_r)$ implies f_i vanishes on all of $V(K)$, which contains $V(\mathbb{Q})$, implying $f_i \in (g_1, \ldots, g_r)$). Since this base-change construction is functorial, it follows that if $V_p \cong_{\mathbb{Q}} V_q$, then over any place v of $\mathbb{Q}$, $V_p(\mathbb{Q}_v) \cong_{\mathbb{Q}_v} V_q(\mathbb{Q}_v)$. In particular, $V_p(\mathbb{Q}_v)$ has a $\mathbb{Q}_v$-point iff $V_q(\mathbb{Q}_v)$ does too.

Lemma. Let ℓ be a prime number congruent to $3 \mod 4$. Then

$$S(V_\ell) = \{2, \ell\}.$$

For this proof, we use two results from [2], the first being Theorem 1 in Chapter III, which reads:

Theorem. If $k = \mathbb{R}$, we have $(a, b) = 1$ if a or b is > 0, and $(a, b) = -1$ if a and b are < 0.

If $k = \mathbb{Q}_p$ and if we write a, b in the form $p^\alpha u, p^\beta v$ where u and v belong to the group $\mathbb{U}$ of p-adic units, we have

$$(a, b) = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha \quad \text{if } p \neq 2$$
$$(a, b) = (-1)^{\varepsilon(u)\varepsilon(v) + \alpha\omega(v) + \beta\omega(u)} \quad \text{if } p = 2.$$

[Recall that $\left(\frac{u}{p}\right)$ denotes the Legendre symbol $\left(\frac{\bar{u}}{p}\right)$ where $\bar{u}$ is the image of u by the homomorphism of reduction modulo $p : \mathbb{U} \to \mathbb{F}_p^*$. As for $\varepsilon(u)$ and $\omega(u)$, they denote respectively the class modulo 2 of $\frac{u-1}{2}$ and of $\frac{u^2-1}{8}$.]

In the above, (a, b) denotes the Hilbert symbol of a and b, which is 1 if $z^2 = ax^2 + by^2$ has a nontrivial solution $(z, x, y) \in k^3$ and is -1 otherwise.

The second result we use is the corollary to Theorem 6 in Chapter IV of [2], which reads (for p a prime number and $k = \mathbb{Q}_p$, and f a quadratic form of rank n with discriminant $d = \det M$ where M is the matrix representing the form f, and Hasse-invariant ε):

Corollary. Let $a \in k^*/k^{*2}$. In order that f represent a, it is necessary and sufficient that

(i) $n = 1$ and $a = d$

(ii) $n = 2$ and $(a, -d) = \varepsilon$

(iii) $n = 3$ and either $a \neq -d$ or $a = -d$ and $(-1, -d) = \varepsilon$

(iv) $n \geqslant 4$

Proof. Fix a place v of $\mathbb{Q}$. If $v = \infty$, then $[\sqrt{\ell}, 0, 1] \in V_\ell(\mathbb{Q}_v)$, so $\infty \notin S(V_\ell)$. Now assume v is a finite place and let $\mathbb{A}^2 : Z \neq 0$. We will now show that $V_\ell(\mathbb{Q}_v) \subseteq \mathbb{A}^2$ when $v \not\equiv 1 \mod 4$ and $\{V_\ell(\mathbb{Q}_v) \setminus \mathbb{A}^2 = [\pm i : 1 : 0]\}$ if $v \equiv 1 \mod 4$ and where we let $i \in \mathbb{Q}_v$ be such that $i^2 = -1$. If we had a point $[x : y : z] \in V(\mathbb{Q}_v) \setminus \mathbb{A}^2$, then $z = 0$, hence $x^2 + y^2 = 0$. Without loss of generality we may assume that $y \neq 0$, so then $(\frac{x}{y})^2 = -1$. Then the form X^2 represents -1 over $\mathbb{Q}_v$. Although not necessary, it's easy to verify that if X^2 represents -1 over $\mathbb{Q}_v$, then $V_\ell(\mathbb{Q}_v) \not\subseteq \mathbb{A}^2$. Suppose we have some $x \in \mathbb{Q}_v$ with $x^2 = -1$. Then $2\nu_v(x) = \nu_v(-1) = 0$ so $\nu_v(x) = 0$ implies that $x \in \mathbb{Z}_v$ because $\mathbb{Z}_v$ is a DVR. Thus $V_\ell(\mathbb{Q}_v) \not\subset \mathbb{A}^2$ iff -1 is a square in $\mathbb{Z}_v^*$.

If $v = 2$, we apply Theorem 4 of Chapter II of [2] to see that an element $2^n u$ of $\mathbb{Q}_2^*$ is a square iff n is even and $u \equiv 1 \mod 8$. In particular, -1 is not a square in $\mathbb{Q}_2$. Now assume v is a finite place different from 2. Then Theorem 3 of Chapter II of [2] tells us that for $x = v^n u$ in $\mathbb{Q}_v^*$, x is a square iff n is even and $\left(\frac{u}{v}\right) = 1$. Thus -1 is a square in $\mathbb{Q}_v$ iff $\left(\frac{-1}{v}\right) = 1$ iff $v \equiv 1 \mod 4$.

We have now shown that $V_\ell(\mathbb{Q}_v) \subset \mathbb{A}^2$ for $v \not\equiv 1 \mod 4$. Now suppose $v \equiv 1 \mod 4$. We know that there is some integer x_0 such that $x_0^2 \equiv -1 \mod v$, and as the derivative of the polynomial $x^2 + 1 \in \mathbb{Z}_v[x]$ has non-vanishing derivative except at $0 \neq x_0$, Hensel's lemma gives a lift to some $i \in \mathbb{Z}_v$ that's a root of $x^2 + 1$, i.e., $i^2 = -1$. Then clearly as we have $(\frac{X}{Y})^2 = -1$, then $\frac{X}{Y} = \pm i$, hence the only points outside of the affine patch are $[i, 1, 0]$ and $[-i, 1, 0]$.

This shows every place in $S(V_\ell)$ is a finite prime not congruent to 1 $\mod 4$. Since $V_\ell(\mathbb{Q}_v) \subset \mathbb{A}^2$ for every such place, we have that $v \in S(V_\ell)$ implies $v \not\equiv 1 \mod 4$ (which implies $S(V_\ell) \subset \mathbb{A}^2$) and $v \neq \infty$. Thus now we're interested in whether the quadratic form $f = X^2 + Y^2$ represents ℓ in $\mathbb{Q}_v$, because by our work, this is equivalent to $V_\ell(\mathbb{Q}_v) \neq \varnothing$ for places not ∞ and $\equiv 1 \mod 4$.

The quadratic form f has discriminant $d = 1$ and Hasse invariant $\varepsilon = (1, 1) = 1$. By the corollary then, f represents ℓ iff $(\ell, -1) = 1$. Now we appeal to the theorem to compute $(\ell, -1)$. If $v = 2$, then we compute

$$(\ell, -1) = (-1)^{1 \cdot 1 + 0 \cdot \omega(\ell) + 0 \cdot 1} = -1$$

which shows that $2 \in S(V_\ell)$. Now assume that $v \equiv 3 \mod 4$. If $v \neq \ell$, we compute that

$$(\ell, -1) = (-1)^{0 \cdot 0 \cdot 1} \left(\frac{\ell}{v}\right)^0 \left(\frac{-1}{v}\right)^0 = 1.$$

Thus the only remaining possibility is that $\ell \in S(V_\ell)$. For $v = \ell$, we have $\alpha = 1$ and $u = 1$, so

$$(\ell, -1) = (-1)^{1 \cdot 0 \cdot 1} \left(\frac{1}{\ell}\right)^0 \left(\frac{-1}{\ell}\right)^1 = -1$$

which also proves that $\ell \in S(V_\ell)$.

