Elliptic Curves - Assignment 2

Matteo Durante, s2303760, Leiden University

22nd March 2019

Exercise 1.a

Let $v_{\phi(P)}(f) = n$ and write $f = t_{\phi(P)}^n g$ for some $g \in \overline{\mathbb{K}}(C_2)$ s.t. $\phi^*(g)(P) = g(\phi(P)) \neq 0$ (actually, $g \in \overline{\mathbb{K}}[C_2]_{\phi(P)}$, $\phi^*(g) \in \overline{\mathbb{K}}[C_1]_P$), $t_{\phi(P)} \in \overline{\mathbb{K}}(C_2)$ a uniformizer of C_2 at $\phi(P)$. Then, $\phi^*(f) = \phi^*(t_{\phi(P)})^n \phi^*(g)$ and $v_P(\phi^*(g)) = 0$, hence we get the following:

$$v_P(\phi^*(f)) = v_P(\phi^*(t_{\phi(P)})^n \phi^*(g)) = n \cdot v_P(\phi^*(t_{\phi(P)})) + v_P(\phi^*(g)) = v_{\phi(P)}(f) \cdot e_\phi(P)$$

Exercise 2

Disclaimer: I will be using a result from the previous assignment to say that Y and $Y - 1$ are uniformizers at specific points of the algebraic variety.

(a) Notice that for a point $(x : y : z) \in C$ to be a zero of f it has to satisfy $y = 0$ and, of course, $y^2 = xz$, hence the only possible zeroes of f are $Q = (1 : 0 : 0)$ and $P = (0 : 0 : 1)$. On the other hand, a pole of f satisfies $z = 0$ and $y^2 = xz$, thus the only possible pole is $Q = (1 : 0 : 0)$.

Now we shall study f at P and Q.

Considering the affine patch of C given by $C_z = C \cap U_2$, i.e. $z = 1$, the curve has equation $h_z = Y^2 - X = 0$ and $f_z := f|_{C_z}$ is represented by Y. On this affine patch, the point P has coordinates $(0, 0)$ and, since $\partial h_z/\partial X = -1 \neq 0$, Y is a uniformizer of C_z at P.

Now, since $f_z = 1 \cdot Y^1$ and 1 is regular and non-zero at P, $v_P(f) = v_P(f_z) = 1$.

On the other hand, considering the affine patch of C given by $C_x = C \cap U_0$, i.e. $x = 1$, the curve has equation $h_x = Y^2 - Z = 0$ and $f_x := f|_{C_x}$ is represented by $Y/Z = 1/Y$. On this affine patch, Q has coordinates $(0, 0)$ and, since $\partial h_x/\partial Z = -1 \neq 0$, Y is a uniformizer of C_x at Q.

Now, since $f_x = 1 \cdot Y^{-1}$ and 1 is regular and non-zero at Q, $v_Q(f) = v_Q(f_x) = -1$.

It follows that $\mathrm{div}(f) = P - Q$.

(b) Notice that for a point $(x : y : z) \in C$ to be a zero of g it has to satisfy $x = 0$ and, of course, $y^2 = xz$, hence the only possible zero of g is $P = (0 : 0 : 1)$. On the other hand, a pole of g satisfies $z = 0$ and $y^2 = xz$, thus the only possible pole is $Q = (1 : 0 : 0)$.

Now we shall study g at P and Q using the same affine patches and uniformizers as before.

We see that, on C_z, g_z can be represented as $X = Y^2 = 1 \cdot Y^2$. Again, since 1 is regular and non-zero at P, $v_P(g) = v_P(g_z) = 2$.

In the same way, on C_x, g_x can be represented as $1/Z = 1/Y^2 = 1 \cdot Y^{-2}$ and, since 1 is regular and non-zero at Q, $v_Q(g) = v_Q(g_x) = -2$.

It follows that $\mathrm{div}(g) = 2P - 2Q$.

(c) We shall consider the function $s = \frac{Y-Z}{Y} \in \mathbb{K}(C)$.

Notice that for a point $(x : y : z) \in C$ to be a zero of s it has to satisfy $y - z = 0$ and, of course, $y^2 = xz$, hence the only possible zeroes are $Q = (1 : 0 : 0)$ and $R = (1 : 1 : 1)$. On the other hand, a pole of s satisfies $y = 0$ and $y^2 = xz$, thus the only possible poles are $P = (0 : 0 : 1)$ and $Q = (1 : 0 : 0)$.

Now we shall study s at P, Q and R using for the first two the same affine patches and uniformizers as before.

We see that, on C_z, s_z can be represented as $\frac{Y-1}{Y} = (Y-1) \cdot Y^{-1}$ and, since $Y - 1$ is regular and non-zero at P, $v_P(s) = v_P(s_z) = -1$.

In the same way, on C_x, s_x can be represented as $\frac{Y-Y^2}{Y} = 1 - Y = (1-Y) \cdot Y^0$ and, since $1 - Y$ is regular and non-zero at Q, $v_Q(s) = v_Q(s_x) = 0$.

Remaining on C_x, we see that R has coordinates $(1, 1)$ on this affine patch. Since $\partial h_x / \partial Z = -1$, $Y - 1$ is a uniformizer of C_x at R.

Now, since $s_x = 1 - Y = -1 \cdot (Y-1)^1$ and -1 is regular and non-zero at R, $v_R(s) = v_R(s_x) = 1$.

We can conclude that $\operatorname{div}(s) = R - P$.

Exercise 5

Let $f \in \mathbb{K}(C)$ be s.t. $\operatorname{div}(f) = D - D'$ and consider the function $\mathcal{L}(D) \xrightarrow{\phi} \mathcal{L}(D')$ given by $g \mapsto fg$. We want to prove that this is an isomorphism between the two vector spaces.

First of all, we prove that it is well defined. Indeed, if $g \in \mathcal{L}(D)$ is s.t. $\operatorname{div}(g) + D \geq 0$, then $\operatorname{div}(fg) + D' = \operatorname{div}(f) + \operatorname{div}(g) + D' = D - D' + \operatorname{div}(g) + D' = \operatorname{div}(g) + D \geq 0$.

It is a $\mathbb{K}$-linear application, for $\phi(0) = f \cdot 0 = 0$ and, given $g, h \in \mathcal{L}(D)$, $\lambda, \mu \in \mathbb{K}$ we have that $\phi(\lambda \cdot g + \mu \cdot h) = f(\lambda \cdot g + \mu \cdot h) = \lambda \cdot fg + \mu \cdot fh = \lambda \cdot \phi(g) + \mu \cdot \phi(h)$.

It is invertible, for we can define another $\mathbb{K}$-linear application $\mathcal{L}(D') \xrightarrow{\psi} \mathcal{L}(D)$ as $g \mapsto g/f$ (indeed, $1/f \in \mathbb{K}(C)$ and, remembering that $\operatorname{div}(1/f) = -\operatorname{div}(f)$, we can check that the map is a well defined $\mathbb{K}$-linear application in same way as we did earlier), which is s.t. $\phi\psi = \operatorname{Id}_{\mathcal{L}(D')}$ and $\psi\phi = \operatorname{Id}_{\mathcal{L}(D)}$.

It follows that the two $\mathbb{K}$-vector spaces are isomorphic, hence they have the same dimension.