■

Now that we have shown $S(V_\ell)$ is invariant under $\mathbb{Q}$-isomorphism and that $S(V_\ell) = \{2, \ell\}$ for $\ell \equiv 3 \mod 4$, it follows that if $V_p \cong_{\mathbb{Q}} V_q$, then $\{2, p\} = \{2, q\}$ so $p = q$ as desired. ■

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 $\deg \phi := [K(\mathbb{P}^1) : \phi^* K(\mathbb{P}^1)] = 5$. 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 $\mathrm{ord}_{P_i}(x - e_i) = 2\,\mathrm{ord}_{P_i}(y) \geqslant 2$ 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 $\mathrm{ord}_{P_i}(x - e_i) = 2\,\mathrm{ord}_{P_i}(y) = 2$. 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 $\mathrm{div}(x - e_i) = 2(P_i) - 2(P_\infty)$, but let's explicitly compute $\mathrm{ord}_{P_\infty}(x - e_i)$. 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 $\mathrm{ord}_O(1 - e_i (x')^2 q) = 0$. This implies that

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

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

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

Now we have

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

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 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

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 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

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

■

Chapter III: The Geometry of Elliptic Curves

Section 1: Weierstrass Equations

Proposition 1.5

Statement. *Let E be an elliptic curve. Then the invariant differential ω associated to a Weierstrass equation for E is holomorphic and nonvanishing, i.e.,* $\operatorname{div} \omega = 0$.

We use all of the same notation as in the book for the proof.

Proof. First, we will verify that $\frac{d(x-x_0)}{F_y(x,y)} = -\frac{d(y-y_0)}{F_x(x,y)}$. Notice that the equality holds iff

$$F_x(x,y)dx + F_y(x,y)dy = F_x(x,y)d(x-x_0) + F_y(x,y)d(y-y_0) = 0.$$

We will now show that for any polynomial $G(x,y)$, it's true that $G_x(x,y)dx+G_y(x,y)dy = d(G(x,y))$. We will prove this by induction on the number of terms in G, with the base case being 1, i.e., G is a monomial. For this case, write $G = cx^iy^j$ for $i,j \geqslant 0$ and $c \in \bar{K}$. Then

$$dG = d(cx^iy^j) = cd(x^iy^j) = c\left[y^jd(x^i) + x^id(y^j)\right] = c\left[iy^jx^{i-1}dx + jx^iy^{j-1}dy\right] = G_xdx + G_ydy.$$

For the inductive step, write $G(x,y) = H(x,y) + M(x,y)$ where M is a monomial in x,y. Then both H, M satisfy the inductive hypothesis, so we see that

$$dG = d(H+M) = dH+dM = (H_xdx+H_ydy)+(M_xdx+M_ydy) = (H_x+M_x)dx+(H_y+M_y)dy = G_xdx+G_ydy$$

as claimed. Now applying this result to F, we get that

$$0 = d(0) = d(F) = F_x(x,y)dx + F_y(x,y)dy.$$

Next, we will verify that the map

$$\phi : E \to \mathbb{P}^1, \quad (x,y) \mapsto x$$

is of degree 2. We must compute $\deg\phi = [\bar{K}(E) : \phi^*\bar{K}(\mathbb{P}^1)] = [\bar{K}(E) : \phi^*\bar{K}(x)] = [\bar{K}(E) : \bar{K}(x)]$ where x in the last expression is the $x \in \bar{K}(E)$ and the x in the expression before is the coordinate function on $\mathbb{P}^1$. We see that $y \in \bar{K}(E)$ is a root of the quadratic polynomial $F(x,T) \in \bar{K}(x)[T]$. We must now show $f(x,T)$ is irreducible over $\bar{K}(x)$. Suppose not, so $F(x,T)$ splits into linear factors over $\bar{K}(x)$, and let $\frac{p(x)}{q(x)} \in \bar{K}(x)$ be a root of $F(x,T)$ with $\gcd(p,q) = 1$. Then

$$0 = F(x, \frac{p}{q}) = \frac{p^2}{q^2} + (a_1x + a_3)\frac{p}{q} - x^3 - a_2x^2 - a_4x - a_6.$$

Multiplying through by q^2, we get the equation in $\bar{K}[x]$:

$$0 = p^2 + (a_1x + a_3)pq - (x^3 + a_2x^2 + a_4x + a_6)q^2.$$

Then

$$0 = p^2 + (a_1x + a_3)pq - (x^3 + a_2x^2 + a_4x + a_6)q^2 \equiv p^2 \mod q$$

implies that $q \mid p$, contrary to assumption p and q share no common factors. Now that x, y generate $\bar{K}(E)$ and y has degree 2 over $\phi^*\bar{K}(\mathbb{P}^1)$, it follows that $\deg\phi = 2$.

From II.2.6a, we know that for any $Q \in \mathbb{P}^1$,

$$\sum_{R \in \phi^{-1}(Q)} e_\phi(R) = \deg\phi = 2.$$

In addition, $\phi^{-1}(x_0)$ is the zero set of the quadratic $F(x_0,y)$, hence has cardinality 1 or 2, and cardinality 2 iff $F(x_0,y)$ has a double root at y_0 (because $F(x_0,y_0) = 0$ by hypothesis) iff $F_y(x_0,y_0) = 0$. We also see that

$$\phi^*t_{\phi P} = \phi^*t_{x_0} = \phi^*(x-x_0) = x - x_0$$

so it follows that $\mathrm{ord}_P(x-x_0) = e_\phi(P)$ is at most 2, with equality iff $F_y(x_0,y_0) = 0$.

Next, we will show that $\mathrm{ord}_P(\omega) = 0$. We can apply II.4.3d to get

$$\mathrm{ord}_P(\frac{d(x-x_0)}{F_y(x,y)}) = \mathrm{ord}_P(\frac{1}{F_y(x,y)}) + \mathrm{ord}_P(x-x_0) - 1 = \mathrm{ord}_P(x-x_0) - \mathrm{ord}_P(F_y(x,y)) - 1.$$

if $p = 0$ or $p \nmid \operatorname{ord}_P(x-x_0)$, where $p = \operatorname{char} K$ here. Supposing this condition is met, if $\operatorname{ord}_P(x-x_0) = 1$, then $F_y(x_0, y_0) \neq 0$ and is regular, hence $\operatorname{ord}_P(F_y(x_0, y_0) = 0$ and the result is 0. If instead $\operatorname{ord}_P(x - x_0) = 2$, then $F_y(x_0, y_0) = 0$, and as $F_y(x, y) = 2y + a_1x + a_3$ is linear, it cannot vanish at P with order more than 1 ($M_P = (x - x_0, y - y_0)$ so $M_P^2 = ((x - x_0)^2, (x - x_0)(y - y_0), (y - y_0)^2)$ and we cannot write a nonzero linear form in x and y as an element of this ideal). Therefore $\operatorname{ord}_P(F_y(x, y)) = 1$, so again $\operatorname{ord}_P(\omega) = 0$.

The last case to consider is $\operatorname{ord}_P(x - x_0) = 2 = \operatorname{char} K$. We also have $F_y(x_0, y_0) = 0$. As E is smooth, it follows that $F_x(x_0, y_0) \neq 0$. Therefore $\operatorname{ord}_P(F_x(x, y)) = 0$, so we just need to compute $\operatorname{ord}_P(y - y_0)$ now. We have a map $\psi : E \to \mathbb{P}^1 \quad (x, y) \mapsto y$ where $\psi^* t_{\psi(P)} = y - y_0$. Now we will compute

$$\deg \psi = [\bar{K}(E) : \bar{K}(y)].$$

We see that $x \in \bar{K}(E)$ satisfies the cubic $F(T, y)$ over $\bar{K}(y)$. We will now show $F(T, y)$ is irreducible over $\bar{K}(y)$. If it were reducible, then it would have a root in $\bar{K}(y)$ because $\deg F(T, y) = 3$, so let $\frac{a(y)}{b(y)} \in \bar{K}(y)$ be a root with $\gcd(a, b) = 1$. Then we have

$$0 = F(\frac{a}{b}, y) = -\frac{a^3}{b^3} - a_2\frac{a^2}{b^2} + (a_1y - a_4)\frac{a}{b} + y^2 + a_3y - a_6$$

so multiplying through by b^3 gives

$$-a^3 - a_2a^2b + (a_1y - a_4)ab^2 + (y^2 + a_3y - a_6)b^3 = 0.$$

Therefore

$$0 = -a^3 - a_2a^2b + (a_1y - a_4)ab^2 + (y^2 + a_3y - a_6)b^3 \equiv -a^3 \mod b$$

so $b \mid a$, contrary to assumption. Therefore x has degree 3 over $\bar{K}(y) = \psi^*\bar{K}(\mathbb{P}^1)$, and as x, y generate $\bar{K}(E)$, it follows that $\deg \psi = [\deg \bar{K}(E) : \psi^*\bar{K}(\mathbb{P}^1)] = 3$. Now we have

$$\sum_{R \in \psi^{-1}(y_0)} e_\psi(R) = \deg \psi = 3.$$

This shows that $\operatorname{ord}_P(y - y_0) = \operatorname{ord}_P(\psi^* t_{\psi P}) = e_\psi(P) \geqslant 2$ iff $F(x, y_0)$ has a multiple root at x_0 iff $F_x(x_0, y_0) = 0$. This is false by hypothesis, so we conclude that $\operatorname{ord}_P(y - y_0) = 1$. Now that $y - y_0$ is a uniformizer at P,

$$\operatorname{ord}_P(\omega) = \operatorname{ord}_P(-\frac{d(y - y_0)}{F_x(x, y)}) = \operatorname{ord}_P(\frac{1}{F_x(x, y)}) = 0.$$

Finally, we will show that $\operatorname{ord}_O(\omega) = 0$ in characteristic 2, where the other characteristics are taken care of in the book. Let t be a uniformizer at O, and continuing the notation, write $x = t^{-2}f$ and $y = t^{-3}g$ where $f(O), g(O) \neq 0, \infty$. We compute

$$\omega = \frac{dy}{F_x(x, y)} = \frac{t^{-4}g + t^{-3}g'}{t^{-4}f^2 + a_4 + a_1t^{-3}g}dt = \frac{g + tg'}{f^2 + a_4t^4 + a_1tg}dt.$$

We see that $g + tg'(O) \neq 0, \infty$ since $g'(O) \neq 0, \infty$ by II.4.3b. Similarly, $f^2 + a_4t^4 + a_1tg \neq 0, \infty$. Therefore

$$\operatorname{ord}_O(\omega) = \operatorname{ord}_O(\frac{g + tg'}{f^2 + a_4t^4 + a_1tg}) = 0$$

completing the case $\operatorname{char} K = 2$. ■

Proposition 1.6

Statement. *If a curve E given by a Weierstrass equation is singular, then there exists a rational map $\phi : E \to \mathbb{P}^1$ of degree one, i.e., the curve E is birational to to $\mathbb{P}^1$.*

We will just justify that we can always make a linear change of variables to assume that the singular point is $(0,0)$, because the rest of the proof in the book is straightforward.

Proof. If the singular point is (x_0, y_0), then we can apply the linear change of coordinates $(x, y) \mapsto (x - x_0, y - y_0)$ to get that the singular point is $(0,0)$. Now we claim that, letting O be the point at infinity, E is never singular at P_∞. In projective coordinates, $E : Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$. Then using the affine chart $Y \neq 1$, our curve is

$$E : z + a_1xz + a_3z^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3$$

and $O = (0,0)$. This is singular at O only if

$$0 = F_x(0,0) = [1 + a_1x + 2a_3z - a_2x^2 - 2a_4xz - 3a_6z^2](0,0) = 1$$

so indeed O is nonsingular. ■

Exercise 17

Statement. Let $\mathcal{K}$ be a definite quaternion algebra. Prove that $\mathcal{K}$ is ramified at ∞.

We let $\mathcal{K} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$ where α^2, β^2 are negative rational numbers and $\alpha\beta = -\beta\alpha$.

Proof. Clearly $M_2(\mathbb{R})$ has 0-divisors, so it suffices to show that $\mathbb{R} \otimes \mathcal{K}$ is a division algebra.

Lemma. Suppose L/K is a field extension, and V is a finite-dimensional K-vector space with basis $v_1, \ldots, v_n$. Then $1 \otimes v_1, \ldots, 1 \otimes v_n$ is a basis for the L-vector space $L \otimes_K V$.

Proof. Suppose $\sum_{i=1}^n \ell_i \otimes v_i = 0$ for some $\ell_1, \ldots, \ell_n \in L$. Let $L^\vee = \mathrm{Hom}_K(L, K)$ be the dual of L as a K-vector space. There is an injective map

$$L \otimes V \hookrightarrow \mathrm{Hom}_K(L^\vee, V), \quad \ell \otimes v \mapsto (f \mapsto f(\ell)v).$$

Using this injection, we get a K-linear map $T : L^\vee \to V$ corresponding to $\sum_i \ell_i \otimes v_i$. Because we assume that this tensor is trivial, so too is T. Let $1 \leqslant j \leqslant n$ be arbitrary. Letting $\ell_j^\vee \in L^\vee$ be the dual of ℓ_j (explicitly, if $\ell_j = 0$ then $\ell_j^\vee = 0$, and otherwise we let $\mathcal{B}$ be a K-basis for L including ℓ_j, and let $\ell_j^\vee(\sum_{\ell \in \mathcal{B}} \lambda_l \ell) = \lambda_{\ell_j}$), we get that

$$0 = T\ell_j^\vee = \sum_i \ell_j^\vee(\ell_i)v_i = \ell_j^\vee(\ell_j)v_j$$

so $\ell_j^\vee(\ell_j) = 0$. This is only possible if $\ell_j = 0$. Now because j was arbitrary, we conclude that each ℓ_j is trivial, hence the $1 \otimes v_i$ are linearly independent. Every pure tensor $\ell \otimes v$ can be written as

$$\ell \otimes v = \ell \otimes \sum_i \lambda_i v_i = \sum_i \lambda_i \ell(1 \otimes v_i)$$

for some $\lambda_i \in K$, so every pure tensor is a finite L-linear combination of the $1 \otimes v_i$. Because every tensor is a finite K-linear combination of pure tensors, it follows that the $1 \otimes v_i$ span $L \otimes V$ as a L-vector space, giving the result. ■

By the lemma, $\{1\otimes 1, 1\otimes\alpha, 1\otimes\beta, 1\otimes\alpha\beta\}$ is an $\mathbb{R}$-basis for $\mathbb{R}\otimes\mathcal{K}$. Thus we take an arbitrary element of $\mathbb{R}\otimes\mathcal{K}$ to be

$$q = a\otimes 1 + b\otimes\alpha + c\otimes\beta + d\otimes\alpha\beta$$

for $a, b, c, d \in \mathbb{R}$. Letting $\bar{q} = a\otimes 1 - b\otimes\alpha - c\otimes\beta - d\otimes\alpha\beta$, we compute

$$q\bar{q} = a^2 - b^2\alpha^2 - c^2\beta^2 + d^2\alpha^2\beta^2\otimes 1 = \bar{q}q$$

using the relation $(\alpha\beta)^2 = -\alpha^2\beta^2$. We let $|q| = q\bar{q} \in \mathbb{R}$. Since $\alpha^2, \beta^2 < 0$, $|q| = 0$ iff $a = b = c = d = 0$ iff $q = 0$. Thus if $q \neq 0$, we have $\frac{\bar{q}}{|q|}q = 1 = q\frac{\bar{q}}{|q|}$, so q is invertible. ■

Exercises

Exercise 19

Statement. Let $\mathcal{K}$ be a quaternion algebra.

(a) Prove that $\mathcal{K}\otimes\overline{\mathbb{Q}} \cong M_2(\overline{\mathbb{Q}})$.

(b) Prove that $\mathcal{K}\otimes\mathcal{K} \cong M_4(\mathbb{Q})$. This shows that $\mathcal{K}$ corresponds to an element of order 2 in the Brauer group $\mathrm{Br}(\mathbb{Q})$.

We $\mathcal{K} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$ subject to the usual relations. First we prove (a):

Proof. Let $s, t \in \bar{\mathbb{Q}}$ be such that $s^2 = \alpha^2$ and $t^2 = \beta^2$. By the lemma in the proof of Exercise 17, we have that $\{1\otimes 1, \alpha\otimes 1, \beta\otimes 1, \alpha\beta\otimes 1\}$ is a $\bar{\mathbb{Q}}$-basis for $\mathcal{K}\otimes\bar{\mathbb{Q}}$. We let $\Phi : \mathcal{K}\otimes\bar{\mathbb{Q}} \to M_2(\bar{\mathbb{Q}})$ be a map of $\bar{\mathbb{Q}}$ vector spaces defined by $1\otimes b \mapsto M_b$ for any element b of the above basis for $\mathcal{K}\otimes\bar{\mathbb{Q}}$, where

$$M_b = \begin{cases} \mathrm{id}, & \text{if } b = 1 \\ s\begin{pmatrix} 1 & -2 \\ 0 & -1 \end{pmatrix}, & \text{if } b = \alpha \\ t\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, & \text{if } b = \beta \\ st\begin{pmatrix} -1 & 2 \\ -1 & 1 \end{pmatrix}, & \text{if } b = \alpha\beta \end{cases}.$$

We compute that

$$M_\alpha M_\beta = st\begin{pmatrix} 1 & -2 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} = st\begin{pmatrix} -1 & 2 \\ -1 & 1 \end{pmatrix} = M_{\alpha\beta}.$$

In addition,

$$-M_\beta M_\alpha = -st\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 0 & -1 \end{pmatrix} = -st\begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix} = M_{\alpha\beta}.$$

We easily observe that $M_\alpha^2 = s^2\mathrm{id} = \alpha^2\mathrm{id}$ and $M_\beta^2 = t^2\mathrm{id} = \beta^2\mathrm{id}$. Because these are the only relations imposed on α and β, it follows that Φ is actually a homomorphism of $\bar{\mathbb{Q}}$-algebras. Because $\dim_{\bar{\mathbb{Q}}} M_2(\bar{\mathbb{Q}}) = 4 = \dim_{\bar{\mathbb{Q}}} \mathcal{K}\otimes\bar{\mathbb{Q}}$, to show Φ is an isomorphism of $\bar{\mathbb{Q}}$-algebras, it suffices to show the M_b are $\bar{\mathbb{Q}}$-linearly independent. Suppose that

$$0 = a\mathrm{id} + bM_\alpha + cM_\beta + dM_{\alpha\beta} = \begin{pmatrix} a + bs + ct - dst & -2bs + 2dst \\ ct - dst & a - bs - ct + dst \end{pmatrix}.$$

The entries not along the diagonal give that $c = ds$ and $b = dt$. The first entry on the diagonal gives

$$0 = a + bs + ct - dst = a + dst + dst - dst = a + dst$$

so $a = -dst$. Thus the second entry on the diagonal gives

$$0 = a - bs - ct + dst = -dst - dst - dst + dst = -2dst$$

which implies that $d = 0$. This gives that $a = b = c = 0$ as well then, so the matrices are linearly independent. ■

For (b), we will follow the hint given in the book:

Proof. First we notice that $\mathcal{K}$ is obviously simple because it's a division algebra (if $q = a+b\alpha+c\beta+d\alpha\beta$, letting $\bar{q} = a - b\alpha - c\beta - d\alpha\beta$ and $|q| = a^2 - b^2\alpha^2 - c^2\beta^2 + d^2\alpha^2\beta^2$ one verifies $\frac{\bar{q}}{|q|} = q^{-1}$). Next, we will show that $\mathcal{K}$ is central, i.e., its center $Z(\mathcal{K})$ is just $\mathbb{Q}$. Suppose $q = a + b\alpha + c\beta + d\alpha\beta \in Z(\mathcal{K})$. Then

$$(b\alpha^2) + (a)\alpha + (d\alpha^2)\beta + (c)\alpha\beta = \alpha q = q\alpha = (b\alpha^2) + (a)\alpha + (-d\alpha^2)\beta + (-c)\alpha\beta$$

so $c = d = 0$. Therefore

$$a\beta + (-b)\alpha\beta = \beta q = q\beta = a\beta + b\alpha\beta$$

so $b = 0$ as well, showing $q \in \mathbb{Q}$ as desired.

Lemma. Suppose A is a simple central K-algebra and B is a simple K-algebra. Then $A \otimes_K B$ is simple.

Proof. Suppose I is a nonzero ideal (in this proof, ideal means two-sided) of $A \otimes B$. Let S be the set of all nonzero elements in I of the form $\sum_{i=1}^n a_i \otimes b_i$ such that the set $\{b_1, \ldots, b_n\}$ is K-linearly independent. Then S is the set of all nonzero elements of I, since if $b_j = \sum_{i \neq j} \lambda_i b_i$,

$$\sum_i a_i \otimes b_i = (a_j \otimes b_j) + \sum_{i \neq j} a_i \otimes b_i = (a_j \otimes \sum_{i \neq j} \lambda_i b_i) + \sum_{i \neq j} a_i \otimes b_i = \sum_{i \neq j} (\lambda_i a_j + a_i) \otimes b_i$$

Let $u = \sum_{i=1}^n a_i \otimes b_i \in S$ be an element minimal in n. There must exist some $1 \leqslant j \leqslant n$ where $a_j \neq 0$. Since $a_i \neq 0$ and A is simple, we have $Aa_jA = A$, so there exist some $a, a' \in A$ with $aa_ja' = 1$. Thus we may replace u by $(a \otimes 1)u(a' \otimes 1)$ to assume that $a_j = 1$. Now let $a \in A$ be arbitrary. We compute

$$(a \otimes 1)u - u(a \otimes 1) = \sum_{i \neq j} [a, a_i] \otimes b_i$$

where $[a, a_i] = aa_i - a_ia$ is the commutator. Because n was minimal, it must be the case that

$$\sum_{i \neq j} [a, a_i] \otimes b_i = 0.$$

Lemma. Suppose V, W are K-vector spaces where $\{w_1, \ldots, w_n\} \subset W \setminus \{0\}$ and $\{v_1, \ldots, v_n\} \subset V$ are linearly independent. Then $\{v_1 \otimes w_1, \ldots, v_n \otimes w_n\} \subset V \otimes_K W$ is linearly independent.

Proof. Suppose that

$$\sum_i \lambda_i (v_i \otimes w_i) = 0.$$

Letting $V^\vee$ be the dual vector space of V, there exists a K-linear map

$$V \otimes W \to \mathrm{Hom}_K(V^\vee, W), \quad v \otimes w \mapsto (f \mapsto f(v)w).$$

Let $T : V^\vee \to W$ be the map corresponding to $\sum_i \lambda_i (a_i \otimes b_i)$. Since we assume this sum is trivial, so too is T. For $v \in V$, let $v^\vee \in V^\vee$ be defined as in the lemma in the proof of Exercise 17. For any $1 \leqslant j \leqslant n$, we then have

$$0 = T(v_j^\vee) = \sum_i \lambda_i v_j^\vee(v_i) w_i = \lambda_j w_j$$

because $v_j^\vee(v_i) = \delta_{ij}$ by definition of $v_j^\vee$ and that the v_i are linearly independent. But because $w_j \neq 0$, it follows that $\lambda_j = 0$, and since j was arbitrary, the claim follows. ■

Because the b_i are linearly independent, we can apply to the lemma to see that $[a, a_i] = 0$ for each i. Since a was arbitrary, it follows that each $a_i \in Z(A) = K$. Thus

$$\sum_i a_i \otimes b_i = \sum_i 1 \otimes a_i b_i = 1 \otimes \sum_i a_i b_i.$$

Letting $b = \sum_i a_i b_i \in B$, we see $b \neq 0$ and $1 \otimes b \in I$. By simplicity of B, we have $BbB = B$, so there exist some $a, c \in B$ where $abc = 1$. Since $1 \otimes b \in I$, we have

$$I \ni (1 \otimes a)(1 \otimes b)(1 \otimes c) = 1 \otimes abc = 1$$

so indeed $I = A \otimes B$. ■

We apply the above lemma to see that $\mathcal{K} \otimes \mathcal{K}^{\mathrm{op}}$ is simple (since $\mathcal{K}$ is central simple clearly implies $\mathcal{K}^{\mathrm{op}}$ is too). Now we define the map

$$\Phi : \mathcal{K} \otimes \mathcal{K}^{\mathrm{op}} \to \mathrm{End}(\mathcal{K}), \quad a \otimes b^{\mathrm{op}} \mapsto (x \mapsto axb).$$

One verifies that this is a homomorphism of $\mathbb{Q}$-algebras, hence its kernel is an ideal of $\mathcal{K} \otimes \mathcal{K}^{\mathrm{op}}$.

Since $\ker \Phi$ is an ideal of $\mathcal{K} \otimes \mathcal{K}^{\mathrm{op}}$, either $\ker \Phi = 0$ or $\ker \Phi = \mathcal{K} \otimes \mathcal{K}^{\mathrm{op}}$. However, we see that

$$\Phi(1 \otimes 1) = \mathrm{id}_{\mathcal{K}}$$

so $\ker \Phi$ is a proper ideal, hence trivial by simplicity. Thus Φ is injective. Because $\dim_{\mathbb{Q}} \mathcal{K} \otimes \mathcal{K}^{\mathrm{op}} = 16 = \dim_{\mathbb{Q}} \mathrm{End}(\mathcal{K})$, it follows that Φ is surjective as well, hence an isomorphism of $\mathbb{Q}$-algebras, so.

$$\mathcal{K} \otimes \mathcal{K}^{\mathrm{op}} \cong \mathrm{End}(\mathcal{K}).$$

Because $\mathcal{K}$ is a 4-dimensional $\mathbb{Q}$-vector space, we get

$$\mathrm{End}(\mathcal{K}) \cong M_4(\mathbb{Q})$$

as well. Thus all that remains is to show that $\mathcal{K}^{\mathrm{op}} \cong \mathcal{K}$ as $\mathbb{Q}$-algebras, i.e., there exists an anti-automorphism of $\mathcal{K}$. Let $\psi(a + b\alpha + c\beta + d\alpha\beta) = a - b\alpha - c\beta - d\alpha\beta$. We know that

$$\psi(q)q \in \mathbb{Q}$$

and $\psi(q)q = 0$ iff $q = 0$. One also verifies that

$$\psi(q_1 q_2) = \psi(q_2)\psi(q_1)$$

and $\psi^2 = \mathrm{id}$. Thus ψ is an anti-automorphism, so finally

$$\mathcal{K} \otimes \mathcal{K} \cong \mathcal{K} \otimes \mathcal{K}^{\mathrm{op}} \cong \mathrm{End}(\mathcal{K}) \cong M_4(\mathbb{Q}).$$

■

Exercise 20

Statement. Let $\mathcal{K}$ be an imaginary quadratic field with ring of integers $\mathcal{O}$. Prove that the orders of $\mathcal{K}$ are precisely the rings $\mathbb{Z} + f\mathcal{O}$ for integers $f > 0$. The integer f is called the *conductor* of the order.

We let $\mathcal{K} = \mathbb{Q}(\sqrt{D})$ where D is a squarefree negative integer. We recall that $\mathcal{O}$ is the maximal finitely generated $\mathbb{Z}$-submodule of $\mathcal{K}$, so any order of $\mathcal{K}$ is automatically a subring of $\mathcal{O}$. It's also a general fact from algebraic number theory that $\mathcal{O} = \mathbb{Z}[\omega]$ where

$$\omega = \begin{cases} \frac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \mod 4 \\ \sqrt{D}, & \text{otherwise} \end{cases}$$

but we only need that $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega$ and $\{1, \omega\}$ is $\mathbb{Z}$-linearly independent.

Proof. Let $\mathcal{R}$ be an order of $\mathcal{K}$. We know that $1 \in \mathcal{R}$, so $\mathbb{Z} \subset \mathcal{R}$. Also, $\mathbb{Z} \neq \mathcal{R}$ otherwise $\mathcal{K} = \mathbb{Q} \otimes \mathcal{R} = \mathbb{Q} \otimes \mathbb{Z} = \mathbb{Q}$ which is absurd. Thus $\operatorname{rank} \mathcal{R} \geqslant 2$. Also, $\operatorname{rank} \mathcal{O} = 2$ and $\mathcal{R} \subset \mathcal{O}$ implies that $\operatorname{rank} \mathcal{R} \leqslant 2$, so $\operatorname{rank} \mathcal{R} = 2$. Now let $\{1, x\}$ be a $\mathbb{Z}$-basis for $\mathcal{R}$. Because $\operatorname{rank} \mathcal{O} = \operatorname{rank} \mathcal{R}$, $e \coloneqq [\mathcal{O} : \mathcal{R}] < \infty$. Then

$$ex = a + f\omega$$

for some $a, f \in \mathbb{Z}$. Therefore $f\omega \in \mathcal{R}$, so

$$\mathbb{Z} + f\mathcal{O} = \mathbb{Z} + \mathbb{Z}f\omega \subset \mathcal{R}.$$

Since $f = [\mathcal{O} : \mathbb{Z} + f\mathcal{O}]$, if we define $d = [\mathcal{R} : \mathbb{Z} + f\mathcal{O}]$, we have

$$e = fd.$$

Note: we know $d < \infty$ because $\mathbb{Z} + f\mathcal{O}$ is a submodule of the free module $\mathcal{O}$ (and $\mathbb{Z}$ is a PID), or alternatively

$$\operatorname{rank} \mathbb{Z} + f\mathcal{O} = \dim_{\mathbb{Q}} \mathbb{Q} \otimes (\mathbb{Z} + f\mathcal{O}) = \dim_{\mathbb{Q}} \mathcal{K} = 2 = \operatorname{rank} \mathcal{R}.$$

Thus

$$fdx = a + f\omega \Rightarrow f(dx - \omega) = a$$

so $dx - \omega \in \mathbb{Z}$ and $\alpha \coloneqq \frac{a}{f} \in \mathbb{Z}$. Therefore

$$dx = \alpha + \omega$$

which shows

$$\mathcal{O} \supset \mathcal{R} = \mathbb{Z} + \mathbb{Z}x \supset \mathbb{Z} + \mathbb{Z}dx = \mathbb{Z} + \mathbb{Z}\omega = \mathcal{O}$$

so equality holds throughout. Therefore $x = b + cdx$ for some $b, c \in \mathbb{Z}$. But this implies that $b = 0$ and $cd = 1$, hence $d = 1$, i.e., $\mathcal{R} = \mathbb{Z} + f\mathcal{O}$ as desired. ∎

Exercise 30

Statement. Let A be a finite abelian group of order N^r. Suppose that for every $D \mid N$ we have $\#A[D] = D^r$, where $A[D]$ denotes the subgroup consisting of all elements annihilated by D. Prove that

$$A \cong (\mathbb{Z}/N\mathbb{Z})^r.$$

Proof. By the structure theorem for finitely generated abelian groups,

$$A \cong \bigoplus_{i=1}^{n} \mathbb{Z}/p_i^{e_i}\mathbb{Z}$$

with each p_i a rational prime. We also let $N = \prod_j q_j^{f_j}$ with each q_j distinct rational primes. Because

$$\prod_i p_i^{e_i} = \#A = N^r = \prod_{q_j} q_j^{rf_j}$$

it follows that each p_i is some q_j, and for each j,

$$\sum_{p_i = q_j} e_i = rf_j.$$

We rewrite

$$A \cong \bigoplus_{q_j} \bigoplus_{p_i = q_j} \mathbb{Z}/q_j^{e_i}\mathbb{Z}$$

Now we will show that for any prime q and positive integers e, f, $\mathbb{Z}/q^e\mathbb{Z}[q^f] = q^{\min\{e,f\}}$. Indeed, if $f \geqslant e$, then every element of $\mathbb{Z}/q^e\mathbb{Z}$ is annihilated by q^f, so $\mathbb{Z}/q^e\mathbb{Z}[q^f] = \#\mathbb{Z}/q^e\mathbb{Z} = q^e$. Now suppose $f < e$ and we consider the multiplication by q^f map on $\mathbb{Z}/q^e\mathbb{Z}$. Its kernel is $q^{e-f}\mathbb{Z}/q^e\mathbb{Z}$, which is isomorphic to $\mathbb{Z}/q^f\mathbb{Z}$, hence has q^f elements. For each q_j, we let $A_j = \bigoplus_{p_i=q_j} \mathbb{Z}/q_j^{e_j}\mathbb{Z}$. We notice that for any $m \geqslant 1$ and any abelian groups B, C, we have $(B \oplus C)[m] = B[m] \oplus C[m]$ because $b \oplus c$ is annihilated by m iff b and c both are. In addition, if q is a prime prime not dividing a $m \geqslant 1$ and $e \geqslant 1$, we have

$$\mathbb{Z}/q^e\mathbb{Z}[m] = 0$$

since every element of $\mathbb{Z}/q^e\mathbb{Z}$ has order dividing q^e, hence cannot also divide m unless it's trivial since $\gcd(m, q^e) = 1$. Thus for any e, j,

$$A[q_j^e] \cong (\bigoplus_j A_j)[q_j^e] \cong A_j[q_j^e] = \bigoplus_{p_i=q_j} (\mathbb{Z}/q_j^{e_i}\mathbb{Z}[q_j^e])$$

hence

$$\#A[q_j^e] = \prod_{p_i=q_j} q_j^{\min\{e,e_i\}} = q_j^{\sum \min\{e,e_i\}}.$$

On the other hand, for $e \leqslant f_j$, we have by hypothesis

$$\#A[q_j^e] = q_j^{er}$$

Putting these two together, we get that for any $e \leqslant f_j$,

$$\sum_{p_i=q_j} \min\{e, e_i\} = er.$$

Letting $e = 1$, we see that

$$\#\{p_i = q_j\} = r.$$

Now let $e_{(j)} = \min_{p_i=q_j}\{e_i\}$ and suppose for a contradiction that $e_{(j)} + 1 \leqslant f_j$. Then

$$re_{(j)} + \#\{e_i > e_{(j)}\} = \#\{p_i = q_j\}e_{(j)} + \#\{e_i > e_{(j)}\} = \sum_{e_i=e_{(j)}} e_{(j)} + \sum_{e_i>e_{(j)}} (e_{(j)} + 1) = (e_{(j)} + 1)r.$$

This shows

$$r = \#\{e_i > e_{(j)}\} < \#\{p_i = q_j\} = r$$

which is clearly impossible, so we get that $e_{(j)} \geqslant f_j$. On the other hand, $e_{(j)} \leqslant f_j$ since

$$rf_j = \nu_{q_j}(\#A) = \sum_{p_i=q_j} e_i \geqslant \sum_{p_i=q_j} e_{(j)} = re_{(j)}$$

with equality iff each $e_i = e_{(j)}$. This shows $e_{(j)} = f_j$, and moreover that each $e_i = e_{(j)} = f_j$. Therefore

$$A_j = \bigoplus_{p_i=q_j} \mathbb{Z}/q_j^{e_i}\mathbb{Z} = \left(\mathbb{Z}/q_j^{f_j}\mathbb{Z}\right)^r.$$

Now

$$A \cong \bigoplus_j A_j \cong \bigoplus_j \left(\mathbb{Z}/q_j^{f_j}\mathbb{Z}\right)^r \cong \left(\bigoplus_j \mathbb{Z}/q_j^{f_j}\mathbb{Z}\right)^r \cong (\mathbb{Z}/N\mathbb{Z})^r$$

■

Chapter IV: The Formal Group of an Elliptic Curve

Exercises

Exercise 1

Statement. Let $F(X,Y) \in R[\![X,Y]\!]$ be a power series satisfying

$$F(X,Y) = X + Y + \dots \quad \text{and} \quad F(X,F(Y,Z)) = F(F(X,Y),Z).$$

(a) Show that there is a unique power series $i(T) \in R[\![T]\!]$ satisfying $F(T,i(T)) = 0$. Prove that $i(T)$ also satisfies $F(i(T),T) = 0$.

(b) Prove that $F(X,0) = X$ and $F(0,Y) = Y$.

Our approach will be to reduce the proof of (a) to that of (b), and then independently prove (b).

Proof. (a) We will assume (b) holds, so we let

$$F(X,Y) = X + Y + \sum_{m,n \geqslant 1} a_{mn} X^m Y^n.$$

We then compute

$$F(T,i(T)) = T + i(T) + \sum_{m,n \geqslant 1} a_{mn} T^m i(T)^n.$$

Therefore, if we want $0 = F(T,i(T))$, we get

$$i(T) \equiv 0 \mod T$$

so we may write

$$i(T) = \sum_{k \geqslant 1} b_k T^k.$$

Continuing the assertion $F(T,i(T)) = 0$, we have

$$0 \equiv T + i(T) \equiv T + b_1 T \mod T^2$$

since for any $m,n \geqslant 1$, since $i(T) \equiv 0 \mod T$, it follows that $T^m i(T) \equiv 0 \mod T^2$. Therefore $b_1 = -1$ is uniquely determined. Now assume for induction that each of $b_1, \dots, b_{\ell-1}$ are all uniquely determined. We have

$$0 \equiv \sum_{k=2}^{\ell} b_k T^k + \sum_{\substack{m,n \geqslant 1 \\ m+n \leqslant \ell}} a_{mn} T^m \left(\sum_{k=1}^{\lfloor (\ell-m)/n \rfloor} b_k T^k \right)^n \mod T^{\ell+1}.$$

We notice that the only possible term of the polynomial

$$\sum_{\substack{m,n \geqslant 1 \\ m+n \leqslant \ell}} a_{mn} T^m \left(\sum_{k=1}^{\lfloor (\ell-m)/n \rfloor} b_k T^k \right)^n$$

involving b_ℓ is when $k = \ell$, but this is never achieved since $m \geqslant 1$. Therefore

$$0 \equiv \sum_{k=2}^{\ell} b_k T^k + \sum_{\substack{m,n \geqslant 1 \\ m+n \leqslant \ell}} a_{mn} T^m \left(\sum_{k=1}^{\lfloor (\ell-m)/n \rfloor} b_k T^k \right)^n \equiv b_\ell T^\ell + P(b_1, \dots, b_{\ell-1}) T^\ell \mod T^{\ell+1}$$

for some polynomial $P(b_1, \ldots, b_{\ell-1})$ because by induction we may assume that $F(T, i(T)) \equiv 0 \mod T^\ell$. More explicitly,

$$P(b_1, \ldots, b_{\ell-1}) = \sum_{\substack{m,n \geqslant 1 \\ m+n \leqslant \ell}} a_{mn} \sum_{\substack{k_1+\cdots+k_n=\ell-m \\ 1 \leqslant k_i \leqslant \lfloor (\ell-m)/n \rfloor}} \prod_{i=1}^{n} b_{k_i}.$$

Therefore $b_\ell = -P(b_1, \ldots, b_{\ell-1})$, so b_ℓ is uniquely determined as well. This proves uniqueness of $i(T)$, and also shows that we may select the b_i (and must by uniqueness) to be such that for each $n \geqslant 1$,

$$F(T, i(T)) \equiv 0 \mod T^n.$$

Therefore, it must be that actually $F(T, i(T)) \in R[\![T]\!]$ must actually equal 0 (for any $f, g \in R[\![T]\!]$, if for all $n \geqslant 1$, $f \equiv g \mod T^n$, then $f = g$).

Now we must show that $F(i(T), T) = 0$ as well. We have

$$T = F(0, T) = F(F(T, i(T)), T) = F(T, F(i(T), T)).$$

For ease of notation, we let $g(T) = F(i(T), T)$, so we must show $g(T) = 0$. We know that

$$T = T + g(T) + \sum_{m,n \geqslant 1} a_{mn} T^m g(T)^n$$

so

$$0 = g(T) + \sum_{m,n \geqslant 1} a_{mn} T^m g(T)^n.$$

Because for any $f, g \in R[\![T]\!]$, if $f \equiv g \mod T^\ell$ for every $\ell \geqslant 1$, then $f = g$, it suffices for our claim to show that for each $\ell \geqslant 1$, $g(T) \equiv 0 \mod T^\ell$. Since each term in the sum is divisible by T, it follows immediately that $g(T) \equiv 0 \mod T$. Now by induction, we assume $g(T) \equiv 0 \mod T^{\ell-1}$. Thus for any $m, n \geqslant 1$, we get that $T^m g(T)^n \equiv 0 \mod T^\ell$, hence

$$0 \equiv g(T) \mod T^\ell$$

as claimed.

For (b), we write $F(X, Y) = \sum_{m,n \geqslant 0} a_{mn} X^m Y^n$ where $a_{00} = 0$ and $a_{10} = a_{01} = 1$. We have

$$F(X, 0) = F(X, F(0, 0)) = F(F(X, 0), 0).$$

Let $G(X) = F(X, 0) = \sum_{n \geqslant 1} \alpha_n X^n$ where $\alpha_n = a_{n0}$, so

$$G(X) = G(G(X)) = \sum_{m \geqslant 1} \alpha_m \left(\sum_{n \geqslant 1} \alpha_n X^n \right)^m.$$

This implies

$$0 = \sum_{m \geqslant 2} a_{m0} G(X)^m.$$

We will show by induction that $\alpha_n = 0$ for $n \geqslant 2$. To show $\alpha_2 = 0$, we have

$$X + \alpha_2 X^2 \equiv G(X) \equiv X + \alpha_2 X^2 + \alpha_2 X^2 \mod X^3$$

which shows that

$$\alpha_2 = 0.$$

Now suppose that $\alpha_2 = \cdots = \alpha_{\ell-1} = 0$, i.e., $G(X) = X + \sum_{n \geqslant \ell} \alpha_n X^n$. Then

$$G(X) = G(X) + \sum_{m \geqslant \ell} \alpha_m \left(X + \sum_{n \geqslant \ell} \alpha_n X^n \right)^m$$

hence

$$0 = \sum_{m \geqslant \ell} \alpha_m \left(X + \sum_{n \geqslant \ell} \alpha_n X^n \right)^m .$$

Considering the equation modulo $X^{\ell+1}$, we get

$$0 \equiv \alpha_\ell X^\ell \mod X^{\ell+1}$$

since $X \sum_{n \geqslant \ell} \alpha_n X^n \equiv 0 \mod X^{\ell+1}$ and for any $m \geqslant \ell$,

$$\left(\sum_{n \geqslant \ell} \alpha_n X^n \right)^m \equiv 0 \mod X^{\ell^2}$$

which implies that this same expression is congruent to 0 modulo $X^{\ell+1}$ since $\ell^2 \geqslant \ell + 1$ because $\ell \geqslant 2$. This shows every term in the binomial expansion of

$$\left(X + \sum_{n \geqslant \ell} \alpha_n X^n \right)^m$$

is congruent to 0 modulo $X^{\ell+1}$, except for the term X^ℓ if $m = \ell$. This shows $\alpha_\ell = 0$ as well as claimed.

An identical proof, replacing $G(X)$ by $F(0, Y) = F(F(0, 0), Y) = F(0, F(0, Y))$ and α_n by a_{0n}, shows also that $F(0, Y) = Y$. ∎

Chapter V: Elliptic Curves over Finite Fields

Exercises

Exercise 1

Statement. Verify the Weil conjectures for $V = \mathbb{P}^N$.

Proof. Rationality: we must compute $\#\mathbb{P}^N(\mathbb{F}_{q^n})$ for each $n \geqslant 1$. First of all, there are $q^n - 1$ distinct $N+1$-tuples of elements in $\mathbb{F}_{q^n}$ that all represent the same point in $\mathbb{P}^n(\mathbb{F}_{q^n})$, one for each nonzero element of $\mathbb{F}_{q^n}$. Thus

$$\#\mathbb{P}^n(\mathbb{F}_{q^n}) = \frac{\#(\mathbb{F}_{q^n}^{N+1} \setminus 0)}{q^n - 1} = \frac{q^{n(N+1)} - 1}{q^n - 1} = \sum_{i=0}^{N} q^{ni}.$$

Thus

$$Z(V/\mathbb{F}_q; T) = \exp\Big(\sum_{n \geqslant 1} \Big(\sum_{i=0}^{N} q^{ni}\Big) \frac{T^n}{n}\Big).$$

Therefore

$$\log Z(V/\mathbb{F}_q; T) = \sum_{n \geqslant 1} \Big(\sum_{i=0}^{N} q^{ni}\Big) \frac{T^n}{n} = \sum_{i=0}^{N} \sum_{n \geqslant 1} \frac{(q^i T)^n}{n} = \sum_{i=0}^{N} -\log(1 - q^i T) = \log\Big(\prod_{i=0}^{N} \frac{1}{1 - q^i T}\Big)$$

which gives

$$Z(V/\mathbb{F}_q;T)=\prod_{i=0}^{N}\frac{1}{1-q^iT}\in\mathbb{Q}(T).$$

Functional Equation: We compute

$$Z(V/\mathbb{F}_q;\frac{1}{q^NT})=\prod_{i=0}^{N}\frac{1}{1-q^{i-N}T^{-1}}=\prod_{i=0}^{N}\frac{q^NT}{q^NT-q^i}=\prod_{i=0}^{N}\frac{q^NT}{-q^i}\frac{1}{1-q^{N-i}T}$$
$$=(-1)^{N+1}q^{N(N+1)/2}T^{N+1}Z(V/\mathbb{F}_q;T).$$

Thus the Euler characteristic ε is $N+1$.

Riemann Hypothesis: We have that for each i, $P_{2i}=1-q^iT\in\mathbb{Z}[T]$ and $P_{2i+1}=1\in\mathbb{Z}[T]$. Then for the odd indices, the polynomial has degree 0, hence the claim about the α_{ij} is vacuous. For $P_{2i}=1-q^iT$, we see it has degree 1 and the only α_{ij} is q^i, so clearly $|\alpha_{ij}|=q^{i/2}$.

■

Exercise 12

Statement. Prove that for every prime $p\geqslant 3$, the elliptic curve

$$E:y^2=x^3+x$$

satisfies

$$\#E(\mathbb{F}_p)\equiv 0 \mod 4.$$

Proof. First we consider the case where $p\equiv 3 \mod 4$. By Example 4.5, we know the primes congruent to 3 modulo 4 are exactly the primes where $E(\mathbb{F}_p)$ is supersingular. We know from Theorem 4.1 (a) that $E(\mathbb{F}_p)$ is supersingular iff $A_p=0$, where A_p is the coefficient of x^{p-1} in the expansion of $(x^3+x)^{(p-1)/2}$ in $\mathbb{F}_p$. For $p\geqslant 5$, we have by Hasse's inequality that

$$|a|\leqslant 2\sqrt{p}<p.$$

Since $a\equiv A_p=0 \mod p$ by the proof of Theorem 4.1 (a) and $|a|<p$, it follows that $a=0$ so $\#E(\mathbb{F}_p)=p+1-a=p+1\equiv 0 \mod 4$.

We explicitly verify that for $p=3$, $E(\mathbb{F}_p)=\{O,(0,0),(2,0),(-2,0)\}$ so also $\#E(\mathbb{F}_p)=p+1$.

Now we may assume that $p\equiv 1 \mod 4$. Clearly it suffices to show $\#E(\mathbb{F}_p)[2]=4$ since the order of a subgroup divides the order of the group containing it. Let $i\in\mathbb{F}_p$ be such that $i^2=-1$. We claim $E(\mathbb{F}_p)[2]=\{O,(0,0),(\pm i,0)\}$. For this claim, it suffices to show that if $P=(x,y)$ is such that $2P=O$, then $y=0$ since $x^3+x=x(x+i)(x-i)$. We explicitly compute the duplication formula for E as follows using the formulas from Chapter III:

$$2(x,y)=\left(\frac{(x^2-1)^2}{4x(x^2+1)},\frac{(x^2-1)x^4+6x^2+1)}{9xy(x^2+1)}\right).$$

Thus $2(x,y)=O$ iff $x=0,x=\pm i$, or $y=0$. But notice that $y=0$ iff $x\in\{\pm i,0\}$ since $y^2=x^3+x=x(x+i)(x-i)$. Then indeed the only 2-torsion points are $\{O,(\pm i,0),(0,0)\}$.

We write $p=m^2+n^2$ where we take m to be odd and n even, and let $\phi\in\mathrm{End}(E)$ be the Frobenius morphism,. By Theorem 2.3.1, we know that ϕ satisfies $\phi^2-a\phi+p=0$ in $\mathrm{End}(E)$. Since $E(\mathbb{F}_p)$ is ordinary, i.e., $\mathrm{End}(E(\mathbb{F}_p))$ is an order in a quadratic imaginary field, and $\mathrm{End}(E)\supset\mathbb{Z}[i]$ where $[i]=(x,y)\mapsto(-x,iy)$ where here $i^2=-1$ in $\mathbb{F}_p$, it follows that actually $\mathrm{End}(E)=\mathbb{Z}[i]$. Now $\phi\bar{\phi}=p=m^2+n^2$ gives that $\phi=a+bi$ up to associates, since $\mathbb{Z}[i]$ is a UFD. This shows that $a\in\{\pm 2m,\pm 2n\}$. But if $a=\pm 2n$, then $a\equiv 0 \mod 4$, which yields

$$\#E(\mathbb{F}_p)=p+1-a\equiv p+1\equiv 2 \mod 4$$

which contradicts our previous assertion, so $a=\pm 2m$ and $\#E(\mathbb{F}_p)=p+1\pm 2m$. ■

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.

[2] Jean-Pierre Serre. *A Course in Arithmetic*. Vol. 7. Graduate Texts in Mathematics. New York: Springer-Verlag, 1973. ISBN: 0-387-90040-3.